LETTER

A Modulus Factorization Algorithm for Self-Orthogonal and Self-Dual Quasi-Cyclic Codes via Polynomial Matrices*

Hajime MATSUI[†a)], ***Member***

SUMMARY A construction method of self-orthogonal and self-dual quasi-cyclic codes is shown which relies on factorization of modulus polynomials for cyclicity in this study. The smaller-size generator polynomial matrices are used instead of the generator matrices as linear codes. An algorithm based on Chinese remainder theorem finds the generator polynomial matrix on the original modulus from the ones constructed on each factor. This method enables us to efficiently construct and search these codes when factoring modulus polynomials into reciprocal polynomials.

key words: *error-correcting codes, finite fields, codes over rings, Chinese remainder theorem, reciprocal polynomials*

1. Introduction

The construction of error-correcting codes and self-dual codes with large minimum distances is a fundamental problem in coding theory [1]. Because their minimum distance can be calculated by the method of [2], we focus on constructing many these codes efficiently in this study. It is shown [3] that generator polynomial matrices are effective for the construction of quasi-cyclic codes which are equivalent to R-modules in $(R/(1-x^m)R)^l$, where $R = \mathbb{F}_q[x]$ and $R/(1-x^m)R$ is the quotient ring by an ideal $(1-x^m)R$ in R. In [4], codes over some rings are constructed by the product of generator polynomial matrices although it cannot efficiently construct self-orthogonal or self-dual codes because their product breaks these properties. In [5], self-orthogonal and self-dual integer codes are constructed by using generator matrices and Chinese remainder theorem. However, self-orthogonal and self-dual quasi-cyclic codes have never been constructed by using generator polynomial matrices and Chinese remainder theorem.

In this paper, we consider the construction of self-orthogonal and self-dual quasi-cyclic codes by modulus factorization, which means that $(R/uR)^l = (R/u_1R)^l \oplus (R/u_2R)^l$ with $u = u_1u_2$ and $\gcd(u_1, u_2) = 1$. The composition of two R-modules in $(R/u_1R)^l$ and $(R/u_2R)^l$ into another R-module in $(R/uR)^l$ can be done by an algorithm which employs Chinese remainder theorem. Our theorems assert that the class of R-modules in $(R/uR)^l$ which have the prescribed property corresponds to the class of pairs of certain R-modules in $(R/u_1R)^l$ and $(R/u_2R)^l$ and vice versa.

The rest of this paper is organized as follows. Section 2 prepares notations for R-modules in $(R/uR)^l$ for some $u \in R$, where we refer to [3]–[5] for details. Section 3 describes the efficient construction of R-modules in $(R/uR)^l$, where we focus on the case of reciprocal u, u_1, u_2 for simplicity, and shows Example 1 of the above construction.

2. Preliminaries

Let $R = \mathbb{F}_q[x]$, $l \in \mathbb{Z}$ be positive, and

$$\mathbb{L} = R^l = \{c = (c_1 \ \cdots \ c_l) \mid c_i \in R, 1 \le i \le l\}.$$

For positive $k \in \mathbb{Z}$, let $M_{k,l}(R)$ be the set of all k-by-l matrices with entries in R and $M_l(R) = M_{l,l}(R)$. For $G \in M_l(R)$ with $\det(G) \neq 0$, let $\mathbb{L}G = \{cG \mid c \in \mathbb{L}\}$. Let $u \in R$ be nonzero and $I \in M_l(R)$ be the identity matrix. Then we denote $u\mathbb{L} = \mathbb{L}uI$ and

$$\frac{\mathbb{L}}{u\mathbb{L}} = \mathbb{L}/u\mathbb{L} = \{c = (c_1 \ \cdots \ c_l) \mid c_i \in R/uR, 1 \le i \le l\}.$$

Let $C \subset \mathbb{L}/u\mathbb{L}$. We say that C is an *R-module* if and only if $\forall r, s \in R, \forall a, b \in C \Longrightarrow ra + sb \in C$. For any R-module $C \subset \mathbb{L}/u\mathbb{L}$, there exists $G \in M_l(R)$ such that $\mathbb{L}G \supset u\mathbb{L}$ and $C = \mathbb{L}G/u\mathbb{L}$, where $\mathbb{L}G/u\mathbb{L}$ denotes the quotient R-module of $\mathbb{L}G$ by $u\mathbb{L}$. Conversely, for any $G \in M_l(R)$, if $\mathbb{L}G \supset u\mathbb{L}$, then $\mathbb{L}G/u\mathbb{L}$ can be defined and fixes an R-module in $\mathbb{L}/u\mathbb{L}$.

Let $C \subset \mathbb{L}/u\mathbb{L}$ be an R-module. We say that $G \in M_l(R)$ is a *generator matrix* of C if and only if $\mathbb{L}G \supset u\mathbb{L}$ and $C = \mathbb{L}G/u\mathbb{L}$.

Note that $\mathbb{L}G \supset u\mathbb{L}$ is equivalent to the fact that there exists $A \in M_l(R)$ such that $AG = uI$. Thus, for any $G \in M_l(R)$, there exists an R-module $C \subset \mathbb{L}/u\mathbb{L}$ such that $C = \mathbb{L}G/u\mathbb{L}$ if and only if $\mathbb{L}G \supset u\mathbb{L}$ if and only if $\exists A \in M_l(R)$ such that $AG = uI$. If $AG = uI$, then it follows from $\det(A)\det(G) = u^l$ that $\det(G)$ divides u^l.

For any subset $\mathcal{S} \subset \mathbb{L}/u\mathbb{L}$, let $|\mathcal{S}|$ denote the number of elements in $\mathcal{S}$.

Lemma 1: (cf. [4]) For any $A \in M_l(R)$ with $\det(A) \neq 0$, we have $|\mathbb{L}/\mathbb{L}A| = \psi(\det(A))$, where $\psi(a) = q^{\deg(a)}$ for $a \in R$. In particular, if $G \in M_l(R)$ is a generator matrix of an R-module $C \subset \mathbb{L}/u\mathbb{L}$, then $|C| = \psi\left(u^l/\det(G)\right)$.

We say that G is *upper triangular* if and only if $G = (g_{i,j}) \in M_l(R)$ satisfies $g_{i,j} = 0$ for all $1 \le j < i \le l$, i.e., G

Manuscript received March 18, 2021.
Manuscript revised April 24, 2021.
Manuscript publicized May 21, 2021.

[†]The author is with Toyota Technological Institute, Nagoya-shi, 468-8511 Japan.

*The contents of the letter were partially presented in [6]. This work was supported in part by JSPS KAKENHI Grant Number JP19K22850.

a) E-mail: matsui@toyota-ti.ac.jp

DOI: 10.1587/transfun.2021EAL2021

is of the form

$$G = \begin{pmatrix} g_{1,1} & g_{1,2} & \cdots & g_{1,l} \\ 0 & g_{2,2} & \cdots & g_{2,l} \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & g_{l,l} \end{pmatrix},$$

and $\det(G) \neq 0$. We say that $G = (g_{i,j}) \in M_l(R)$ is *reduced* if and only if G satisfies the following three conditions:

1. G is upper triangular,
2. $\deg(g_{i,j}) < \deg(g_{j,j})$ for all $1 \leq i < j \leq l$,
3. $g_{i,i}$ is monic [4] for all $1 \leq i \leq l$.

Let $GL_l(R)$ be the group of invertible matrices in $M_l(R)$. Note that we have $\mathbb{L}U = \mathbb{L}$ for some $U \in M_l(R)$ if and only if $U \in GL_l(R)$. We fix any $G \in M_l(R)$ with $\det(G) \neq 0$. Then there exist $U \in GL_l(R)$ and reduced $G' \in M_l(R)$ such that $UG = G'$. In other words, there exists reduced $G' \in M_l(R)$ such that $\mathbb{L}G = \mathbb{L}G'$. It is shown [4] that there exists one and only one reduced G' among UG for all $U \in GL_l(R)$.

From now on, unless otherwise noted, $G \in M_l(R)$ indicates the reduced generator matrix of an R-module $C = \mathbb{L}G/u\mathbb{L} \subset \mathbb{L}/u\mathbb{L}$.

Let $T_l(R) = \{G \in M_l(R) \mid G \text{ is reduced}\}$. For a nonzero $u \in R$, let

$$\{G\}_u = \{G \in T_l(R) \mid AG = uI \text{ for some } A \in M_l(R)\},$$

i.e., $\{G\}_u$ is the set of the reduced generator matrices of all R-modules in $\mathbb{L}/u\mathbb{L}$. Thus, we have the following one-to-one and onto correspondences [4]

$$\begin{array}{ccc} \{G\}_u & \to & \{R\text{-module } \mathbb{M} \mid \mathbb{L} \supset \mathbb{M} \supset u\mathbb{L}\} \\ G & \mapsto & \mathbb{L}G \\ & \to & \{R\text{-module } C \mid C \subset \mathbb{L}/u\mathbb{L}\} \\ & \mapsto & \mathbb{L}G/u\mathbb{L}. \end{array}$$

From now on, let $u, u_1, u_2 \in R$ be nonzero with $u = u_1u_2$ and $\gcd(u_1, u_2) = 1$. Our first aim is to relate $\{G\}_u$ with $\{G_1\}_{u_1}$ and $\{G_2\}_{u_2}$. This is done by Theorem 1.

Proposition 1: (cf. [5]) For $s = 1, 2$, let $G_s = \left(g_{i,j}^{(s)}\right) \in M_l(R)$ be reduced such that $\mathbb{L}G_s \supset \mathbb{L}u_s$. Then there exists reduced $G = (g_{i,j}) \in M_l(R)$ such that $\mathbb{L}G = \mathbb{L}G_1 \cap \mathbb{L}G_2$ and $g_{i,i} = g_{i,i}^{(1)} g_{i,i}^{(2)}$ for all $1 \leq i \leq l$.

Remark 1: By Proposition 1, an algorithm which computes G is extracted as Algorithm 1 in [5]. If we estimate the computational complexity of Algorithm 1 as the total number of finite-field operations, it is evaluated approximately as $O\left(l^3 \deg(u)\right)$, which is the same order as that of multiplying generator matrices in [4].

Proposition 2: (cf. [5]) Let $G \in M_l(R)$ be reduced such that $\mathbb{L}G \supset u\mathbb{L}$. Then there exists reduced $G_1 = \left(g_{i,j}^{(1)}\right) \in M_l(R)$ such that $\mathbb{L}G_1 = \mathbb{L}G + u_1\mathbb{L}$ and, for all $1 \leq i \leq l$, $g_{i,i}^{(1)} = \gcd\left(g_{i,i}, u_1\right)$.

Theorem 1: (cf. [5]) Let

$$\alpha : \{G_1\}_{u_1} \times \{G_2\}_{u_2} \to \{G\}_u \quad [(G_1, G_2) \mapsto G]$$

be a map defined by $\mathbb{L}G_1 \cap \mathbb{L}G_2 = \mathbb{L}G$ with Proposition 1. Moreover, let

$$\beta : \{G\}_u \to \{G_1\}_{u_1} \times \{G_2\}_{u_2} \quad [G \mapsto (G_1, G_2)]$$

be a map defined by $\mathbb{L}G + u_1\mathbb{L} = \mathbb{L}G_1$ and $\mathbb{L}G + u_2\mathbb{L} = \mathbb{L}G_2$ with Proposition 2. Then both α and β are bijective maps and inverse each other.

3. Duality

Let $m \in \mathbb{Z}$ be positive. For $a \in R$, we define $a^{\langle m \rangle} \in R$ by

$$a^{\langle m \rangle} = a_0 + \sum_{i=1}^{m-1} a_{m-i} x^i \text{ if } a \equiv \sum_{i=0}^{m-1} a_i x^i \bmod (1 - x^m).$$

If $\deg(a) < m$, we have $a^{\langle m \rangle} \equiv x^m a(x^{-1}) \bmod (1 - x^m)$. Because $0^{\langle m \rangle} = (1 - x^m)^{\langle m \rangle} = 0$, $\left[a \mapsto a^{\langle m \rangle}\right]$ can be seen as a map $R/(1 - x^m)R \to R/(1 - x^m)R$. The following lemma shows that $\left[a \mapsto a^{\langle m \rangle}\right]$ is a ring automorphism.

Lemma 2: For $a, b \in R$, we have $(ab)^{\langle m \rangle} \equiv a^{\langle m \rangle} b^{\langle m \rangle} \bmod (1 - x^m)$.

Proof. Because the map $\left[a \mapsto a^{\langle m \rangle}\right]$ is $\mathbb{F}_q$-linear, we may prove only for x^i, x^j for $0 \leq i, j < m$. Note that $\left(x^i\right)^{\langle m \rangle} \left(x^j\right)^{\langle m \rangle} \equiv x^{m-i} x^{m-j} \equiv x^{2m-i-j}$ and $\left(x^{i+j}\right)^{\langle m \rangle} \equiv x^{m-(i+j \bmod m)} \bmod (1 - x^m)$. The lemma is proved by $x^{2m-i-j} \equiv x^{m-(i+j \bmod m)} \bmod (1 - x^m)$. □

For $a \in R$, we denote $\widetilde{a} = x^{\deg(a)} a(x^{-1})$, i.e., the reciprocal polynomial of a. We say that a is *self-reciprocal* if and only if $\gamma\widetilde{a} = a$ for some $\gamma \in \mathbb{F}_q \setminus \{0\}$.

Lemma 3: If $\deg(a) < m$ for $a \in R$, then $x^{\deg(a)} a^{\langle m \rangle} \equiv \widetilde{a}$ and $a^{\langle m \rangle} \equiv x^{m-\deg(a)} \widetilde{a} \bmod (1 - x^m)$.

Proof. If $a = \sum_{i=0}^{m-1} a_i x^i$, then

$$a^{\langle m \rangle} \equiv \sum_{i=0}^{\deg(a)} a_i x^{m-i} \bmod (1 - x^m),$$

$$x^{\deg(a)} a^{\langle m \rangle} \equiv \sum_{i=0}^{\deg(a)} a_i x^{-i+\deg(a)} = \widetilde{a} \bmod (1 - x^m).$$

Multiplying $x^{m-\deg(a)}$, we have $x^m a^{\langle m \rangle} \equiv x^{m-\deg(a)} \widetilde{a} \bmod (1 - x^m)$. Because $x^m a^{\langle m \rangle} = a^{\langle m \rangle} - (1 - x^m) a^{\langle m \rangle}$, we have $a^{\langle m \rangle} \equiv x^{m-\deg(a)} \widetilde{a} \bmod (1 - x^m)$. □

Lemma 4: Suppose that $u_1 \in R$ divides $1 - x^m$. For $a, b \in R$, if $a \equiv b \bmod u_1$, then $a^{\langle m \rangle} \equiv b^{\langle m \rangle} \bmod \widetilde{u_1}$. Moreover, if u_1 is self-reciprocal, then $a^{\langle m \rangle} \equiv b^{\langle m \rangle} \bmod u_1$.

Proof. If $a = b + c_1 u_1$ for some $c_1 \in R$, then $a^{\langle m \rangle} \equiv b^{\langle m \rangle} + c_1^{\langle m \rangle} u_1^{\langle m \rangle} \bmod (1 - x^m)$. Because $\widetilde{u_1}$ divides $1 - x^m$ and $u_1^{\langle m \rangle} \equiv 0 \bmod \widetilde{u_1}$ by Lemma 3, the lemma is proved. □

Remark 2: If u_1 is not self-reciprocal, then $a^{\langle m \rangle} \equiv b^{\langle m \rangle}$

$\bmod u_1$ is not true in general, e.g., $1+x+x^3 \equiv 0 \bmod (1+x+x^3)$ but $\left(1+x+x^3\right)^{\langle 7\rangle} \equiv 1+x^4+x^6 \equiv x \not\equiv 0 \bmod (1+x+x^3)$.

For $G = \left(g_{i,j}\right) \in M_{k,l}(R)$, we define $G^* \in M_{l,k}(R)$ by $G^* \equiv \left(g_{j,i}^{\langle m\rangle}\right) \bmod (1-x^m)$.

Lemma 5: For $F \in M_{h,k}(R)$ and $G \in M_{k,l}(R)$, we have $(FG)^* \equiv G^*F^* \bmod (1-x^m)$.

Proof. Because $(FG)^*$ is defined by the transpose and $^{\langle m\rangle}$ $\bmod (1-x^m)$, the lemma is proved immediately. □

Let $u \in R$ divide $1-x^m$. Let $C \subset \mathbb{L}/u\mathbb{L}$ be an R-module and let

$$\widehat{C} = \left\{a \in \mathbb{L}/u\mathbb{L} \,|\, a\left(b^*\right) \equiv 0 \bmod u, \forall b \in C\right\}. \tag{1}$$

Then an R-module $\widehat{C}$ is called the *dual* R-module of C.

Lemma 6: If $G \in M_l(R)$ indicates the reduced generator matrix of an R-module $C = \mathbb{L}G/u\mathbb{L}$, then $\widehat{C} = \{a \in \mathbb{L}/u\mathbb{L} \,|\, aG^* \equiv (0 \ \cdots \ 0) \bmod u\}$.

Proof. It is sufficient to show that $\widehat{C} \supset \widehat{C}'$ if we denote $\widehat{C}' = \{a \in \mathbb{L}/u\mathbb{L} \,|\, aG^* \equiv (0 \ \cdots \ 0) \bmod u\}$. Suppose $a \in \widehat{C}'$. For any $b \in C$, there exists $c \in \mathbb{L}$ such that $b \equiv cG \bmod u$. Then $a\left(b^*\right) \equiv a\left((cG)^*\right) \equiv a\left(G^*c^*\right) = \left(aG^*\right)c^* \equiv 0 \bmod u$. □

If $u = 1-x^m$, the following proposition shows the relationship between the operation $a(b^*)$ in $\mathbb{L}/u\mathbb{L}$ and the Euclidean inner product in $\left(\mathbb{F}_q\right)^{ml}$.

Proposition 3: For $a, b \in \mathbb{L}/(1-x^m)\mathbb{L}$, we have $a\left(b^*\right) \equiv 0 \bmod (1-x^m)$ if and only if $\vec{a}\left(\left(\vec{b}^{(v)}\right)^\top\right) = 0$ for all $0 \le v < m$, where $n = ml$, $\vec{a} = [\vec{a}_1 \ \cdots \ \vec{a}_l] \in \left(\mathbb{F}_q\right)^n$ indicates the concatenating vector of $\vec{a}_1, \cdots, \vec{a}_l$ related to $a = (a_1 \ \cdots \ a_l) \in \mathbb{L}/(1-x^m)\mathbb{L}$ by, for all $1 \le i \le l$,

$$a_i = \sum_{j=0}^{m-1} a_{i,j}x^j \mapsto \vec{a}_i = \left(a_{i,0}, a_{i,1}, \cdots, a_{i,m-1}\right) \in \left(\mathbb{F}_q\right)^m,$$

$\vec{b}^{(v)} \in \left(\mathbb{F}_q\right)^n$ indicates the vector related to $x^v b \in \mathbb{L}/(1-x^m)\mathbb{L}$, and $^\top$ indicates transpose. In particular, if $u = 1-x^m$, then $\widehat{C}$ in (1) agrees with the dual code $C^\perp = \left\{\vec{a} \in \left(\mathbb{F}_q\right)^n \,\middle|\, \vec{a}\left(\vec{b}^\top\right) = 0, \forall \vec{b} \in C\right\}$ of C as $\mathbb{F}_q$-linear codes.

Proof. Note that, for $f, g \in \mathbb{F}_q[x]$ with $\deg(f), \deg(g) < m$,

$$\begin{aligned} f \cdot x^m g(x^{-1}) &= \sum_{i=0}^{m-1} f_i x^i \sum_{j=1}^{m} g_{m-j}x^j \\ &= \sum_{v=1}^{m}\left(\sum_{i=0}^{v-1} f_i g_{m-v+i}\right)x^v + \sum_{v=1}^{m-1}\left(\sum_{i=v}^{m-1} f_i g_{i-v}\right)x^{m+v}. \end{aligned}$$

Because $g^{\langle m\rangle} \equiv x^m g(x^{-1}) \bmod (1-x^m)$, we have

$$\begin{aligned} f\left(g^{\langle m\rangle}\right) &\equiv \sum_{v=1}^{m}\left(\sum_{i=0}^{v-1} f_i g_{m-v+i} + \sum_{i=v}^{m-1} f_i g_{i-v}\right)x^v \\ &= \sum_{v=0}^{m-1}\left(\vec{f}\left(\vec{g}^{(m-v)}\right)^\top\right)x^v \quad \bmod (1-x^m), \end{aligned}$$

which leads the lemma because

$$\begin{aligned} a\left(b^*\right) &= \sum_{i=1}^{l} a_i\left(b_i^{\langle m\rangle}\right) \equiv \sum_{i=1}^{l}\sum_{v=0}^{m-1}\left(\vec{a}_i\left(\vec{b}_i^{(m-v)}\right)^\top\right)x^v \\ &= \sum_{v=0}^{m-1}\left(\sum_{i=1}^{l}\vec{a}_i\left(\vec{b}_i^{(m-v)}\right)^\top\right)x^v = 0 \quad \bmod (1-x^m) \end{aligned}$$

deduces that $\sum_{i=1}^{l}\vec{a}_i\left(\vec{b}_i^{(m-v)}\right)^\top = 0$ for all $0 \le v < m$. □

Assumption 1: From now on, we suppose that $u \in R$ divides $1-x^m$ and is self-reciprocal.

If u is irreducible and $\deg(u) \ge 2$, the following proposition shows the relationship between the operation $a(b^*)$ in $\mathbb{L}/u\mathbb{L}$ and the Hermitian inner product in $\left(\mathbb{F}_{q^{\deg(u)}}\right)^l$.

Proposition 4: Assume that $u \in R$ is irreducible and $\deg(u) \ge 2$. If we identify $R/uR = \mathbb{F}_{q^{\deg(u)}}$, then, for $f \in R/uR$, we have $f^{\langle m\rangle} = f^{q^{\deg(u)/2}}$. In particular, if u satisfies the assumptions, then $\widehat{C}$ in (1) agrees with the Hermitian dual code $C^{\perp_{\mathrm{H}}} = \left\{\bar{a} \in \left(\mathbb{F}_{q^{\deg(u)}}\right)^l \,\middle|\, \bar{a}\left(\bar{b}^\dagger\right) = 0, \forall \bar{b} \in C\right\}$ of C as $\mathbb{F}_{q^{\deg(u)}}$-linear codes, where $\bar{a} \in \left(\mathbb{F}_{q^{\deg(u)}}\right)^l$ indicates the vector related to $a = (a_1 \ \cdots \ a_l) \in \mathbb{L}/u\mathbb{L}$ by

$$\mathbb{L}/u\mathbb{L} = (R/uR)^l \ni a \mapsto \bar{a} = (\bar{a}_1, \cdots, \bar{a}_l) \in \left(\mathbb{F}_{q^{\deg(u)}}\right)^l$$

and $\bar{b}^\dagger = \left(\bar{b}_1^{q^{\deg(u)/2}}, \cdots, \bar{b}_l^{q^{\deg(u)/2}}\right)^\top \in \left(\mathbb{F}_{q^{\deg(u)}}\right)^l$.

Proof. Because $\left[f \mapsto f^{\langle m\rangle}\right]$ belongs to the Galois group of order $\deg(u)$ which is cyclic and generated by $[f \mapsto f^q]$ and the order of $\left[f \mapsto f^{\langle m\rangle}\right]$ is equal to two, $\deg(u)$ must be even and $f^{\langle m\rangle} = f^{q^{\deg(u)/2}}$. Another proof is given directly as follows. It suffices to prove that, for all $1 \le i < \deg(u)$, $x^{m-i} \equiv \left(x^i\right)^{q^{\deg(u)/2}} \bmod u$, which is equivalent to $1 \equiv x^{1+q^{\deg(u)/2}} \bmod u$. We can suppose $\gcd(q,m) = 1$. Let the cyclotomic coset corresponding to u be $\left\{j, jq, \cdots, jq^{\deg(u)-1} \bmod m\right\}$ for some j. If $\gcd(j,m) > 1$, by dividing j, m by $\gcd(j,m)$, we can suppose $\gcd(j,m) = 1$. Because u is self-reciprocal, $\deg(u)$ is even and m divides $(j + jq^{\deg(u)/2})$. Thus, m divides $(1+q^{\deg(u)/2})$, which completes the proof. □

Proposition 5: If $F = (f_{i,j}) \in M_l(R)$ satisfies $KF = uI$ for some $K = (k_{i,j}) \in M_l(R)$, then $u\mathbb{L} + \mathbb{L}F^* = \mathbb{L}\widetilde{F}$, where $\widetilde{F} \in M_l(R)$ is given by

$$\widetilde{F} \equiv \mathrm{diag}\left[x^{\deg(f_{1,1})}, \cdots, x^{\deg(f_{l,l})}\right]F^* \bmod (1-x^m) \tag{2}$$

and $\mathrm{diag}[d_1, \cdots, d_l] \in M_l(R)$ is the diagonal matrix whose i-th entry is d_i for all $1 \le i \le l$.

Proof. It follows from (2) that $u\mathbb{L} + \mathbb{L}F^* \supset \mathbb{L}\widetilde{F}$. On the

other hand, because $\mathrm{diag}\left[x^{m-\deg(f_{i,1})},\cdots,x^{m-\deg(f_{i,l})}\right]\widetilde{F} \equiv x^m F^* \equiv F^* \bmod (1-x^m)$, we have $\mathbb{L}F^* \subset \mathbb{L}\widetilde{F} + u\mathbb{L}$. If $u\mathbb{L} \subset \mathbb{L}\widetilde{F}$ is shown, then $u\mathbb{L} + \mathbb{L}F^* \subset \mathbb{L}\widetilde{F}$. Because of $KF = uI$ and Lemma 5, $F^*K^* \equiv u^{\langle m\rangle} I \bmod (1-x^m)$. Let $N \in M_l(R)$ be defined by $K^*\mathrm{diag}\left[\gamma x^{\deg(k_{1,1})},\cdots,\gamma x^{\deg(k_{l,l})}\right] \equiv N \bmod (1-x^m)$. Then we have $\widetilde{F}N \equiv \gamma\widetilde{u}I = uI \bmod (1-x^m)$, where we use $k_{i,i}f_{i,i} = u$ and Lemma 3. Because we may assume that K and F are upper triangular, $\widetilde{F}N$ is lower triangular. Then there exists lower triangular $T \in M_l(R)$ such that $\widetilde{F}N = uI + (1-x^m)T$. Because the diagonal elements of $\widetilde{F}N$ equal $\gamma\widetilde{f_{i,i}}\widetilde{k_{i,i}} = \gamma\widetilde{u} = u$ for all $1 \le i \le l$, the diagonal elements of T equal 0. Then there exists $P \in GL_l(R)$ such that $uIP = uI + (1-x^m)T$. Thus, we have $\widetilde{F}NP^{-1} = uI$ and it follows from $\left(NP^{-1}\right)\widetilde{F} = uI$ that $\mathbb{L}\widetilde{F} \supset u\mathbb{L}$, which completes the proof. □

Consider a homomorphism of R-modules

$$\frac{\mathbb{L}}{u\mathbb{L}} \to \frac{\mathbb{L}}{u\mathbb{L}} \quad [a \mapsto aG^*].$$

Let $\widetilde{C}$ denote $\widetilde{C} = (u\mathbb{L} + \mathbb{L}G^*)/u\mathbb{L}$, i.e., the image of this map. Then there exists an exact sequence of R-modules

$$0 \to \widehat{C} \to \frac{\mathbb{L}}{u\mathbb{L}} \to \widetilde{C} \to 0$$

and an equality $\left|\widehat{C}\right|\left|\widetilde{C}\right| = |\mathbb{L}/u\mathbb{L}|$.

Corollary 1: A generator matrix of $\widetilde{C}$ is given by $\widetilde{G}$ of (2). In particular, we have $\left|\widetilde{C}\right| = |C|$ and $\left|\widehat{C}\right||C| = |\mathbb{L}/u\mathbb{L}|$.

Proof. $\widetilde{C} = (u\mathbb{L} + \mathbb{L}G^*)/u\mathbb{L} = \mathbb{L}\widetilde{G}/u\mathbb{L}$ follows from Proposition 5. Then $\left|\widetilde{C}\right| = |C|$ follows from $\deg(f_{i,i}) = \deg(g_{i,i})$ if $\widetilde{G} = (f_{i,j})$ and $G = (g_{i,j})$. □

Corollary 2: If $AG = uI$ for some $A = (a_{i,j}) \in M_l(R)$, then a generator matrix of $\widehat{C}$ is given by $\widetilde{A}$ of (2).

Proof. Because of $AG = uI = GA$ and Lemma 5, $A^*G^* \equiv u^{\langle m\rangle} I \bmod (1-x^m)$. By Lemma 4, we have $u^{\langle m\rangle} \equiv 0 \bmod u$. Thus, $A^*G^* \equiv 0I \bmod u$ and $(u\mathbb{L} + \mathbb{L}A^*)/u\mathbb{L} \subset \widehat{C}$. On the other hand, by $GA = uI$, Proposition 5 deduces $u\mathbb{L} + \mathbb{L}A^* = \mathbb{L}\widetilde{A}$. Thus, we have $\mathbb{L}\widetilde{A}/u\mathbb{L} \subset \widehat{C}$. Because the diagonal elements of $\widetilde{A}$ are equal to $\widetilde{a_{i,i}}$ for all $1 \le i \le l$,

$$\left|\frac{\mathbb{L}\widetilde{A}}{u\mathbb{L}}\right| = q^{\sum_{i=1}^{l}\deg(g_{i,i})}, \quad \left|\frac{\mathbb{L}\widetilde{G}}{u\mathbb{L}}\right| = q^{\sum_{i=1}^{l}\deg(a_{i,i})},$$

$$\left|\frac{\mathbb{L}\widetilde{A}}{u\mathbb{L}}\right|\left|\frac{\mathbb{L}\widetilde{G}}{u\mathbb{L}}\right| = q^{l\deg(u)} = \left|\frac{\mathbb{L}}{u\mathbb{L}}\right|, \quad \left|\widehat{C}\right|\left|\widetilde{C}\right| = |\mathbb{L}/u\mathbb{L}|$$

deduce $\left|\mathbb{L}\widetilde{A}/u\mathbb{L}\right| = \left|\widehat{C}\right|$, hence $\mathbb{L}\widetilde{A}/u\mathbb{L} = \widehat{C}$. □

We say that C is *self-orthogonal* if and only if $C \subset \widehat{C}$, which is equivalent to $GG^* \equiv 0I \bmod u$. We denote $\{G\}_u^* = \{G \in \{G\}_u \mid GG^* \equiv 0I \bmod u\}$.

Theorem 2: (cf. [5]) Let $u, u_1, u_2 \in R$ satisfy $u = 1 - x^m$, $u = u_1u_2$, $\gcd(u_1, u_2) = 1$, and u_1 and u_2 are self-reciprocal. Furthermore, we again denote α, β the restriction maps of α, β to $\{G_1\}_{u_1}^* \times \{G_2\}_{u_2}^*$, $\{G\}_u^*$, respectively. Then both α and β are bijective maps and inverse each other.

We say that C is *self-dual* if and only if $C = \widehat{C}$. For self-orthogonal C, because we have $|C| \le \left|\widehat{C}\right|$ and $|C|^2 \le |\mathbb{L}/u\mathbb{L}|$, C is self-dual if and only if $|C|^2 = |\mathbb{L}/u\mathbb{L}|$. We denote $\{G\}_u^{**} = \left\{G \in \{G\}_u^* \,\middle|\, |\mathbb{L}G/u\mathbb{L}|^2 = |\mathbb{L}/u\mathbb{L}|\right\}$.

Corollary 3: (cf. [5]) Let the notation be as in Theorem 2. We again denote α, β the restriction maps of α, β of Theorem 2 to $\{G_1\}_{u_1}^{**} \times \{G_2\}_{u_2}^{**}$, $\{G\}_u^{**}$, respectively. Then both α and β are bijective maps and inverse each other.

Example 1: Set $q = 2$, $l = 3$, $u_1 = 1 + x$, $u_2 = 1 + x + x^2 + x^3 + x^4$, and $u = u_1u_2$. Consider R-modules $C_1 = \mathbb{L}G_1/u_1\mathbb{L}$, $C_2 = \mathbb{L}G_2/u_2\mathbb{L}$, $C = \mathbb{L}G/u\mathbb{L}$ by

$$A_1G_1 = (1+x)I = \begin{pmatrix}1&0&0\\0&11&1\\0&0&1\end{pmatrix}\begin{pmatrix}11&0&0\\0&1&1\\0&0&11\end{pmatrix},$$

$$A_2G_2 = (1+x+x^2+x^3+x^4)I = \begin{pmatrix}11111&1111&0\\0&1&0\\0&0&1\end{pmatrix}\begin{pmatrix}1&1111&0\\0&11111&0\\0&0&11111\end{pmatrix},$$

$$AG = (1+x^5)I = \begin{pmatrix}11111&0111&1111\\0&11&1\\0&0&1\end{pmatrix}\begin{pmatrix}11&0111&11111\\0&11111&11111\\0&0&100001\end{pmatrix},$$

where, e.g., 0111 denotes $x + x^2 + x^3 \in R$. Then C_1, C_2, C are self-orthogonal because

$$G_1G_1^* = \begin{pmatrix}11&0&0\\0&1&1\\0&0&11\end{pmatrix}\begin{pmatrix}10001&0&0\\0&1&0\\0&1&10001\end{pmatrix} \equiv 0I \mod (1+x),$$

$$G_2G_2^* = \begin{pmatrix}1&1111&0\\0&11111&0\\0&0&11111\end{pmatrix}\begin{pmatrix}1&0&0\\10111&11111&0\\0&0&11111\end{pmatrix} \equiv 0I \mod (1+x+x^2+x^3+x^4),$$

$$GG^* = \begin{pmatrix}11&0111&11111\\0&11111&11111\\0&0&100001\end{pmatrix}\begin{pmatrix}10001&0&0\\00111&11111&0\\11111&11111&100001\end{pmatrix} \equiv 0I \mod (1+x^5).$$

Moreover, we have $\alpha(G_1, G_2) = G$ in terms of Theorem 2, in other words, by Proposition 1, we can find $B_1, B_2 \in M_l(R)$ such that $B_1G_1 = B_2G_2 = G$ as follows.

$$\begin{pmatrix}1&0111&1111\\0&11111&0\\0&0&11111\end{pmatrix}\begin{pmatrix}11&0&0\\0&1&1\\0&0&11\end{pmatrix} = \begin{pmatrix}11&1&1\\0&1&1\\0&0&11\end{pmatrix}\begin{pmatrix}1&1111&0\\0&11111&0\\0&0&11111\end{pmatrix} = G.$$

4. Conclusions

In this study, we have shown that self-orthogonal and self-dual quasi-cyclic codes can be constructed by using generator polynomial matrices and the factorization of $1 - x^m$ into reciprocal polynomials. The flow of the whole discussion is the same as in the case of integer codes [5], but in the case of QC codes, the actual bijections can be constructed by using Proposition 5. We have mainly described the case with two factors u_1, u_2, but the same is true for the case with three or more factors. In future work, the results will be generalized to the case which does not satisfy Assumption 1. Another work will focus on generalizing the results to the case of generalized quasi-cyclic codes.

References

[1] W.C. Huffman, "On the classification and enumeration of self-dual codes," Finite Fields and Their Applications, vol.11, no.3, pp.451–490, Aug. 2005.
[2] M. Grassl, "Searching for linear codes with large minimum distance," Discovering Mathematics with Magma — Reducing the Abstract to the Concrete, W. Bosma and J. Cannon, eds., pp.287–313, Springer, Heidelberg, 2006.
[3] H. Matsui, "On generator and parity-check polynomial matrices of generalized quasi-cyclic codes," Finite Fields and Their Applications, vol.34, pp.280–304, July 2015.
[4] H. Matsui, "Multiplicative structure and Hecke rings of generator matrices for codes over quotient rings of Euclidean domains," MDPI Mathematics, vol.5, no.4, 82, doi: 10.3390/math5040082, Dec. 2017.
[5] H. Matsui, "A modulus factorization algorithm for self-orthogonal and self-dual integer codes," IEICE Trans. Fundamentals, vol.E101-A, no.11, pp.1952–1956, Nov. 2018.
[6] H. Matsui, "A modulus factorization algorithm for self-orthogonal and self-dual quasi-cyclic codes," The 42nd Symposium on Information Theory and its Applications (SITA2019), pp.273–276, Kirishima, Kagoshima, Japan, Nov. 2019.