JOURNAL OF THE
CHUNGCHEONG MATHEMATICAL SOCIETY
Volume **33**, No. 2, May 2020
http://dx.doi.org/10.14403/jcms.2020.33.2.255

ON THE EXISTENCE OF MDS SELF-DUAL CODES OVER FINITE CHAIN RINGS

Sunghyu Han*

Abstract. We studied the MDS self-dual codes over finite chain rings. We stated the projection and lifting of codes over the finite chain rings with respect to the MDS self-dual codes, and then we applied the results to the MDS self-dual codes over Galois rings.

1. Introduction

Coding theory started with binary codes, meaning, codes over $\mathbb{F}_2$. Then, it was developed for codes over finite fields $\mathbb{F}_{p^r}$ and various rings. Among the various rings, there have been many studies on codes over $\mathbb{Z}_{p^m}$. The Galois rings $GR(p^m, r)$ contain $\mathbb{F}_{p^r}$ and $\mathbb{Z}_{p^m}$. In this study, we were interested in the linear codes over Galois rings, more generally, the linear codes over the finite chain rings that contain Galois rings.

In coding theory, the minimum distance is very important because it indicates the ability of the codes for error correction. Therefore, maximum distance separable (MDS) codes have attracted much attention. Moreover, self-dual codes have also been investigated, because they are closely related to other mathematical structures such as block designs, lattices, modular forms, and sphere packings [13]. Codes that contain both structures, termed MDS self-dual codes, have been investigated for finite fields [6], finite rings $\mathbb{Z}_{p^m}$ [10], and nontrivial Galois rings $GR(p^m, r)$. For the $p = 2$ case in $GR(p^m, r)$, the codes were investigated in [2], and using an extended Reed-Solomon codes, MDS self-dual codes of length $n = 2^r$ were constructed. For $p \equiv 1 \pmod 4$ with any r or $p \equiv -1 \pmod 4$ with even r in $GR(p^m, r)$, the codes were studied in [9], and using the building-up construction, various MDS self-dual

Received April 05, 2020; Accepted April 18, 2020.
2010 Mathematics Subject Classification: Primary 94B05.
Key words and phrases: finite chain ring, Galois ring, MDS code, self-dual code.
*Supported by Education and Research promotion program of KOREATECH in 2020.

codes over $GR(p^m, 2)$ were constructed. For $p \equiv -1 \pmod 4$ with odd r in $GR(p^m, r)$, the codes were studied in [8], and using the building-up construction, various MDS self-dual codes over $GR(p^m, 3)$ were constructed.

In [4], Dougherty et al. studied the projection and lifting of codes over finite chain rings. They also studied the minimum distance, MDS codes, and self-dual codes related to the projection and lifting of codes over finite chain rings. In this study, we continued their research to investigate MDS self-dual codes over Galois rings. The results of this study were as follows. First, we stated the projection and lifting of codes over finite chain rings with respect to the MDS self-dual codes. Second, we applied the first result to study the MDS self-dual codes over Galois rings.

This paper is organized as follows. In Section 2, we provide basic facts for finite chain rings, Galois rings, linear codes, self-dual codes, and MDS codes. In Section 3, we show our first main result, which is about the relationship between the projection and lifting for MDS self-dual codes over finite chain rings. In Section 4, we show our second main result, which is about MDS self-dual codes over Galois rings using the results from section 3. All computations in this paper were performed using the computer algebra system Magma [1].

2. Preliminaries

In this section, we provided basic facts for finite chain rings, Galois rings, linear codes, self-dual codes, and MDS codes.

2.1. Finite chain rings

In this subsection, we gave various facts about finite chain rings [4]. Let R be a finite chain ring, $\mathfrak{m}$ be the unique maximal ideal of R, and γ be the generator of the unique maximal ideal $\mathfrak{m}$. Then $\mathfrak{m} = \langle\gamma\rangle = R\gamma$, where $R\gamma = \langle\gamma\rangle = \{\beta\gamma \mid \beta \in R\}$. We have:

$$R = \langle\gamma^0\rangle \supset \langle\gamma^1\rangle \supset \cdots \supset \langle\gamma^i\rangle \supset \cdots \supset \langle\gamma^e\rangle = \{0\}. \tag{2.1}$$

Let e be the minimal number such that $\langle\gamma^e\rangle = \{0\}$. The number e is called the nilpotency index of γ.

Let $\mathbb{F} = R/\mathfrak{m} = R/\langle\gamma\rangle$ be the residue field with characteristic p, where p is a prime number. We know that $|\mathbb{F}| = q = p^r$ for some integers q and r. The following lemma is known [12]:

LEMMA 2.1. *Let R be a finite chain ring with maximal ideal $\mathfrak{m} = \langle\gamma\rangle$, where γ is a generator of $\mathfrak{m}$ with nilpotency index e. For any $0 \neq r \in R$ there is a unique integer i, $0 \leq i < e$ such that $r = \mu\gamma^i$, with μ a unit. The unit μ is unique modulo γ^{e-i}. Let $V \subseteq R$ be a set of representatives for the equivalence classes of R under congruence modulo γ. Then*

1. *for all $r \in R$ there exist unique $r_0, \ldots, r_{e-1} \in V$ such that $r = \sum_{i=0}^{e-1} r_i\gamma^i$;*
2. *$|V| = |\mathbb{F}|$;*
3. *$|\langle\gamma^j\rangle| = |\mathbb{F}|^{e-j}$ for $0 \leq j \leq e-1$.*

By Lemma 2.1, the cardinality of R is

$$|R| = |\mathbb{F}| \cdot |\langle\gamma\rangle| = |\mathbb{F}| \cdot |\mathbb{F}|^{e-1} = |\mathbb{F}|^e = p^{er}. \tag{2.2}$$

We also know that for any element a of R, it can be written uniquely as

$$a = a_0 + a_1\gamma + a_2\gamma^2 + \cdots + a_{e-1}\gamma^{e-1}, \tag{2.3}$$

where $a_i \in \mathbb{F}$. For an arbitrary positive integer i, we define R_i as

$$R_i = \{a_0 + a_1\gamma + a_2\gamma^2 + \cdots + a_{i-1}\gamma^{i-1} \mid a_i \in \mathbb{F}\} \tag{2.4}$$

where $\gamma^{i-1} \neq 0$, but $\gamma^i = 0$ in R_i, and define two operations over R_i as

$$\sum_{l=0}^{i-1} a_l\gamma^l + \sum_{l=0}^{i-1} b_l\gamma^l = \sum_{l=0}^{i-1}(a_l + b_l)\gamma^l \tag{2.5}$$

$$\sum_{l=0}^{i-1} a_l\gamma^l \cdot \sum_{l'=0}^{i-1} b_{l'}\gamma^{l'} = \sum_{s=0}^{i-1}\Big(\sum_{l+l'=s} a_l b_{l'}\Big)\gamma^s \tag{2.6}$$

It can be seen that all R_i are finite rings. We define R_∞ as the ring of formal power series as follows:

$$R_\infty = \mathbb{F}[[\gamma]] = \{\sum_{l=0}^{\infty} a_l\gamma^l \mid a_l \in \mathbb{F}\}. \tag{2.7}$$

For two positive integers $i < j$, we define a map as follows:

$$\Psi_i^j : R_j \to R_i \tag{2.8}$$

$$\sum_{l=0}^{j-1} a_l\gamma^l \mapsto \sum_{l=0}^{i-1} a_l\gamma^l \tag{2.9}$$

If we replace R_j with R_∞, then we denote Ψ_i^∞ by Ψ_i. Let a and b be two arbitrary elements in R_j. Hence, we obtain

$$\Psi_i^j(a+b) = \Psi_i^j(a) + \Psi_i^j(b), \ \Psi_i^j(ab) = \Psi_i^j(a)\Psi_i^j(b). \tag{2.10}$$

If $a, b \in R_\infty$, we have

$$\Psi_i(a+b) = \Psi_i(a) + \Psi_i(b),\ \Psi_i(ab) = \Psi_i(a)\Psi_i(b). \tag{2.11}$$

We note that the two maps Ψ_i and Ψ_i^j can be extended naturally from R_∞^n to R_i^n and R_j^n to R_i^n, respectively.

2.2. Galois rings

In this subsection, we provide various facts about Galois rings [14]. Let p and m be a fixed prime and positive integer, respectively. First, consider the following canonical projection:

$$\mu : \mathbb{Z}_{p^m} \to \mathbb{Z}_p \tag{2.12}$$

which is defined by

$$\mu(c) = c \pmod{p}. \tag{2.13}$$

The Map μ can be extended naturally to the following map:

$$\mu : \mathbb{Z}_{p^m}[x] \to \mathbb{Z}_p[x] \tag{2.14}$$

which is defined by

$$\mu(b_0 + b_1 x + \cdots + b_n x^n) = \mu(b_0) + \mu(b_1)x + \cdots + \mu(b_n)x^n. \tag{2.15}$$

This extended μ is a ring homomorphism with kernel (p).

Let $f(x)$ be a polynomial in $\mathbb{Z}_{p^m}[x]$. Then, $f(x)$ is called basic irreducible if $\mu(f(x))$ is irreducible. The Galois ring is constructed as

$$GR(p^m, r) = \mathbb{Z}_{p^m}[x]/(f(x)), \tag{2.16}$$

where $f(x)$ is a monic basic irreducible polynomial in $\mathbb{Z}_{p^m}[x]$ of degree r. The elements of $GR(p^m, r)$ are the residue classes of the form

$$b_0 + b_1 x + \cdots + b_{r-1}x^{r-1} + (f(x)), \tag{2.17}$$

where $b_i \in \mathbb{Z}_{p^m} (0 \le i \le r-1)$.

A polynomial $h(x)$ in $\mathbb{Z}_{p^m}[x]$ is called a basic primitive polynomial if $\mu(h(x))$ is a primitive polynomial. It is known fact that there is a monic basic primitive polynomial $h(x)$ of degree r over $\mathbb{Z}_{p^m}$ and $h(x)|(x^{p^r-1}-1)$ in $\mathbb{Z}_{p^m}[x]$. Let $h(x)$ be a monic basic primitive polynomial in $\mathbb{Z}_{p^m}[x]$ of degree r. Consider the following element:

$$\xi = x + (h(x)) \in GR(p^m, r) = \mathbb{Z}_{p^m}[x]/(h(x)). \tag{2.18}$$

Then, the order of ξ is $p^r - 1$. Teichmüller representatives are defined as follows:

$$T = \{0, 1, \xi, \xi^2, \ldots, \xi^{p^r-2}\}. \tag{2.19}$$

Then, every element $a \in GR(p^m, r)$ can be uniquely represented by the form

$$a = a_0 + a_1 p + a_2 p^2 + \cdots + a_{m-1} p^{m-1}, \tag{2.20}$$

where $a_i \in T, (0 \le i \le m-1)$.

The Galois ring $GR(p^m, r)$ is a finite chain ring of length m, and its ideals are linearly ordered by inclusion,

$$GR(p^m, r) = \langle p^0 \rangle \supset \langle p^1 \rangle \supset \cdots \supset \langle p^i \rangle \supset \cdots \supset \langle p^m \rangle = \{0\}. \tag{2.21}$$

The p and m in this subsection correspond to γ and e in subsection 2.1, respectively.

2.3. Codes over finite chain rings

Let R be a finite chain ring. An R-submodule $C \le R^n$ is called a linear code of length n over R. Unless otherwise specified all codes are assumed linear. The elements in C are called codewords. The weight of a codeword $c = (c_1, c_2, \ldots, c_n)$ in C is the number of nonzero $c_j, (1 \le j \le n)$. The minimum weight of C is the smallest nonzero weight of any codeword in C.

We define the inner product, that is, for $\mathbf{x}, \mathbf{y} \in R^n$, we define

$$\mathbf{x} \cdot \mathbf{y} = x_1 y_1 + \cdots + x_n y_n. \tag{2.22}$$

For a code C of length n over R, let

$$C^{\perp} = \{\mathbf{x} \in R^n \,\big|\, \mathbf{x} \cdot \mathbf{c} = 0, \forall\, \mathbf{c} \in C\} \tag{2.23}$$

be the dual code of C. If $C \subseteq C^{\perp}$, then we say that C is self-orthogonal, and if $C = C^{\perp}$, then we say that C is self-dual.

In [15], it was proven that for a linear code C over a Frobenius ring,

$$|C| \cdot |C^{\perp}| = |R|^n. \tag{2.24}$$

Note that finite chain rings are Frobenius [3].

It is known that a generator matrix for a code C over a finite chain ring is permutation-equivalent to a matrix of the form

$$G = \begin{pmatrix} I_{k_0} & A_{0,1} & A_{0,2} & A_{0,3} & \cdots & A_{0,e-1} & A_{0,e} \\ 0 & \gamma I_{k_1} & \gamma A_{1,2} & \gamma A_{1,3} & \cdots & \gamma A_{1,e-1} & \gamma A_{1,e} \\ 0 & 0 & \gamma^2 I_{k_2} & \gamma^2 A_{2,3} & \cdots & \gamma^2 A_{2,e-1} & \gamma^2 A_{2,e} \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & \gamma^{e-1} I_{k_{e-1}} & \gamma^{e-1} A_{e-1,e} \end{pmatrix}, \tag{2.25}$$

where e is the nilpotency index of γ. The generator matrix G is said to be in a standard form. All generator matrices in a standard

form for a code C over a finite chain ring have the same parameters $k_0, k_1, k_2, \ldots, k_{e-1}$ [12, Theorem 3.3]. The rank of C, denoted by $\mathrm{rank}(C)$, is defined as the number of nonzero rows of its generator matrix G in a standard form. Therefore $\mathrm{rank}(C) = \sum_{i=0}^{e-1} k_i$. We call k_0 in G the free rank of a code C. If $\mathrm{rank}(C) = k_0$, then C is called a free code. We say that C is an $[n, k, d]$ linear code, if the code length is n, the rank of C is k, and the minimum weight of C is d. It is immediate that a code C with the generator matrix in Equation (2.25) has cardinality

(2.26)
$$|C| = |\mathbb{F}|^{\sum_{i=0}^{e-1}(e-i)k_i} = (p^r)^{\sum_{i=0}^{e-1}(e-i)k_i} = (p^{re})^{k_0}(p^{r(e-1)})^{k_1}\cdots(p^r)^{k_{e-1}}.$$

In this case, the code C is said to have the type:

(2.27)
$$1^{k_0}(\gamma)^{k_1}(\gamma^2)^{k_2}\cdots(\gamma^{e-1})^{k_{e-1}}.$$

2.4. Codes over R_∞

In this subsection we are interested in codes over R_∞. See [4] for detailed information. Most terminologies in the previous subsection can be similarly defined for codes over R_∞. Specifically, linear codes over R_∞, codewords, minimum weight, inner product, dual code, self-orthogonal, and self-dual are defined in the same way as that of the previous subsection.

Let $\mathcal{C}$ be a nonzero linear code over R_∞ of length n, then any generator matrix of $\mathcal{C}$ is permutation equivalent to a matrix of the following form:

(2.28)
$$G = \begin{pmatrix} \gamma^{m_0}I_{k_0} & \gamma^{m_0}A_{0,1} & \gamma^{m_0}A_{0,2} & \gamma^{m_0}A_{0,3} & \cdots & \gamma^{m_0}A_{0,r-1} & \gamma^{m_0}A_{0,r} \\ 0 & \gamma^{m_1}I_{k_1} & \gamma^{m_1}A_{1,2} & \gamma^{m_1}A_{1,3} & \cdots & \gamma^{m_1}A_{1,r-1} & \gamma^{m_1}A_{1,r} \\ 0 & 0 & \gamma^{m_2}I_{k_2} & \gamma^{m_2}A_{2,3} & \cdots & \gamma^{m_2}A_{2,r-1} & \gamma^{m_2}A_{2,r} \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & \gamma^{m_{r-1}}I_{k_{r-1}} & \gamma^{m_{r-1}}A_{r-1,r} \end{pmatrix},$$

where $0 \le m_0 < m_1 < \cdots < m_{r-1}$ for some integer r. The column blocks have sizes $k_0, k_1, \ldots, k_{r-1}$, and the $k_i (0 \le i \le r-1)$ are nonnegative integers. The generator matrix G is said to be in a standard form. The rank of $\mathcal{C}$ is defined as follows:

(2.29)
$$\mathrm{rank}(\mathcal{C}) = k = \sum_{i=0}^{r-1} k_i.$$

A code $\mathcal{C}$ of length n with rank k over R_∞ is called a γ-adic $[n, k]$ code. A code $\mathcal{C}$ with generator matrix of the form given in Equation (2.28) is said to be of type

(2.30)
$$(\gamma^{m_0})^{k_0}(\gamma^{m_1})^{k_1}\cdots(\gamma^{m_{r-1}})^{k_{r-1}}.$$

We say that $\mathcal{C}$ is free if $\mathcal{C}$ has type 1^k.

Let i and j be two integers such that $1 \leq i \leq j < \infty$. We say that an $[n,k]$ code C_1 over R_i lifts to an $[n,k]$ code C_2 over R_j, denoted by $C_1 \preceq C_2$, if C_2 has a generator matrix G_2 such that $\Psi_i^j(G_2)$ is a generator of C_1. Hence, it can be proven that $C_1 = \Psi_i^j(C_2)$. If $\mathcal{C}$ is an $[n,k]$ γ-adic code, then for any $i < \infty$, we call $\Psi_i(\mathcal{C})$ a projection of $\mathcal{C}$. We denote $\Psi_i(\mathcal{C})$ using $\mathcal{C}^i$.

We know that for a γ-adic $[n,k]$ code $\mathcal{C}$ of type 1^k, $\mathcal{C}^i = \Psi_i(\mathcal{C})$ is an $[n,k]$ code of type 1^k over R_i. In the following, we consider codes over chain rings that are projections of γ-adic codes. Note that $\mathcal{C}^i \preceq \mathcal{C}^{i+1}$ for all i. Thus if a code $\mathcal{C}$ over R_∞ of type 1^k is given, then we obtain a series of lifts of codes as follows:

$$\mathcal{C}^1 \preceq \mathcal{C}^2 \preceq \cdots \preceq \mathcal{C}^i \preceq \cdots \tag{2.31}$$

Conversely, let C_1 be an $[n,k]$ code over $\mathbb{F} = R/\langle\gamma\rangle = R_1$, and let G_1 be its generator matrix. It is clear that we can define a series of generator matrices $G_{i+1} \in M_{k\times n}(R_{i+1})$ such that $\Psi_i^{i+1}(G_{i+1}) = G_i$, $(i \geq 1)$, where $M_{k\times n}(R_i)$ denotes all the matrices with k rows and n columns over R_i. This defines a series of lifts C_i of C_1 to R_i for all $i \geq 2$. Then, this series of lifts determines a code $\mathcal{C}$ such that $\mathcal{C}^i = C_i$, where the code is not necessarily unique.

2.5. MDS codes

It is known [11] that for a (linear or nonlinear) code C of length n over any finite alphabet A

$$d \leq n - \log_{|A|}(|C|) + 1. \tag{2.32}$$

Codes meeting this bound are called MDS codes. Further, if C is a linear code over a finite chain ring, then

$$d \leq n - \operatorname{rank}(C) + 1. \tag{2.33}$$

Codes meeting this bound are called MDR (Maximum Distance with respect to Rank) codes [5, 12]. MDR codes do not imply MDS codes. See the following example.

Example 2.2. *Let C be a linear code generated by $G = (2)$ over $\mathbb{Z}_4$. Then, $n = 1$, $\operatorname{rank}(C) = 1$, and $d = 1$. Therefore, C is MDR code. Because $\log_{|A|}(|C|) = \log_4 2 = \frac{1}{2}$, C is not MDS.*

The following lemma states the necessary and sufficient condition for MDS codes.

LEMMA 2.3. *Let C be a linear code over a finite chain ring R. Then, C is MDS if and only if C is MDR and free.*

Proof. Suppose that C is MDS. If C is not free, then $\log_{|R|}(|C|) < \mathrm{rank}(C)$. Therefore, $d \leq n - \mathrm{rank}(C) + 1 < n - \log_{|R|}(|C|) + 1$. However, this is a contradiction. Hence, C should be free and $\log_{|R|}(|C|) = \mathrm{rank}(C)$. Therefore, C is MDR.

Suppose that C is MDR and free. Let $\mathrm{rank}(C) = k$ and $|R| = p^{er}$. Then, $|C| = (p^{er})^k$. Because $|R| = p^{er}$, we have $\log_{|R|}(|C|) = k = \mathrm{rank}(C)$. Therefore, C is MDS. □

The following theorem states that the weight distribution of MDS codes over $GR(p^m, r)$ of code length n is uniquely determined.

THEOREM 2.4. [12, Theorem 5.10] *Let C be a MDS code over $GR(p^m, r)$ of code length n and minimum weight d. For $d \leq w \leq n$, denote by A_w the number of words of weight w in C. Then,*

$$A_w = \binom{n}{w} \sum_{i=0}^{w-d} \binom{w}{i} \left(p^{mr(w+1-d-i)} - 1\right). \tag{2.34}$$

For codes over R_∞ we say that an MDR code is MDS if it is of type 1^k for some k. For a code C over a finite chain ring (or R_∞), we say that C is an MDS self-dual code if C is MDS and self-dual.

3. MDS self-dual codes over finite chain rings

In this section, we state the projection and lifting of codes over finite chain rings with respect to MDS self-dual codes. We start with the following theorem:

THEOREM 3.1. [4, Theorem 2.11] *Let $\mathcal{C}$ be a γ-adic $[n, k]$ code of type 1^k. Then the following two results are true.*

1. *the minimum Hamming distance $d_H(\mathcal{C}^i)$ of C^i is $d = d_H(\mathcal{C}^1)$ for all $1 \leq i < \infty$;*
2. *the minimum Hamming distance $d_\infty = d_H(\mathcal{C})$ of $\mathcal{C}$ is at least $d = d_H(\mathcal{C}^1)$.*

From the above theorem, we can obtain the following:

THEOREM 3.2. *If C is an MDS code over R_j $(1 < j < \infty)$ then $\Psi_i^j(C)$ is an MDS code over R_i for all $1 \leq i < j$.*

Proof. Because C is an MDS code over R_j $(1 < j < \infty)$, C is an $[n, k, d]$ code of type 1^k, $d = n - k + 1$, and with a generator matrix $G = [I \mid A]$. Let $\mathcal{C}$ be a γ-adic code with the same generator matrix G. Then $\mathcal{C}$ is a γ-adic $[n, k]$ code of type 1^k, $C = \mathcal{C}^j$, and $\Psi_i^j(C) = \Psi_i(\mathcal{C}) = \mathcal{C}^i$. Thus, according to Theorem 3.1, $d(\Psi_i^j(C)) = d(C) = n - k + 1$. Clearly, $\Psi_i^j(C)$ is free. Therefore, $\Psi_i^j(C)$ is MDS. □

THEOREM 3.3. [4, Theorem 2.13] *Let C be a linear code over R_i, and $\tilde{C}$ be a lifted code of C over R_j, where $j > i$. If C is an MDS code over R_i then $\tilde{C}$ is an MDS code over R_j.*

THEOREM 3.4. [4, Theorem 3.4] *If $\mathcal{C}$ is a self-dual code of length n over R_∞, then $\Psi_i(\mathcal{C})$ is a self-dual code of length n over R_i for all $1 \le i < \infty$.*

From the above theorem, we can obtain the following:

THEOREM 3.5. *If C is a free self-dual code of length n over R_j $(1 \le j \le \infty)$, then $\Psi_i^j(C)$ is a free self-dual code of length n over R_i for all $1 \le i < j$.*

Proof. Let C be an $[n, k]$ self-dual code. Because C is free, C has a generator matrix $G = [I|A]$. Suppose that $j = \infty$. Then, following Theorem 3.4, $\Psi_i^j(C)$ is self-dual for all $1 \le i < j$. Clearly, $\Psi_i^j(C)$ is free. Suppose that $j < \infty$. Let $\mathbf{v}$ and $\mathbf{w}$ be codewords in C. Then, we have

$$[\mathbf{v}, \mathbf{w}] = \sum_{l=1}^{n} v_l w_l \equiv 0 \pmod{\gamma^j}. \tag{3.1}$$

So,

$$\Psi_i^j([\mathbf{v}, \mathbf{w}]) \equiv 0 \pmod{\gamma^i}. \tag{3.2}$$

Note that

$$\Psi_i^j([\mathbf{v}, \mathbf{w}]) = \Psi_i^j\Big(\sum_{l=1}^{n} v_l w_l\Big) = \sum_{l=1}^{n} \Psi_i^j(v_l)\Psi_i^j(w_l) = [\Psi_i^j(\mathbf{v}), \Psi_i^j(\mathbf{w})]. \tag{3.3}$$

Thus, $\Psi_i^j(C)$ is self-orthogonal. Note that $\Psi_i^j(C)$ is free. Using Eqn. (2.24), we can conclude that $\Psi_i^j(C)$ is self-dual. □

The following theorem can be found in [4]: The proof is important in this study; hence, it was included.

THEOREM 3.6. [4, Theorem 3.7] *Let R be a finite chain ring, $\mathbb{F} = R/\langle\gamma\rangle$, where $|\mathbb{F}| = q = p^r, 2 \neq p$ a prime. Then, any self-dual code C over $\mathbb{F}$ can be lifted to a self-dual code over R_∞.*

Proof. Let $G_1 = (I|A_1)$ be a generator matrix of C over $R_1(= \mathbb{F})$. Because C is self-orthogonal, we have:

$$I + A_1 A_1^T \equiv 0 \pmod{\gamma}. \tag{3.4}$$

We show in the following by induction that there exist matrices $G_i = (I|A_i)$ such that $\Psi_i^{i+1}(G_{i+1}) = G_i$ and $I + A_i A_i^T \equiv 0 \pmod{\gamma^i}$ for all i. Suppose we have that $I + A_i A_i^T = \gamma^i S_i$. Let $A_{i+1} = A_i + \gamma^i M$, we want to find a matrix M such that

$$I + A_{i+1} A_{i+1}^T \equiv 0 \pmod{\gamma}^{i+1}. \tag{3.5}$$

We know that

$$I + A_{i+1} A_{i+1}^T = I + A_i A_i^T + \gamma^i (A_i M^T + M A_i^T) = \gamma^i (S_i + A_i M^T + M A_i^T). \tag{3.6}$$

This indicates that the matrix M should satisfy

$$S_i + A_i M^T + M A_i^T \equiv 0 \pmod{\gamma}. \tag{3.7}$$

Let $M \equiv 2^{-1} S_i A_i \pmod{\gamma}$. Then

$$\begin{aligned} S_i + A_i M^T + M A_i^T &\equiv S_i + 2^{-1}(A_i A_i^T S_i^T + S_i A_i A_i^T) \\ &\equiv S_i + 2^{-1}(-S_i - S_i) \equiv 0 \pmod{\gamma}. \end{aligned} \tag{3.8}$$

Therefore, $2^{-1} S_i A_i \pmod{\gamma}$ is a solution for M. □

From the above theorem, we can obtain the following:

THEOREM 3.7. *Let R be a finite chain ring, $\mathbb{F} = R/\langle\gamma\rangle$, where $|\mathbb{F}| = q = p^r, 2 \neq p$ a prime. Let C be a free self-dual code over R_i $(1 \leq i < \infty)$. Then, C can be lifted to a self-dual code over R_j $(1 < j \leq \infty)$.*

Proof. The proof is almost the same as that of the above theorem. □

From the above, we can obtain the following:

THEOREM 3.8. *If C is an MDS self-dual code of length n over R_j $(1 \leq j < \infty)$, then $\Psi_i^j(C)$ is an MDS self-dual code of length n over R_i for all $1 \leq i < j$.*

Proof. Using Theorems 3.2 and 3.5. □

THEOREM 3.9. *Let R be a finite chain ring, $\mathbb{F} = R/\langle\gamma\rangle$, where $|\mathbb{F}| = q = p^r, 2 \neq p$ a prime. Let C be an MDS self-dual code over R_i $(1 \leq i < \infty)$. Then, C can be lifted to an MDS self-dual code over R_j $(1 < j \leq \infty)$.*

Proof. Using Theorems 3.3 and 3.7. □

THEOREM 3.10. *Let R be a finite chain ring, $\mathbb{F} = R/\langle\gamma\rangle$, where $|\mathbb{F}| = q = p^r$, for a prime p and a positive integer r. Let C be an $[n, k, d]$ MDS self-dual code. Then, we have the following:*

1. *If $p = 2$ or $p^r \equiv 1 \pmod 4$, then n is even.*
2. *If $p^r \equiv -1 \pmod 4$, then $n \equiv 0 \pmod 4$.*

Proof. Let $C_1 = \Psi_1^j(C)$. Then C_1 is an $[n, k, d]$ MDS self-dual code over $\mathbb{F}_q$ by Theorem 3.8. Therefore, $k = n/2$ and n should be even. This proves the first statement. Let $G = [I \mid A]$ be a generator matrix of C_1. Then, $AA^T = -I$. Therefore, A is an $\frac{n}{2} \times \frac{n}{2}$ antiorthogonal matrix. The existence of an antiorthogonal matrix is studied in [8]. According to Table 2 in [8], $\frac{n}{2}$ should be even if $p^r \equiv -1 \pmod 4$. This proves the second statement. the result follows. □

Using Theorems 3.8 and 3.9, the existence of MDS self-dual codes over R_i is equivalent to those over $\mathbb{F}_q$, if q is odd. For the existence of MDS self-dual codes over $\mathbb{F}_q$, (odd q), we can refer to [6].

4. MDS self-dual codes over Galois rings

In this section, we study MDS self-dual codes over Galois rings $GR(p^m, r)$.

4.1. MDS self-dual codes over Galois rings with odd characteristic

First, we assume that p is an odd prime. From the previous section, we know that the existence of MDS self-dual codes over $GR(p^m, r)$ is the same as that over $\mathbb{F}_{p^r}$. Specifically, if we have an $[n, n/2]$ MDS self-dual code over $\mathbb{F}_{p^r}$, then we can construct an $[n, n/2]$ MDS self-dual code over $GR(p^m, r)$ for all $m \geq 1$ using the method in the proof of Theorem 3.6. In the following we provide examples.

EXAMPLE 4.1. *Let C be a $[2, 1, 2]$ MDS self-dual code over $\mathbb{F}_5$ with the generator matrix $G = [1\ 2]$. To construct a $[2, 1, 2]$ MDS self-dual*

code over $GR(5^{10},1)$*, we apply the method in the proof of Theorem 3.6, and we have* $A_{10}=[a_{10}]$ *with*

$$\begin{aligned} a_{10} &= 2121342303_{(5)} \\ &= 2*5^0+1*5^1+2*5^2+1*5^3+3*5^4 \\ &+ 4*5^5+2*5^6+3*5^7+0*5^8+3*5^9 \end{aligned} \tag{4.1}$$

Thus, $G_{10}=[1\ a_{10}]$ *produces a* $[2,1,2]$ *MDS self-dual code over* $GR(5^{10},1)$.

EXAMPLE 4.2. *Let* C *be a* $[4,2,3]$ *MDS self-dual code over* $\mathbb{F}_3$ *with the generator matrix:*

$$G=\begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 2 & 1 \end{pmatrix}. \tag{4.2}$$

To construct a $[4,2,3]$ *MDS self-dual code over* $GR(3^{10},1)$*, we apply the method in the proof of Theorem 3.6, and we have* A_{10} *with*

$$\begin{aligned} A_{10} &= \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}+3\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}+3^2\begin{pmatrix} 2 & 0 \\ 2 & 2 \end{pmatrix} \\ &+ 3^3\begin{pmatrix} 2 & 0 \\ 2 & 2 \end{pmatrix}+3^4\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}+3^5\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ &+ 3^6\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}+3^7\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}+3^8\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}+3^9\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \end{aligned} \tag{4.3}$$

4.2. MDS self-dual codes over Galois rings with even characteristic

Let $p=2$. Consider $R=GR(2^m,r)$. Because of MDS conjecture, we only considered the code lengths up to 2^r. Suppose that $m=1$. Then $R=\mathbb{F}_{2^r}$.

THEOREM 4.3. [7, Theorem 3] *For* $R=GR(2,r)=\mathbb{F}_{2^r}$*, there exist MDS self-dual codes* $C=[2k,k,k+1]$ *over* R *for all* $k=1,\cdots,2^{r-1}$.

If MDS conjecture is true, then the case $m=1$ is completed. MDS self-dual codes over $GR(2^m,r),(m\geq 1)$ have been constructed using Reed-Solomon codes [2].

THEOREM 4.4. [2] *Let* $R=GR(2^m,r), n=2^r-1(>2)$*, and* $m\geq 1$*. Then, there exists an MDS self-dual code over* R *with parameters* $[2^r,2^{r-1},2^{r-1}+1]$*, which is an extended RS code.*

THEOREM 4.5. *For Galois ring* $R=GR(2^m,r)$*, we have the following:*

1. *If* $m\geq 2$*, then there is no MDS self-dual code over* R *for code length* $n\equiv 2 \pmod 4$.

2. *If $m \geq 2$ and r is odd, then there is no $[4, 2, 3]$ MDS self-dual code over R.*

Proof. Suppose that C is an $[n, n/2]$ MDS self-dual code over $GR(2^m, r)$ with a generator matrix $G = [I \mid A]$. Then, $AA^T = -I$ and A is an $\frac{n}{2} \times \frac{n}{2}$ antiorthogonal matrix. Antiorthogonal matrices were studied in [8]. According to Table 2 in [8], $n/2$ should be even. Therefore, $n \equiv 0 \pmod 4$. This proves the first statement. In addition, if r is odd, $n/2$ cannot be two by Table 2 in [8]. Therefore, n cannot be four. This proves the second statement. □

THEOREM 4.6. *Let $R = GR(2^m, r)$, $m \geq 2$, and even r. Then, there is a $[4, 2, 3]$ MDS self-dual code over R.*

Proof. According to Table 2 in [8], -1 is a two square sum. Let $\alpha, \beta \in R$ such that $\alpha^2 + \beta^2 = -1$. Let

$$G = \begin{pmatrix} 1 & 0 & \alpha & \beta \\ 0 & 1 & -\beta & \alpha \end{pmatrix} = (I_2 \mid A). \tag{4.4}$$

Let C be the code generated by G. We claim that C is an MDS self-dual code. It is clear that C is self-dual. To prove that C is MDS, we have to show that the minimum weight of C is three. First, we claim that α and β are units. Suppose that α is not a unit. Then $\alpha = 2\alpha_1$ for some $\alpha_1 \in R$. So, $4\alpha_1^2 + \beta^2 = -1$. Apply Ψ_2^m. So, $\Psi_2^m(4\alpha_1^2 + \beta^2) = \Psi_2^m(-1)$. Then $(\Psi_2^m(\beta))^2 = -1$. This is a contradiction. Therefore, α and β are units. For $x \neq 0$ and $y \neq 0$, we note that $c_1 = [x\ 0]G$ and $c_2 = [0\ y]G$ have weight three. Suppose that $c = [x\ y]G$ has weight two. Then, $[x\ y]A = [0\ 0]$. So, $[x\ y] = [0\ 0]A^{-1} = [0\ 0]$. Therefore, the weight of c is zero. This is a contradiction. Therefore, C has the minimum weight three and C is MDS. □

In Table 1, we show the existence of MDS self-dual codes of code length n over $GR(2^m, r), (m \geq 2)$. In this table, 'X', 'O', and '?' represents the nonexistence, existence, and tentatively unknown existence, respectively. Using Theorems 4.4, 4.5, and 4.6, the table can be verified. From the table, we do not know the existence of MDS self-dual codes of code length $n = 8$ and 10 over $GR(2^m, r), (m \geq 2)$.

In the following example, we apply the method in the proof of Theorem 3.6 to $GR(2^m, r)$. The method is only effective for the odd characteristic. Therefore, we apply a modified method to the even characteristic.

EXAMPLE 4.7. *Let*

$$G = \begin{pmatrix} 1 & 0 & w & w^2 \\ 0 & 1 & w^2 & w \end{pmatrix} \tag{4.5}$$

TABLE 1. Existence of MDS self-dual codes of code length n over $GR(2^m, r), (m \geq 2)$

$r \backslash n$	2	4	6	8	10	12	14	16
1	X							
2	X	O						
3	X	X	X	O				
4	X	O	X	?	X	?	X	O

be a generator matrix for an MDS self-dual $[4, 2, 3]$ *code over* $\mathbb{F}_4 = \mathbb{Z}_2[x]/(f(x))$, $f(x) = x^2 + x + 1$, $w = x + (f(x))$. *Let* $G = [I \mid A_1]$*: Then*

$$A_1 = \begin{pmatrix} w & w^2 \\ w^2 & w \end{pmatrix}. \tag{4.6}$$

Consider $GR(2^2, 2) = \mathbb{Z}_4[x]/(f(x))$. *Note that* $I + A_1 A_1^T = 2S_1$, *where*

$$S_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \tag{4.7}$$

Let $A_2 = A_1 + 2M$. *We want to find* M *such that* $I + A_2 A_2^T \equiv 0 \pmod 4$. *This is equivalent to* $S_1 + M A_1^T + A_1 M^T \equiv 0 \pmod 2$. *Let*

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}. \tag{4.8}$$

Then, from $S_1 + M A_1^T + A_1 M^T \equiv 0 \pmod 2$, *we have*

$$\begin{pmatrix} 0 & (a+d)w^2 + (b+c)w \\ (a+d)w^2 + (b+c)w & 0 \end{pmatrix} \equiv \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \pmod 2. \tag{4.9}$$

Let $a = b = 1, c = d = 0$. *So,*

$$M = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \tag{4.10}$$

and

$$A_2 = A_1 + 2M = \begin{pmatrix} 2 + w & 2 + w^2 \\ w^2 & w \end{pmatrix}. \tag{4.11}$$

Thus, $G_2 = [I \mid A_2]$ *generates a self-dual code* C. *We can verify that the minimum weight* C *is three. Therefore,* C *is a* $[4, 2, 3]$ *MDS self-dual code over* $GR(2^2, 2) = \mathbb{Z}_4[x]/(f(x))$.

We continue this process. Consider $GR(2^3, 2) = \mathbb{Z}_8[x]/(f(x))$. *Note that* $I + A_2A_2^T = 4S_2$, *where*

$$S_2 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}. \tag{4.12}$$

Let $A_3 = A_2 + 4M$. *We want to find* M *such that* $I + A_3A_3^T \equiv 0 \pmod 8$. *This is equivalent to* $S_2 + MA_2^T + A_2M^T \equiv 0 \pmod 2$. *Let*

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}. \tag{4.13}$$

Then from $S_2 + MA_2^T + A_2M^T \equiv 0 \pmod 2$, *we have*

(4.14)
$$\begin{pmatrix} 0 & (a+d)w^2 + (b+c)w \\ (a+d)w^2 + (b+c)w & 0 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \pmod 2.$$

Therefore there is no solution for M. *Hence, we do not succeed in this case.*

5. Conclusions

In this research, we studied the projection and lifting of codes over finite chain rings with respect to MDS self-dual codes. In particular, for the odd characteristic case, we can lift MDS self-dual codes over finite fields to MDS self-dual codes over finite chain rings. For the even characteristic case, we studied various aspects of the existence of MDS self-dual codes over Galois rings. Many aspects remain to be studied in the future, including the existence of MDS self-dual codes of length 8 and 12 over $GR(2^m, r)$, $(m \geq 2)$.

References

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

[2] S.T. Dougherty, J.-L. Kim, and H. Kulosman, *MDS codes over finite principal ideal rings*, Designs, Codes and Cryptography, **50** (2009), 77–92.

[3] S.T. Dougherty, J.-L. Kim, H. Kulosman, and H. Liu, *Self-dual codes over commutative Frobenius rings*, Finte Fields and Their Applications, **16** (2010), 14–26.

[4] S.T. Dougherty, H. Liu, and Y.H. Park, *Lifted codes over finite chain rings*, Math. J. Okayama Univ., **53** (2011), 39–53.

[5] S.T. Dougherty and K. Shiromoto, *MDR Codes over* $\mathbb{Z}_k$, IEEE-IT, **46** (2000) 265–269.

[6] X. Fang, K. Lebed, H. Liu, and J. Luo, *New MDS Self-dual Codes over Finite Fields of Odd Characteristic*, https://arxiv.org/pdf/1811.02802v9.pdf

[7] M. Grassl and T.A. Gulliver, *On self-dual MDS codes*, In: Proceedings of ISIT, (2008) 1954-1957.
[8] S. Han, *MDS Self-Dual Codes and Antiorthogonal Matrices over Galois Rings*, MDPI Information, **10** 153 (2019), 1–12.
[9] J.-L. Kim and Y. Lee, *Construction of MDS Self-dual codes over Galois rings*, Des. Codes Cryptogr., **45** (2007), 247–258 .
[10] H. Lee and Y. Lee, *Construction of self-dual codes over finite rings* $\mathbb{Z}_{p^m}$, Journal of Combinatorial Theory, Series A, **115** (2008), 407–422.
[11] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, Amsterdam, The Netherlands: North-Holland, 1977.
[12] G.H. Norton and A. Salagean, *On the Hamming distance of linear codes over a finite chain ring*, IEEE Trans. Inform. Theory, **46** (2000), 1060–1067.
[13] E. Rains and N.J.A. Sloane, *Self-dual codes*, In: Pless, V.S.; Huffman, W.C. (eds.) Handbook of Coding Theory. Elsevier, Amsterdam, 1998.
[14] Z.-X. Wan, *Finite Fields and Galois Rings*, World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2012.
[15] J. Wood, *Duality for modules over finite rings and applications to coding theory*, Amer. J. Math., **121** (1999), 555-575.

*
School of Liberal Arts
KoreaTech
Cheonan 31253, Republic of Korea
E-mail: sunghyu@koreatech.ac.kr