*J. Appl. & Pure Math. Vol.* **4***(2022), No. 3 - 4, pp. 211 - 219*
https://doi.org/10.23091/japm.2022.211

# ON THE CONSTRUCTION OF MDS SELF-DUAL CODES OVER GALOIS RINGS[†]

SUNGHYU HAN

Abstract. We study MDS(maximum distance separable) self-dual codes over Galois ring $R = GR(2^m, r)$. We prove that there exists an MDS self-dual code over $R$ of length $n$ if $(n-1)$ divides $(2^r - 1)$, and $2^m$ divides $n$. We also provide the current state of the problem for the existence of MDS self-dual codes over Galois rings.

AMS Mathematics Subject Classification : 94B05.
*Key words and phrases* : Galois ring, MDS code, self-dual code.

## 1. Introduction

In this paper, we study the construction of MDS(maximum distance separable) self-dual codes over Galois rings. There are many researches for MDS self-dual codes. Grassl and Gulliver [5] gave almost complete results for MDS self-dual codes over finite fields with even characteristic. For finite fields with odd characteristic, there is an extensive result [4]. For MDS self-dual codes over the rings $\mathbb{Z}_{p^m}$, there is also a research [10]. The next step is Galois rings $GR(p^m, r)$ which include finite fields and the rings $\mathbb{Z}_{p^m}$. For $p = 2$ case, the codes were studied in [1], where MDS self-dual codes of length $n = 2^r$ were constructed using an extended Reed-Solomon codes. For $p \equiv 1 \pmod 4$ with any $r$ or $p \equiv -1 \pmod 4$ with even $r$, the codes were investigated in [9], where various MDS self-dual codes over $GR(p^m, 2)$ were constructed using the building-up construction. For $p \equiv -1 \pmod 4$ with odd $r$, the codes were investigated in [6], where various MDS self-dual codes over $GR(p^m, 3)$ were constructed using the building-up construction.

In [2], Dougherty et al. studied minimum distance, MDS codes, and self-dual codes related to projection and lifting of codes over finite chain rings. This study was developed in [7], where MDS self-dual codes over Galois rings were described

Received March 31, 2022. Revised May 20, 2022. Accepted May 23, 2022.
[†]This paper was supported by professor research year program of KOREATECH in 2022.

with respect to the projection and the lifting of codes. In this paper, we continue the study. The results of this paper are as follows. First we prove that there exists an MDS self-dual code over $GR(2^m, r)$ with parameters $[n, n/2, n/2+1]$, if $(n-1) \mid (2^r-1)$ and $2^m \mid n$. Second, we give the current state of the problem for the existence of 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. And then we give the results for the existence of MDS self-dual codes over finite chain rings. In Section 3, we describe our main results, which are about the existence of MDS self-dual codes over Galois rings. In Section 4, we summarize this paper and give some future works.

## 2. Preliminaries

We provide well-known facts for finite chain rings, Galois rings, linear codes, self-dual codes, and MDS codes. After that we present the results for the existence of MDS self-dual codes over finite chain rings.

**2.1. Finite chain rings.** We give basic facts about finite chain rings [2]. Let $R$ be a finite chain ring, $\mathfrak{m}$ the unique maximal ideal of $R$, and let $\gamma$ 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

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

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

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

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

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

$$R_i = \{a_0 + a_1\gamma + a_2\gamma^2 + \cdots + a_{i-1}\gamma^{i-1} \mid a_i \in \mathbb{F}\} \tag{3}$$

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

$$\sum_{l=0}^{i-1} a_l\gamma^l + \sum_{l=0}^{i-1} b_l\gamma^l = \sum_{l=0}^{i-1}(a_l + b_l)\gamma^l \tag{4}$$

$$\sum_{l=0}^{i-1} a_l\gamma^l \; \cdot \; \sum_{l'=0}^{i-1} b_{l'}\gamma^{l'} = \sum_{s=0}^{i-1}(\sum_{l+l'=s} a_l b_{l'})\gamma^s \tag{5}$$

It is easy to get that all the $R_i$ are finite rings.

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

$$\Psi_i^j : R_j \quad \rightarrow \quad R_i \tag{6}$$

$$\sum_{l=0}^{j-1} a_l \gamma^l \quad \mapsto \quad \sum_{l=0}^{i-1} a_l \gamma^l \tag{7}$$

Let $a, b$ be two arbitrary elements in $R_j$. It is easy to get that

$$\Psi_i^j(a+b) = \Psi_i^j(a) + \Psi_i^j(b), \ \Psi_i^j(ab) = \Psi_i^j(a)\Psi_i^j(b). \tag{8}$$

We note that the map $\Psi_i^j$ can be extended naturally from $R_j^n$ to $R_i^n$.

**2.2. Galois rings.** We give basic facts about Galois rings [13]. Let $p$ and $m$ be a fixed prime and a positive integer, respectively. First, we consider the following canonical projection:

$$\mu : \mathbb{Z}_{p^m} \to \mathbb{Z}_p \tag{9}$$

which is defined by

$$\mu(c) = c \pmod{p}. \tag{10}$$

The Map $\mu$ can be extended naturally to the following map:

$$\mu : \mathbb{Z}_{p^m}[x] \to \mathbb{Z}_p[x] \tag{11}$$

which is defined by

$$\mu(b_0 + b_1 x + \cdots + b_n x^n) = \mu(b_0) + \mu(b_1)x + \cdots + \mu(b_n)x^n. \tag{12}$$

This extended $\mu$ 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

$$GR(p^m, r) = \mathbb{Z}_{p^m}[x]/(f(x)), \tag{13}$$

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

$$b_0 + b_1 x + \cdots + b_{r-1}x^{r-1} + (f(x)), \tag{14}$$

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:

$$\xi = x + (h(x)) \in GR(p^m, r) = \mathbb{Z}_{p^m}[x]/(h(x)). \tag{15}$$

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

$$T = \{0, 1, \xi, \xi^2, \ldots, \xi^{p^r-2}\}. \tag{16}$$

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

$$a = a_0 + a_1 p + a_2 p^2 + \cdots + a_{m-1}p^{m-1}, \tag{17}$$

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,

$$GR(p^m, r) = \langle p^0 \rangle \supset \langle p^1 \rangle \supset \cdots \supset \langle p^i \rangle \supset \cdots \supset \langle p^m \rangle = \{0\}. \tag{18}$$

The $p$ and $m$ in this subsection correspond to $\gamma$ and $e$ in subsection 2.1, respectively.

**2.3. Codes over finite chain rings.** Let $R$ be a finite chain ring. An $R$-submodule $C \leq R^n$ 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 $c = (c_1, c_2, \dots, c_n)$ in $C$ is the number of nonzero $c_j, (1 \leq j \leq n)$. 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

$$\mathbf{x} \cdot \mathbf{y} = x_1 y_1 + \cdots + x_n y_n. \tag{19}$$

For a code $C$ of length $n$ over $R$, let

$$C^{\perp} = \{\mathbf{x} \in R^n \,\big|\, \mathbf{x} \cdot \mathbf{c} = 0, \forall\, \mathbf{c} \in C\} \tag{20}$$

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.

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

$$G = \begin{pmatrix} I_{k_0} & A_{0,1} & A_{0,2} & A_{0,3} & \cdots & A_{0,e-1} & A_{0,e} \\ 0 & \gamma I_{k_1} & \gamma A_{1,2} & \gamma A_{1,3} & \cdots & \gamma A_{1,e-1} & \gamma A_{1,e} \\ 0 & 0 & \gamma^2 I_{k_2} & \gamma^2 A_{2,3} & \cdots & \gamma^2 A_{2,e-1} & \gamma^2 A_{2,e} \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & \gamma^{e-1} I_{k_{e-1}} & \gamma^{e-1} A_{e-1,e} \end{pmatrix}, \tag{21}$$

where $e$ is the nilpotency index of $\gamma$. 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 $k_0, k_1, k_2, \dots, k_{e-1}$ [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 (21) has cardinality

$$|C| = |\mathbb{F}|^{\sum_{i=0}^{e-1}(e-i)k_i} = (p^r)^{\sum_{i=0}^{e-1}(e-i)k_i} = (p^{re})^{k_0}(p^{r(e-1)})^{k_1} \cdots (p^r)^{k_{e-1}}. \tag{22}$$

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

$$1^{k_0}(\gamma)^{k_1}(\gamma^2)^{k_2} \cdots (\gamma^{e-1})^{k_{e-1}}. \tag{23}$$

Let $i$ and $j$ be two integers such that $1 \leq i \leq j$. 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 matrix of $C_1$. Hence, it can be proven that $C_1 = \Psi_i^j(C_2)$.

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

$$d \leq n - \log_{|A|}(|C|) + 1. \tag{24}$$

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

$$d \leq n - \operatorname{rank}(C) + 1. \tag{25}$$

Codes meeting this bound are called MDR (Maximum Distance with respect to Rank) codes [3, 12]. MDR codes do not imply MDS codes. See the following example.

**Example 2.1.** 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 2.2.** [7, 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.*

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

**Theorem 2.3.** [12, Theorem 5.10] *Let $C$ be a MDS code over $GR(p^m, r)$ of 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,*

$$A_w = \binom{n}{w} \sum_{i=0}^{w-d} \binom{w}{i} \left(p^{mr(w+1-d-i)} - 1\right). \tag{26}$$

For a code $C$ over a finite chain ring, we say that $C$ is an MDS self-dual code if $C$ is MDS and self-dual.

**2.5. MDS self-dual codes over finite chain rings.** In this subsection, we describe MDS self-dual codes over finite chain rings with respect to projection and lifting [7].

**Theorem 2.4.** [7, Theorem 3.8] *Let $R$ be a finite chain ring. If $C$ is an MDS self-dual code of length $n$ over $R_j$ then $\Psi_i^j(C)$ is an MDS self-dual code of length $n$ over $R_i$ for all $1 \leq i < j$.*

**Theorem 2.5.** [7, 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 $R_i$. Then $C$ can be lifted to an MDS self-dual code over $R_j$ for all $i < j$.*

**Theorem 2.6.** [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 MDS self-dual code of length $n$. 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 $n \equiv 0 \pmod 4$.*

Using Theorems 2.4 and 2.5, 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 [4].

## 3. MDS self-dual codes over Galois rings

In this subsection, we describe MDS self-dual codes over Galois rings [7]. If $p$ is an odd prime, then by the previous subsection, we know that the existence of MDS self-dual codes over $GR(p^m, r)$ is the same as that over $\mathbb{F}_{p^r}$. More 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 [2, Theorem 3.7].

Suppose that $p = 2$. By the previous subsection, we know that if we have an MDS self-dual code over $GR(2^m, r)$ of length $n$, then we have an MDS self-dual code over $GR(2^\ell, r)$ of length $n$ for all $1 \leq \ell \leq m$ using the projection map. But the converse direction is not guaranteed.

**Theorem 3.1.** [5, 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 over finite fields [8, Section 7.4] is true, then the case $m = 1$ is completed. From now we assume that $m \geq 2$.

**Theorem 3.2.** [7, 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 $R$.*

**Theorem 3.3.** [7, 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 $R$.*

Now, we give our main result of this paper.

**Theorem 3.4.** *Let $R = GR(2^m, r)$, and $n$ be a positive integer such that $(n-1) \mid (2^r - 1)$ and $2^m \mid n$. Then there exists an MDS self-dual code over $R$ with parameters $[n, n/2, n/2+1]$.*

*Proof.* The proof is based on the proof of Theorem 4.6 in [1] and the Example 5.6 in [12]. Let $\xi \in R$ be a primitive $(2^r - 1)$th root of unity such that $\bar{\xi}$ is a primitive $(2^r - 1)$th root of unity in $\mathbb{F}_{2^r}$. Let $\alpha = \xi^{\frac{2^r-1}{n-1}}$. Then $\alpha$ is a primitive

$(n-1)$th root of unity such that $\bar{\alpha}$ is a primitive $(n-1)$th root of unity in $\mathbb{F}_{2^r}$. Then the Reed-Solomon code $C$ over $R$ with distance $d = n/2$ is generated by $g(x) = (x-\alpha)(x-\alpha^2)\cdots(x-\alpha^{d-1})$. Then $C$ is an $[n-1, n/2, n/2]$ MDS code and has the following parity check matrix:

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & (\alpha^2)^2 & \cdots & (\alpha^2)^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha^{d-1} & (\alpha^{d-1})^2 & \cdots & (\alpha^{d-1})^{n-1} \end{bmatrix}. \tag{27}$$

Let $h(x) \in R[x]$ be the check polynomial of $C$, i.e., $x^n - 1 = g(x)h(x)$, hence $h(x) = (x-\alpha^d)(x-\alpha^{d+1})\cdots(x-\alpha^n)$. The reciprocal polynomial
$h^* = x^{\deg(h)}h(1/x) = (1-\alpha^d x)(1-\alpha^{d+1}x)\cdots(1-\alpha^n x)$.

The dual code $C^\perp$ is generated by $g_1(x) = \frac{1}{h(0)}h^*(x) = (x-1)(x-\alpha)(x-\alpha^2)\cdots(x-\alpha^{d-1})$, and is an $[n-1, n/2-1, n/2+1]$ MDS code. Since $g(x)$ divides $g_1(x)$, $C^\perp$ is self-orthogonal. Futhermore since the all-one vector $\mathbf{1}$ is not in $C^\perp$ but in $C$, we have $C = C^\perp + \mathbf{1}$. Now we extend $C$, say $C_1$, by adding 1 at the end of $\mathbf{1}$, and zero 0 at the end of any codewords generating $C^\perp$ (and obviously by combining them). Then $C_1$ is an $[n, n/2, n/2+1]$ MDS code. By construction, $C_1$ is also self-dual and has the following generator matrix:

$$G = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} & 0 \\ 1 & \alpha^2 & (\alpha^2)^2 & \cdots & (\alpha^2)^{n-1} & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 1 & \alpha^{d-1} & (\alpha^{d-1})^2 & \cdots & (\alpha^{d-1})^{n-1} & 0 \end{bmatrix}. \tag{28}$$

This completes the proof. □

**Remark 3.1.** In [1], Dougherty et al. proved that there exists an MDS self-dual code over $R = GR(2^m, r)$ with parameters $[2^r, 2^{r-1}, 2^{r-1}+1]$, which is an extended RS code. But in the statement they missed a condition. The constructed MDS self-dual code contains all-one vector $\mathbf{1}$. Therefore $m \leq r$. If $m > r$, then $\mathbf{1}$ is not self-orthogonal. So, we should add the condition, $m \leq r$.

Following Theorem 3.4, if we have positive integers $n$ and $m$ such that $(n-1) \mid (2^r - 1)$ and $2^m \mid n$, then we know that there exist the MDS self-dual codes of length $n$ over $GR(2^m, r)$ which are generalized Reed-Solomon codes. Therefore it is important to know the integers. In the following we calculate them. To simplify the calculation, we only consider the cases $n \geq 8$ and $m \geq 2$. We introduce the notation $2^m \parallel n$ which means that $2^m \mid n$ but $2^{m+1} \nmid n$. We give positive integer pairs $(n, m)$ such that $(n-1) \mid (2^r - 1)$ and $2^m \parallel n$, $(n \geq 8$, $m \geq 2)$. If $r = 1$ or $r = 2$, then there is no such pairs. Therefore we start with $r = 3$.

(1) $r = 3$: $2^r - 1 = 7$. $(n, m) = (8, 3)$.

(2) $r = 4$: $2^r - 1 = 15 = 3 \times 5$. $(n, m) = (16, 4)$.

Table 1. Positive integer pairs $(n, m)$ such that $(n-1) \mid (2^r-1)$ and $2^m \parallel n$, $(n \geq 8,\ m \geq 2)$.

| $r$ | $(n, m)$ | $r$ | $(n, m)$ |
|---|---|---|---|
| 3 | (8, 3) | 7 | (128, 7) |
| 4 | (16, 4) | 8 | (16, 4), (52, 2), (256, 8) |
| 5 | (32, 5) | 9 | (8, 3), (512, 9) |
| 6 | (8, 3), (64, 6) | 10 | (12, 2), (32, 5), (1024, 10) |

Table 2. Existence of MDS self-dual codes of 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 $(m \leq 3)$, ? $(m > 3)$ | | | | |
| 4 | X | O | X | ? | X | ? | X | O$(m \leq 4)$, ? $(m > 4)$ |

(3) $r = 5$: $2^r - 1 = 31$. $(n, m) = (32, 5)$.
(4) $r = 6$: $2^r - 1 = 63 = 3^2 \times 7$. $(n, m) = (8, 3), (64, 6)$.
(5) $r = 7$: $2^r - 1 = 127$. $(n, m) = (128, 7)$.
(6) $r = 8$: $2^r - 1 = 255 = 3 \times 5 \times 17$. $(n, m) = (16, 4), (52, 2), (256, 8)$.
(7) $r = 9$: $2^r - 1 = 511 = 7 \times 73$. $(n, m) = (8, 3), (512, 9)$.
(8) $r = 10$: $2^r - 1 = 1023 = 3 \times 11 \times 31$. $(n, m) = (12, 2), (32, 5), (1024, 10)$.

In table 1, we summarize the calculation.

In Table 2, we show the existence of MDS self-dual codes of 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 3.2, 3.3, and 3.4, the table can be verified. From the table, for $r = 3$ case, we know the existence of MDS self-dual codes of length 8 over $GR(2^m, 3)$, if $m \leq 3$. But if $m > 3$ then we don't know the existence. For $r = 4$ case, we don't know the existence of MDS self-dual codes of length 8 and 12 over $GR(2^m, 4)$.

## 4. Summary

In this paper, we presented the results for the existence of MDS self-dual codes over Galois rings. We proved that there exists an MDS self-dual code over $GR(2^m, r)$ with parameters $[n, n/2, n/2 + 1]$, if $(n - 1) \mid (2^r - 1)$ and $2^m \mid n$. And then we gave the current state of the problem for 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 over $GR(2^2, 4)$ or $GR(2^4, 3)$.

**Acknowledgments** : The author thank the referees for their valuable comments which improved the clarity of this paper.

## References

1. S.T. Dougherty, J.-L. Kim, H. Kulosman, *MDS codes over finite principal ideal rings*, Des. Codes Cryptogr. **50** (2009), 77-92.
2. S.T. Dougherty, H. Liu, Y.H. Park, *Lifted codes over finite chain rings*, Math. J. Okayama Univ. **53** (2011), 39-53.
3. S.T. Dougherty, K. Shiromoto, *MDR Codes over* $\mathbb{Z}_k$, IEEE Trans. Inform. Theory **46** (2000), 265-269.
4. X. Fang, K. Lebed, H. Liu, J. Luo, *New MDS self-dual codes over finite fields of odd characteristic*, Des. Codes Cryptogr. **88** (2020), 1127-1138.
5. M. Grassl, T.A. Gulliver, *On self-dual MDS codes*, In: Proceedings of ISIT (2008), 1954-1957.
6. S. Han, *MDS self-dual codes and antiorthogonal matrices over Galois rings*, MDPI Information **10** (2019), 1-12.
7. S. Han, *On the existence of MDS self-dual codes over finite chain rings*, J. Chungcheong Math. Soc. **33** (2020), 255-270.
8. W.C. Huffman, V.S. Pless, *Fundamentals of Error-correcting Codes*, Cambridge: Cambridge University Press, 2003.
9. J.-L. Kim, Y. Lee, *Construction of MDS Self-dual codes over Galois rings*, Des. Codes Cryptogr. **45** (2007), 247-258.
10. H. Lee, 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, N.J.A. Sloane, *The Theory of Error-Correcting Codes*, Amsterdam, The Netherlands, North-Holland, 1977.
12. G.H. Norton, A. Salagean, *On the Hamming distance of linear codes over a finite chain ring*, IEEE Trans. Inform. Theory **46** (2000), 1060-1067.
13. Z.-X. Wan, *Finite Fields and Galois Rings*, World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2012.

**Sunghyu Han** received M.Sc. and Ph.D. from Yonsei University. Since 2009 he has been at KoreaTech. His research interests include Coding Theory.

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