J. Appl. Math. Comput. (2016) 50:577–587
DOI 10.1007/s12190-015-0885-7

ORIGINAL RESEARCH

Bounds on quasi-cyclic codes over finite chain rings

Jian Gao[1] · **Linzhi Shen**[1] · **Fang-Wei Fu**[1]

Received: 18 January 2015 / Published online: 25 March 2015

Abstract In this short correspondence, we mainly consider quasi-cyclic (QC) codes over finite chain rings. We study module structures and trace representations of QC codes, which lead to some lower bounds on the minimum Hamming distance of QC codes.

Keywords Quasi-cyclic code · Module structure · Trace representation · Minimum Hamming distance

Mathematics Subject Classification 11T71 · 94B05 · 94B15

1 Introduction

Let R denote a finite chain ring with nilpotency index s, γ a generator of its maximal ideal and $\mathbb{F}_q$ the residue field $R/\langle\gamma\rangle$. The ideals of R form a chain as $\langle 0\rangle = \langle\gamma^s\rangle \subseteq \langle\gamma^{s-1}\rangle \subseteq \cdots \subseteq \langle\gamma\rangle \subseteq \langle 1\rangle = R$.

Define the ring surjective homomorphism $^- : R \to \overline{R} = \mathbb{F}_q$ by $r \mapsto \overline{r}$, where $\overline{r}$ denotes $r + \langle\gamma\rangle$. Extending the ring homomorphism $^- : R[x] \to \mathbb{F}_q[x]$ by $r_0 + r_1x + \cdots + r_nx^n \mapsto \overline{r}_0 + \overline{r}_1x + \cdots + \overline{r}_nx^n$, and the image of $f(x) \in R[x]$ under the map $^-$ is denoted by $\overline{f}(x) \in \mathbb{F}_q[x]$.

A polynomial $f(x) \in R[x]$ is said to be *basic irreducible* if $\overline{f}(x)$ is irreducible in $\mathbb{F}_q[x]$, and *basic primitive* if $\overline{f}(x)$ is primitive in $\mathbb{F}_q[x]$. If $f(x)$ is a monic basic irreducible polynomial with degree m over R, then the residue class ring $R[x]/\langle f(x)\rangle$ is called the m-th *Galois extension ring* of R, and denoted as $\mathcal{R}$. $\mathcal{R}$ is also a finite

✉ Jian Gao
jiangao@mail.nankai.edu.cn

[1] Chern Institute of Mathematics and LPMC, Nankai University, Tianjin, People's Republic of China

chain ring, with maximal ideal $\langle\gamma\rangle$ and nilpotency index s. If ξ is a root of $f(x)$, then $\mathcal{R} = R[\xi]$, i.e., $\mathcal{R}$ is a *free module* of rank m over R with $\{1, \xi, \ldots, \xi^{m-1}\}$ as a basis. If $f(x)$ is a basic primitive polynomial over R, and ξ is the root of $f(x)$, then the order of ξ is $q^m - 1$. Let the *Teichmüller set* be $\mathcal{T} = \{0, 1, \xi, \ldots, \xi^{q^m-2}\}$. Then each element r of $\mathcal{R}$ can be expressed uniquely as $r = r_0 + r_1\gamma + \cdots + r_{s-1}\gamma^{s-1}$, where $r_0, r_1, \ldots, r_{s-1} \in \mathcal{T}$. Further information on finite chain rings can be found in [8].

Quasi-cyclic (QC) codes are an important class of linear codes and have good algebra structures [2,3,5–7]. They have proved to be a rich source of good codes [1,3,10]. Recently, there are more and more interesting work on QC codes over finite chain rings [1,2,7,10]. Minimum Hamming distance related to the ability of error-correcting is a very important parameter of codes, and its estimation is crucial to search or construct good codes. This is one of the motivations to generalize some bounds on the minimum Hamming distance of QC codes over finite fields to finite chain rings. In [6], Lally studied the structural properties of QC codes over finite fields. A lower bound on the minimum Hamming distance of a QC code in terms of the minimum Hamming distance of one cyclic code and one linear code related to the generators of QC code was given. In [5], Güneri–Özbudak gave another lower bound on the minimum Hamming distance of a QC code over finite fields by using the trace representation of a QC code.

In this short correspondence, following the approached given in [5,6], we also present two different minimum Hamming distance bounds on QC codes over finite chain rings. The correspondence is organized as follows. In Sect. 2, we discuss trace representations of cyclic codes. In Sect. 3, we discuss module structures of QC codes over finite chain rings, which are generalizations of QC codes over finite fields. This point of view for studying QC codes could give a lower bound on the minimum Hamming distance and a construction method of linear codes over finite fields. In Sect. 4, we discuss the trace representation of QC codes over finite chain rings, which lead to another lower bound on the minimum Hamming distance.

2 Cyclic codes

Let R^n be the set of n-tuples over R. $\mathscr{C}$ is a linear code of length n over R if and only if $\mathscr{C}$ is an R-submodule of R^n. Let T be the *cyclic shift operator* $T: R^n \to R^n$, which transforms $v = (v_0, v_1, \ldots, v_{n-1})$ into $vT = (v_{n-1}, v_0, \ldots, v_{n-2})$. A linear code $\mathscr{C}$ is called the *cyclic code* of length n if it is invariant under T. We assume n to be a positive integer not divisible by the characteristic of the finite field $\mathbb{F} = \mathbb{F}_q$. Therefore $x^n - 1$ has a unique decomposition as a product of monic basic irreducible pairwise coprime polynomials in $R[x]$. Let $f(x)$ be a factor of $x^n - 1$ over R. Denote $\widehat{f}(x) = (x^n - 1)/f(x)$. It is well known that the cyclic code of length n over R can be regarded as an ideal of $R[x]/\langle x^n - 1\rangle$.

Proposition 2.1 (cf. [11] Theorem 2.9) *Let $f_1, f_2, \ldots, f_r$ be pairwise coprime monic polynomials of degree $\geqslant 1$ over R, $f = f_1 f_2 \ldots f_r$ and $\mathcal{R}_f = R[x]/\langle f\rangle$. Let $\widehat{f_i} = f/f_i$. Then there exist $a_i, b_i \in R[x]$ such that $a_i f_i + b_i \widehat{f_i} = 1$. Let $e_i = b_i \widehat{f_i} + \langle f\rangle$. Then*

(1) $e_1, e_2, \ldots, e_r$ are mutually orthogonal non-zero idempotents of $\mathcal{R}_f$;

(2) $1 = e_1 + e_2 + \cdots + e_r$ *in* $\mathcal{R}_f$*;*
(3) Let $\mathcal{R}_f e_i = \langle e_i \rangle$ *be the principal ideal of* $\mathcal{R}_f$ *generated by* e_i*. Then* e_i *is the identity of* $\mathcal{R}_f e_i$ *and* $\mathcal{R}_f e_i = \langle \widehat{f_i} + \langle f \rangle \rangle$*;*
(4) $\mathcal{R}_f = \oplus_{i=1}^{r} \mathcal{R}_f e_i$*;*
(5) The map $R[x]/\langle f_i \rangle \to \mathcal{R}_f e_i$ *defined by* $g + \langle f_i \rangle \mapsto \langle g + \langle f \rangle \rangle e_i$ *is a well-defined isomorphism of rings;*
(6) $\mathcal{R}_f = R[x]/\langle f \rangle \cong \oplus_{i=1}^{r} R[x]/\langle f_i \rangle$.

Let $\mathscr{C}$ *be a cyclic code of length n generated by* $g(x)$ *over R. Unlike the case over finite fields,* $g(x)$ *may be not a divisor of* $x^n - 1$*. It is related to whether* $\mathscr{C}$ *is a free R-module or not.*

Proposition 2.2 (cf. [9] Proposition 4.11) *Let* $\mathscr{C}$ *be a linear code over finite chain ring R. Then the following properties are equivalent*

(1) $\mathscr{C}$ *is the Hensel lift of a cyclic code over* $\overline{R}$*;*
(2) $\mathscr{C}$ *is a cyclic code and free;*
(3) There exists a polynomial $g(x) \in R[x]$ *such that* $\mathscr{C} = \langle g(x) \rangle$ *and* $g(x) | x^n - 1$.

Suppose that ξ is an n-th primitive root of unity and $\mathcal{R}$ is the smallest Galois extension ring of R containing the n-th primitive root of unity ξ. Therefore $x^n - 1 = (x-1)(x-\xi)\cdots(x-\xi^{n-1})$ over $\mathcal{R}$. Define the map π as follows

$$\begin{aligned} &\pi : \mathcal{R}[x]/\langle x^n - 1 \rangle \to \oplus_{i=0}^{n-1} \mathcal{R}[x]/\langle x - \xi^i \rangle \\ &c(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1} \mapsto (c(1), c(\xi), \ldots, c(\xi^{n-1})). \end{aligned}$$

If $c(x) \in R[x]/\langle x^n - 1 \rangle$, then from Proposition 2.1, we can deduce π is an $R[x]$-module homomorphism. Denote $c(\xi^i) = A_i$ and $A(z) = \sum_{i=0}^{n-1} A_i z^{n-i}$. The polynomial $A(z)$ is called *Mattson-Solomon polynomial* associated with $c(x)$. Clearly,

$$(A_0, \ldots, A_{n-1}) = (c_0, \ldots, c_{n-1}) \begin{pmatrix} 1 & 1 & \ldots & 1 \\ 1 & \xi & \ldots & \xi^{n-1} \\ \vdots & \vdots & \vdots & \vdots \\ 1 & \xi^{n-1} & \ldots & \xi^{(n-1)^2} \end{pmatrix}.$$

For this reason $A(z)$ is sometimes called the *discrete Fourier transform* of $c(x)$. The inverse transform is given by

$$c_j = \frac{1}{n} \sum_{k=0}^{n-1} A_k \xi^{-jk}, \quad j = 0, 1, \ldots, n-1.$$

Suppose that $\mathcal{R}$ is an m-th Galois extension ring of finite chain ring R. It is well known that $\mathcal{R}$ is also a local ring with maximal ideal $\langle \gamma \rangle$ and the residue field $\mathcal{R}/\langle \gamma \rangle$ is $\mathbb{F}_{q^m}$. Every element r of $\mathcal{R}$ can also be expressed uniquely in the form $r = r_0 + r_1\gamma + \cdots + r_{s-1}\gamma^{s-1}$, where $r_0, r_1, \ldots, r_{s-1}$ belong to the Teichmüller set $\mathcal{T} =$

$\{0, 1, \zeta, \ldots, \zeta^{q^m-2}\}$, where ζ is a (q^m-1)-th basic primitive element in $\mathcal{R}$. Define the Frobenius map ϕ on $\mathcal{R}$ to be the map induced by the map $r_0+r_1\gamma+\cdots+r_{s-1}\gamma^{s-1} \mapsto r_0^q+r_1^q\gamma+\cdots+r_{s-1}^q\gamma^{s-1}$, acting as the identity on R. Since the degree of the extension $\mathcal{R}$ over R is m, ϕ^m is the identity map. For any $r \in \mathcal{R}$, we define the trace of r to be $Tr_{\mathcal{R}/R}(r) = r + \phi(r) + \cdots + \phi^{m-1}(r)$. Since $\phi^i(r) = r_0^{q^i} + r_1^{q^i}\gamma + \cdots + r_{s-1}^{q^i}\gamma^{s-1}$, we have

$$Tr_{\mathcal{R}/R}(r) = Tr_{\mathcal{R}/R}(r_0) + Tr_{\mathcal{R}/R}(r_1)\gamma + \cdots + Tr_{\mathcal{R}/R}(r_{s-1})\gamma^{s-1}.$$

By the Hensel lift, there is a one-to-one correspondence between factors of $x^n - 1$ and the q-cyclotomic cosets of $\mathbb{Z}_n$. Denote by U_i $(1 \le i \le r)$ the cyclotomic coset corresponding to f_i. Let $\mathcal{R}_i$ be the Galois extension ring of R corresponding to the basic irreducible polynomial f_i, i.e., $\mathcal{R}_i = R[x]/\langle f_i\rangle$. Then for a fixed $u_i \in U_i$, we have

$$nc_j = \sum_{i=1}^{r} Tr_{\mathcal{R}_i/R}(A_i\xi^{-ju_i}).$$

Sometimes this is called the *trace representation* of the cyclic code over finite chain ring R.

In the following, we give a slightly different trace representation of the cyclic code over finite chain ring R.

Proposition 2.3 *Let $\mathscr{C}$ be a free cyclic code of length n over finite chain ring R. Suppose that non-negative integers $i_1, i_2, \ldots, i_k$ are in different q-cyclotomic cosets in $\mathbb{Z}_n$. Let ξ be an n-th primitive root of unity and $\xi^{i_1}, \xi^{i_2}, \ldots, \xi^{i_k}$ be roots of the polynomial $m(x) = \prod_{j=1}^{k} M_j(x)$, where $m(x)$ is the generator polynomial of $\mathscr{C}^\perp$ and $M_j(x)$ is the minimal polynomial of ξ^{i_j} over R. Then for any codeword $c(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}$ of $\mathscr{C}$, we have*

$$c_v = \sum_{j=1}^{k} Tr_{\mathcal{R}/R}(a_j\xi^{vi_j}),$$

where $a_j \in \mathcal{R}$, $v = 0, 1, \ldots, n-1$, and $\mathcal{R}$ is the smallest Galois extension ring of R containing the n-th primitive root of unity ξ.

Proof Let $k = 1$. Consider the following set

$$\mathcal{C} = \left\{(c_0, \ldots, c_{n-1}) \in R^n \mid c_v = Tr_{\mathcal{R}/R}(a_j\xi^{vi_1}), \quad v = 0, 1, \ldots, n-1\right\}.$$

Obviously, $\mathcal{C}$ is a nonzero linear code of length n over R. If $c_{a_j}(x) = \sum_{v=0}^{n-1} Tr_{\mathcal{R}/R}(a_j\xi^{vi_1})x^v$, then $c_{a_j\xi^{-i_1}}(x) = c_{a_j}(x)x$ in $R[x]/\langle x^n - 1\rangle$ implying that $\mathcal{C}$ is cyclic. On the other hand the free cyclic code $\langle M_1(x)\rangle$ is contained in the dual code $\mathcal{C}^\perp$ of $\mathcal{C}$, which implies that $\langle M_1(x)\rangle^\perp \supseteq \mathcal{C}$. It should be noted that $\langle M_1(x)\rangle^\perp$ is a minimal free cyclic code with rank equal to the degree of $M_1(x)$, i.e., the minimal

polynomial of ξ^{i_1} over R. Since R is a principal ideal ring, the cyclic code $\mathcal{C}$ is also free over R implying that $\mathcal{C} = \langle M_1(x)\rangle^{\perp}$.

For $k \geq 2$, using the fact that any free cyclic code is the direct sum of some minimal free cyclic codes, we can get the result immediately. □

It is easy to see that $c_v = 0$ if each $a_j = 0, j = 1, 2, \ldots, k$. But sometimes c_v may be identically zero even if there is $\{l_1, l_2, \ldots, l_d\} \subseteq \{1, 2, \ldots, k\}$ such that $a_{l_z} \neq 0, z = 1, 2, \ldots, d$. Therefore we could ask a question that when c_v is zero except the case $a_j = 0$ for each $j \in \{1, 2, \ldots, k\}$? In the following we give an answer about this question. The next theorem is a generalization of the relevant result in reference [4] from finite fields to rings, which will be used in the proof precess of Lemma 4.2.

Theorem 2.4 *Let U_{vi_j} be a q-cyclotomic coset containing vi_j mod n for each $j = 1, 2, \ldots, k$. Let $a_1, a_2, \ldots, a_k \in \mathcal{R} \setminus \{0\}$. Then $c_v = 0$ if and only if $|U_{vi_j}| = \tau_{vi_j} \neq m$ and $Tr_{\mathcal{R}/\widetilde{\mathcal{R}}_j}(a_j) = 0$, where $\widetilde{\mathcal{R}}_j$ is the τ_{vi_j}-th Galois extension ring of R for all $j = 1, 2, \ldots, k$.*

Proof First, we will prove $c_v = 0$ if and only if $Tr_{\mathcal{R}/R}(a_j\xi^{vi_j}) = 0$ for all $j = 1, 2, \ldots, k$. Let $a_j = a_{j0} + a_{j1}\gamma + \cdots + a_{j,s-1}\gamma^{s-1}$, where $a_{jg} \in \mathcal{T} = \{0, 1, \zeta, \ldots, \zeta^{q^m-2}\}$, ζ is a basic primitive element in $\mathcal{R}$, $j = 1, 2, \ldots, k$ and $g = 0, 1, \ldots, s-1$. Then $c_v = 0$ if and only if

$$\begin{aligned}\sum_{j=1}^{k} Tr_{\mathcal{R}/R}(a_j\xi^{vi_j}) &= \sum_{j=1}^{k} Tr_{\mathcal{R}/R}(a_{j0}\xi^{vi_j}) + \gamma\sum_{j=1}^{k} Tr_{\mathcal{R}/R}(a_{j1}\xi^{vi_j}) \\ &\quad + \cdots + \gamma^{s-1}\sum_{j=1}^{k} Tr_{\mathcal{R}/R}(a_{j,s-1}\xi^{vi_j}) \\ &= 0\end{aligned}$$

if and only if $\sum_{j=1}^{k} Tr_{\mathcal{R}/R}(a_{jg}\xi^{vi_j}) = 0$ for all $g = 0, 1, \ldots, s-1$ if and only if $Tr_{\mathcal{R}/R}(a_{jg}\xi^{vi_j}) = 0$ for all $j = 1, 2, \ldots, k$ and $g = 0, 1, \ldots, s-1$ if and only if $Tr_{\mathcal{R}/R}(a_j\xi^{vi_j}) = 0$ for all $j = 1, 2, \ldots, k$.

Second, we will prove $Tr_{\mathcal{R}/R}(a_j\xi^{vi_j}) = 0$ if and only if $|U_{vi_j}| = \tau_{vi_j} \neq m$ and $Tr_{\mathcal{R}/\widetilde{\mathcal{R}}_j}(a_j) = 0$. Since τ_{vi_j} necessarily divides m, $\widetilde{\mathcal{R}}$ is a subring of $\mathcal{R}$. Therefore $Tr_{\mathcal{R}/\widetilde{\mathcal{R}}}$ makes sense. From $a_j \in \mathcal{R} \setminus \{0\}$, we have $|U_{vi_j}| \neq m$. By Theorem 2.2 in [4], we deduce that there are $q^{(m-\tau_{vi_j})s}$ a_j's in $\mathcal{R}$ such that $Tr_{\mathcal{R}/R}(a_j\xi^{vi_j}) = 0$. The number of elements in the kernel of $Tr_{\mathcal{R}/\widetilde{\mathcal{R}}}$ is also $q^{ms}/q^{\tau_{vi_j}s} = q^{(m-\tau_{vi_j})s}$. For any b_j in this kernel, we have $Tr_{\mathcal{R}/R}(b_j\xi^{vi_j}) = Tr_{\widetilde{\mathcal{R}}/R}(Tr_{\mathcal{R}/\widetilde{\mathcal{R}}}(b_j\xi^{vi_j})) = Tr_{\widetilde{\mathcal{R}}/R}(\xi^{vi_j}Tr_{\mathcal{R}/\widetilde{\mathcal{R}}}(b_j)) = 0$. Thus we have a_j must be in the kernel of $Tr_{\mathcal{R}/\widetilde{\mathcal{R}}}$. Conversely, reading the above equality from left to right, replacing b_j by a_j, proves the claim. □

3 Module structure of quasi-cyclic codes

A linear code $\mathscr{C}$ is called *quasi-cyclic* (QC) code if it is invariant under T^ℓ for some positive integer ℓ. The smallest ℓ such that $T^\ell(\mathscr{C}) = \mathscr{C}$ is called the index of $\mathscr{C}$. Clearly, ℓ is a divisor of N. Let $N = n\ell$. Define an R-module isomorphism as follows

$$\begin{aligned}\rho :\ & R^{n\ell} \to (R[x]/\langle x^n - 1\rangle)^\ell \\ & (v_{00}, \ldots, v_{0,\ell-1}, v_{10}, \ldots, v_{1,\ell-1}, \ldots, v_{n-1,0}, \ldots, v_{n-1,\ell-1}) \\ & \quad \mapsto (v_0(x), \ldots, v_{\ell-1}(x)),\end{aligned}$$

where $v_i(x) = \sum_{j=0}^{n-1} v_{ji}x^j$, $i = 0, 1, \ldots, \ell - 1$. Then, for any

$$(v_0(x), v_1(x), \ldots, v_{\ell-1}(x)) \in \rho(\mathscr{C})$$

we have $[x v_0(x), x v_1(x), \ldots, x v_{\ell-1}(x)] \in \rho(\mathscr{C})$. Therefore, $\mathscr{C}$ is a QC code of length $n\ell$ with index ℓ if and only if $\rho(\mathscr{C})$ is an $R[x]/\langle x^n-1\rangle$-submodule of $(R[x]/\langle x^n-1\rangle)^\ell$. This definition of the QC code is known as conventional row circulant. In this section, we will introduce another module structure on a QC code by extending the work of Lally [6].

Let $v = (v_{00}, \ldots, v_{0,\ell-1}, \ldots, v_{n-1,0}, \ldots, v_{n-1,\ell-1}) \in R^{n\ell}$. Define an R-module isomorphism between $R^{n\ell}$ and $\mathcal{R}^n$ by associating with each ℓ-tuple $(v_{i0}, v_{i1}, \ldots, v_{i,\ell-1})$, $i = 0, 1, \ldots, n - 1$, and the element $v_i \in \mathcal{R}$ represented as $v_i = v_{i0} + v_{i1}\xi + \cdots + v_{\ell-1}\xi^{\ell-1}$, where the set $\{1, \xi, \xi^2, \ldots, \xi^{\ell-1}\}$ forms an R-basis of $\mathcal{R}$. Then every element in $R^{n\ell}$ is in one-to-one correspondence with an element in $\mathcal{R}^n$. The operator T^ℓ for some element

$$(v_{00}, v_{01}, \ldots, v_{0,\ell-1}, \ldots, v_{n-1,0}, v_{n-1,1}, \ldots, v_{n-1,\ell-1}) \in R^{n\ell}$$

corresponds to the element $(v_{n-1}, v_0, \ldots, v_{n-2})$ of $\mathcal{R}^n$. Indicating the block positions with increasing powers of x, the vector $v \in R^{n\ell}$ can be associated with the polynomial $v_0 + v_1x + \cdots + v_{n-1}x^{n-1} \in \mathcal{R}[x]$. An $R[x]/\langle x^n - 1\rangle$-module isomorphism between $R^{n\ell}$ and $\mathcal{R}[x]/\langle x^n - 1\rangle$, which is defined as $\psi(v) = v_0 + v_1x + \cdots + v_{n-1}x^{n-1}$. In this setting, multiplication by x of any element of $\mathcal{R}[x]/\langle x^n - 1\rangle$ is equivalent to applying T^ℓ to operate the element of $R^{n\ell}$. It follows that there is a one-to-one correspondence between $R[x]/\langle x^n - 1\rangle$-submodule of $\mathcal{R}[x]/\langle x^n - 1\rangle$ and the QC code of length $n\ell$ with index ℓ over R. Note that a QC code of length $n\ell$ with index ℓ can also be viewed as an R-submodule of $\mathcal{R}[x]/\langle x^n - 1\rangle$ because of the equivalence of $R^{n\ell}$ and $\mathcal{R}[x]/\langle x^n - 1\rangle$.

Let $\mathscr{C}$ be a QC code of length $n\ell$ with index ℓ over R, and assume that generated by elements $v_1(x), v_2(x), \ldots, v_r(x) \in \mathcal{R}[x]/\langle x^n - 1\rangle$ as an $R[x]/\langle x^n - 1\rangle$-submodule of $\mathcal{R}[x]/\langle x^n - 1\rangle$. Then $\mathscr{C} = \{a_1(x)v_1(x) + a_2(x)v_2(x) + \cdots + a_r(x)v_r(x) |\ a_i(x) \in R[x]/\langle x^n - 1\rangle, i = 1, 2, \ldots, r\}$. As discussed above, $\mathscr{C}$ is also an R-submodule of $\mathcal{R}[x]/\langle x^n-1\rangle$. For an R-submodule of $\mathcal{R}[x]/\langle x^n-1\rangle$, $\mathscr{C}$ is generated by the following set $\{v_1(x), \ldots, x^{n-1}v_1(x), \ldots, v_r(x), \ldots, x^{n-1}v_r(x)\}$.

If $\mathscr{C}$ is generated by a single element $v(x)$ as an $R[x]/\langle x^n - 1\rangle$-submodule of $\mathcal{R}[x]/\langle x^n - 1\rangle$, then $\mathscr{C}$ is called the 1-*generator* QC code. Let the preimage of $v(x)$

in $R^{n\ell}$ be v. Then for the 1-generator QC code $\mathscr{C}$, we have $\mathscr{C}$ is generated by the set $\{v, T^{\ell}v, \ldots, T^{\ell(n-1)}v\}$. It is the conventional of row circulant definition of 1-generator QC code. In fact, let $v(x) = v_0 + v_1x + \cdots + v_{n-1}x^{n-1}$ be a polynomial in $\mathcal{R}[x]/\langle x^n - 1\rangle$, where $v_i = v_{i0} + v_{i1}\xi + \cdots + v_{i,\ell-1}\xi^{\ell-1}$, $i = 0, 1, \ldots, n-1$. Then $v(x)$ becomes an ℓ-tuple of polynomials over R each of degree at most $n-1$ with the fixed R-basis $\{1, \xi, \xi^2, \ldots, \xi^{\ell-1}\}$. Therefore, $v(x)$ becomes an element of $(R[x]/\langle x^n - 1\rangle)^{\ell}$. So $\mathscr{C}$ is an $R[x]/\langle x^n - 1\rangle$-submodule of $(R[x]/\langle x^n - 1\rangle)^{\ell}$, i.e. the conventional row circulant definition of QC code.

Since $R[x]/\langle x^n - 1\rangle$ is a subring of $\mathcal{R}[x]/\langle x^n - 1\rangle$ and $\mathscr{C}$ is an $R[x]/\langle x^n - 1\rangle$-submodule of $\mathcal{R}[x]/\langle x^n - 1\rangle$, it is in particular a submodule of an $\mathcal{R}[x]/\langle x^n - 1\rangle$-submodule of $\mathcal{R}[x]/\langle x^n - 1\rangle$, i.e. a cyclic code $\widetilde{\mathscr{C}}$ of length n over $\mathcal{R}$. Therefore $d(\mathscr{C}) \geq d(\widetilde{\mathscr{C}})$, where $d(\mathscr{C})$ and $d(\widetilde{\mathscr{C}})$ are minimum Hamming distances of $\mathscr{C}$ and $\widetilde{\mathscr{C}}$, respectively.

The next result extends Lally's relevant result [6] to chain rings and its proof is the same, hence is omitted.

Theorem 3.1 *Let $\mathscr{C}$ be an r-generator QC code of length $n\ell$ with index ℓ over R and generated by the set $\{v_1(x), v_2(x), \ldots, v_r(x)\}$, where $v_i(x) \in \mathcal{R}[x]/\langle x^n - 1\rangle$, $i = 1, 2, \ldots, r$. Then $\mathscr{C}$ has a lower bound on the minimum Hamming distance given by $d(\mathscr{C}) \geq d(\widetilde{\mathscr{C}})d(\mathscr{B})$, where $\widetilde{\mathscr{C}}$ is the cyclic code of length n over $\mathcal{R}$ with generator polynomials $v_1(x), v_2(x), \ldots, v_r(x)$, i.e. $\widetilde{\mathscr{C}} = \langle v_1(x), \ldots, v_r(x)\rangle$ and $\mathscr{B}$ is a linear code of length ℓ generated by the set $\{\mathcal{V}_{ij}, i = 1, 2, \ldots, r, j = 0, 1, \ldots, n-1\} \subseteq R^{\ell}$ where each $\mathcal{V}_{ij}$ is the vector equivalent of the j-th coefficient of $v_i(x)$ with respect to an R-basis $\{1, \xi, \ldots, \xi^{\ell-1}\}$.*

In the rest of this section, we give an application of the above discussion. This application leads to construction of QC codes over finite fields.

Let $R = \mathbb{F}_q + u\mathbb{F}_q + \cdots + u^{\ell-1}\mathbb{F}_q$, where $u^{\ell} = 0$ and ℓ is a positive integer. Consider a cyclic code $\widetilde{\mathscr{C}}$ of length n generated by a polynomial $v(x)$ over R. Let $\mathscr{C}$ be a linear code of length $n\ell$ spanned by $\{v(x), xv(x), \ldots, x^{n-1}v(x)\}$ over $\mathbb{F}_q$. Then $\mathscr{C}$ is a 1-generator QC code of length $n\ell$ with index ℓ. If $v(x) = v_0 + v_1x + \cdots + v_{n-1}x^{n-1} \in R[x]/\langle x^n - 1\rangle$, then each v_i is an ℓ-tuple with respect to the fixed $\mathbb{F}_q$-basis $\{1, u, \ldots, u^{\ell-1}\}$ of R. Now let the set $\{v_0, v_1, \ldots, v_{n-1}\}$ generate a linear code $\mathscr{B}$ of length ℓ over $\mathbb{F}_q$. By Theorem 3.1, we have the following result directly.

Theorem 3.2 *Let $\mathscr{C}$ be a QC code of length $n\ell$ with index ℓ over finite field $\mathbb{F}_q$ generated by the set $\{v(x), xv(x), \ldots, x^{n-1}v(x)\}$, where $v(x) = v_0 + v_1x + \cdots + v_{n-1}x^{n-1} \in R[x]/\langle x^n - 1\rangle$. Then*

(1) $\mathscr{C}$ has a lower bound on the minimum Hamming distance given by $d(\mathscr{C}) \geq d(\widetilde{\mathscr{C}})d(\mathscr{B})$, where $\widetilde{\mathscr{C}}$ is a cyclic code of length n over R generated by the polynomial $g(x) \in R[x]/\langle x^n - 1\rangle$, and $\mathscr{B}$ is a linear code of length ℓ generated by $\{v_0, v_1, \ldots, v_{n-1}\}$ where each v_i is an ℓ-tuple with respect to a fixed $\mathbb{F}_q$-basis $\{1, u, \ldots, u^{\ell-1}\}$ of R.

(2) If the cyclic code $\widetilde{\mathscr{C}}$ in (1) is free and the generator polynomial $g(x)$ has $\delta - 1$ consecutive roots in some Galois extension ring of R, and if the set $\{v_0, v_1, \ldots, v_{n-1}\}$ generates a cyclic code $\mathscr{B}$ over finite field $\mathbb{F}_q$ of length ℓ such that the generator

polynomial of $\mathscr{B}$ has $\varepsilon - 1$ consecutive roots in some Galois extension field of $\mathbb{F}_q$, then $d(\mathscr{C}) \geq \delta\varepsilon$.

Example 3.3 Let $R = \mathbb{F}_2 + u\mathbb{F}_2 + u^2\mathbb{F}_2$. Suppose $R = \{0, 1, u, v, uv, u^2, v^2, v^3\}$, where $u^3 = 0$, $v = 1 + u$, $v^2 = 1 + u^2$, $v^3 = 1 + u + u^2$, $uv = u + u^2$. It is well known that $x^7 - 1 = (x + v^3)(x^3 + uvx^2 + v^2x + v^3)(x^3 + vx^2 + ux + v^3)$, where $x + v^3$, $x^3 + uvx^2 + v^2x + v^3$ and $x^3 + vx^2 + ux + v^3$ are basic irreducible polynomials over R. Let $\mathcal{R} = R[x]/\langle x^3 + uvx^2 + v^2x + v^3\rangle$. Since $x^3 + uvx^2 + v^2x + v^3$ is a basic primitive polynomial over R, the root ξ of $x^3 + uvx^2 + v^2x + v^3$ is a primitive element in $\mathcal{R}$. Taking $v(x) = (x + v^3)(x^3 + uvx^2 + v^2x + v^3) = x^4 + x^3 + (1 + u + u^2)x^2 + u^2x + (1 + u^2)$, then the cyclic code $\widetilde{\mathscr{C}}$ of length 7 generated by $v(x)$ is free with the minimum Hamming distance of $\widetilde{\mathscr{C}}$ at least 4. The non-zero coefficients of $v(x)$ correspond to the elements $(1, 0, 1)$, $(0, 0, 1)$, $(1, 1, 1)$, $(1, 0, 0)$, $(1, 0, 0)$ with respect to the $\mathbb{F}_2$-basis $\{1, u, u^2\}$ of R and they generate a cyclic code $\mathscr{B}$ of length 3 with the minimum Hamming distance 1 over $\mathbb{F}_2$. Therefore, $\mathscr{C}$ is a 1-generator QC code of length 21 with dimension 3 and minimum Hamming distance at least $4 \times 1 = 4$ over finite field $\mathbb{F}_2$. In fact $\mathscr{C}$ is a QC code with parameters $[21, 3, 8]$ over $\mathbb{F}_2$.

4 Trace representation of quasi-cyclic codes

Let $x^n - 1 = f_1 f_2 \ldots f_r$, where each $f_i, i = 1, 2, \ldots, r$, is a basic irreducible polynomial with degree ℓ_i over R. Then from Proposition 2.1, we have

$$(R[x]/\langle x^n - 1\rangle)^\ell \cong \oplus_{i=1}^r (R[x]/\langle f_i\rangle)^\ell.$$

Therefore if $\mathscr{C}$ is a QC code of length $n\ell$ with index ℓ over R then $\mathscr{C} = \oplus_{i=1}^r \mathscr{C}_i$, where $\mathscr{C}_i, i = 1, 2, \ldots, r$, is a linear code of length ℓ over the ℓ_i-th Galois extension ring $\mathcal{R}_i$ of R. This is called the canonical decomposition of the QC code $\mathscr{C}$. The following result of Ling-Solé [7] gives a trace representation for QC codes over finite chain rings.

Theorem 4.1 (cf. Theorem 5.1 [7]) *Let $x^n - 1 = f_1 f_2 \ldots f_r$, where each $f_i, i = 1, 2, \ldots, r$, is the basic irreducible polynomial with degree ℓ_i over R. Denote $\mathcal{R}_i = R[x]/\langle f_i\rangle$. Let U_i denote the q-cyclotomic coset mod n corresponding to f_i. Fix a representatives $u_i \in U_i$ from each cyclotomic coset. Let $\mathscr{C}_i$ be a linear code of length ℓ over $\mathcal{R}_i$ for all $i = 1, 2, \ldots, r$. For $\widetilde{\boldsymbol{c}}_i \in \mathscr{C}_i$ and each $j = 0, 1, \ldots, n - 1$, let the vector $\boldsymbol{c}_j = \sum_{i=1}^r Tr_{\mathcal{R}_i/R}(\widetilde{\boldsymbol{c}}_i \xi^{-ju_i})$. Then the code*

$$\mathscr{C} = \{(\boldsymbol{c}_0, \boldsymbol{c}_1, \ldots, \boldsymbol{c}_{n-1}) | \, \widetilde{\boldsymbol{c}}_i \in \mathscr{C}_i\}$$

is a QC code of length $n\ell$ with index ℓ over R. Conversely, every QC code of length $n\ell$ with index ℓ over R is obtained through this construction.

Let $R \subset \widetilde{R} \subset \mathcal{R}$ be Galois extension. If $\omega \in \mathcal{R}$ such that $Tr_{\mathcal{R}/\widetilde{R}}(\omega) = 1$, then for any $\vartheta \in \widetilde{R}$ we have $Tr_{\widetilde{R}/R}(\vartheta) = Tr_{\mathcal{R}/R}(\omega\vartheta)$.

Our goal is to extend the minimum Hamming distance bound of Güneri–Ozbudak [5] for QC codes to finite chain rings. The following result will be essential for this purpose and it also extends the result of Proposition 4.6 in [5].

Lemma 4.2 *Let $\mathscr{C}$ be a QC code defined as above. Let $\omega_1, \omega_2, \ldots, \omega_r \in \mathcal{R}$ be elements with $Tr_{\mathcal{R}/\mathcal{R}_i}(\omega_i) = 1$ for all $i = 1, 2, \ldots, r$. Then*

(1) Any codeword $(\boldsymbol{c}_0, \boldsymbol{c}_1, \ldots, \boldsymbol{c}_{n-1}) \in \mathscr{C}$ is of the form

$$\boldsymbol{c}_j = \sum_{i=1}^{r} Tr_{\mathcal{R}/R}(\widetilde{\boldsymbol{c}}_i \omega_i \xi^{-ju_i})$$

for all $j = 0, 1, \ldots, n-1$.

(2) The columns of any codeword $c \in \mathscr{C}$ lie in a free cyclic code $\mathscr{B}$ of length n over R, which dual code $\mathscr{B}^{\perp}$ has roots $\xi^{-u_1}, \xi^{-u_2}, \ldots, \xi^{-u_r}$, where ξ is an n-th primitive root of unity in $\mathcal{R}$;

(3) For any column

$$\widehat{\boldsymbol{c}}_v = \left(\Sigma_{i=1}^{r} Tr_{\mathcal{R}/R}(\widetilde{c}_{i,v}\omega_i), \ldots, \Sigma_{i=1}^{r} Tr_{\mathcal{R}/R}(\widetilde{c}_{i,v}\omega_i \xi^{-(n-1)u_i})\right),$$

where $\widetilde{\boldsymbol{c}}_i = (\widetilde{c}_{i1}, \widetilde{c}_{i2}, \ldots, \widetilde{c}_{i\ell}) \in \mathcal{R}_i$ and $v = 1, 2, \ldots, \ell$, we have $\widehat{\boldsymbol{c}}_v = \boldsymbol{0}$ if and only if $\widetilde{c}_{1,v} = \widetilde{c}_{2,v} = \cdots = \widetilde{c}_{r,v} = 0$.

Proof (1) Clearly, $\sum_{i=1}^{r} Tr_{\mathcal{R}/R}(\widetilde{\boldsymbol{c}}_i \omega_i \xi^{-ju_i}) = \sum_{i=1}^{r} Tr_{\mathcal{R}_i/R}(\widetilde{\boldsymbol{c}}_i \xi^{-ju_i}) = \mathbf{c}_j$;

(2) For any column

$$\widehat{\mathbf{c}}_v = \left(\Sigma_{i=1}^{r} Tr_{\mathcal{R}/R}(\widetilde{c}_{i,v}\omega_i), \ldots, \Sigma_{i=1}^{r} Tr_{\mathcal{R}/R}(\widetilde{c}_{i,v}\omega_i \xi^{-(n-1)u_i})\right),$$

the v-th component $\widehat{c}_v = \sum_{i=1}^{r} Tr_{\mathcal{R}/R}(\widetilde{c}_{i,v}\omega_i \xi^{-vu_i})$ where

$$\widetilde{\mathbf{c}}_i = (\widetilde{c}_{i1}, \widetilde{c}_{i2}, \ldots, \widetilde{c}_{i\ell}) \in \mathcal{R}_i$$

and $v = 1, 2, \ldots, \ell$. Since $\widetilde{c}_{i,v}\omega_i \in \mathcal{R}$, from Proposition 2.3, we have $\widehat{\mathbf{c}}_v$ lies in a free cyclic code $\mathscr{B}$ of length n over R, which dual code $\mathscr{B}^{\perp}$ has roots $\xi^{-u_1}, \xi^{-u_2}, \ldots, \xi^{-u_r}$;

(3) $\widehat{\mathbf{c}}_v = \mathbf{0}$ if and only if each v-th component is zero for all $v = 0, 1, \ldots, n-1$ if and only if $\Sigma_{i=1}^{r} Tr_{\mathcal{R}/R}(\widetilde{c}_{i,v}\omega_i \xi^{-vu_i}) = 0$ if and only if $Tr_{\mathcal{R}/R}(\widetilde{c}_{i,v}\omega_i \xi^{-vu_i}) = 0$ for all $i = 1, 2, \ldots, r$.

(i) If $\ell_1 = \ell_2 = \cdots = \ell_r = m$, then $Tr_{\mathcal{R}/R}(\widetilde{c}_{i,v}\omega_i \xi^{-vu_i}) = 0$ for all $i = 1, 2, \ldots, r$ if and only if $\widetilde{c}_{1,v} = \widetilde{c}_{2,v} = \cdots = \widetilde{c}_{r,v} = 0$;

(ii) If there exists a set $\{j_1, j_2, \ldots, j_d\} \subseteq \{1, 2, \ldots, r\}$ such that $\ell_{j_k} < m$ for all $k \in \{j_1, j_2, \ldots, j_d\}$ and $\ell_p = m$ for all $p \in \{1, 2, \ldots, r\} \backslash \{j_1, j_2, \ldots, j_d\}$, then $Tr_{\mathcal{R}/R}(\widetilde{c}_{i,v}\omega_i \xi^{-vu_i}) = 0$ for all $i = 1, 2, \ldots, r$ if and only if $\widetilde{c}_{\ell_p,v} = 0$ and $Tr_{\mathcal{R}/\mathcal{R}_i}(\widetilde{c}_{\ell_{j_k}}\omega_i) = \widetilde{c}_{\ell_{j_k}} Tr_{\mathcal{R}/\mathcal{R}_i}(\omega_i) = \widetilde{c}_{\ell_{j_k}} = 0$. Therefore, we have proved $\widehat{\mathbf{c}}_v = \mathbf{0}$ if and only if $\widetilde{c}_{1,v} = \widetilde{c}_{2,v} = \cdots = \widetilde{c}_{r,v} = 0$. □

As a consequence of Lemma 4.2, we can exhibit a minimum Hamming distance bound for the QC code. We assume that

$$d(\mathscr{C}_1) \geq d(\mathscr{C}_2) \geq \cdots \geq d(\mathscr{C}_r).$$

For any nonempty subset $\mathcal{I} = \{i_1, i_2, \ldots, i_t\} \subseteq \{1, 2, \ldots, r\}$ with $1 \leq i_1 < i_2 < \cdots < i_t \leq r$, let $\mathscr{B}_{\mathcal{I}} = \mathscr{B}_{i_1,i_2,\ldots,i_t}$ be a free cyclic code of length n over R, which dual code $\mathscr{B}_{\mathcal{I}}^{\perp}$ has roots $\xi^{-u_{i_1}}, \xi^{-u_{i_2}}, \ldots, \xi^{-u_{i_t}}$. If $\emptyset \neq \mathcal{I}_1 \subset \mathcal{I}_2 \subseteq \{1, 2, \ldots, r\}$, then $\mathscr{B}_{\mathcal{I}_1} \subset \mathscr{B}_{\mathcal{I}_2}$ and hence $d(\mathscr{B}_{\mathcal{I}_1}) \geq d(\mathscr{B}_{\mathcal{I}_2})$.

For $\mathcal{I}$ defined above, we define

$$d_{\mathcal{I}} = d_{i_1,i_2,\ldots,i_t} = \begin{cases} d(\mathscr{C}_{i_1})d(\mathscr{B}_{i_1}) & \text{if } t = 1 \\ \sum_{j=1}^{t}(d(\mathscr{C}_{i_j}) - d(\mathscr{C}_{i_{j+1}}))d(\mathscr{B}_{i_1,i_2,\ldots,i_j}) & \text{if } t = 2. \end{cases}$$

Let $\mathcal{J} = \mathcal{I}\backslash\{i_\mu\}$ for some $\mu \in \{2, 3, \ldots, t\}$. Then $d_{\mathcal{J}} \geq d_{\mathcal{I}}$ (see Lemma 4.7 in [5].)

The following extends Theorem 4.8 in [5] to QC codes over finite chain rings.

Theorem 4.3 *Let $\mathscr{C}$ be a QC code as discussed above. Then the minimum Hamming distance of $\mathscr{C}$ satisfies*

$$d(\mathscr{C}) \geq \min\{d_r, d_{r-1,r}, \ldots, d_{1,2,\ldots,r}\}.$$

Proof Let c be a nonzero codeword of $\mathscr{C}$. Suppose that $\widetilde{\mathbf{c}}_{i_k} \in \mathscr{C}_i$ for all $k = 1, 2, \ldots, t$, where $\{i_1, i_2, \ldots, i_t\} \subseteq 1, 2, \ldots, r$ and $1 \leq i_1 < i_2 < \cdots < i_t \leq r$. If $t = 1$, then by Lemma 4.2 (2) there exists at least $d(\mathscr{C}_1)$ nonzero columns in $\mathscr{C}$ implying the minimum possible weight for such code is $d(\mathscr{C}) \geq d(\mathscr{C}_{i_1})d(\mathscr{B}_{i_1})$. If $t \geq 2$, then the weight for such code $\mathscr{C}$ is minimized if $\mathrm{Supp}(\widetilde{\mathbf{c}}_{i_t}) \subseteq \mathrm{Supp}(\widetilde{\mathbf{c}}_{i_{t-1}}) \subseteq \cdots \subseteq \mathrm{Supp}(\widetilde{\mathbf{c}}_{i_1})$, where $\mathrm{Supp}(\widetilde{\mathbf{c}}_{i_k})$ denotes the nonzero coordinates of $\widetilde{\mathbf{c}}_{i_k}$ for all $k = 1, 2, \ldots, t$. By the proof process of Theorem 4.5 in [5], the lowest possible weight for such code in this case is

$$d(\mathscr{C}) \geq d_{\mathcal{I}} = (d(\mathscr{C}_{i_1}) - d(\mathscr{C}_{i_2}))d(\mathscr{B}_{i_1}) + \cdots + d(\mathscr{C}_{i_t})d\mathscr{B}_{i_1,i_2,\ldots,i_t},$$

which implies that $d(\mathscr{C}) \geq \min\{d_{\mathcal{I}} | \ \mathcal{I} = \{i_1, i_2, \ldots, i_t\} \subseteq \{1, 2, \ldots, r\}\ with\ i_1 < i_2 < \cdots < i_t\}$. Let $\mathcal{N} \subseteq \{1, 2, \ldots, r\}$ and let i be the minimal element in $\mathcal{N}$. Adjoining one element at a time, we have $\mathcal{N} \subseteq \mathcal{N}_1 \subseteq \cdots \subseteq \{i, i+1, \ldots, r\}$. Then $d_{\mathcal{N}} \geq d_{\mathcal{N}_1} \geq \cdots \geq d_{i,i+1,\ldots,r}$. Hence, the minimum Hamming distance of $\mathscr{C}$ is equal to $d(\mathscr{C}) \geq \min\{d_r, d_{r-1,r}, \ldots, d_{1,2,\ldots,r}\}$. □

Example 4.4 Consider a QC code $\mathscr{C}$ of length 14 with index 2 generated by $(a_0(x), a_1(x))$ over $R = \mathbb{F}_2 + u\mathbb{F}_2$, where $a_0(x) = x^4 + x^2 + x$ and $a_1(x) = x^4 + x^3 + x^2 + 1$. Since $(R[x]/\langle x^7 - 1\rangle)^2 \cong (R[x]/\langle x - 1\rangle)^2 \oplus (R[x]/\langle x^3 + x^2 + 1\rangle)^2 \oplus (R[x]/\langle x^3 + x + 1\rangle)^2$, we have $\mathscr{C} = \oplus_{i=1}^{3}\mathscr{C}_i$ where $\mathscr{C}_1$ is a linear code of length 2 generated by $(1, 0)$ over R, $\mathscr{C}_2$ is a linear code of length 2 generated by $(1, x^2 + x + 1)$ over $R[x]/\langle x^3 + x^2 + 1\rangle$ and $\mathscr{C}_3$ is a zero code over $R[x]/\langle x^3 + x + 1\rangle$. Clearly, $d(\mathscr{C}_1) = d(\mathscr{C}_2) = 1, d(\mathscr{C}_3) = 0$. Hence Theorem 4.3 yields $d(\mathscr{C}) \geq \min\{6, 3\} = 3$. In fact, its minimum Hamming distance is 7 actually.

Example 4.5 Consider a QC code $\mathscr{C}$ of length 21 with index 3 generated by two vectors $(x^2+x^3, x^2+x^3, x^2+x^3+x^5+x^6)$ and $(0, x^3+x^4, x^3+x^4)$ over $R=\mathbb{F}_2+u\mathbb{F}_2$. Let $\mathcal{R}=\mathbb{F}_8+u\mathbb{F}_8$. Then $\mathscr{C}$ can be viewed as an $R[x]/\langle x^7-1\rangle$-submodule of $\mathcal{R}[x]/\langle x^7-1\rangle$, and generated by $(1+\xi+\xi^2)x^2+(1+\xi+\xi^2)x+\xi^2x^5+\xi^2x^6$ and $(\xi+\xi^2)x^3+(\xi+\xi^2)x^4$. Then, by Theorem 3.1, one can verify that $d(\mathscr{C})\geq 2$. Since $(R[x]/\langle x^7-1\rangle)^3\cong(R[x]/\langle x-1\rangle)^3\oplus(R[x]/\langle x^3+x^2+1\rangle)^3\oplus(R[x]/\langle x^3+x+1\rangle)^3$, we have $\mathscr{C}=\oplus_{i=1}^3\mathscr{C}_i$ where $\mathscr{C}_1$ is a zero code of length 3 over R, $\mathscr{C}_2$ is a linear code of length 3 generated by $(1, 1, x^3+1)$ and $(0, x, x)$ over $R[x]/\langle x^3+x^2+1\rangle$ and $\mathscr{C}_3$ is a linear code of length 3 generated by $(x^2+x+1, x^2+x+1, x^2+1)$ and $(0, x^2+1, x^2+1)$ over $R[x]/\langle x^3+x+1\rangle$. Clearly, $d(\mathscr{C}_1)=0$ and $d(\mathscr{C}_1)=d(\mathscr{C}_2)=2$. Hence, by Theorem 4.3, $d(\mathscr{C})\geq\min\{8,4\}=4$. In fact, its minimum Hamming distance is 4 actually. This example shows that sometimes Theorem 4.3 can give a sharp bound on minimum Hamming distance of QC codes. This property can also be found in Examples of [5].

Acknowledgments This research is supported by the National Key Basic Research Program of China (Grant No. 2013CB834204), and the National Natural Science Foundation of China (Grant Nos. 61171082 and 61301137).

References

1. Aydin, N., Ray-Chaudhuri, D.: Quasi-cyclic codes over $\mathbb{Z}_4$ and some new binary codes. IEEE Trans. Inf. Theory **48**, 2065–2069 (2002)
2. Bhaintwal, M., Wasan, S.: On quasi-cyclic codes over $\mathbb{Z}_q$. Appl. Algebra Eng. Commun. Comput. **20**, 459–480 (2009)
3. Cao, Y., Gao, J.: Constructing quasi-cyclic codes from linear algebra theory. Des. Codes Crypt. **67**, 59–75 (2013)
4. Güneri, C.: Artin–Schreier curves and weights of two-dimensional cyclic codes. Finite Fields Appl. **10**, 481–505 (2004)
5. Güneri, C., Özbudak, F.: A bound on the minimum distance of quasi-cyclic codes. SIAM J. Discret. Math. **26**, 1781–1796 (2012)
6. Lally, K.: Quasicyclic codes of index ℓ over $\mathbb{F}_q$ viewed as $\mathbb{F}_q[x]$-submodules of $\mathbb{F}_{q^\ell}[x]/(x^m-1)$, in applied algebra, algebraic algorithms and error-correcting codes. Lect. Notes Comput. Sci. **2643**, 244–253 (2003)
7. Ling, S., Solé, P.: On the algebra structure of quasi-cyclic codes II: chain rings. Des. Codes Crypt. **30**, 113–130 (2003)
8. MacDonald, B.: Finite Rings with Identity. Dekker, New York (1974)
9. Norton, G., Sâlâgean, A.: On the stucture of linear and cyclic codes over a finite chain ring. Appl. Algebra Eng. Commun. Comput. **6**, 489–506 (2000)
10. Siap, I., Abualrub, T., Yildiz, B.: One generator quasi-cyclic codes over $\mathbb{F}_2+u\mathbb{F}_2$. J. Frank. Inst. **349**, 284–292 (2012)
11. Wan, Z.-X.: Cyclic codes over Galois rings. Algebra Colloq. **6**(3), 291–304 (1999)