Notes on Quasi-Cyclic Codes with Cyclic Constituent Codes

Minjia Shi, Yiping Zhang and Patrick Solé

Abstract Quasi-cyclic codes are generalizations of the familiar linear cyclic codes. By using the results of [4], the authors in [2, 3] showed that a quasi-cyclic code $\mathscr{C}$ over $\mathbb{F}_q$ of length ℓm and index ℓ with m being pairwise coprime to ℓ and the characteristic of $\mathbb{F}_q$ is equivalent to a cyclic code if the constituent codes of $\mathscr{C}$ are cyclic, where q is a prime power and the equivalence is given in [3]. In this paper, we apply an algebraic method to prove that a quasi-cyclic code with cyclic constituent codes is equivalent to a cyclic code. Moreover, the main result (see Theorem 4) includes Proposition 9 in [3] as a special case.

Keywords Quasi-cyclic codes · Constituent codes · Cyclic codes · Circulant matrix · Similar circulant matrix

MSC 2010 codes: Primary 94B05 · Secondary 94B15

M. Shi (✉)
Key Laboratory of Intelligent Computing & Signal Processing,
Ministry of Education, Anhui University, No. 3 Feixi Road, Hefei 230039,
Anhui, People's Republic of China
e-mail: smjwcl.good@163.com

M. Shi
National Mobile Communications Research Laboratory, Southeast University,
Nanjing 210096, People's Republic of China

M. Shi
School of Mathematical Sciences of Anhui University, Hefei 230601, Anhui,
People's Republic of China

Y. Zhang
School of Wendian, Anhui University, Hefei 230601, Anhui, China
e-mail: yipingzhang0123@163.com

P. Solé
CNRS/LAGA, University of Paris 8, 93 526 Saint-Denis, France
e-mail: sole@enst.fr

T. Abualrub et al. (eds.), *Mathematics Across Contemporary Sciences*,
Springer Proceedings in Mathematics & Statistics 190,
DOI 10.1007/978-3-319-46310-0_12

1 Introduction

Quasi-cyclic codes over finite fields form an important class of block codes that include cyclic codes as a special case. In [4], Ling and Solé viewed each quasi-cyclic code as a code over a polynomial ring, and extracted a description of each quasi-cyclic code as being constructed from linear codes of shorter lengths over larger fields, which are called the constituent codes of the quasi-cyclic code. It is interesting to ask what kind of codes we will obtain if constituent codes of a quasi-cyclic code are cyclic. Such codes can enjoy the ease of encoding of cyclic codes by polynomial division for instance.

In [1], quasi-cyclic codes of length 5ℓ and index ℓ over $\mathbb{F}_q$ were obtained from a pair of codes over $\mathbb{F}_q$ and $\mathbb{F}_{q^4}$, respectively, by a combinatorial construction called here the quintic construction. They enjoy a designed trellis description and a suboptimal coset decoding algorithm. They are shown to be cyclic when the constituent codes are cyclic of odd length coprime to 5. Lim [3] generalized the result in [1] to the general case by a similar method. In [2], Güneri and Özbudak considered the same issue. If the constituent codes of a quasi-cyclic code $\mathscr{C}$ of length $m\ell$ and index ℓ are cyclic, the authors show that $\mathscr{C}$ can be viewed as a 2-D cyclic code of size $m \times \ell$ over $\mathbb{F}_q$. Moreover, in case m and ℓ are also coprime to each other, $\mathscr{C}$ must be equivalent to a cyclic code. However, the results of Refs. [2], [3] relied on the structures of quasi-cyclic codes of the Ref. [4].

In this paper, we apply an algebraic method to investigate the same issue. Moreover, the equivalence in Proposition 9 of [3] is a special case of Theorem 4, which provides many equivalences. Throughout this paper we require that $(m, q) = (\ell, q) = (m, \ell) = 1$, where $q = p^k$ for some positive integer k, p is a prime.

2 The Circulant Matrix Decomposition of a Cyclic Code

Cyclic codes are generated by shift registers and play an important role in random error-correcting and burst error-correcting. Cyclic codes were first studied by Prange in 1957, and the study of the algebraic properties of cyclic codes developed rapidly since then. An $[n, k]_q$ code C is called cyclic provided that, for each codeword $\mathbf{c} = (c_0, c_1, c_2, \ldots, c_{n-1}) \in C$, the vector $(c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \in C$. In this section, we require that $(n, p) = 1$.

Definition 1 Let C be a cyclic code of length n over $\mathbb{F}_q$ and $A \subseteq C$, then a *circulant matrix* A containing the codeword $(a_0, a_1, \ldots, a_{n-1})$ is defined as follows

$$A = \begin{pmatrix} a_0 & a_1 & a_2 & \ldots & a_{n-1} \\ a_{n-1} & a_0 & a_1 & \ldots & a_{n-2} \\ \ldots & & \ldots & & \ldots \\ a_1 & a_2 & a_3 & \ldots & a_0 \end{pmatrix}.$$

Remark 1 A can be considered as a set of n codewords of C. In our case, codeword repetition in A is omitted if necessary.

Lemma 1 *A cyclic code C of length n over $\mathbb{F}_q$ can be decomposed into a finite disjoint union of circulant matrices.*

Proof If $\mathbf{c} = (a_0, a_1, \ldots, a_{n-1}) \in C$, then we have $A \subseteq C$. For any $\mathbf{c}' = (b_0, b_1, \ldots, b_{n-1}) \in C$ and $\mathbf{c}' \notin A$, following the construction of the circulant matrix, then $A \cap B = \emptyset$, where B is the circulant matrix containing $\mathbf{c}'$, this operation will be stopped after finite steps.

Take the $[7, 4, 3]$ Hamming code C for example, which is a cyclic code with generator polynomial $1 + x^2 + x^3$, according to Lemma 1, we have $C =$

$$\begin{pmatrix} 1&0&1&1&1&0&0\\ 0&1&0&1&1&1&0\\ 0&0&1&0&1&1&1\\ 1&0&0&1&0&1&1\\ 1&1&0&0&1&0&1\\ 1&1&1&0&0&1&0\\ 0&1&1&1&0&0&1 \end{pmatrix} \bigcup \begin{pmatrix} 1&1&0&1&0&0&0\\ 0&1&1&0&1&0&0\\ 0&0&1&1&0&1&0\\ 0&0&0&1&1&0&1\\ 1&0&0&0&1&1&0\\ 0&1&0&0&0&1&1\\ 1&0&1&0&0&0&1 \end{pmatrix} \bigcup \begin{pmatrix} 0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0\\ 0&0&0&0&0&0&0 \end{pmatrix} \bigcup \begin{pmatrix} 1&1&1&1&1&1&1\\ 1&1&1&1&1&1&1\\ 1&1&1&1&1&1&1\\ 1&1&1&1&1&1&1\\ 1&1&1&1&1&1&1\\ 1&1&1&1&1&1&1\\ 1&1&1&1&1&1&1 \end{pmatrix}.$$

Following Definition 1, we can prove the following lemma, which plays an important role in obtaining our results.

Lemma 2 *Let C be a cyclic code of length n over $\mathbb{F}_q$, then A is a circulant matrix if and only if $A = P_n diag(f(1), f(\zeta), \ldots, f(\zeta^{n-1}))P_n^{-1}$, where*

$$P_n = \begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ 1 & \zeta & \zeta^2 & \ldots & \zeta^{n-1} \\ 1 & \zeta^2 & \zeta^{2\times 2} & \ldots & \zeta^{2(n-1)} \\ \vdots & & \vdots & & \vdots \\ 1 & \zeta^{n-1} & \zeta^{2(n-1)} & \ldots & \zeta^{(n-1)(n-1)} \end{pmatrix}$$

is a Vandermonde matrix, ζ is a primitive n-th root of unity, $(a_0, \cdots, a_{n-1})$ is the first row of A and $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1}$.

Proof It is clear that P_n is invertible since ζ is a primitive n-th root of unity. Moreover, it is easy to check that

$$AP_n = \begin{pmatrix} f(1) & f(\zeta) & \ldots & f(\zeta^{n-1}) \\ f(1) & \zeta f(\zeta) & \ldots & \zeta^{n-1} f(\zeta^{n-1}) \\ \ldots & \ldots & \ldots & \ldots \\ f(1) & \zeta^{n-1} f(\zeta) & \ldots & \zeta^{(n-1)(n-1)} f(\zeta^{n-1}) \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 1 & \ldots & 1 \\ 1 & \zeta & \ldots & \zeta^{n-1} \\ \ldots & \ldots & \ldots & \ldots \\ 1 & \zeta^{n-1} & \ldots & \zeta^{(n-1)(n-1)} \end{pmatrix} diag(f(1), f(\zeta), \ldots, f(\zeta^{n-1})).$$

Equivalently, $A = P_n diag(f(1), f(\zeta), \ldots, f(\zeta^{n-1})) P_n^{-1}$. The converse part is straightforward.

3 Quasi-cyclic Codes with Cyclic Constituent Codes

A linear code $\mathscr{C}$ is a quasi-cyclic code of length ℓm with index ℓ if $\mathscr{C}$ is invariant under a shift by ℓ places, namely, for any $(a_{00}, a_{01}, \ldots, a_{0,\ell-1}, a_{10}, \ldots, a_{1,\ell-1}, \ldots, a_{m-1,0}, \ldots, a_{m-1,\ell-1}) \in \mathscr{C}$, we have $(a_{m-1,0}, a_{m-1,1}, \ldots, a_{m-1,\ell-1}, a_{00}, \ldots, a_{0,\ell-1}, \ldots, a_{m-2,0}, \ldots, a_{m-2,\ell-1}) \in \mathscr{C}$. The *constituent codes* of such a code are codes of length ℓ over extension alphabets that appear in the CRT decomposition of [4]. See [4] for details. They are not cyclic in general. The class of quasi-cyclic codes with cyclic constituents is a strict subclass of all quasi-codes. In [2], the authors proved that if m and ℓ are both relatively prime to q, and the constituents of the quasi-cyclic code (of length ℓm and index ℓ) are all cyclic codes, then $\mathscr{C}$ is a 2-D cyclic code. Therefore, a linear code $\mathscr{C}$ of length ℓm is a quasi-cyclic code of length ℓm and index ℓ with cyclic constituent codes if $(a_{00}, a_{01}, a_{02}, \ldots, a_{0,\ell-1}, a_{10}, \ldots, a_{1,\ell-1}, \ldots, a_{m-1,0}, \ldots, a_{m-1,\ell-1}) \in \mathscr{C}$ implies that

$$(a_{m-1,\ell-1}, a_{m-1,0}, \ldots, a_{m-1,\ell-2}, a_{0,\ell-1}, \ldots, a_{0,\ell-2}, \ldots, a_{m-2,\ell-1}, \ldots, a_{m-2,\ell-2}) \in \mathscr{C}.$$

Definition 2 Let $\mathscr{C}$ be a quasi-cyclic code of length ℓm and index ℓ with cyclic constituent codes, then a *similar circulant matrix* A' containing the codeword

$$(a_{00}, a_{01}, \ldots, a_{0,\ell-1}, a_{10}, \ldots, a_{1,\ell-1}, \ldots, a_{m-1,0}, \ldots, a_{m-1,\ell-1})$$

is defined as follows

$$\begin{pmatrix} a_{00} & a_{01} & \cdots & a_{0,\ell-1} & a_{10} & \cdots & a_{1,\ell-1} & \cdots & a_{m-1,0} & \cdots & a_{m-1,\ell-1} \\ a_{m-1,\ell-1} & a_{m-1,0} & \cdots & a_{m-1,\ell-2} & a_{0,\ell-1} & \cdots & a_{0,\ell-2} & \cdots & a_{m-2,\ell-1} & \cdots & a_{m-2,\ell-2} \\ a_{m-2,\ell-2} & a_{m-2,\ell-1} & \cdots & a_{m-2,\ell-3} & a_{m-1,\ell-2} & \cdots & a_{m-1,\ell-3} & \cdots & a_{m-3,\ell-2} & \cdots & a_{m-3,\ell-3} \\ \cdots & & \cdots & & & \cdots & & & \cdots & & \\ a_{11} & a_{12} & \cdots & a_{10} & a_{21} & \cdots & a_{20} & \cdots & a_{01} & \cdots & a_{00} \end{pmatrix}.$$

Remark 2 A' can be considered as a set of ℓm codewords of $\mathscr{C}$. Codeword repetition in A' is omitted if necessary. Note that A' is a $\ell m \times \ell m$ matrix.

Similar to the proof of Lemma 1, we have the following corollary.

Corollary 1 *Let $\mathscr{C}$ be a quasi-cyclic code of length ℓm and index ℓ with cyclic constituent codes, then the code $\mathscr{C}$ can be decomposed into finite disjoint unions of similar circulant matrices.*

We denote by S_n the symmetric group of n elements. The following lemma will be clear from matrix theory.

Lemma 3 *Let D_1 and D_2 be $n \times n$ matrices, for $\sigma \in S_n$, $\sigma(D_1)$ represents the action of σ on coordinates of every row of D_1, $\sigma^T(D_1)$ represents the action of σ on coordinates of every column of D_1, which means if*

$$D_1 = \begin{pmatrix} d_{00} & d_{01} & d_{02} & \dots & d_{0,n-1} \\ d_{10} & d_{11} & d_{12} & \dots & d_{1,n-1} \\ \dots & & \dots & & \dots \\ d_{n-1,0} & d_{n-1,1} & d_{n-1,2} & \dots & d_{n-1,n-1} \end{pmatrix},$$

then we have

$$\sigma(D_1) = \begin{pmatrix} d_{0,\sigma(0)} & d_{0,\sigma(1)} & d_{0,\sigma(2)} & \dots & d_{0,\sigma(n-1)} \\ d_{1,\sigma(0)} & d_{1,\sigma(1)} & d_{1,\sigma(2)} & \dots & d_{1,\sigma(n-1)} \\ \dots & & \dots & & \dots \\ d_{n-1,\sigma(0)} & d_{n-1,\sigma(1)} & d_{n-1,\sigma(2)} & \dots & d_{n-1,\sigma(n-1)} \end{pmatrix},$$

$$\sigma^T(D_1) = \begin{pmatrix} d_{\sigma(0),0} & d_{\sigma(0),1} & d_{\sigma(0),2} & \dots & d_{\sigma(0),n-1} \\ d_{\sigma(1),0} & d_{\sigma(1),1} & d_{\sigma(1),2} & \dots & d_{\sigma(1),n-1} \\ \dots & & \dots & & \dots \\ d_{\sigma(n-1),0} & d_{\sigma(n-1),1} & d_{\sigma(n-1),2} & \dots & d_{\sigma(n-1),n-1} \end{pmatrix}$$

and $D_1D_2 = \sigma(D_1)\sigma^T(D_2)$.

Lemma 4 *Let ε be a primitive ℓm-th root of unity, then there exists a permutation $\theta \in S_{\ell m}$ such that $\theta(A') = P_{\ell m} \Lambda P_{\ell m}^{-1}$, where*

$$P_{\ell m} = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \varepsilon & \varepsilon^2 & \dots & \varepsilon^{\ell m-1} \\ 1 & \varepsilon^2 & \varepsilon^{2\times 2} & \dots & \varepsilon^{2(\ell m-1)} \\ \vdots & & \vdots & & \vdots \\ 1 & \varepsilon^{\ell m-1} & \varepsilon^{2(\ell m-1)} & \dots & \varepsilon^{(\ell m-1)(\ell m-1)} \end{pmatrix}$$

is a Vandermonde matrix, $\Lambda = diag(g(1), g(\varepsilon), g(\varepsilon^2), \dots, g(\varepsilon^{\ell m-1}))$ is a diagonal matrix, and $g(y) = a_{00} + a_{11}y + \dots + a_{i_m,i_\ell}y^i + \dots + a_{m-1,\ell-1}y^{\ell m-1}$ with $i_m = i \pmod m$, $i_\ell = i \pmod \ell$, $i = 0, 1, 2, \dots, \ell m - 1$.

Proof Let $\xi \in \{1, \varepsilon, \varepsilon^2, \dots, \varepsilon^{\ell m-1}\}$ and $P'_{\ell m}$ be obtained from the matrix $P_{\ell m}$ under certain row shift, then there exists a permutation θ such that $\theta^T(P'_{\ell m}) = P_{\ell m}$. Since $gcd(\ell, m) = 1$, according to the Chinese Remainder Theorem, we can establish a one-to-one correspondence between the coefficient of the term ξ^i in $g(\xi)$ and ξ^i denoted by $a_{i_m,i_\ell} \leftrightarrow \xi^i$, this correspondence can make the calculation of $g(y)$ easily. Let $P'_{\ell m}(\xi)$ be any column vector of $P'_{\ell m}$, and $A'P'_{\ell m}(\xi) = (b_0, b_1, \dots, b_{\ell m-1})^T$. Set $b_0 = g(\xi)$, by this correspondence and the elements of the first row of A', we can determine $P'_{\ell m}(\xi) = (1, \xi^{tm}, \xi^{2tm}, \dots, \xi^i, \dots, \xi^{\ell m-1})^T$, where t is the multiplicative inverse of m module ℓ. Thus θ is determined by $P'_{\ell m}(\xi)$. The elements of the j-th row of A' can be expressed as

$$(a_{00}^{(j)}, a_{01}^{(j)}, \dots, a_{0,\ell-1}^{(j)}, a_{10}^{(j)}, a_{11}^{(j)}, \dots, a_{1,\ell-1}^{(j)}, \dots, a_{m-1,0}^{(j)}, a_{m-1,1}^{(j)}, \dots, a_{m-1,\ell-1}^{(j)}),$$

where $1 \le j \le \ell m$.

Next, we try to calculate b_j $(j = 1, 2, \dots, \ell m - 1)$. If we fix j, by the construction of the similar circulant matrix A', since $1 \le i + j \le 2\ell m - 2$, we know that in the $(j+1)$-th row of A',

$$a_{i_m,i_\ell}^{(1)} = a_{(i+j)_m,(i+j)_\ell}^{(j+1)} \leftrightarrow \xi^{(i+j)_{\ell m}},$$

and $\xi^{(i+j)_{\ell m}} = \xi^{i+j}$ for $\xi^{\ell m} = 1$. Then

$$b_j = \sum_{i=0}^{\ell m-1} a_{i_m,i_\ell}^{(j+1)} \xi^i = \sum_{i+j=0}^{i+j=\ell m-1} a_{(i+j)_m,(i+j)_\ell}^{(j+1)} \xi^{i+j} = \xi^j \sum_{i+j=0}^{i+j=\ell m-1} a_{(i+j)_m,(i+j)_\ell}^{(j+1)} \xi^i$$

$$= \xi^j \sum_{i+j=0}^{i+j=\ell m-1} a_{i_m,i_\ell}^{(1)} \xi^i = \xi^j \sum_{i=0}^{\ell m-1} a_{i_m,i_\ell}^{(1)} \xi^i = \xi^j b_0. \quad (1)$$

From (1), we have

$$A' P'_{\ell m}(\xi) = (b_0, b_1, \dots, b_{\ell m-1})^T = g(\xi)(1, \xi, \xi^2, \dots, \xi^{\ell m-1})^T. \quad (2)$$

Set $\xi = 1, \varepsilon, \varepsilon^2, \dots, \varepsilon^{\ell m-1}$, from (2), we have

$$A'(P'_{\ell m}(1), P'_{\ell m}(\varepsilon), P'_{\ell m}(\varepsilon^2), \dots, P'_{\ell m}(\varepsilon^{\ell m-1}))^T = A' P'_{\ell m},$$

then

$$A' P'_{\ell m} = \begin{pmatrix} g(1) & g(\varepsilon) & \dots & g(\varepsilon^{\ell m-1}) \\ g(1) & \varepsilon g(\varepsilon) & \dots & \varepsilon^{\ell m-1} g(\varepsilon^{\ell m-1}) \\ \dots & & \dots & \dots \\ g(1) & \varepsilon^{\ell m-1} g(\varepsilon) & \dots & \varepsilon^{(\ell m-1)(\ell m-1)} g(\varepsilon^{\ell m-1}) \end{pmatrix} = P_{\ell m} \Lambda. \quad (3)$$

Thus $A' P'_{\ell m} = P_{\ell m} \Lambda$. From Lemma 3, we have $A' P'_{\ell m} = \theta(A') \theta^T(P'_{\ell m}) = \theta(A') P_{\ell m} = P_{\ell m} \Lambda$. Consequently, $\theta(A') = P_{\ell m} \Lambda P_{\ell m}^{-1}$.

Corollary 2 *A similar circulant matrix A' is equivalent to a circulant matrix.*

Proof From Lemmas 4 and 2, we know that $\theta(A')$ is a circulant matrix, so A' is equivalent to a circulant matrix $\theta(A')$. Moreover, from the expressions of $f(x)$ and $g(y)$, the circulant matrix $\theta(A')$ is none other than the circulant matrix containing the codeword $(a_{00}, a_{11}, \dots, a_{i_m,i_\ell}, \dots, a_{m-1,\ell-1})$.

Theorem 1 *A quasi-cyclic code $\mathscr{C}$ of length ℓm and index ℓ with cyclic constituent codes is equivalent to a cyclic code.*

Proof From Corollary 1, we can write $\mathscr{C} = A'_1 \cup A'_2 \cup \cdots \cup A'_k = \cup_{i=1}^{k} A'_i$, from Lemma 4, let θ be a permutation that $\theta(A'_1)$ is a circulant matrix, and according to the proof of Lemma 4, the permutation θ is universally applicable for the matrices A'_i, thus $\theta(A'_i)(i = 1, \ldots, k)$ are all circulant matrices. Now we prove that $\theta(\mathscr{C})$ is a linear cyclic code. For $\theta(\mathbf{c}) \in \theta(\mathscr{C})$, then there exists i such that $\theta(\mathbf{c}) \in \theta(A'_i)$, from the construction of the circulant matrix, then $\theta(\mathscr{C})$ is cyclic. The linearity of $\theta(\mathscr{C})$ is obtained by the linearity of $\mathscr{C}$. In more details, for $\theta(\mathbf{c}), \theta(\mathbf{c}') \in \theta(\mathscr{C})$, there exist $\mathbf{c}, \mathbf{c}' \in \mathscr{C}$, in such a way that, for $k_1, k_2 \in \mathbb{F}_p$, $k_1\mathbf{c} + k_2\mathbf{c}' \in \mathscr{C}$ we have $\theta(k_1\mathbf{c} + k_2\mathbf{c}') = k_1\theta(\mathbf{c}) + k_2\theta(\mathbf{c}') \in \theta(\mathscr{C})$. Therefore, $\theta(\mathscr{C})$ is a linear cyclic code and $\mathscr{C}$ is equivalent to a cyclic code $\theta(\mathscr{C})$.

Theorem 1 in fact gives an alternative proof of Proposition 9 in [3] by a different method.

Lemma 5 (See Proposition 9 in [3]) *Let q be a prime power, and let $\mathbb{F}_q$ denote a finite field. Let ℓ and m be coprime positive integers with m coprime to q, and let $\mathscr{C}$ be a quasi-cyclic code of length ℓm and index ℓ with cyclic constituent codes over $\mathbb{F}_q$, let t denote the multiplicative inverse of m module ℓ, then $\mathscr{C}$ is equivalent to a cyclic code C, the equivalence is given by $\mathbf{d} = (d_0, d_1, \ldots, d_{\ell m-1}) \in C$, its pre-image $\mathbf{c}$ in $\mathscr{C}$ is given by*

$$(d_{(0)tm+0}, d_{tm+0}, d_{2tm+0}, \ldots, d_{(\ell-1)tm+0}, d_{(\ell-1)tm+1}, d_{(0)tm+1}, d_{tm+1}, \ldots, d_{(\ell-2)tm+1},$$

$$\ldots, d_{(\ell-m+1)tm+(m-1)}, d_{(\ell-m+2)tm+(m-1)}, d_{(\ell-m+3)tm+(m-1)}, \ldots, d_{(\ell-m)tm+(m-1)}).$$

Theorem 2 *The results of Theorem 1 are equivalent to those of Lemma 5.*

Proof According to Corollary 2, the codeword

$$(a_{00}, \ldots, a_{0,\ell-1}, a_{10}, \ldots, a_{1,\ell-1}, \ldots, a_{m-1,0}, \ldots, a_{m-1,\ell-1}) \in \mathscr{C}$$

is equivalent to the codeword $(a_{00}, a_{11}, \ldots, a_{i_m,i_\ell}, \ldots, a_{m-1,\ell-1}) \in \theta(\mathscr{C})$. Let

$$(a_{00}, a_{11}, \ldots, a_{i_m,i_\ell}, \ldots, a_{m-1,\ell-1}) = (y_0, y_1, y_2, \ldots, y_i, \ldots, y_{\ell m-1}),$$

in such a way that $a_{i_m,i_\ell} = y_i$, where $0 \le i \le \ell m - 1$. For any $a_{i,j}$, write

$$k_m = i, k_\ell = j \Leftrightarrow k \equiv i \pmod{m}, k \equiv j \pmod{\ell}. \tag{4}$$

Note that $mt = 1 \pmod{\ell}$, and $0 \le k \le \ell m - 1$, it is easy to check that $k = (j - i)_\ell mt + i$ is a solution of the congruence Eq. (4). Therefore

$$(a_{00}, a_{01}, a_{02}, \ldots, a_{0,\ell-1}, a_{10}, \ldots, a_{1,\ell-1}, \ldots, a_{m-1,0}, \ldots, a_{m-1,\ell-1})$$

$$= (y_{(0)tm+0}, y_{tm+0}, y_{2tm+0}, \ldots, y_{(\ell-1)tm+0}, y_{(\ell-1)tm+1}, y_{(0)tm+1}, y_{tm+1}, \ldots, y_{(\ell-2)tm+1},$$

$$\ldots, y_{(\ell-m+1)tm+(m-1)}, y_{(\ell-m+2)tm+(m-1)}, y_{(\ell-m+3)tm+(m-1)}, \ldots, y_{(\ell-m)tm+(m-1)}),$$

which is the same as Lemma 5.

4 The Generator Polynomial of $\theta(\mathscr{C})$

In this section, we make an attempt to describe the generator polynomials of $\mathscr{C}$ and $\theta(\mathscr{C})$ over $\mathbb{F}_q$ without using the results of [4].

Definition 3 For $\mathbf{c} = (a_{00}, a_{01}, a_{02}, \ldots, a_{0,\ell-1}, a_{10}, a_{11}, a_{12} \ldots, a_{1,\ell-1}, \ldots, a_{m-1,0}, \ldots, a_{m-1,\ell-1}) \in \mathscr{C}$, we define a mapping ϕ which maps from the codeword $\mathbf{c} \in \mathscr{C}$ to bivariate polynomial ring $\mathbb{F}_q[x, y]/\langle x^m - 1, y^\ell - 1\rangle$.

$$\phi : \mathbf{c} \mapsto \phi(\mathbf{c}) = a_{00} + a_{01}y + a_{02}y^2 + \cdots + a_{ij}x^i y^j + \cdots + a_{m-1,\ell-1}x^{m-1}y^{\ell-1},$$

where $0 \le i \le m-1, 0 \le j \le \ell-1$.

Theorem 3 *J is a principal ideal of $\mathbb{F}_q[x, y]/\langle x^m - 1, y^\ell - 1\rangle$ if and only if $\mathscr{C}$ is a quasi-cyclic code of length ℓm and index ℓ with cyclic constituent codes, where $J = \phi(\mathscr{C})$.*

Proof For $\mathbf{c} = (a_{00}, a_{01}, a_{02}, \ldots, a_{0,\ell-1}, a_{10}, \ldots, a_{1,\ell-1}, \ldots, a_{m-1,0}, \ldots, a_{m-1,\ell-1}) \in \mathscr{C}$, namely, $\phi(\mathbf{c}) = a_{00} + a_{01}y + a_{02}y^2 + \cdots + a_{ij}x^i y^j + \cdots + a_{m-1,\ell-1}x^{m-1} y^{\ell-1} \in J$, then we have $x\phi(\mathbf{c}) = a_{00}x + a_{01}xy + a_{02}xy^2 + \cdots + a_{ij}x^{i+1}y^j + \cdots + a_{m-1,\ell-1}y^{\ell-1} \in J$. Therefore

$$(a_{m-1,0}, a_{m-1,1}, a_{m-1,2}, \ldots, a_{m-1,\ell-1}, a_{00}, \ldots, a_{0,\ell-1}, \ldots, a_{m-2,0}, \ldots, a_{m-2,\ell-1}) \in \mathscr{C} \quad (5)$$

and $y\phi(\mathbf{c}) = a_{00}y + a_{01}y^2 + a_{02}y^3 + \cdots + a_{ij}x^i y^{j+1} + \cdots + a_{m-1,\ell-1}x^{m-1} \in J$, then

$$(a_{0,\ell-1}, a_{00}, a_{01}, \ldots, a_{0,\ell-2}, a_{1,\ell-1}, \ldots, a_{1,\ell-2}, \ldots, a_{m-1,\ell-1}, \ldots, a_{m-1,\ell-2}) \in \mathscr{C} \quad (6)$$

Moreover, J is a principal ideal, then $x^i y^j \phi(\mathbf{c}) \in J$, and

$$\phi^{-1}(x^i y^j \phi(\mathbf{c})) \in \mathscr{C}. \quad (7)$$

Since J is a principal ideal, then $\mathscr{C}$ is linear. Moreover, $\mathscr{C}$ satisfies Eqs. (5)-(7), so that $\mathscr{C}$ is a quasi-cyclic code with cyclic constituent codes.

Next, we consider the converse part. From Theorem 1, $\theta(\mathscr{C})$ is a cyclic code, then $\theta(\mathscr{C})$ is a principal ideal of $\mathbb{F}_q[z]/\langle z^{\ell m}-1\rangle$, let the generator polynomial of $\theta(\mathscr{C})$ be

$$g(z)=\sum_{i=0}^{\ell m-1} a_{i_m,i_\ell} z^i,$$

then $\theta(\mathbf{c})=(a_{00},a_{11},\ldots,a_{i_m,i_\ell},\ldots,a_{m-1,\ell-1})\in\theta(\mathscr{C})$, according to Corollary 2, we have

$$\mathbf{c}=(a_{00},a_{01},a_{02},\ldots,a_{0,\ell-1},a_{10},\ldots,a_{1,\ell-1},\ldots,a_{m-1,0},\ldots,a_{m-1,\ell-1})\in\mathscr{C}.$$

Now we claim that $\phi(\mathscr{C})=\langle\phi(\mathbf{c})\rangle$. Clearly, $\phi(\mathbf{c})\in\phi(\mathscr{C})$, thus

$$\langle\phi(\mathbf{c})\rangle\subseteq\phi(\mathscr{C}). \tag{8}$$

It is easy to check that $xy\phi(\mathbf{c})=$

$$\phi(a_{m-1,\ell-1},a_{m-1,0},\ldots,a_{m-1,\ell-2},a_{0,\ell-1},\ldots,a_{0,\ell-2},\ldots,a_{m-2,\ell-1},\ldots,a_{m-2,\ell-2}).$$

And $(a_{m-1,\ell-1},a_{m-1,0},\ldots,a_{m-1,\ell-2},a_{0,\ell-1},\ldots,a_{0,\ell-2},\ldots,a_{m-2,\ell-1},\ldots,a_{m-2,\ell-2})$ is exactly the second row of the similar circulant matrix A' containing $\mathbf{c}$. From Lemma 4, $xy\phi(\mathbf{c})$ is equivalent to $zg(z)$, since $zg(z)$ is the second row of $\theta(A')$, similarly, $z^2g(z)$ is equivalent to $x^2y^2\phi(\mathbf{c})$, and so on.

Since the coordinate transformation θ is a linear mapping, then we can define a mapping Ψ which maps from the polynomial (codeword) of $\theta(\mathscr{C})$ to the equivalent polynomial (codeword) of $\langle\phi(\mathbf{c})\rangle$. Namely,

$$\Psi: f(z)g(z)\in\theta(\mathscr{C})\mapsto f(xy)\phi(\mathbf{c})\in\langle\phi(\mathbf{c})\rangle\subseteq\phi(\mathscr{C}).$$

Next we prove the mapping Ψ is bijective. For $\theta(\mathbf{c}')\in\theta(\mathscr{C})$, since $\theta(\mathscr{C})$ is a principal ideal, we can write $\theta(\mathbf{c}')=f_1(z)g(z)$, from the equivalence between $\mathscr{C}$ and $\theta(\mathscr{C})$, we can obtain $\phi(\mathbf{c}')=f_1(xy)\phi(\mathbf{c})\in\phi(\mathscr{C})$. It is clear that Ψ is injective. Now it is sufficient to prove that $x^iy^j\phi(\mathbf{c})$ has its pre-image in $\theta(\mathscr{C})$, rewrite

$$x^iy^j=x^{k_1m+i}y^{k_2\ell+j},$$

and it is clear that the equation $k_1m+i=k_2\ell+j$ has integer solution (k_1,k_2), one can choose the pair (k_1,k_2) such that k_1m+i is the smallest. Set $k_1m+i=k_2\ell+j=e$, then $x^iy^j\phi(\mathbf{c})$ has pre-image $z^eg(z)\in\theta(\mathscr{C})$ for some positive integer e. Thus the mapping Ψ is bijective. Consequently,

$$|\theta(\mathscr{C})|=|\phi(\mathscr{C})|=|\langle\phi(\mathbf{c})\rangle|. \tag{9}$$

Combining (8) and (9), we obtain $\langle\phi(\mathbf{c})\rangle=\phi(\mathscr{C})$.

From the proof of Theorem 3, we have the following corollaries.

Corollary 3 *Let $\mathscr{C}$ be a quasi-cyclic code of length ℓm and index ℓ with cyclic constituent codes, then $\phi(\mathscr{C})$ is a principal ideal of $\mathbb{F}_q[x, y]/\langle x^m - 1, y^\ell - 1\rangle$. Similar to the case of cyclic codes, $\phi(\mathbf{c}) = a_{00} + a_{01}y + a_{02}y^2 + \cdots + a_{ij}x^i y^j + \cdots + a_{m-1,\ell-1}x^{m-1}y^{\ell-1}$ is a generator polynomial of $\mathscr{C}$. Namely, $\mathscr{C}$ can be constructed by a principal ideal of $\mathbb{F}_q[x, y]/\langle x^m - 1, y^\ell - 1\rangle$.*

Corollary 4 *Let $\mathscr{C}$ be a quasi-cyclic code of length ℓm and index ℓ with cyclic constituent codes, and $\mathscr{C}$ has a generator polynomial $\phi(\mathbf{c}) = a_{00} + a_{01}y + a_{02}y^2 + \cdots + a_{ij}x^i y^j + \cdots + a_{m-1,\ell-1}x^{m-1}y^{\ell-1}$, then $\theta(\mathscr{C})$ is a cyclic code with the generator polynomial $g(z) = \sum_{i=0}^{\ell m-1} a_{i_m,i_\ell} z^i$.*

5 General Equivalences

In this section, we will give more general equivalences which include θ in Lemma 4 and the equivalence of Proposition 9 in [3] as a special case.

Theorem 4 *Let $\mathscr{C}$ be a quasi-cyclic code of length ℓm and index ℓ with cyclic constituent codes, then there exists another permutation θ' such that $\theta'(\mathscr{C})$ is a cyclic code and similar to the proof of Theorem 3, we can obtain another generator polynomial of $\phi(\mathscr{C})$.*

Proof If $\mathscr{C}$ is a quasi-cyclic code of length ℓm and index ℓ with cyclic constituent codes and $gcd(k_3, \ell) = gcd(k_4, m) = 1$, where k_3 and k_4 are positive integers, then for

$$(a_{00}, a_{01}, a_{02}, \ldots, a_{0,\ell-1}, a_{10}, \ldots, a_{1,\ell-1}, \ldots, a_{m-1,0}, \ldots, a_{m-1,\ell-1}) \in \mathscr{C},$$

we have

$$(a_{m-k_4,\ell-k_3}, a_{m-k_4,\ell-k_3+1}, \ldots, a_{m-k_4,\ell-1}, a_{m-k_4,0}, \ldots, a_{m-k_4,\ell-k_3-1},$$

$$a_{m-k_4+1,\ell-k_3}, \ldots, a_{m-k_4+1,\ell-k_3-1}, \ldots, a_{m-k_4-1,\ell-k_3}, \ldots, a_{m-k_4-1,\ell-k_3-1}) \in \mathscr{C}.$$

Similar to Definition 1, we can define a similar circulant matrix E' containing the codeword $(a_{00}, a_{01}, a_{02}, \ldots, a_{0,\ell-1}, a_{10}, \ldots, a_{1,\ell-1}, \ldots, a_{m-1,0}, \ldots, a_{m-1.\ell-1})$

$$E' = \begin{pmatrix} a_{00} & \cdots & a_{0,\ell-1} & \cdots & a_{m-1,0} & \cdots & a_{m-1,\ell-1} \\ a_{m-k_4,\ell-k_3} & \cdots & a_{m-k_4,\ell-k_3-1} & \cdots & a_{m-k_4-1,\ell-k_3}, & \cdots & a_{m-k_4-1,\ell-k_3-1} \\ a_{m-2k_4,\ell-2k_3} & \cdots & a_{m-2k_4,\ell-2k_3-1} & \cdots & a_{m-2k_4-1,\ell-2k_3} & \cdots & a_{m-2k_4-1,\ell-2k_3-1} \\ \cdots & & \cdots & & \cdots & & \cdots \\ a_{k_4,k_3} & \cdots & a_{k_4,k_3-1} & \cdots & a_{k_4-1,k_3} & \cdots & a_{k_4-1,k_3-1} \end{pmatrix}.$$

Parallel to the proof of Lemma 4 and Corollary 2, there exists another permutation θ' such that $\theta'(E')$ is a circulant matrix.

Take $m = 5, \ell = 3, p = 2, k_3 = 2$ and $k_4 = 1$ for example. Let E' be a similar circulant matrix containing the codeword $(a_{00}, a_{01}, a_{02}, a_{10}, a_{11}, a_{12}, a_{20}, a_{21}, a_{22}, a_{30}, a_{31}, a_{32}, a_{40}, a_{41}, a_{42})$, namely,

$$E' = \begin{pmatrix}
a_{00} & a_{01} & a_{02} & a_{10} & a_{11} & a_{12} & a_{20} & a_{21} & a_{22} & a_{30} & a_{31} & a_{32} & a_{40} & a_{41} & a_{42} \\
a_{41} & a_{42} & a_{40} & a_{01} & a_{02} & a_{00} & a_{11} & a_{12} & a_{10} & a_{21} & a_{22} & a_{20} & a_{31} & a_{32} & a_{30} \\
a_{32} & a_{30} & a_{31} & a_{42} & a_{40} & a_{41} & a_{02} & a_{00} & a_{01} & a_{12} & a_{10} & a_{11} & a_{22} & a_{20} & a_{21} \\
a_{20} & a_{21} & a_{22} & a_{30} & a_{31} & a_{32} & a_{40} & a_{41} & a_{42} & a_{00} & a_{01} & a_{02} & a_{10} & a_{11} & a_{12} \\
a_{11} & a_{12} & a_{10} & a_{21} & a_{22} & a_{20} & a_{31} & a_{32} & a_{30} & a_{41} & a_{42} & a_{40} & a_{01} & a_{02} & a_{00} \\
a_{02} & a_{00} & a_{01} & a_{12} & a_{10} & a_{11} & a_{22} & a_{20} & a_{21} & a_{32} & a_{30} & a_{31} & a_{42} & a_{40} & a_{41} \\
a_{40} & a_{41} & a_{42} & a_{00} & a_{01} & a_{02} & a_{10} & a_{11} & a_{12} & a_{20} & a_{21} & a_{22} & a_{30} & a_{31} & a_{32} \\
a_{31} & a_{32} & a_{30} & a_{41} & a_{42} & a_{40} & a_{01} & a_{02} & a_{00} & a_{11} & a_{12} & a_{10} & a_{21} & a_{22} & a_{20} \\
a_{22} & a_{20} & a_{21} & a_{32} & a_{30} & a_{31} & a_{42} & a_{40} & a_{41} & a_{02} & a_{00} & a_{01} & a_{12} & a_{10} & a_{11} \\
a_{10} & a_{11} & a_{12} & a_{20} & a_{21} & a_{22} & a_{30} & a_{31} & a_{32} & a_{40} & a_{41} & a_{42} & a_{00} & a_{01} & a_{02} \\
a_{01} & a_{02} & a_{00} & a_{11} & a_{12} & a_{10} & a_{21} & a_{22} & a_{20} & a_{31} & a_{32} & a_{30} & a_{41} & a_{42} & a_{40} \\
a_{42} & a_{40} & a_{41} & a_{02} & a_{00} & a_{01} & a_{12} & a_{10} & a_{11} & a_{22} & a_{20} & a_{21} & a_{32} & a_{30} & a_{31} \\
a_{30} & a_{31} & a_{32} & a_{40} & a_{41} & a_{42} & a_{00} & a_{01} & a_{02} & a_{10} & a_{11} & a_{12} & a_{20} & a_{21} & a_{22} \\
a_{21} & a_{22} & a_{20} & a_{31} & a_{32} & a_{30} & a_{41} & a_{42} & a_{40} & a_{01} & a_{02} & a_{00} & a_{11} & a_{12} & a_{10} \\
a_{12} & a_{10} & a_{11} & a_{22} & a_{20} & a_{21} & a_{32} & a_{30} & a_{31} & a_{42} & a_{40} & a_{41} & a_{02} & a_{00} & a_{01}
\end{pmatrix}.$$

Set

$$h(y) = a_{01} + a_{10}y + a_{22}y^2 + a_{31}y^3 + a_{40}y^4 + a_{02}y^5 + a_{11}y^6 + a_{20}y^7 + a_{32}y^8 + a_{41}y^9$$
$$+ a_{00}y^{10} + a_{12}y^{11} + a_{21}y^{12} + a_{30}y^{13} + a_{42}y^{14}.$$

Let ε be a primitive 15-th root of unity, and $\xi \in \{1, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{14}\}$.

$$Q'_{3\times 5}(\xi) = (\xi^{10}, 1, \xi^5, \xi, \xi^6, \xi^{11}, \xi^7, \xi^{12}, \xi^2, \xi^{13}, \xi^3, \xi^8, \xi^4, \xi^9, \xi^{14})^T,$$

$$P_{3\times 5}(\xi) = (1, \xi, \xi^2, \xi^3, \xi^4, \xi^5, \xi^6, \xi^7, \xi^8, \xi^9, \xi^{10}, \xi^{11}, \xi^{12}, \xi^{13}, \xi^{14})^T,$$

and the correspondence between the coefficient of the term ξ^i in $h(\xi)$ and ξ^i is $a_{01} \leftrightarrow 1, a_{10} \leftrightarrow \xi, a_{22} \leftrightarrow \xi^2, a_{31} \leftrightarrow \xi^3, a_{40} \leftrightarrow \xi^4, a_{02} \leftrightarrow \xi^5, a_{11} \leftrightarrow \xi^6, a_{20} \leftrightarrow \xi^7, a_{32} \leftrightarrow \xi^8, a_{41} \leftrightarrow \xi^9, a_{00} \leftrightarrow \xi^{10}, a_{12} \leftrightarrow \xi^{11}, a_{21} \leftrightarrow \xi^{12}, a_{30} \leftrightarrow \xi^{13}, a_{42} \leftrightarrow \xi^{14}$.

It is easy to check that $E'Q'_{3\times 5}(\xi) = h(\xi)P_{3\times 5}(\xi)$, according to Lemma 4, there exists a permutation θ' in S_{15} such that

$$\theta'(E') = (P_{3\times 5}(1), \ldots, P_{3\times 5}(\xi^{14}))diag(h(1), \ldots, h(\xi^{14})(P_{3\times 5}(1), \ldots, P_{3\times 5}(\xi^{14}))^{-1}.$$

Consequently, E' is equivalent to the circulant matrix E containing the codeword

$$(a_{01}, a_{10}, a_{22}, a_{31}, a_{40}, a_{02}, a_{11}, a_{20}, a_{32}, a_{41}, a_{00}, a_{12}, a_{21}, a_{30}, a_{42}),$$

namely,

$$E = \begin{pmatrix}
a_{01} & a_{10} & a_{22} & a_{31} & a_{40} & a_{02} & a_{11} & a_{20} & a_{32} & a_{41} & a_{00} & a_{12} & a_{21} & a_{30} & a_{42} \\
a_{42} & a_{01} & a_{10} & a_{22} & a_{31} & a_{40} & a_{02} & a_{11} & a_{20} & a_{32} & a_{41} & a_{00} & a_{12} & a_{21} & a_{30} \\
a_{30} & a_{42} & a_{01} & a_{10} & a_{22} & a_{31} & a_{40} & a_{02} & a_{11} & a_{20} & a_{32} & a_{41} & a_{00} & a_{12} & a_{21} \\
a_{21} & a_{30} & a_{42} & a_{01} & a_{10} & a_{22} & a_{31} & a_{40} & a_{02} & a_{11} & a_{20} & a_{32} & a_{41} & a_{00} & a_{12} \\
a_{12} & a_{21} & a_{30} & a_{42} & a_{01} & a_{10} & a_{22} & a_{31} & a_{40} & a_{02} & a_{11} & a_{20} & a_{32} & a_{41} & a_{00} \\
a_{00} & a_{12} & a_{21} & a_{30} & a_{42} & a_{01} & a_{10} & a_{22} & a_{31} & a_{40} & a_{02} & a_{11} & a_{20} & a_{32} & a_{41} \\
a_{41} & a_{00} & a_{12} & a_{21} & a_{30} & a_{42} & a_{01} & a_{10} & a_{22} & a_{31} & a_{40} & a_{02} & a_{11} & a_{20} & a_{32} \\
a_{32} & a_{41} & a_{00} & a_{12} & a_{21} & a_{30} & a_{42} & a_{01} & a_{10} & a_{22} & a_{31} & a_{40} & a_{02} & a_{11} & a_{20} \\
a_{20} & a_{32} & a_{41} & a_{00} & a_{12} & a_{21} & a_{30} & a_{42} & a_{01} & a_{10} & a_{22} & a_{31} & a_{40} & a_{02} & a_{11} \\
a_{11} & a_{20} & a_{32} & a_{41} & a_{00} & a_{12} & a_{21} & a_{30} & a_{42} & a_{01} & a_{10} & a_{22} & a_{31} & a_{40} & a_{02} \\
a_{02} & a_{11} & a_{20} & a_{32} & a_{41} & a_{00} & a_{12} & a_{21} & a_{30} & a_{42} & a_{01} & a_{10} & a_{22} & a_{31} & a_{40} \\
a_{40} & a_{02} & a_{11} & a_{20} & a_{32} & a_{41} & a_{00} & a_{12} & a_{21} & a_{30} & a_{42} & a_{01} & a_{10} & a_{22} & a_{31} \\
a_{31} & a_{40} & a_{02} & a_{11} & a_{20} & a_{32} & a_{41} & a_{00} & a_{12} & a_{21} & a_{30} & a_{42} & a_{01} & a_{10} & a_{22} \\
a_{22} & a_{31} & a_{40} & a_{02} & a_{11} & a_{20} & a_{32} & a_{41} & a_{00} & a_{12} & a_{21} & a_{30} & a_{42} & a_{01} & a_{10} \\
a_{10} & a_{22} & a_{31} & a_{40} & a_{02} & a_{11} & a_{20} & a_{32} & a_{41} & a_{00} & a_{12} & a_{21} & a_{30} & a_{42} & a_{01}
\end{pmatrix}.$$

And the equivalence is given by $\theta' = (1\ 11\ 4\ 2)(3\ 6\ 12\ 9)(5\ 7\ 8\ 13)(10\ 14)(15)$ in S_{15}. However, $\theta = (2\ 11\ 14\ 5)(3\ 6\ 12\ 9)(4\ 7\ 13\ 10)$ in S_{15} by Lemma 4 and Corollary 2.

Similar to the proof of Theorem 1, $\theta'(\mathscr{C})$ is a cyclic code. Now we try to give another generator polynomial of $\phi(\mathscr{C})$. According to Definition 3,

$$\phi : \mathbf{c} \mapsto \phi(\mathbf{c}) = a_{00} + a_{01}y + a_{02}y^2 + \cdots + a_{ij}x^i y^j + \cdots + a_{m-1,\ell-1}x^{m-1}y^{\ell-1}.$$

And the linear mapping $\Psi_{(k_3,k_4)}$ (similar to Ψ in Theorem 3) is defined as follows,

$$\Psi_{(k_3,k_4)} : f(z)g(z) \in \theta(\mathscr{C}) \mapsto f(x^{k_4}y^{k_3})\phi(\mathbf{c}) \in \langle \phi(\mathbf{c}) \rangle \subseteq \phi(\mathscr{C}).$$

According to the proof of Theorem 3, $\Psi_{(k_3,k_4)}$ is one-to-one since $gcd(k_3, \ell) = gcd(k_4, m) = 1$. Then parallel to the proof of Theorem 3, the generator polynomial of $\phi(\mathscr{C})$ can be obtained.

Remark 3 According to the proof of Theorem 4, θ' relies on k_3 and k_4, and the similar circulant matrix A' in Sect. 3 is the case when $k_3 = k_4 = 1$.

6 Application Examples

In this section, we are ready to give some examples to illustrate the discussed results.

Example 1 If $\mathscr{C}$ is a quasi-cyclic code over $\mathbb{F}_q$ of length 6 and index 2 with cyclic constituent codes, where $(q, 6) = 1$, and let

$$B' = \begin{pmatrix} a_{00} & a_{01} & a_{10} & a_{11} & a_{20} & a_{21} \\ a_{21} & a_{20} & a_{01} & a_{00} & a_{11} & a_{10} \\ a_{10} & a_{11} & a_{20} & a_{21} & a_{00} & a_{01} \\ a_{01} & a_{00} & a_{11} & a_{10} & a_{21} & a_{20} \\ a_{20} & a_{21} & a_{00} & a_{01} & a_{10} & a_{11} \\ a_{11} & a_{10} & a_{21} & a_{20} & a_{01} & a_{00} \end{pmatrix}$$

be a similar circulant matrix of $\mathscr{C}$, where $\ell = 2, m = 3$, ε is a primitive 6-th root of unity, and $g(y) = a_{00} + a_{11}y + a_{20}y^2 + a_{01}y^3 + a_{10}y^4 + a_{21}y^5$. According to the proof of Lemma 4, the correspondence is $a_{00} \leftrightarrow 1, a_{11} \leftrightarrow \varepsilon, a_{20} \leftrightarrow \varepsilon^2, a_{01} \leftrightarrow \varepsilon^3, a_{10} \leftrightarrow \varepsilon^4, a_{21} \leftrightarrow \varepsilon^5$. Write

$$B' P'_{2\times 3}(\varepsilon) = (b_0, b_1, b_2, b_3, b_4, b_5)^T.$$

Set $b_0 = g(\varepsilon)$, then we have $P'_{2\times 3}(\varepsilon) = (1, \varepsilon^3, \varepsilon^4, \varepsilon, \varepsilon^2, \varepsilon^5)^T$. Then

$$B'(1, \varepsilon^3, \varepsilon^4, \varepsilon, \varepsilon^2, \varepsilon^5)^T = g(\varepsilon)(1, \varepsilon, \varepsilon^2, \varepsilon^3, \varepsilon^4, \varepsilon^5)^T.$$

Therefore

$$B' = \begin{pmatrix} a_{00} & a_{01} & a_{10} & a_{11} & a_{20} & a_{21} \\ a_{21} & a_{20} & a_{01} & a_{00} & a_{11} & a_{10} \\ a_{10} & a_{11} & a_{20} & a_{21} & a_{00} & a_{01} \\ a_{01} & a_{00} & a_{11} & a_{10} & a_{21} & a_{20} \\ a_{20} & a_{21} & a_{00} & a_{01} & a_{10} & a_{11} \\ a_{11} & a_{10} & a_{21} & a_{20} & a_{01} & a_{00} \end{pmatrix} \Leftrightarrow \theta(B') = \begin{pmatrix} a_{00} & a_{11} & a_{20} & a_{01} & a_{10} & a_{21} \\ a_{21} & a_{00} & a_{11} & a_{20} & a_{01} & a_{10} \\ a_{10} & a_{21} & a_{00} & a_{11} & a_{20} & a_{01} \\ a_{01} & a_{10} & a_{21} & a_{00} & a_{11} & a_{20} \\ a_{20} & a_{01} & a_{10} & a_{21} & a_{00} & a_{11} \\ a_{11} & a_{20} & a_{01} & a_{10} & a_{21} & a_{00} \end{pmatrix}.$$

And the equivalence is given by $\theta = (24)(35)$ in S_6.

Example 2 Let $\mathscr{C}$ be a quasi-cyclic code over $\mathbb{F}_5$ of length 6 and index 2 with cyclic constituent codes and the generator polynomial of $\phi(\mathscr{C})$ is $1 + xy + x^2(100110) \in \mathbb{F}_5[x, y]/\langle x^3 - 1, y^2 - 1\rangle$, where the codeword $\mathbf{c} = (100110)$ is the corresponding polynomial $1 + xy + x^2$ by Definition 3. Equivalently, $\phi(\mathscr{C}) = \langle \phi(\mathbf{c})\rangle$, then from Corollary 4, $\theta(\mathscr{C}) = \langle 1 + z + z^2\rangle(111000) \in \mathbb{F}_5[z]/\langle z^6 - 1\rangle$. And the linear mapping is

$$\Psi : \langle \phi(1 + z + z^2)\rangle \mapsto \langle 1 + xy + x^2\rangle,$$

according to the mapping Ψ, we have

$$1 \mapsto 1, z \mapsto xy = xy, z^2 \mapsto x^2y^2 = x^2, z^3 \mapsto x^3y^3 = y, z^4 \mapsto x^4y^4 = x, z^5 \mapsto x^5y^5 = x^2y$$

In more details:

$$\begin{aligned}
\phi(\mathbf{c}) &= 1 + xy + x^2 \ (100110) \Leftrightarrow g(z) = 1 + z + z^2 \ (111000)\\
xy\phi(\mathbf{c}) &= y + xy + x^2 \ (010110) \Leftrightarrow zg(z) = z^3 + z + z^2 \ (011100)\\
x^2\phi(\mathbf{c}) &= x + y + x^2 \ (011010) \Leftrightarrow z^2g(z) = z^3 + z^4 + z^2 \ (001110)\\
y\phi(\mathbf{c}) &= y + x + x^2y \ (011001) \Leftrightarrow z^3g(z) = z^3 + z^4 + z^5 \ (000111)\\
x\phi(\mathbf{c}) &= x + x^2y + 1 \ (101001) \Leftrightarrow z^4g(z) = 1 + z^4 + z^5 \ (100011)\\
x^2y\phi(\mathbf{c}) &= 1 + xy + x^2y \ (100101) \Leftrightarrow z^5g(z) = 1 + z + z^5 \ (110001)
\end{aligned}$$

and $f(z)g(z) \mapsto f(xy)\phi(\mathbf{c})$ is given by the linearity of $\mathscr{C}$ and $\theta(\mathscr{C})$. And the equivalence is given by $\theta = (24)(35)$ in S_6.

Example 3 Let $\mathscr{C}$ be a quasi-cyclic code over $\mathbb{F}_5$ of length 12 and index 4 with cyclic constituent codes, and

$$\phi(\mathscr{C}) = \langle 1 + y^3 + xy + x^2y^2\rangle(100101000010) \in \mathbb{F}_5[x, y]/\langle x^3 - 1, y^4 - 1\rangle,$$

then $\theta(\mathscr{C}) = \langle 1 + z + z^2 + z^3\rangle(111100000000) \in \mathbb{F}_5[z]/\langle z^{12} - 1\rangle$, the linear mapping is $\Psi : \langle\phi(1 + z + z^2 + z^3)\rangle \mapsto \langle 1 + y^3 + xy + x^2y^2\rangle$, and

$$1 \mapsto 1, z \mapsto xy, z^2 \mapsto x^2y^2, z^3 \mapsto x^3y^3 = y^3, z^4 \mapsto x^4y^4 = x, z^5 \mapsto x^5y^5 = x^2y, z^6 \mapsto x^6y^6 = y^2,$$

$$z^7 \mapsto x^7y^7 = xy^3, z^8 \mapsto x^8y^8 = x^2, z^9 \mapsto x^9y^9 = y, z^{10} \mapsto x^{10}y^{10} = xy^2, z^{11} \mapsto x^{11}y^{11} = x^2y^3.$$

And the equivalence is given by $\theta = (2\ 10\ 6)(3\ 7\ 11)$ in S_{12}.

Acknowledgements This research is supported by National Natural Science Foundation of China (61202068, 61672036 and 11526045), the Open Research Fund of National Mobile Communications Research Laboratory, Southeast University (2015D11), Technology Foundation for Selected Overseas Chinese Scholar, Ministry of Personnel of China (05015133) and Key Projects of Support Program for outstanding young talents in Colleges and Universities (gxyqZD2016008).

References

1. Bracco, A.D., Natividad, A.M., Solé, P.: On quintic quasi-cyclic codes. Discrete Appl. Math. **156**, 3362–3375 (2008)
2. Güneri, C., Özbudak, F.: A relation between quasi-cyclic codes and 2-D cyclic codes. Finite Fields Their Appl. **18**, 123–132 (2012)
3. Lim, C.J.: Quasi-cyclic codes with cyclic constituent codes. Finite Fields Their Appl. **13**, 516–534 (2007)
4. Ling, S., Solé, P.: On the algebraic structure of quasi-cyclic codes I: Finite fields. IEEE Trans. Inform. Theory **47**, 2751–2760 (2001)