Korean J. Math. **32** (2024), No. 3, pp. 485–496
https://dx.doi.org/10.11568/kjm.2024.32.3.485

QUASI-CYCLIC SELF-DUAL CODES WITH FOUR FACTORS

Hyun Jin Kim†, Whan-Hyuk Choi∗,‡, and Jung-Kyung Lee⊤

Abstract. In this study, we examine ℓ-quasi-cyclic self-dual codes of length ℓm over $\mathbb{F}_2$, provided that the polynomial $X^m - 1$ has exactly four distinct irreducible factors in $\mathbb{F}_2[X]$. We find the standard form of generator matrices of codes over the ring $R \cong \mathbb{F}_q[X]/(X^m - 1)$ and the conditions for the codes to be self-dual. We explicitly determine the forms of generator matrices of self-dual codes of lengths 2 and 4 over R.

1. Introduction

Quasi-cyclic codes are recognized as being *asymptotically good* [8] and are linked to other areas such as convolutional codes and S-boxes [2, 5]. Self-dual codes are also well known for their connection with other combinatorial structures, such as designs and lattices [1, 3, 4], as well as invariant theory [13].

Cyclic codes, which are considered a special case of quasi-cyclic codes with an index of 1, demonstrate that quasi-cyclic codes can also be considered as modules over the group algebra of a cyclic group. Ling and Solé [10, 12] have examined quasi-cyclic codes over finite fields $\mathbb{F}_q$ as linear codes over the ring $\mathcal{R} = \mathbb{F}_q[X]/(X^m - 1)$, particularly when m, a positive integer, is coprime to q. Their research established a one-to-one correspondence between quasi-cyclic codes over $\mathbb{F}_q$ with an index of ℓ and a length of ℓm and linear codes over a factor ring $\mathcal{R}$ of length ℓ [10].

This paper delves into quasi-cyclic codes over $\mathbb{F}_q$ with an index of ℓ and a length of ℓm. We note that ℓ-quasi-cyclic codes over $\mathbb{F}_q$ of this length lm have permutation automorphisms of order m without fixed points [14]. Han et al. [6] have explored scenarios in which $X^m - 1$ decomposes into *two* distinct irreducible factors in $\mathbb{F}_q[X]$,

---

Received April 24, 2024. Revised September 7, 2024. Accepted September 8, 2024.
2010 Mathematics Subject Classification: 94B05, 11T71.
Key words and phrases: quasi-cyclic code, self-dual code, automorphism, reciprocal polynomials, linear codes.

∗ Corresponding author.

† This work was supported by the National Research Foundation of Korea(NRF) grant founded by the Korean government(NRF-2020R1F1A1A01071645).

‡ This work was supported by 2023 Research Grant from Kangwon National University and the National Research Foundation of Korea (NRF) grant funded by the Korea government (NRF-2022R1C1C2011689).

⊤ This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korean government(NRF-2019R1G1A1099148).

demonstrating that the *building-up* construction can generate every ℓ-quasi-cyclic self-dual code of length ℓm over a finite field $\mathbb{F}_q$. When $X^m - 1$ is split into *three* distinct irreducible factors in $\mathbb{F}_q[X]$, Kim and Lee [9] differentiated two types of the ring $\mathcal{R}$ based on the action of the conjugation map on the minimal ideals of $\mathcal{R}$, which led to the discovery of optimal self-dual codes of lengths 68 and 70 under their construction [7].

This study extends previous research by investigating the generator matrices of all ℓ-quasi-cyclic self-dual codes over $\mathbb{F}_q$ with a length ℓm for each positive even integer ℓ, particularly when $X^m - 1$ contains exactly four irreducible factors in $\mathbb{F}_q[X]$ and precisely two of these factors are self-reciprocal.

In this paper, we assume that $X^m - 1$ has *exactly four* distinct irreducible factors in $\mathbb{F}_q[X]$ with *exactly two* of those factors being self-reciprocal, where the degree m is a positive integer relatively prime to q.

This paper is structured as follows: Section 2 provides essential definitions, facts, and notations required for this study. Section 3 explores the standard forms of generator matrices for linear codes over the ring $\mathcal{R}$. Section 4 examines self-dual codes over $\mathcal{R}$ of the second type and establishes the forms of generator matrices for self-dual codes of lengths 2 and 4. All computations in this study are performed using MAGMA [15].

2. Preliminaries

In this section, we introduce fundamental concepts related to quasi-cyclic self-dual codes, referencing [10–12] for more comprehensive details.

Let $\mathscr{R}$ be a commutative ring with identity. A linear code $\mathcal{C}$ of length n over $\mathscr{R}$ is an $\mathscr{R}$-submodule of $\mathscr{R}^n$. The *free rank* of a code $\mathcal{C}$ is the highest rank among all free $\mathscr{R}$-submodules contained within $\mathcal{C}$. If a code $\mathcal{C}$ is a free $\mathscr{R}$-submodule of $\mathscr{R}^n$, then $\mathcal{C}$ is called a *free code*. The standard shift operator on $\mathscr{R}^n$ is denoted by T. A linear code $\mathcal{C}$ over $\mathscr{R}$ is called *ℓ-quasi-cyclic* or *quasi-cyclic of index ℓ* if it remains invariant under T^ℓ. We can easily show that if ℓ and the code length n are coprime, the code $\mathcal{C}$ is permutation equivalent to a cyclic code. Therefore, throughout this study, we assume that the code length n is equal to ℓm for some positive integer m.

Let $\mathbb{F}_q[X]$ be a polynomial ring, and $\mathcal{R} := \mathbb{F}_q[X]/(X^m - 1)$. Let us assume that m is coprime to the characteristic of $\mathbb{F}_q$. In [10], it is proved that quasi-cyclic codes with index ℓ and length ℓm over $\mathbb{F}_q$ have a one-to-one correspondence with linear codes of length ℓ over $\mathcal{R}$. The correspondence is given by the map ϕ, which we defined as follows. Suppose that $\mathcal{C}$ be a quasi-cyclic code over $\mathbb{F}_q$ of length ℓm and index ℓ with a codeword $\mathbf{c}$ denoted by

$$\mathbf{c} = (c_{00}, c_{01}, \ldots, c_{0l-1}, c_{10}, \ldots, c_{1l-1}, \ldots, c_{m-10}, \ldots, c_{m-1l-1}).$$

Let ϕ be a map $\phi : \mathbb{F}_q{}^{\ell m} \to \mathcal{R}^\ell$ defined by

$$\phi(\mathbf{c}) = (\mathbf{c}_0(X), \mathbf{c}_1(X), \ldots, \mathbf{c}_{l-1}(X)) \in \mathcal{R}^\ell,$$

where

$$\mathbf{c}_j(X) = \sum_{i=0}^{m-1} c_{ij} X^i \in \mathcal{R}, \text{ for } j = 0, \ldots, l-1.$$

We denote by $\phi(\mathcal{C})$ the image of $\mathcal{C}$ under ϕ.

The dual of $\mathcal{C}$, denoted by $\mathcal{C}^{\perp}$, is defined with respect to an inner product over $\mathcal{R}$. A code $\mathcal{C}$ is called *self-dual* if $\mathcal{C} = \mathcal{C}^{\perp}$.

We define a *conjugation* map $^{-}$ on $\mathcal{R}$ by $\overline{X} = X^{-1}$, where $X^{-1} = X^{m-1}$, and it is an identity map on $\mathbb{F}_q$. It is extended $\mathbb{F}_q$-linearly. We also define the *Hermitian inner product* on $\mathcal{R}^{\ell}$ by $\langle \mathbf{x}, \mathbf{y} \rangle = \sum_{j=0}^{l-1} x_j \overline{y}_j$ for $\mathbf{x} = (x_0, \ldots, x_{\ell-1})$ and $\mathbf{y} = (y_0, \ldots, y_{\ell-1})$.

For $\mathbf{a}, \mathbf{b} \in \mathbb{F}_q^{\ell m}$, $\langle \phi(\mathbf{a}), \phi(\mathbf{b}) \rangle = 0$ if and only if $T^{\ell k}(\mathbf{a}) \cdot \mathbf{b} = 0$ for every $0 \le k \le m-1$, where $\cdot$ denotes the Euclidean inner product [10]. It follows that $\phi(\mathcal{C})^{\perp} = \phi(\mathcal{C}^{\perp})$, where $\phi(\mathcal{C})^{\perp}$ is the Hermitian dual of $\phi(\mathcal{C})$, and $\mathcal{C}^{\perp}$ is the Euclidean dual of $\mathcal{C}$. In particular, a quasi-cyclic code $\mathcal{C}$ over $\mathbb{F}_q$ is Euclidean self-dual if and only if a code $\phi(\mathcal{C})$ over $\mathcal{R}$ is Hermitian self-dual [10]. Two linear codes over $\mathbb{F}_q$ (resp. $\mathcal{R}$) are called *equivalent* if there is a monomial map (resp. permutation map) such that it sends one to another.

For a matrix $A_{m\times n}$, we define the matrix $\overline{A}_{m\times n}$ by the conjugation action of entries of $A_{m\times n}$, that is, if $A = (a_{ij})_{m\times n}$ then $\overline{A} = (\overline{a_{ij}})_{m\times n}$. We denote the transpose of $A_{m\times n}$ by $A^{\top}_{m\times n}$, that is, $A^{\top}_{m\times n} = (a_{ji})_{n\times m}$.

3. Standard form

We use the following notations throughout this study. Let q be a power of prime. We consider a factor ring $\mathcal{R} = \mathbb{F}_q[X]/(X^m - 1)$ for a prime m. If $X^m - 1 = N_0(X)N_1(X)N_2(X)N_3(X)$ which is a product of four distinct irreducible factors in $\mathbb{F}_q[X]$, where $N_0(X) = X - 1$, then $\mathcal{R} \cong \mathcal{I}_0 \oplus \mathcal{I}_1 \oplus \mathcal{I}_2 \oplus \mathcal{I}_3$, where $\mathcal{I}_i$ is the minimal ideal of $\mathcal{R}$ generated by $\frac{X^m-1}{N_i(X)}$ for $i = 0, 1, 2, 3$. We have $\mathcal{I}_i \cong \mathbb{F}_{q^{t_i}}$, where t_i is the degree of $N_i(X)$ for $i = 0, 1, 2, 3$. Hence $\mathcal{R} \cong \mathbb{F}_{q^{t_0}} \oplus \mathbb{F}_{q^{t_1}} \oplus \mathbb{F}_{q^{t_2}} \oplus \mathbb{F}_{q^{t_3}}$. The unit group of a field $\mathbb{F}$ is denoted by $\mathbb{F}^{\times}$. We define an isomorphsim Φ from $\mathcal{R}$ to $R := \mathbb{F}_{q^{t_0}} \oplus \mathbb{F}_{q^{t_1}} \oplus \mathbb{F}_{q^{t_2}} \oplus \mathbb{F}_{q^{t_3}}$ by $\Phi(L_i) = f_0$ where $L_i = \frac{X^m-1}{N_i(X)}$ for $i = 0, 1, 2, 3$ and $f_0 = (e_0, 0, 0, 0), f_1 = (0, e_1, 0, 0), f_2 = (0, 0, e_2, 0), f_3 = (0, 0, 0, e_3)$ for some $e_i \in \mathbb{F}^{\times}_{q^{t_i}}$ with $i = 0, 1, 2, 3$. We note that $f_0^{-1} = (e_0^{-1}, 0, 0, 0), f_1^{-1} = (0, e_1^{-1}, 0, 0), f_2^{-1} = (0, 0, e_2^{-1}, 0), f_3^{-1} = (0, 0, 0, e_3^{-1})$.

We note that $\overline{\mathcal{I}}_0 = \mathcal{I}_0$. We define the type of the ring $\mathcal{R} = \mathbb{F}_q[X]/(X^m - 1)$ depending on how the conjugation map acts on $\mathcal{I}_i$ for $i = 0, 1, 2, 3$. We say that $\mathcal{R}$ is of *the first type*, denoted by $\mathcal{R}_1$ if $\overline{\mathcal{I}}_i = \mathcal{I}_i$ for $i = 1, 2, 3$, and it is of *the second type*, denoted by $\mathcal{R}_2$ if $\overline{\mathcal{I}}_2 = \mathcal{I}_3$. In the following theorem, we find a standard form of a generator matrix of a linear code over R.

Theorem 3.1. *We keep the notations given above. Let $R = \mathbb{F}_{q^{t_0}} \times \mathbb{F}_{q^{t_1}} \times \mathbb{F}_{q^{t_2}} \times \mathbb{F}_{q^{t_3}} \cong \mathbb{F}_q[X]/(X^m - 1)$, where m is relatively prime to q and the factorization of $X^m - 1$ over $\mathbb{F}_q$ has four distinct irreducible factors and t_i is a positive integer for $i = 0, 1, 2, 3$. Let $f_0 = (e_0, 0, 0, 0), f_1 = (0, e_1, 0, 0), f_2 = (0, 0, e_2, 0), f_3 = (0, 0, 0, e_3)$, where $e_i \in \mathbb{F}^{\times}_{q^{t_i}}$.*

Then every linear code $\mathcal{C}$ over R of length ℓ has generator matrix (up to equivalence) in the following form:

$$G = \begin{bmatrix} I_{k_0} & A_1 & A_2 & A_3 & D_0 \\ O & B_1 & M_1 & M_2 & D_1 \\ O & O & B_2 & M_3 & D_2 \\ O & O & O & B_3 & D_3 \end{bmatrix}, \tag{1}$$

where I_{k_0} is the identity matrix of degree k_0, and
$B_1 = \operatorname{diag}\big((f_0+f_1+f_2)I_{k_{1,1}}, (f_0+f_1+f_3)I_{k_{1,2}}, (f_0+f_2+f_3)I_{k_{1,3}}, (f_1+f_2+f_3)I_{k_{1,4}}\big)$,
$B_2 = \operatorname{diag}\big((f_0+f_1)I_{k_{2,1}}, (f_0+f_2)I_{k_{2,2}}, (f_0+f_3)I_{k_{2,3}}, (f_1+f_2)I_{k_{2,4}}, (f_1+f_3)I_{k_{2,5}}, (f_2+f_3)I_{k_{2,6}}\big)$,
$B_3 = \operatorname{diag}\big(f_0 I_{k_{3,1}}, f_1 I_{k_{3,2}}, f_2 I_{k_{3,3}}, f_3 I_{k_{3,4}}\big)$
are diagonal matrices, and
$A_1 = \begin{bmatrix} f_3 A_{k_{1,1}} & f_2 A_{k_{1,2}} & f_1 A_{k_{1,3}} & f_0 A_{k_{1,4}} \end{bmatrix}$,
$A_2 = \begin{bmatrix} (f_2+f_3)A_{k_{2,1}} & (f_1+f_3)A_{k_{2,2}} & (f_1+f_2)A_{k_{2,3}}, (f_0+f_3)A_{k_{2,4}} & (f_0+f_2)A_{k_{2,5}} & (f_0+f_1)A_{k_{2,6}} \end{bmatrix}$,
$A_3 = \begin{bmatrix} (f_1+f_2+f_3)A_{k_{3,1}} & (f_0+f_2+f_3)A_{k_{3,2}} & (f_0+f_1+f_3)A_{k_{3,3}} & (f_0+f_1+f_2)A_{k_{3,4}} \end{bmatrix}$,
where $A_{k_{i,j}}$ is $k_0 \times k_{i,j}$ matrix over R, and

$$M_1 = \begin{bmatrix} f_2 M_{k_{1,1},k_{2,1}} & f_1 M_{k_{1,1},k_{2,2}} & (f_1+f_2)M'_{k_{1,1},k_{2,3}} & f_0 M_{k_{1,1},k_{2,4}} & (f_0+f_2)M'_{k_{1,1},k_{2,5}} & (f_0+f_1)M'_{k_{1,1},k_{2,6}} \\ f_3 M_{k_{1,2},k_{2,1}} & f_3 M_{k_{1,2},k_{2,2}} & f_1 M_{k_{1,2},k_{2,3}} & f_3 M_{k_{1,2},k_{2,4}} & f_0 M_{k_{1,2},k_{2,5}} & (f_0+f_1)M'_{k_{1,2},k_{2,6}} \\ O_{k_{1,3},k_{2,1}} & f_3 M_{k_{1,3},k_{2,2}} & f_2 M_{k_{1,3},k_{2,3}} & f_3 M_{k_{1,3},k_{2,4}} & f_2 M_{k_{1,3},k_{2,5}} & f_0 M_{k_{1,3},k_{2,6}} \\ O_{k_{1,4},k_{2,1}} & O_{k_{1,4},k_{2,2}} & O_{k_{1,4},k_{2,3}} & f_3 M_{k_{1,4},k_{2,4}} & f_2 M_{k_{1,4},k_{2,5}} & f_1 M_{k_{1,4},k_{2,6}} \end{bmatrix},$$

$$M_2 = \begin{bmatrix} (f_1+f_2)M_{k_{1,1},k_{3,1}} & (f_0+f_2)M_{k_{1,1},k_{3,2}} & (f_0+f_1)M_{k_{1,1},k_{3,3}} & (f_0+f_1+f_2)M'_{k_{1,1},k_{3,4}} \\ (f_1+f_3)M_{k_{1,2},k_{3,1}} & (f_0+f_3)M_{k_{1,2},k_{3,2}} & (f_0+f_1+f_3)M''_{k_{1,2},k_{3,3}} & (f_0+f_1)M_{k_{1,2},k_{3,4}} \\ (f_2+f_3)M_{k_{1,3},k_{3,1}} & (f_0+f_2+f_3)M'''_{k_{1,3},k_{3,2}} & (f_0+f_3)M_{k_{1,3},k_{3,3}} & (f_0+f_2)M_{k_{1,3},k_{3,4}} \\ (f_1+f_2+f_3)M''''_{k_{1,4},k_{3,1}} & (f_2+f_3)M_{k_{1,4},k_{3,2}} & (f_1+f_3)M_{k_{1,4},k_{3,3}} & (f_1+f_2)M_{k_{1,4},k_{3,4}} \end{bmatrix},$$

$$M_3 = \begin{bmatrix} f_1 M_{k_{2,1},k_{3,1}} & f_0 M_{k_{2,1},k_{3,2}} & (f_0+f_1)M'_{k_{2,1},k_{3,3}} & (f_0+f_1)M'_{k_{2,1},k_{3,4}} \\ f_2 M_{k_{2,2},k_{3,1}} & f_2 M_{k_{2,2},k_{3,2}} & f_0 M_{k_{2,2},k_{3,3}} & (f_0+f_2)M'_{k_{2,2},k_{3,4}} \\ f_3 M_{k_{2,3},k_{3,1}} & f_3 M_{k_{2,3},k_{3,2}} & f_3 M_{k_{2,3},k_{3,3}} & f_0 M_{k_{2,3},k_{3,4}} \\ O_{k_{2,4},k_{3,1}} & f_2 M_{k_{2,4},k_{3,2}} & f_1 M_{k_{2,4},k_{3,3}} & (f_1+f_2)M'_{k_{2,4},k_{3,4}} \\ O_{k_{2,5},k_{3,1}} & f_3 M_{k_{2,5},k_{3,2}} & f_3 M_{k_{2,5},k_{3,3}} & f_1 M_{k_{2,5},k_{3,4}} \\ O_{k_{2,6},k_{3,1}} & O_{k_{2,6},k_{3,2}} & f_3 M_{k_{2,6},k_{3,3}} & f_2 M_{k_{2,6},k_{3,4}} \end{bmatrix},$$

where $M_{k_{i,j},k_{s,t}}$ is a $k_{i,j} \times k_{s,t}$ matrix over R, and $M'_{k_{i,j},k_{s,t}}$ is a $k_{i,j} \times k_{s,t}$ matrix over R such that for its entries, the components corresponding to the coefficient can't consist of all nonzero, and $M''_{k_{i,j},k_{s,t}}$ is a $k_{i,j} \times k_{s,t}$ matrix over R such that for its entries, the components corresponding to f_0 and f_1 can't consist of all nonzero, and $M'''_{k_{i,j},k_{s,t}}$ is a $k_{i,j} \times k_{s,t}$ matrix over R such that for its entries, the component corresponding to f_0 is zero or the components corresponding to f_2 and f_3 are both zero, and $M''''_{k_{i,j},k_{s,t}}$ is a $k_{i,j} \times k_{s,t}$ matrix over R such that for its entries, just one of the components corresponding to f_1, f_2, and f_3 is nonzero, and D_0 is $k_0 \times k_4$ matrix over R, and

$$D_1 = \begin{bmatrix} D_{1,1} \\ D_{1,2} \\ D_{1,3} \\ D_{1,4} \end{bmatrix}, D_2 = \begin{bmatrix} D_{2,1} \\ D_{2,2} \\ D_{2,3} \\ D_{2,4} \\ D_{2,5} \\ D_{2,6} \end{bmatrix}, D_3 = \begin{bmatrix} D_{3,1} \\ D_{3,2} \\ D_{3,3} \\ D_{3,4} \end{bmatrix}$$

where $D_{i,j}$ is a $k_{i,j} \times k_4$ matrix over R such that every non-zero entry of $D_{i,j}$ is contained in the ideal $\langle g_{i,j}\rangle$ of R, where $g_{i,j}$ is the coefficient of $I_{k_{i,j}}$ in B_i.

In particular, this code $\mathcal{C}$ has free rank k_0,its length ℓ is equal to $k_0 + \sum_{i=j}^{4} k_{1,j} + \sum_{i=j}^{6} k_{2,j} + \sum_{i=j}^{4} k_{3,j} + k_4$, and its rank is equal to
$(k_0 \sum_{i=0}^{3} t_i + k_{1,1}(t_0+t_1+t_2) + k_{1,2}(t_0+t_1+t_3) + k_{1,3}(t_0+t_2+t_3) + k_{1,4}(t_1+t_2+t_3) + k_{2,1}(t_0+t_1) + k_{2,2}(t_0+t_2) + k_{2,3}(t_0+t_3) + k_{2,4}(t_1+t_2) + k_{2,5}(t_1+t_3) + k_{2,6}(t_2+t_3) + k_{3,1}t_0 + k_{3,2}t_1 + k_{3,3}t_2 + k_{3,4}t_3) / \big(\sum_{i=0}^{3} t_i\big)$.

Proof. We note that R is a commutative ring with unity $1_R = (1,1,1,1)$, zero $0_R = (0,0,0,0)$ and $f_0f_1 = f_0f_2 = f_0f_3 = f_1f_2 = f_1f_3 = f_2f_3 = 0_R$. The unit group $R^\times$ of R is $\mathbb{F}_q^\times \times \mathbb{F}_{q^{t_1}}^\times \times \mathbb{F}_{q^{t_2}}^\times \times \mathbb{F}_{q^{t_3}}^\times$.

Let G' be a generator matrix for $\mathcal{C}$. First, we note that there are four possible cases for each row of G'. The first case is a row of G_0 containing a unit of R.

The second case is that a row contains a nonzero element in $\langle f_{i_1}+f_{i_2}+f_{i_3}\rangle$ where $i_1, i_2, i_3 = 0,1,2,3$. The third case is that a row contains a nonzero element in $\langle f_{i_1}+f_{i_2}\rangle$ where $i_1, i_2 = 0,1,2,3$. The last case is that a row contains a nonzero element in $\langle f_i\rangle$ where $i=0,1,2,3$.

We can transform G' into G_0 such that the first k_0 rows (respectively, the first k_0 columns) of G_0 are equal to the first k_0 (respectively, the first k_0 columns) of G in (1) by column permutations and elementary row operations; we may assume that k_0 is the total number of rows containing units. Deleting the first k_0 rows and the first k_0 columns of G_0, we get G_0':

$$G_0 = \begin{bmatrix} I_{k_0} & \cdots \\ O & \\ \vdots & G_0' \\ O & \end{bmatrix}.$$

We may assume that G_0' has no unit entries; otherwise, we can increase k_0.

By column permutations and elementary row operations, we can transform G_0' into G_1 such that all entries of the first $k_{1,1}$ rows and the first $k_{1,1}$ columns of G_1 belong to $\langle f_0+f_1+f_2\rangle$. We claim that all the entries of the first $k_{1,1}$ columns of G_1 after the $k_{1,1}$th row are zeros by elementary row operations. In fact, the first $k_{1,1}$ columns of G_1 have no entry contained in $\langle f_3\rangle$; otherwise, k_0 is increased, which is a contradiction. If the first $k_{1,1}$ columns of G_1 after the $k_{1,1}$th row have an entry contained in $\langle f_i\rangle$ where $i=0,1,2$, then it is easy to see that we can easily make them zeros by elementary row operations.

By similar reasoning for the other cases, we can transform G' in the following form:

$$G'' = \begin{bmatrix} I_{k_0} & A_1' & A_2' & A_3' & D_0' \\ O & B_1' & M_1' & M_2' & D_1' \\ O & O & B_2' & M_3' & D_2' \\ O & O & O & B_3' & D_3' \end{bmatrix}.$$

Moreover, we can transform B_1' into B_1 in (1) by elementary row operations.

$$B_1' = \begin{bmatrix} (f_0+f_1+f_2)I_{k_{1,1}} & B_{1,1} & B_{1,2} & B_{1,3} \\ O & (f_0+f_1+f_3)I_{k_{1,2}} & B_{1,4} & B_{1,5} \\ O & O & (f_0+f_2+f_3)I_{k_{1,3}} & B_{1,6} \\ O & O & O & (f_1+f_2+f_3)I_{k_{1,4}} \end{bmatrix}$$

We note that the matrix $B_{1,1}$ has no entry contained in $\langle f_2\rangle$; it is easy to see that if $B_{1,1}$ has no entry contained in $\langle f_2\rangle$, then k_0 is increased, which is a contradiction. If $B_{1,1}$ has no entry contained in $\langle f_2\rangle$, then elementary row operations can transform it into zeros. Analogously, matrix $B_{1,i}$ can be transformed into O by elementary row operations for $i=2,3,4,5,6$. Furthermore, $A_1', A_2', A_3', M_1', M_2'$, and M_3' can be transformed into the A_1, A_2, A_3, M_1, M_2, and M_3 in (1) by elementary row operations without change of rank. Thus, we can transform G'' into G in (1).

This code $\mathcal{C}$ has rank $\log_{|R|}|\mathcal{C}| = (k_0\sum_{i=0}^3 t_i + k_{1,1}(t_0+t_1+t_2) + k_{1,2}(t_0+t_1+t_3) + k_{1,3}(t_0+t_2+t_3) + k_{1,4}(t_1+t_2+t_3) + k_{2,1}(t_0+t_1) + k_{2,2}(t_0+t_2) + k_{2,3}(t_0+t_3) + k_{2,4}(t_1+t_2) + k_{2,5}(t_1+t_3) + k_{2,6}(t_2+t_3) + k_{3,1}t_0 + k_{3,2}t_1 + k_{3,3}t_2 + k_{3,4}t_3)/\left(\sum_{i=0}^3 t_i\right)$ since $|\mathcal{C}| = q^{k_0\sum_{i=0}^3 t_i + k_{1,1}\sum_{i=0}^2 t_i + k_{1,2}\sum_{i=0,1,3} t_i + k_{1,3}\sum_{i=0,2,3} t_i + k_{1,4}\sum_{i=1}^3 t_i} \cdot q^{k_{2,1}(t_0+t_1)+k_{2,2}(t_0+t_2)+k_{2,3}(t_0+t_3)} \cdot q^{k_{2,4}(t_1+t_2)+k_{2,5}(t_1+t_3)+k_{2,6}(t_2+t_3)} \cdot q^{k_{3,1}t_0+k_{3,2}t_1+k_{3,3}t_2+k_{3,4}t_3}$. □

In the following corollary, we find the standard form of generator matrices of linear codes over the ring $\mathcal{R}$, which follows from Theorem 3.1 using the map Φ^{-1}.

COROLLARY 3.2. *Let $\mathcal{R} = \mathbb{F}_q[X]/(X^m - 1)$, where m is relatively prime to q and the factorization of $X^m - 1$ over $\mathbb{F}_q$ has four distinct irreducible factors $N_0(X), N_1(X), N_2(X)$, and $N_3(X)$. Let $L_i = \frac{X^m-1}{N_i}$ for $i = 0, 1, 2, 3$. Then a linear code $\mathcal{C}$ over the ring $\mathcal{R}$ of length ℓ has a generator matrix in the following form (up to equivalence):*

$$\begin{bmatrix} I_{k_0} & \mathcal{A}_1 & \mathcal{A}_2 & \mathcal{A}_3 & \mathcal{D}_0 \\ O & \mathcal{B}_1 & \mathcal{M}_1 & \mathcal{M}_2 & \mathcal{D}_1 \\ O & O & \mathcal{B}_2 & \mathcal{M}_3 & \mathcal{D}_2 \\ O & O & O & \mathcal{B}_3 & \mathcal{D}_3 \end{bmatrix}, \tag{2}$$

where I_{k_0} is the identity matrix of degree k_0, and
$\mathcal{B}_1 = \mathrm{diag}\left(N_3 I_{k_{1,1}}, N_2 I_{k_{1,2}}, N_1 I_{k_{1,3}}, N_0 I_{k_{1,4}}\right)$,
$\mathcal{B}_2 = \mathrm{diag}\left((L_0L_1) I_{k_{2,1}}, (L_0L_2) I_{k_{2,2}}, (L_0L_3) I_{k_{2,3}}, (L_1L_2) I_{k_{2,4}}, (L_1L_3) I_{k_{2,5}}, (L_2L_3) I_{k_{2,6}}\right)$,
$\mathcal{B}_3 = \mathrm{diag}\left(L_0 I_{k_{3,1}}, L_1 I_{k_{3,2}}, L_2 I_{k_{3,3}}, L_3 I_{k_{3,4}}\right)$
are diagonal matrices, and
$\mathcal{A}_1 = \begin{bmatrix} L_3\mathcal{A}_{k_{1,1}} & L_2\mathcal{A}_{k_{1,2}} & L_1\mathcal{A}_{k_{1,3}} & L_0\mathcal{A}_{k_{1,4}} \end{bmatrix}$,
$\mathcal{A}_2 = \begin{bmatrix} (L_2L_3)\mathcal{A}_{k_{2,1}} & (L_1L_3)\mathcal{A}_{k_{2,2}} & (L_1L_2)\mathcal{A}_{k_{2,3}} & (L_0L_3)\mathcal{A}_{k_{2,4}} & (L_0L_2)\mathcal{A}_{k_{2,5}} & (L_0L_1)\mathcal{A}_{k_{2,6}} \end{bmatrix}$,
$\mathcal{A}_3 = \begin{bmatrix} N_0\mathcal{A}_{k_{3,1}} & N_1\mathcal{A}_{k_{3,2}} & N_2\mathcal{A}_{k_{3,3}} & N_3\mathcal{A}_{k_{3,4}} \end{bmatrix}$,
where $\mathcal{A}_{k_{i,j}}$ is $k_0 \times k_{i,j}$ matrix over $\mathcal{R}$, and

$$\mathcal{M}_1 = \begin{bmatrix} L_2\mathcal{M}_{k_{1,1},k_{2,1}} & L_1\mathcal{M}_{k_{1,1},k_{2,2}} & (L_1L_2)\mathcal{M}'_{k_{1,1},k_{2,3}} & L_0\mathcal{M}_{k_{1,1},k_{2,4}} & (L_0L_2)\mathcal{M}'_{k_{1,1},k_{2,5}} & (L_0L_1)\mathcal{M}'_{k_{1,1},k_{2,6}} \\ L_3\mathcal{M}_{k_{1,2},k_{2,1}} & L_3\mathcal{M}_{k_{1,2},k_{2,2}} & L_1\mathcal{M}_{k_{1,2},k_{2,3}} & L_3\mathcal{M}_{k_{1,2},k_{2,4}} & L_0\mathcal{M}_{k_{1,2},k_{2,5}} & (L_0L_1)\mathcal{M}'_{k_{1,2},k_{2,6}} \\ O_{k_{1,3},k_{2,1}} & L_3\mathcal{M}_{k_{1,3},k_{2,2}} & L_2\mathcal{M}_{k_{1,3},k_{2,3}} & L_3\mathcal{M}_{k_{1,3},k_{2,4}} & L_2\mathcal{M}_{k_{1,3},k_{2,5}} & L_0\mathcal{M}_{k_{1,3},k_{2,6}} \\ O_{k_{1,4},k_{2,1}} & O_{k_{1,4},k_{2,2}} & O_{k_{1,4},k_{2,3}} & L_3\mathcal{M}_{k_{1,4},k_{2,4}} & L_2\mathcal{M}_{k_{1,4},k_{2,5}} & L_1\mathcal{M}_{k_{1,4},k_{2,6}} \end{bmatrix},$$

$$\mathcal{M}_2 = \begin{bmatrix} (L_1L_2)\mathcal{M}_{k_{1,1},k_{3,1}} & (L_0L_2)\mathcal{M}_{k_{1,1},k_{3,2}} & (L_0L_1)\mathcal{M}_{k_{1,1},k_{3,3}} & N_3\mathcal{M}'_{k_{1,1},k_{3,4}} \\ (L_1L_3)\mathcal{M}_{k_{1,2},k_{3,1}} & (L_0L_3)\mathcal{M}_{k_{1,2},k_{3,2}} & N_2\mathcal{M}''_{k_{1,2},k_{3,3}} & (L_0L_1)\mathcal{M}_{k_{1,2},k_{3,4}} \\ (L_2L_3)\mathcal{M}_{k_{1,3},k_{3,1}} & N_1\mathcal{M}'''_{k_{1,3},k_{3,2}} & (L_0L_3)\mathcal{M}_{k_{1,3},k_{3,3}} & (L_0L_2)\mathcal{M}_{k_{1,3},k_{3,4}} \\ N_0\mathcal{M}''''_{k_{1,4},k_{3,1}} & (L_2L_3)\mathcal{M}_{k_{1,4},k_{3,2}} & (L_1L_3)\mathcal{M}_{k_{1,4},k_{3,3}} & (L_1L_2)\mathcal{M}_{k_{1,4},k_{3,4}} \end{bmatrix},$$

$$\mathcal{M}_3 = \begin{bmatrix} L_1\mathcal{M}_{k_{2,1},k_{3,1}} & L_0\mathcal{M}_{k_{2,1},k_{3,2}} & (L_0L_1)\mathcal{M}'_{k_{2,1},k_{3,3}} & (L_0L_1)\mathcal{M}'_{k_{2,1},k_{3,4}} \\ L_2\mathcal{M}_{k_{2,2},k_{3,1}} & L_2\mathcal{M}_{k_{2,2},k_{3,2}} & L_0\mathcal{M}_{k_{2,2},k_{3,3}} & (L_0L_2)\mathcal{M}'_{k_{2,2},k_{3,4}} \\ L_3\mathcal{M}_{k_{2,3},k_{3,1}} & L_3\mathcal{M}_{k_{2,3},k_{3,2}} & L_3\mathcal{M}_{k_{2,3},k_{3,3}} & L_0\mathcal{M}_{k_{2,3},k_{3,4}} \\ O_{k_{2,4},k_{3,1}} & L_2\mathcal{M}_{k_{2,4},k_{3,2}} & L_1\mathcal{M}_{k_{2,4},k_{3,3}} & (L_1L_2)\mathcal{M}'_{k_{2,4},k_{3,4}} \\ O_{k_{2,5},k_{3,1}} & L_3\mathcal{M}_{k_{2,5},k_{3,2}} & L_3\mathcal{M}_{k_{2,5},k_{3,3}} & L_1\mathcal{M}_{k_{2,5},k_{3,4}} \\ O_{k_{2,6},k_{3,1}} & O_{k_{2,6},k_{3,2}} & L_3\mathcal{M}_{k_{2,6},k_{3,3}} & L_2\mathcal{M}_{k_{2,6},k_{3,4}} \end{bmatrix},$$

where $\mathcal{M}_{k_{i,j},k_{s,t}}$ is a $k_{i,j} \times k_{s,t}$ matrix over $\mathcal{R}$, and $\mathcal{M}'_{k_{i,j},k_{s,t}}$ is a $k_{i,j} \times k_{s,t}$ matrix over $\mathcal{R}$ such that for its entries, the components corresponding to the coefficient can't consist of all nonzero, and $\mathcal{M}''_{k_{i,j},k_{s,t}}$ is a $k_{i,j} \times k_{s,t}$ matrix over $\mathcal{R}$ such that for its entries, the components corresponding to L_0 and L_1 can't consist of all nonzero, and $\mathcal{M}'''_{k_{i,j},k_{s,t}}$ is a $k_{i,j} \times k_{s,t}$ matrix over $\mathcal{R}$ such that for its entries, the component corresponding to L_0 is zero or the components corresponding to L_2 and L_3 are both zero, and $\mathcal{M}''''_{k_{i,j},k_{s,t}}$ is a $k_{i,j} \times k_{s,t}$ matrix over $\mathcal{R}$ such that for its entries, just one of the components corresponding to L_1, L_2, and L_3 is nonzero, $\mathcal{D}_0$ is $k_0 \times k_4$ matrix over $\mathcal{R}$,

$$\mathcal{D}_1 = \begin{bmatrix} \mathcal{D}_{1,1} \\ \mathcal{D}_{1,2} \\ \mathcal{D}_{1,3} \\ \mathcal{D}_{1,4} \end{bmatrix}, \mathcal{D}_2 = \begin{bmatrix} \mathcal{D}_{2,1} \\ \mathcal{D}_{2,2} \\ \mathcal{D}_{2,3} \\ \mathcal{D}_{2,4} \\ \mathcal{D}_{2,5} \\ \mathcal{D}_{2,6} \end{bmatrix}, \mathcal{D}_3 = \begin{bmatrix} \mathcal{D}_{3,1} \\ \mathcal{D}_{3,2} \\ \mathcal{D}_{3,3} \\ \mathcal{D}_{3,4} \end{bmatrix},$$

where $\mathcal{D}_{i,j}$ is a $k_{i,j} \times k_4$ matrix over $\mathcal{R}$ such that every non-zero entry of $\mathcal{D}_{i,j}$ is contained in the ideal $\langle g_{i,j} \rangle$ of $\mathcal{R}$, where $g_{i,j}$ is the coefficient of $I_{k_{i,j}}$ in $\mathcal{B}_i$.

4. Hermitian self-dual codes over $\mathcal{R}$

We next study Hermitian self-dual codes over $\mathcal{R}$ to find conditions for a linear code over $\mathcal{R}$ to be Hermitian self-dual in terms of its generator matrix in the standard form.

THEOREM 4.1. *Let q be a power of prime and let $\mathcal{R}$ have the second type, where m is relatively prime to q, and the factorization of $X^m - 1$ over $\mathbb{F}_q$ has four distinct irreducible factors. Then every self-dual code over $\Phi(\mathcal{R})$ with generator matrix of the form* (1) *satisfies that $k_0 = k_4, k_{1,1} = k_{3,3}, k_{1,2} = k_{3,4}, k_{1,3} = k_{3,2}, k_{1,4} = k_{3,1}, k_{2,1} = k_{2,6}, k_{2,2} = k_{2,4}, k_{2,3} = k_{2,5}$.*

Proof. We suppose that $\mathcal{R}$ is of the second type, which means that the conjugation map permutes $\mathcal{I}_2$ and $\mathcal{I}_3$ as $\overline{\mathcal{I}}_2 = \mathcal{I}_3$, $\overline{\mathcal{I}}_3 = \mathcal{I}_2$, whereas $\overline{\mathcal{I}}_0 = \mathcal{I}_0$, $\overline{\mathcal{I}}_1 = \mathcal{I}_1$. In this case, we choose elements $e_2 := \overline{e}_3$ and $e_3 := \overline{e}_2$. Firstly, we define the matrix G^* over $\Phi(\mathcal{R}) = R$ as follows:

$$G^* = \begin{bmatrix} -\widetilde{A}_1^\top & B_3^* & O & O & O \\ -\widetilde{A}_2^\top & -\overline{M}_1^\top & B_2^* & O & O \\ -\widetilde{A}_3^\top & -\overline{M}_2^\top & -\overline{M}_3^\top & B_1^* & O \\ -\overline{D}_0^\top & -\overline{D}_1^\top & -\overline{D}_2^\top & -\overline{D}_3^\top & I_{k_4} \end{bmatrix} \tag{3}$$

with
$B_1^* = \operatorname{diag}\big((f_1+f_2+f_3)I_{k_{3,1}}, (f_0+f_2+f_3)I_{k_{3,2}}, (f_0+f_1+f_2)I_{k_{3,3}}, (f_0+f_1+f_3)I_{k_{3,4}}\big)$,
$B_2^* = \operatorname{diag}\big((f_2+f_3)I_{k_{2,1}}, (f_1+f_2)I_{k_{2,2}}, (f_1+f_3)I_{k_{2,3}}, (f_0+f_2)I_{k_{2,4}}, (f_0+f_3)I_{k_{2,5}}, (f_0+f_1)I_{k_{2,6}}\big)$,
$B_3^* = \operatorname{diag}\big(f_2 I_{k_{1,1}}, f_3 I_{k_{1,2}}, f_1 I_{k_{1,3}}, f_0 I_{k_{1,4}}\big)$,
$\widetilde{A}_1 = \big[f_2^2\overline{A}_{k_{1,1}}, f_3^2\overline{A}_{k_{1,2}}, f_1^2\overline{A}_{k_{1,3}}, f_0^2\overline{A}_{k_{1,4}}\big]$,
$\widetilde{A}_2 = \big[(f_2^2+f_3^2)\overline{A}_{k_{2,1}}, (f_1^2+f_2^2)\overline{A}_{k_{2,2}}, (f_1^2+f_3^2)\overline{A}_{k_{2,3}}, (f_0^2+f_2^2)\overline{A}_{k_{2,4}}, (f_0^2+f_3^2)\overline{A}_{k_{2,5}}, (f_0^2+f_1^2)\overline{A}_{k_{2,6}}\big]$,
$\widetilde{A}_3 = \big[(f_1^2+f_2^2+f_3^2)\overline{A}_{k_{3,1}}, (f_0^2+f_2^2+f_3^2)\overline{A}_{k_{3,2}}, (f_0^2+f_1^2+f_2^2)\overline{A}_{k_{3,3}}, (f_0^2+f_1^2+f_3^2)\overline{A}_{k_{3,4}}\big]$,
where $A_{k_{i,j}}$ is defined in (1) for $i = 1,2,3$, $j = 0,1,2,3$, and M_i and D_j are defined in (1) for $i = 1,2,3$ and $j = 0,1,2,3$.

Let $\mathcal{C}^*$ be a code generated by G^*. Then we claim that $\mathcal{C}^* \subset \mathcal{C}^\perp$ by showing $G\overline{G^*}^\top = O$. Considering the computation of $G\overline{G^*}^\top$, it is enough to show that the product of each block matrix of $\overline{G^*}$ with all the other block matrices of G is zero. Since

$$\overline{M}_1^\top = \begin{bmatrix} f_3\overline{M}_{k_{1,1},k_{2,1}}^\top & f_2\overline{M}_{k_{1,2},k_{2,1}}^\top & O_{k_{1,3},k_{2,1}}^\top & O_{k_{1,4},k_{2,1}}^\top \\ f_1\overline{M}_{k_{1,1},k_{2,2}}^\top & f_2\overline{M}_{k_{1,2},k_{2,2}}^\top & f_2\overline{M}_{k_{1,3},k_{2,2}}^\top & O_{k_{1,4},k_{2,2}}^\top \\ (f_1+f_3)\overline{M'}_{k_{1,1},k_{2,3}}^\top & f_1\overline{M}_{k_{1,2},k_{2,3}}^\top & f_3\overline{M}_{k_{1,3},k_{2,3}}^\top & O_{k_{1,4},k_{2,3}}^\top \\ f_0\overline{M}_{k_{1,1},k_{2,4}}^\top & f_2\overline{M}_{k_{1,2},k_{2,4}}^\top & f_2\overline{M}_{k_{1,3},k_{2,4}}^\top & f_2\overline{M}_{k_{1,4},k_{2,4}}^\top \\ (f_0+f_3)\overline{M'}_{k_{1,1},k_{2,5}}^\top & f_0\overline{M}_{k_{1,2},k_{2,5}}^\top & f_3\overline{M}_{k_{1,3},k_{2,5}}^\top & f_3\overline{M}_{k_{1,4},k_{2,5}}^\top \\ (f_0+f_1)\overline{M'}_{k_{1,1},k_{2,6}}^\top & (f_0+f_1)\overline{M'}_{k_{1,2},k_{2,6}}^\top & f_0\overline{M}_{k_{1,3},k_{2,6}}^\top & f_1\overline{M}_{k_{1,4},k_{2,6}}^\top \end{bmatrix},$$

$$\overline{M}_2^\top = \begin{bmatrix} (f_1+f_3)\overline{M}_{k_{1,1},k_{3,1}}^\top & (f_1+f_2)\overline{M}_{k_{1,2},k_{3,1}}^\top & (f_2+f_3)\overline{M}_{k_{1,3},k_{3,1}}^\top & (f_1+f_2+f_3)\overline{M''''}_{k_{1,4},k_{3,1}}^\top \\ (f_0+f_3)\overline{M}_{k_{1,1},k_{3,2}}^\top & (f_0+f_2)\overline{M}_{k_{1,2},k_{3,2}}^\top & (f_0+f_2+f_3)\overline{M'''}_{k_{1,3},k_{3,2}}^\top & (f_2+f_3)\overline{M}_{k_{1,4},k_{3,2}}^\top \\ (f_0+f_1)\overline{M}_{k_{1,1},k_{3,3}}^\top & (f_0+f_1+f_2)\overline{M''}_{k_{1,2},k_{3,3}}^\top & (f_0+f_2)\overline{M}_{k_{1,3},k_{3,3}}^\top & (f_1+f_2)\overline{M}_{k_{1,4},k_{3,3}}^\top \\ (f_0+f_1+f_3)\overline{M'}_{k_{1,1},k_{3,4}}^\top & (f_0+f_1)\overline{M}_{k_{1,2},k_{3,4}}^\top & (f_0+f_3)\overline{M}_{k_{1,3},k_{3,4}}^\top & (f_1+f_3)\overline{M}_{k_{1,4},k_{3,4}}^\top \end{bmatrix},$$

$$\overline{M}_3^\top = \begin{bmatrix} f_1\overline{M}_{k_{2,1},k_{3,1}}^\top & f_3\overline{M}_{k_{2,2},k_{3,1}}^\top & f_2\overline{M}_{k_{2,3},k_{3,1}}^\top & O_{k_{2,4},k_{3,1}}^\top & O_{k_{2,5},k_{3,1}}^\top & O_{k_{2,6},k_{3,1}}^\top \\ f_0\overline{M}_{k_{2,1},k_{3,2}}^\top & f_3\overline{M}_{k_{2,2},k_{3,2}}^\top & f_2\overline{M}_{k_{2,3},k_{3,2}}^\top & f_3\overline{M}_{k_{2,4},k_{3,2}}^\top & f_2\overline{M}_{k_{2,5},k_{3,2}}^\top & O_{k_{2,6},k_{3,2}}^\top \\ (f_0+f_1)\overline{M'}_{k_{2,1},k_{3,3}}^\top & f_0\overline{M}_{k_{2,2},k_{3,3}}^\top & f_2\overline{M}_{k_{2,3},k_{3,3}}^\top & f_1\overline{M}_{k_{2,4},k_{3,3}}^\top & f_2\overline{M}_{k_{2,5},k_{3,3}}^\top & f_2\overline{M}_{k_{2,6},k_{3,3}}^\top \\ (f_0+f_1)\overline{M'}_{k_{2,1},k_{3,4}}^\top & (f_0+f_3)\overline{M'}_{k_{2,2},k_{3,4}}^\top & f_0\overline{M}_{k_{2,3},k_{3,4}}^\top & (f_1+f_3)\overline{M'}_{k_{2,4},k_{3,4}}^\top & f_1\overline{M}_{k_{2,5},k_{3,4}}^\top & f_3\overline{M}_{k_{2,6},k_{3,4}}^\top \end{bmatrix},$$

where $M_{k_{i,j},k_{s,t}}$ are defined in (1), it is routine to check that $G\overline{G^*}^\top = O$ by direct computations of block matrices.

The fact that $G\overline{G^*}^\top = O$ implies $\mathcal{C}^* \subset \mathcal{C}^\perp = \mathcal{C}$. Comparing each rank of the generator matrix of $\mathcal{C}$ of the form (1) and the generator matrix of $\mathcal{C}^*$ of the form (3), we conclude that $k_{1,1} = k_{3,3}, k_{1,2} = k_{3,4}, k_{1,3} = k_{3,2}, k_{1,4} = k_{3,1}, k_{2,1} = k_{2,6}, k_{2,2} = k_{2,4}, k_{2,3} = k_{2,5}$. The free rank of $\mathcal{C}^*$ is less than or equal to the free rank of $\mathcal{C}$. Since $|\mathcal{C}| = |\mathcal{R}|^{l/2}$, it follows that $k_0 = k_4$. Therefore, we conclude that the code $\mathcal{C}^*$ generated by G^* is the Hermian dual of $\mathcal{C}$, and the theorem follows. □

We explicitly determine the forms of generator matrices of all self-dual codes over $\Phi(\mathcal{R})$ of length ≤ 4.

Proposition 4.2. *Let q be a power of 2 or a power of an odd prime with $q \equiv 1$ (mod 4). Let $\mathcal{R} = \mathbb{F}_q[X]/(X^m - 1)$ be a ring of the second type. Every self-dual code $\mathcal{C}$ over $\Phi(\mathcal{R})$ of length two is equivalent to a code with a generator matrix of one of the following cases:*

i) $G = \begin{bmatrix} 1 & a \end{bmatrix}$, where $a\overline{a} = -1$,

ii) $G = \begin{bmatrix} f_0 + f_1 + f_i & \alpha f_0 + \beta f_1 \\ 0 & f_i \end{bmatrix}$ for $i = 2$ or 3, where $\alpha \in \mathbb{F}_{q^{t_0}}$ and $\beta \in \mathbb{F}_{q^{t_1}}$ such that $\alpha\overline{\alpha} = \beta\overline{\beta} = -1$

Proof. i) It is straightforward by the definition of self-dual codes over $\Phi(\mathcal{R})$.

ii) If $\mathcal{C}$ is of free rank zero, then $\mathcal{C}$ has a generator matrix of the form $G = \begin{bmatrix} a_1 & a_2 \\ 0 & a_3 \end{bmatrix}$, up to equivalence. Since $\mathcal{C}$ is self-dual, we have $a_3 = f_i$, where $i = 2, 3$. By Theorems 3.1 and 4.1, we have that $a_1 = f_0 + f_1 + f_i$ and $a_2 = \alpha f_0 + \beta f_1$. □

Proposition 4.3. *Let q be a power of an even prime or odd prime with $q \equiv 1$ (mod 4). Let $\mathcal{R} = \mathbb{F}_q[X]/(X^m - 1)$ be a ring of the second type. Every self-dual code $\mathcal{C}$ over $\Phi(\mathcal{R})$ of length two is equivalent to a code with a generator matrix of one of the following cases:*

i) $G = \begin{bmatrix} 1 & 0 & a_1 & a_2 \\ 0 & 1 & a_3 & a_4 \end{bmatrix}$, where $a_1\overline{a}_1 + a_2\overline{a}_2 = -1$, $a_3\overline{a}_3 + a_4\overline{a}_4 = -1$, and $a_1\overline{a}_3 + a_2\overline{a}_4 = 0$.

ii) $G = \begin{bmatrix} 1 & b_1 & b_2 & b_3 \\ 0 & b_4 & b_5 & b_6 \\ 0 & 0 & b_7 & b_8 \end{bmatrix}$, where the values of b_4 and b_7 determine one of the following seven sub-cases (here, the coefficients $\alpha_i, \beta_i, \gamma_i$, and δ_i for all i are elements in $\mathbb{F}_{q^{t_0}}, \mathbb{F}_{q^{t_1}}, \mathbb{F}_{q^{t_2}}$, and $\mathbb{F}_{q^{t_3}}$, respectively.) :

ii-1) $b_4 = f_0 + f_1 + f_2$ and $b_7 = f_2$. In this case,

$b_1 = \delta_1 f_3$,
$b_2 = \alpha_1 f_0 + \beta_1 f_1 + \delta_2 f_3$,
$b_3 = \alpha_2 f_0 + \beta_2 f_1 + \gamma_1 f_2 + \delta_3 f_3$,
$b_5 = \alpha_3 f_0 + \beta_3 f_1$,
$b_6 = \alpha_4 f_0 + \beta_4 f_1 + \gamma_2 f_2$,
$b_8 = \gamma_3 f_2$

with $\alpha_1\overline{\alpha}_1 + \alpha_2\overline{\alpha}_2 = \beta_1\overline{\beta}_1 + \beta_2\overline{\beta}_2 = \gamma_1\overline{\delta}_3 = -1$, $\alpha_1\overline{\alpha}_3 + \alpha_2\overline{\alpha}_4 = \beta_1\overline{\beta}_3 + \beta_2\overline{\beta}_4 = \delta_1 + \delta_3\overline{\gamma}_2 = 0$, $\alpha_3\overline{\alpha}_3 + \alpha_4\overline{\alpha}_4 = -1$, $\beta_3\overline{\beta}_3 + \beta_4\overline{\beta}_4 = -1$, $\delta_2 + \delta_3\overline{\gamma}_3 = 0$.

ii-2) $b_4 = f_0 + f_1 + f_3$ *and* $b_7 = f_3$. *In this case,*
$b_1 = \gamma_1 f_2$,
$b_2 = \alpha_1 f_0 + \beta_1 f_1 + \gamma_2 f_2$,
$b_3 = \alpha_2 f_0 + \beta_2 f_1 + \gamma_3 f_2 + \delta_1 f_3$,
$b_5 = \alpha_3 f_0 + \beta_3 f_1$,
$b_6 = \alpha_4 f_0 + \beta_4 f_1 + \delta_2 f_3$,
$b_8 = \delta_3 f_3$ *with* $\gamma_2 + \gamma_3 \overline{\delta}_3$,
with $\alpha_1\overline{\alpha}_1 + \alpha_2\overline{\alpha}_2 = \beta_1\overline{\beta}_1 + \beta_2\overline{\beta}_2 = \gamma_3\overline{\delta}_1 = -1$, $\alpha_1\overline{\alpha}_3 + \alpha_2\overline{\alpha}_4 = \beta_1\overline{\beta}_3 + \beta_2\overline{\beta}_4 = \gamma_1 + \gamma_3\overline{\delta}_2 = 0, \alpha_3\overline{\alpha}_3 + \alpha_4\overline{\alpha}_4 = -1, \beta_3\overline{\beta}_3 + \beta_4\overline{\beta}_4 = -1.$

ii-3) $b_4 = f_0 + f_2 + f_3$ *and* $b_7 = f_1$. *In this case,*
$b_1 = \beta_1 f_1$,
$b_2 = \alpha_1 f_0 + \gamma_1 f_2 + \delta_1 f_3$,
$b_3 = \alpha_2 f_0 + \gamma_2 f_2 + \delta_2 f_3$,
$b_6 = \alpha_3 f_0 + \gamma_3 f_2 + \delta_3 f_3$,
$b_8 = \beta_2 f_1$, *with* $\alpha_1\overline{\alpha}_1 + \alpha_2\overline{\alpha}_2 = \beta_1\overline{\beta}_1 = \gamma_1\overline{\delta}_1 + \gamma_2\overline{\delta}_2 = -1$, $\beta_2\overline{\beta}_2 = -1$,
either $b_5 = \alpha_4 f_0$ *with* $\alpha_4\overline{\alpha}_4 + \alpha_3\overline{\alpha}_3 = \gamma_3\overline{\delta}_3 = -1, \alpha_1\overline{\alpha}_4 + \alpha_2\overline{\alpha}_3 = \gamma_2\overline{\delta}_3 = \delta_2\overline{\gamma}_3 = 0$, *or* $b_5 = \gamma_4 f_2 + \delta_4 f_3$ *with* $\alpha_3\overline{\alpha}_3 = \gamma_3\overline{\delta}_3 + \gamma_4\overline{\delta}_4 = -1, \alpha_2\overline{\alpha}_3 = \gamma_1\overline{\delta}_4 + \gamma_2\overline{\delta}_3 = \delta_1\overline{\gamma}_4 + \delta_2\overline{\gamma}_3 = 0$.

ii-4) $b_4 = f_1 + f_2 + f_3$ *and* $b_7 = f_0$. *In this case,*
$b_8 = \alpha_1 f_0$,
$b_1 = \alpha_2 f_0$,
$b_2 = \beta_1 f_1 + \gamma_1 f_2 + \delta_1 f_3$,
$b_3 = \beta_2 f_1 + \gamma_2 f_2 + \delta_2 f_3$,
$b_6 = \beta_3 f_1 + \gamma_3 f_2 + \delta_3 f_3$ *with* $\alpha_1\overline{\alpha}_1 = -1\alpha_2\overline{\alpha}_2 = \beta_1\overline{\beta}_1 + \beta_2\overline{\beta}_2 = \gamma_1\overline{\delta}_1 = -1$,
if $b_5 = \beta_4 f_1$ *then* $\gamma_2 = \delta_2 = 0, \beta_4\overline{\beta}_4 + \beta_3\overline{\beta}_3 = \gamma_3\overline{\delta}_3 = -1, \beta_1\overline{\beta}_4 + \beta_2\overline{\beta}_3 = 0$,
if $b_5 = \gamma_4 f_2$ *then* $\gamma_2 = 0, \beta_3\overline{\beta}_3 = \gamma_3\overline{\delta}_3 = -1, \delta_1\overline{\gamma}_4 + \delta_2\overline{\gamma}_3 = 0$,
if $b_5 = \delta_4 f_3$ *then* $\delta_2 = 0, \beta_3\overline{\beta}_3 = \gamma_3\overline{\delta}_3 = -1, \gamma_1\overline{\delta}_4 + \gamma_2\overline{\delta}_3 = 0$.

ii-5) $b_4 = f_0 + f_1$ *and* $b_7 = f_2 + f_3$. *In this case,*
$b_1 = \gamma_1 f_2 + \delta_1 f_3$,
$b_2 = \alpha_1 f_0 + \beta_1 f_1$,
$b_3 = \alpha_2 f_0 + \beta_2 f_1 + \gamma_2 f_2 + \delta_2 f_3$,
$b_5 = 0$,
$b_6 = \alpha_3 f_0 + \beta_3 f_1$,
$b_8 = \gamma_3 f_2 + \delta_3 f_3$ *with with* $\alpha_1\overline{\alpha}_1 + \alpha_2\overline{\alpha}_2 = \beta_1\overline{\beta}_1 + \beta_2\overline{\beta}_2 = \gamma_1\overline{\delta}_1 + \gamma_2\overline{\delta}_2 = -1$, $\alpha_3\overline{\alpha}_3 = \beta_3\overline{\beta}_3 = -1, \alpha_2\overline{\alpha}_3 = \beta_2\overline{\beta}_3 = 0$, $\gamma_3\overline{\delta}_3 = -1$, $\gamma_2\overline{\delta}_3 = \delta_2\overline{\gamma}_3 = 0$.

ii-6) $b_4 = f_0 + f_2$ *and* $b_7 = f_1 + f_2$. *In this case,*
$b_1 = \beta_1 f_1 + \delta_1 f_3$,
$b_2 = \alpha_1 f_0 + \delta_2 f_3$,
$b_3 = \alpha_2 f_0 + \beta_2 f_1 + \gamma_1 f_2 + \delta_3 f_3$,
$b_5 = 0$,
$b_6 = \alpha_3 f_0 + \gamma_2 f_2$,
$b_8 = \beta_3 f_1 + \gamma_3 f_2$ *with* $\alpha_1\overline{\alpha}_1 + \alpha_2\overline{\alpha}_2 = \beta_1\overline{\beta}_1 + \beta_2\overline{\beta}_2 = \gamma_1\overline{\delta}_3 = -1$, $\alpha_3\overline{\alpha}_3 = -1, \delta_1 + \delta_3\overline{\gamma}_2 = 0$, $\beta_3\overline{\beta}_3 = -1, \delta_2 + \delta_3\overline{\gamma}_3 = 0$.

ii-7) $b_4 = f_0 + f_3$ *and* $b_7 = f_1 + f_3$. *In this case,*
$b_1 = \beta_1 f_1 + \gamma_1 f_2$,
$b_2 = \alpha_1 f_0 + \gamma_2 f_2$,
$b_3 = \alpha_2 f_0 + \beta_2 f_1 + \gamma_3 f_2 + \delta_1 f_3$,

$b_5 = 0,$
$b_6 = \alpha_3 f_0 + \delta_2 f_3,$
$b_8 = \beta_3 f_1 + \delta_3 f_3$ *with* $\alpha_1\overline{\alpha}_1 + \alpha_2\overline{\alpha}_2 = \beta_1\overline{\beta}_1 + \beta_2\overline{\beta}_2 = \gamma_3\overline{\delta}_1 = -1,\ \alpha_3\overline{\alpha}_3 = -1, \gamma_1 + \gamma_3\overline{\delta}_2 = 0,\ \beta_3\overline{\beta}_3 = -1, \gamma_2 + \gamma_3\overline{\delta}_3 = 0.$

iii) $G = \begin{bmatrix} h_1 & h_2 & h_3 & h_4 \\ 0 & h_5 & h_6 & h_7 \\ 0 & 0 & h_8 & h_9 \\ 0 & 0 & 0 & h_{10} \end{bmatrix}$*, where the values of* h_1*,* h_5*,* h_8 *and* h_{10} *determine one of the following seven sub-cases(here, the coefficients* $\alpha_i, \beta_i, \gamma_i$*, and* δ_i *for all* i *are elements in* $\mathbb{F}_{q^{t_0}}, \mathbb{F}_{q^{t_1}}, \mathbb{F}_{q^{t_2}}$*, and* $\mathbb{F}_{q^{t_3}}$*, respectively.):*

iii-1) $h_1 = f_0 + f_1 + f_2, h_5 = f_0 + f_1 + f_2, h_8 = f_2, h_{10} = f_2$. *In this case,*
$h_2 = 0,$
$h_3 = \alpha_1 f_0 + \beta_1 f_1,$
$h_4 = \alpha_2 f_0 + \beta_2 f_1,$
$h_6 = \alpha_3 f_0 + \beta_3 f_1,$
$h_7 = \alpha_4 f_0 + \beta_4 f_1,$
$h_9 = 0$ *with* $\alpha_1\overline{\alpha}_1 + \alpha_2\overline{\alpha}_2 = -1, \beta_1\overline{\beta}_1 + \beta_2\overline{\beta}_2 = -1, \alpha_1\overline{\alpha}_3 + \alpha_2\overline{\alpha}_4 = 0, \beta_1\overline{\beta}_3 + \beta_2\overline{\beta}_4 = 0, \alpha_3\overline{\alpha}_3 + \alpha_4\overline{\alpha}_4 = -1, \beta_3\overline{\beta}_3 + \beta_4\overline{\beta}_4 = -1.$

iii-2) $h_1 = f_0 + f_1 + f_2, h_5 = f_0 + f_1 + f_3, h_8 = f_2, h_{10} = f_3$. *In this case,*
$h_2 = 0,$
$h_3 = \alpha_1 f_0 + \beta_1 f_1,$
$h_7 = \alpha_4 f_0 + \beta_4 f_1,$
$h_9 = 0,$
if $h_4 = \alpha_2 f_0$ *and* $h_6 = \alpha_3 f_0$ *then* $\alpha_1\overline{\alpha}_1 + \alpha_2\overline{\alpha}_2 = -1, \beta_1\overline{\beta}_1 = -1, \alpha_1\overline{\alpha}_3 + \alpha_2\overline{\alpha}_4 = 0, \alpha_3\overline{\alpha}_3 + \alpha_4\overline{\alpha}_4 = -1, \beta_4\overline{\beta}_4 = -1,$
if $h_4 = \beta_2 f_1$ *and* $h_6 = \beta_3 f_1$ *then* $\alpha_1\overline{\alpha}_1 = -1, \beta_1\overline{\beta}_1 + \beta_2\overline{\beta}_2 = -1, \beta_1\overline{\beta}_3 + \beta_2\overline{\beta}_4 = 0, \alpha_4\overline{\alpha}_4 = -1, \beta_3\overline{\beta}_3 + \beta_4\overline{\beta}_4 = -1.$

iii-3) $h_1 = f_0 + f_1 + f_2, h_5 = f_0 + f_2, h_8 = f_1 + f_2, h_{10} = f_2$. *In this case,*
$h_2 = \beta_1 f_1,$
$h_3 = \alpha_1 f_0,$
$h_4 = 0,$
$h_6 = 0,$
$h_7 = \alpha_2 f_0,$
$h_9 = \beta_2 f_1$ *with* $\beta_1\overline{\beta}_1 = -\alpha_1\overline{\alpha}_1 = \alpha_2\overline{\alpha}_2 = \beta_2\overline{\beta}_2 = -1.$

iii-4) $h_1 = f_0 + f_1 + f_3, h_5 = f_0 + f_1 + f_3, h_8 = f_3, h_{10} = f_3$. *In this case,*
$h_2 = 0,$
$h_3 = \alpha_1 f_0 + \beta_1 f_1,$
$h_4 = \alpha_2 f_0 + \beta_2 f_1,$
$h_6 = \alpha_3 f_0 + \beta_3 f_1,$
$h_7 = \alpha_4 f_0 + \beta_4 f_1,$
$h_9 = 0$ *with* $\alpha_1\overline{\alpha}_1 + \alpha_2\overline{\alpha}_2 = -1, \beta_1\overline{\beta}_1 + \beta_2\overline{\beta}_2 = -1, \alpha_1\overline{\alpha}_3 + \alpha_2\overline{\alpha}_4 = 0, \beta_1\overline{\beta}_3 + \beta_2\overline{\beta}_4 = 0, \alpha_3\overline{\alpha}_3 + \alpha_4\overline{\alpha}_4 = -1, \beta_3\overline{\beta}_3 + \beta_4\overline{\beta}_4 = -1.$

iii-5) $h_1 = f_0 + f_1 + f_3, h_5 = f_0 + f_3, h_8 = f_1 + f_3, h_{10} = f_3$. *In this case,*
$h_2 = \beta_1 f_1,$
$h_3 = \alpha_1 f_0,$
$h_4 = 0,$
$h_6 = 0,$

$h_7 = \alpha_2 f_0,$
$h_9 = \beta_2 f_1$ *with* $\beta_1\overline{\beta}_1 = \alpha_1\overline{\alpha}_1 = \alpha_2\overline{\alpha}_2 = \beta_2\overline{\beta}_2 = -1.$

iii-6) $h_1 = f_0 + f_2 + f_3, h_5 = f_0 + f_2 + f_3, h_8 = f_1, h_{10} = f_1$. *In this case,*
$h_2 = 0,$
$h_3 = \alpha_1 f_0,$
$h_4 = \gamma_1 f_2 + \delta_1 f_3,$
$h_6 = \gamma_2 f_2 + \delta_2 f_3,$
$h_7 = \alpha_2 f_0,$
$h_9 = 0$ *with* $\alpha_1\overline{\alpha}_1 = \gamma_1\overline{\delta}_1 = \gamma_2\overline{\delta}_2 = \alpha_2\overline{\alpha}_2 = -1.$

iii-7) $h_1 = f_0 + f_2 + f_3, h_5 = f_1 + f_2 + f_3, h_8 = f_0, h_{10} = f_1$. *In this case,*
$h_2 = 0,$
$h_3 = \gamma_1 f_2 + \delta_1 f_3,$
$h_4 = \alpha_1 f_0,$
$h_6 = \beta_1 f_1,$
$h_7 = \gamma_2 f_2 + \delta_2 f_3,$
$h_9 = 0$ *with* $\gamma_1\overline{\delta}_1 = \alpha_1\overline{\alpha}_1 = \beta_1\overline{\beta}_1 = \gamma_2\overline{\delta}_2 = -1.$

Proof. It is straightforward, as evident from Theorems 3.1 and 4.1. □

References

[1] E. F. Assmus and J. D. Key, *Designs and Their Codes*, Cambridge: Cambridge University Press, 1992.

[2] I. Bouyukliev, D. Bikov and S. Bouyuklieva, *S-Boxes from binary quasi-cyclic codes*, Electronic Notes in Discrete Mathematics **57** (2017), 67–72.
https://doi.org/10.1016/j.endm.2017.02.012

[3] J. H. Conway and N. J. A. Sloane, *Sphere Packing, Lattices and Groups*, 3rd ed., New York: Springer-Verlag, 1999.

[4] W. Ebeling, *Lattices and Codes: A Course Partially Based on Lectures by F. Hirzebruch*, Advanced Lectures in Mathematics, Braunschweig: Vieweg, 1994.

[5] M. Esmaeili, T. A. Gulliver, N. P. Secord and S. A. Mahmoud, *A link between quasi-cyclic codes and convolution codes*, IEEE Transactions on Information Theory **44** (1998), 431–435.
https://doi.org/10.1109/18.651076

[6] S. Han, J. L. Kim, H. Lee and Y. Lee, *Construction of quasi-cyclic self-dual codes*, Finite Fields and Their Applications **18** (2012), 612–633.
https://doi.org/10.1016/j.ffa.2011.12.006

[7] W. C. Huffman, *Automorphisms of codes with applications to extremal doubly even codes of length 48*, IEEE Transactions on Information Theory **28** (1982), 511–521.
https://doi.org/10.1109/TIT.1982.1056499

[8] T. Kasami, *A Gilbert–Varshamov bound for quasi-cyclic codes of rate 1/2*, IEEE Transactions on Information Theory **20** (1974), 679.
https://doi.org/10.1109/TIT.1974.1055262

[9] H. J. Kim and Y. Lee, *Extremal quasi-cyclic self-dual codes over finite fields*, Finite Fields and Their Applications **52** (2018), 301–318.
https://doi.org/10.1016/j.ffa.2018.04.013

[10] S. Ling and P. Solé, *On the algebraic structure of quasi-cyclic codes I: finite fields*, IEEE Transactions on Information Theory **47** (2001), 2751–2760.
https://doi.org/10.1109/18.959257

[11] S. Ling and P. Solé, *On the algebraic structure of quasi-cyclic codes II: chain rings*, Designs, Codes and Cryptography **30** (2003), 113–130.
https://doi.org/10.1023/A:1024715527805

[12] S. Ling and P. Solé, *On the algebraic structure of quasi-cyclic codes III: generator theory*, IEEE Transactions on Information Theory **51** (2005), 2692–2700.
https://doi.org/10.1109/TIT.2005.850142

[13] G. Nebe, E. M. Rains and N. J. A. Sloane, *Self-Dual Codes and Invariant Theory*, Berlin: Springer, 2006.

[14] V. Yorgov, *Binary self-dual codes with automorphism of odd order*, Problems of Information Transmission **19** (1983), 260–270.

[15] W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system I: the user language*, Journal of Symbolic Computation **24** (1997), 235–265.

Hyun Jin Kim
University College, Yonsei University, Incheon 21983, Republic of Korea.
E-mail: guswls41@yonsei.ac.kr

Whan-Hyuk Choi
[1]Kangwon Research Institute of Mathematical Sciences,
Kangwon National University, Chuncheon 24341, Republic of Korea.

[2]Department of Mathematics, Kangwon National University,
Chuncheon, 24341, Republic of Korea.
E-mail: whchoi@kangwon.ac.kr

Jung-Kyung Lee
College of Liberal Arts, Anyang University, Anyang 14028, Republic of Korea.
E-mail: leejk@anyang.ac.kr