JOURNAL OF THE
CHUNGCHEONG MATHEMATICAL SOCIETY
Volume **36**, No. 3, August 2023
http://dx.doi.org/10.14403/jcms.2023.36.3.181

MDS SELF-DUAL CODES OVER GALOIS RINGS WITH EVEN CHARACTERISTIC

Sunghyu Han

Abstract. Let $GR(2^m, r)$ be a Galois ring with even characteristic. We are interested in the existence of MDS(Maximum Distance Separable) self-dual codes over $GR(2^m, r)$. In this paper, 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 $8 \mid n$.

1. Introduction

Let $R = GR(p^m, r)$ be a Galois ring. We are interested in the existence of MDS(Maximum Distance Separable) self-dual codes over R. If $m = 1$, then $R = GR(p, r)$ is the finite field $\mathbb{F}_{p^r}$. MDS self-dual codes over finite fields are studied extensively. If $p = 2$ then we have the following result.

Theorem 1.1. [5, Theorem 3] *For $R = GR(2, r) = \mathbb{F}_{2^r}$, there exist an MDS self-dual code $C = [2k, k, k + 1]$ over R for all $k = 1, \cdots, 2^{r-1}$.*

If MDS conjecture over finite fields [9, Section 7.4] is true, then the research for $\mathbb{F}_{2^r}$ is completed. For odd prime p, there are many research papers for MDS self-dual codes over $\mathbb{F}_{p^r}$ (see [3] as an example) and the research has not been completed.

MDS self-dual codes over Galois rings are studied [7]. If p is odd, then the existence of MDS self-dual codes over $GR(p^m, r)$ is equivalent to those over $\mathbb{F}_{p^r}$ [7, Theorem 3.8, Theorem 3.9]. In other words, if we have an MDS self-dual code over $GR(p^m, r)$, then we can make an MDS self-dual code over $\mathbb{F}_{p^r}$ using the canonical projection map. Conversely,

---

Received April 10, 2023; Accepted August 21, 2023.
2020 Mathematics Subject Classification: Primary 94B05; Secondary 13B05.
Key words and phrases: Galois ring, MDS code, self-dual code.
This paper was supported by the Education and Research Promotion Program of KOREATECH in 2023.

if we have an MDS self-dual code over $\mathbb{F}_{p^r}$, then we can make an MDS self-dual code over $GR(p^m, r)$ using lifting process.

If p is even, then the projection map is still working but the lifting process can not be applied. Therefore the study of MDS self-dual codes over Galois rings with even characteristic is not easy. This paper is all about MDS self-dual codes over $GR(2^m, r)$. If $m = 1$, $GR(2^m, r) = \mathbb{F}_2^r$. Therefore the research is done by Theorem 1.1. We assume that $m \geq 2$. There are some results for this case.

Theorem 1.2. [7, Theorem 4.5, Theorem 4.6] *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 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.*
3. *If $m \geq 2$ and r is even, then there exist a $[4, 2, 3]$ MDS self-dual code over R.*

Theorem 1.3. [8, 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 $[n, n/2, n/2 + 1]$.*

The purpose of this paper is to develop Theorem 1.3. We replace the condition $2^m \mid n$ of Theorem 1.3 with $8 \mid n$. Therefore the main result of this paper is the following. 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 $8 \mid n$.

This paper is organized as follows. In Section 2, we provide basic facts for Galois rings, linear codes, MDS codes, self-dual codes, generalized Reed-Solomon codes, and the stronger version of Hensel's lemma. 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

2.1. Galois rings

In this subsection, we present some well-known facts about Galois rings (see [15] as an example). Let p be a fixed prime and m be a positive integer. First, we consider the following canonical projection

$$\mu : \mathbb{Z}_{p^m} \to \mathbb{Z}_p \tag{2.1}$$

which is defined by

$$\mu(c) = c \pmod{p}. \tag{2.2}$$

The map μ can be extended naturally to the following map

$$\mu : \mathbb{Z}_{p^m}[x] \to \mathbb{Z}_p[x] \tag{2.3}$$

which is defined by

$$\mu(a_0 x + a_1 x + \cdots + a_n x^n) = \mu(a_0) + \mu(a_1)x + \cdots + \mu(a_n)x^n. \tag{2.4}$$

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. A Galois ring is constructed as

$$GR(p^m, r) = \mathbb{Z}_{p^m}[x]/(f(x)), \tag{2.5}$$

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 residue classes of the form

$$a_0 + a_1 x + \cdots + a_{r-1}x^{r-1} + (f(x)), \tag{2.6}$$

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

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 a well-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 and $h(x)|(x^{p^r-1} - 1)$. Consider the following element

$$\xi = x + (h(x)) \in GR(p^m, r) = \mathbb{Z}_{p^m}[x]/(h(x)). \tag{2.7}$$

The order of ξ is $p^r - 1$. Teichmüller representatives are defined as follows.

$$T = \{0, 1, \xi, \xi^2, \ldots, \xi^{p^r-2}\}. \tag{2.8}$$

Every element $t \in GR(p^m, r)$ can be uniquely represented by the form

$$t = t_0 + pt_1 + p^2 t_2 + \cdots + p^{m-1}t_{m-1}, \tag{2.9}$$

where $t_i \in T, (0 \leq i \leq m-1)$. Moreover, t is a unit if and only if $t_0 \neq 0$, and t is a zero divisor or 0 if and only if $t_0 = 0$.

The Galois ring $R = GR(p^m, r)$ is a local ring with a unique maximal ideal $M = (p)$. The canonical projection map is defined by

$$\begin{aligned} {}^{-} \ : \ & R \to R/M \\ & r \to \overline{r} = r + M. \end{aligned}$$

It is known that $\overline{\xi}$ is a primitive element in $R/M (= \mathbb{F}_{p^r})$.

2.2. Linear codes over $GR(p^m, r)$

A linear code C of length n over $GR(p^m, r)$ is a submodule of $GR(p^m, r)^n$, and the elements in C are called codewords. The distance $d(\mathbf{u}, \mathbf{v})$ between two elements $\mathbf{u}, \mathbf{v} \in GR(p^m, r)^n$ is the number of coordinates in which $\mathbf{u}, \mathbf{v}$ differ. The minimum distance of a code C is the smallest distance between distinct codewords. The weight of a codeword $\mathbf{c} = (c_1, c_2, \cdots, c_n)$ in C is the number of nonzero c_j. The minimum weight of C is the smallest nonzero weight of any codeword in C. If C is a linear code, then the minimum distance and the minimum weight are the same.

A generator matrix for a linear code C over $GR(p^m, r)$ is permutation equivalent to the following one in the standard form [12, 13]:

(2.10)

$$G = \begin{pmatrix} I_{k_0} & A_{0,1} & A_{0,2} & A_{0,3} & \cdots & A_{0,m-1} & A_{0,m} \\ 0 & pI_{k_1} & pA_{1,2} & pA_{1,3} & \cdots & pA_{1,m-1} & pA_{1,m} \\ 0 & 0 & p^2 I_{k_2} & p^2 A_{2,3} & \cdots & p^2 A_{2,m-1} & p^2 A_{2,m} \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & p^{m-1} I_{k_{m-1}} & p^{m-1} A_{m-1,m} \end{pmatrix},$$

where the columns are grouped into square blocks of sizes $k_0, k_1, \ldots, k_{m-1}$. The rank of C, denoted by $\mathrm{rank}(C)$, is defined to be the number of nonzero rows of its generator matrix G in a standard form. Therefore $\mathrm{rank}(C) = \sum_{i=0}^{m-1} k_i$. 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 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. In this paper, we assume that all codes are linear unless we state otherwise.

2.3. MDS codes

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

$$d \leq n - \log_{|A|}(|C|) + 1. \tag{2.11}$$

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

$$d \leq n - \mathrm{rank}(C) + 1. \tag{2.12}$$

Codes meeting this bound are called maximum distance with respect to rank (MDR) codes [2, 13]. The following lemma states the necessary and sufficient condition for MDS codes over Galois rings (see [6] as an example).

LEMMA 2.1. *Let C be a linear code over $GR(p^m, r)$. Then, C is MDS if and only if C is MDR and free.*

2.4. Self-dual codes

We define the usual inner product: for $\mathbf{x}, \mathbf{y} \in GR(p^m, r)^n$,

$$\mathbf{x} \cdot \mathbf{y} = x_1 y_1 + \cdots + x_n y_n. \tag{2.13}$$

For a code C of length n over $GR(p^m, r)$, let

$$C^\perp = \{\mathbf{x} \in GR(p^m, r)^n \,\big|\, \mathbf{x} \cdot \mathbf{c} = 0, \forall\, \mathbf{c} \in C\} \tag{2.14}$$

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

2.5. Generalized Reed-Solomon codes over $GR(p^m, r)$

In this subsection, we describe generalized Reed-Solomon codes over $R = GR(p^m, r)$ [13, 14]. We start with the following definition (see [13, Definition 2.2], [14, Definition 5] as examples).

DEFINITION 2.2. Let $R = GR(p^m, r)$. A subset S of R is subtractive if $s - t$ is unit for all $s, t \in S$ with $s \neq t$.

LEMMA 2.3. ([13, Lemma 2.5, Corollary 2.6]) *Let R be a finite local ring, M be the maximal ideal of R, and $K = R/M$ the residue field. For an element $r \in R$, we denote by $\overline{y}$ its image under the canonical projection from R onto K. Then we have the following.*

1. *For $r, r' \in R$, $\overline{r} \neq \overline{r'}$ if and only if $r - r'$ is a unit of R.*
2. *For $S \subseteq R$, $|S| = |\overline{S}|$ if and only if S is subtractive.*

LEMMA 2.4. *Let $R = GR(p^m, r)$ and $T = \{0, 1, \xi, \xi^2, \ldots, \xi^{p^r-2}\}$ be the set of the Teichmüller representatives of R. Then we have the following.*

1. *If $A \subseteq T$, then A is subtractive.*
2. *For $B \subseteq R$, if B is subtractive then $|B| \leq |T|$.*

Proof. We know that $R/(p) = \mathbb{F}_{p^r}$, where (p) is the unique maximal ideal of R, and $\overline{\xi}$ is a primitive element of $\mathbb{F}_{p^r}$. Therefore $\overline{T} = \mathbb{F}_{p^r}$, $|T| = |\overline{T}|$, and $|A| = |\overline{A}|$. So, A is subtractive by Lemma 2.3 (ii). This proves (i). Let $B \subseteq R$. Suppose that B is subtractive. Then $|B| = |\overline{B}| \leq |\mathbb{F}_{p^r}| = |\overline{T}| = |T|$. This proves (ii). $\square$

Now we define the generalized Reed-Solomon codes over Galois rings (see [13, Example 3.7], [14, Definition 22] as examples).

Definition 2.5. Let $R = GR(p^m, r)$ and n, k be two positive integers such that $1 \le k \le n$. Let P_k be the set of polynomials over R of degree less than k, including the zero polynomial in $R[x]$. Let $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$ be a subtractive subset of R, $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n) \in R^n$, and $v = (v_1, v_2, \dots, v_n) \in R^n$, where v_i is unit for $1 \le i \le n$. Then the generalized Reed-Solomon code, $GRS_k(\alpha, v)$ is defined by

$$GRS_k(\alpha, v) = \{(v_1 f(\alpha_1), v_2 f(\alpha_2), \dots, v_n f(\alpha_n)) \mid f \in P_k\}.$$

The following theorem is very important in the main section. The proof can be found in [14, Proposition 23, Corollary 24, Proposition 25, Theorem 28].

Theorem 2.6. *We have the followings for the $GRS_k(\alpha, v)$ defined above.*

1. *$GRS_k(\alpha, v)$ is an $[n, k, d]$ MDS code with $d = n - k + 1$.*
2. *A generator matrix of $GRS_k(\alpha, v)$ is given by*

$$G = \begin{pmatrix} v_1 & v_2 & \cdots & v_n \\ v_1\alpha_1 & v_2\alpha_2 & \cdots & v_n\alpha_n \\ v_1\alpha_1^2 & v_2\alpha_2^2 & \cdots & v_n\alpha_n^2 \\ \vdots & \vdots & & \vdots \\ v_1\alpha_1^{k-1} & v_2\alpha_2^{k-1} & \cdots & v_n\alpha_n^{k-1} \end{pmatrix}. \tag{2.15}$$

3. *The dual code of $GRS_k(\alpha, v)$ is given by*

$$GRS_k(\alpha, v)^\perp = GRS_{n-k}(\alpha, v'),$$

where

$$v' = ({v_1}', {v_2}', \dots, {v_n}') \text{ and } {v_i}' = \Big(v_i \prod_{j \ne i} (\alpha_i - \alpha_j)\Big)^{-1}.$$

We generalize a result in [10, Corollary 2.4] by the following theorem.

Theorem 2.7. *With the notations above, let $u_i = \big(\prod_{j\ne i}(\alpha_i - \alpha_j)\big)^{-1}$, $(1 \le i \le n)$ and λ be a unit in $GR(p^m, r)$. Suppose that $\lambda u_i = v_i^2$ for some unit $v_i \in GR(p^m, r)$, $(1 \le i \le n)$. Let $v = (v_1, v_2, \dots, v_n)$. Then $GRS_{\frac{n}{2}}(\alpha, v)$ is an MDS self-dual code.*

Proof. Since $GRS_{\frac{n}{2}}(\alpha, v)$ is MDS, we only have to prove that $GRS_{\frac{n}{2}}(\alpha, v)$ is self-dual. Note that by Theorem 2.6 (iii), $GRS_{\frac{n}{2}}(\alpha, \mathbf{1})^\perp = GRS_{\frac{n}{2}}(\alpha, u)$, where $\mathbf{1} = (1, 1, \dots, 1)$ and $u = (u_1, u_2, \dots, u_n)$. Let c and c' be two codewords in $GRS_{\frac{n}{2}}(\alpha, v)$ with $c = (v_1 f(\alpha_1), v_2 f(\alpha_2), \ldots, v_n f(\alpha_n))$ and $c' = (v_1 g(\alpha_1), v_2 g(\alpha_2), \ldots, v_n g(\alpha_n))$, $(f, g \in P_{\frac{n}{2}})$. Then

$$\begin{aligned} c \cdot c' &= (v_1 f(\alpha_1) v_1 g(\alpha_1), v_2 f(\alpha_2) v_2 g(\alpha_2), \ldots, v_n f(\alpha_n) v_n g(\alpha_n)) \\ &= (f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_n)) \cdot (v_1^2 g(\alpha_1), v_2^2 g(\alpha_2), \ldots, v_n^2 g(\alpha_n)) \\ &= (f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_n)) \cdot (\lambda u_1 g(\alpha_1), \lambda u_2 g(\alpha_2), \ldots, \lambda u_n g(\alpha_n)) \\ &= \lambda (f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_n)) \cdot (u_1 g(\alpha_1), u_2 g(\alpha_2), \ldots, u_n g(\alpha_n)). \end{aligned}$$

Since $(f(\alpha_1), f(\alpha_2), \ldots, f(\alpha_n)) \in GRS_{\frac{n}{2}}(\alpha, \mathbf{1})$ and $(u_1 g(\alpha_1), u_2 g(\alpha_2), \ldots, u_n g(\alpha_n)) \in GRS_{\frac{n}{2}}(\alpha, u)$, we have $c \cdot c' = 0$. Therefore $GRS_{\frac{n}{2}}(\alpha, v)$ is self-dual. This completes the proof. □

We generalize a result in [16, Lemma 3] by the following lemma.

LEMMA 2.8. *Let $R = GR(p^m, r)$ and ξ be a primitive $(p^r - 1)$th root of unity in R. Let $n | (p^r - 1)$ be a positive integer and $\alpha = \xi^{\frac{p^r - 1}{n}}$. Then for any $0 \leq i \leq n - 1$ we have*

$$\prod_{0 \leq j \leq n-1, j \neq i} (\alpha^i - \alpha^j) = \alpha^{i(n-1)} n.$$

Proof. The proof is almost same to the one [16, Lemma 3]. We include the proof for a completeness. Note that α is a primitive n-th root of unity. We have

$$\prod_{0 \leq j \leq n-1, j \neq i} (\alpha^i - \alpha^j) = \alpha^{i(n-1)} \prod_{0 \leq j \leq n-1, j \neq i} (1 - \alpha^{j-i}) = \alpha^{i(n-1)} \prod_{1 \leq j \leq n-1} (1 - \alpha^j).$$

Since $x^n - 1 = \prod_{j=0}^{n-1} (x - \alpha^j)$, we have

$$\prod_{j=1}^{n-1} (x - \alpha^j) = \frac{x^n - 1}{x - 1} = 1 + x + x^2 + \cdots + x^{n-1}$$

Taking $x = 1$, we have $\prod_{j=1}^{n-1} (1 - \alpha^j) = n$. □

2.6. The stronger version of Hensel's lemma

In this subsection we give the stronger version of Hensel's lemma. We don't give a complete explanation of the stronger version of Hensel's lemma. Undefined notations and terminologies can be found in [1, 4]. We start with the following definitions (see [4, Definition 2.1.2, Definition 2.1.4] as an example).

Definition 2.9. Let $\mathbb{R}_+ = \{x \in \mathbb{R} : x \geq 0\}$. Fix a prime number $p \in \mathbb{Z}$. The p-adic valuation on $\mathbb{Z}$ is the function

$$v_p : \mathbb{Z}\backslash\{0\} \to \mathbb{R}_+$$

defined as follows: for each integer $n \in \mathbb{Z}$, $n \neq 0$, let $v_p(n)$ be the unique positive integer satisfying

$$n = p^{v_p(n)} n' \text{ with } p \nmid n'.$$

We extend v_p to the field of rational numbers as follows: if $x = a/b \in \mathbb{Q}\backslash\{0\}$, then

$$v_p(x) = v_p(a) - v_p(b).$$

Definition 2.10. For any $x \in \mathbb{Q}$, we define the p-adic absolute value of x by

$$|x|_p = p^{-v_p(x)}$$

if $x \neq 0$, and we set $|0|_p = 0$.

We give the stronger version of Hensel's Lemma (see [1] as an example).

Theorem 2.11. *Let $f(X) \in \mathbb{Z}_p[X]$ and $a \in \mathbb{Z}_p$ satisfy*

$$|f(a)|_p < |f'(a)|_p^2.$$

There is a unique $\alpha \in \mathbb{Z}_p$ such that $f(\alpha) = 0$ in $\mathbb{Z}_p$ and $|\alpha - a|_p < |f'(a)|_p$.

Proof. We don't give a complete proof of the theorem. But we give the idea of the proof which will be used in the main section of this paper. Define a sequence $\{a_n\}$ in Q_p by $a_1 = a$ and

$$a_{n+1} = a_n - \frac{f(a_n)}{f'(a_n)}, \ (n \geq 1).$$

Set $t = |\frac{f(a)}{f'(a)^2}|_p < 1$. Then we can show by induction on n that

1. $|a_n|_p \leq 1$, i.e., $a_n \in \mathbb{Z}_p$,
2. $|f'(a_n)|_p = |f'(a_1)|_p$,
3. $|f(a_n)|_p \leq |f'(a_1)|_p^2 \cdot t^{2^{n-1}}$.

The unique α is the limit of the sequence $\{a_n\}$. We omit the details which can be found [1, Section 5]. □

3. Main results

We are interested in the existence of MDS self-dual codes over $GR(2^m, r)$. We start with the following lemma.

LEMMA 3.1. *Let n be a positive integer such that $n \equiv 0 \pmod 8$. Let $f(x) = x^2 + (n-1)$. Then there is an integer solution for $f(x) \equiv 0 \pmod{2^m}$ for all $m \geq 1$.*

Proof. Let $p = 2$, $a = 1$, and $|n|_p = 2^{-r}$, $(r \geq 3)$. Then $|f(a)|_p = |n|_p = 2^{-r}$ and $|f'(a)|_p^2 = |2a|_p^2 = |2|_p^2 = \frac{1}{4}$. Therefore

$$|f(a)|_p < |f'(a)|_p^2$$

which is the condition of Theorem 2.11. We define a sequence $\{a_\ell\}$,

$$a_1 = a = 1,\ a_{\ell+1} = a_\ell - \frac{a_\ell^2 + (n-1)}{2a_\ell},\ (\ell \geq 1)$$

and note that $|a_\ell|_p \leq 1$ as in the proof of Theorem 2.11. Let $t = |\frac{f(a)}{f'(a)^2}|_p$. Since $t = 2^{2-r}$, we have

$$|f(a_\ell)|_p \leq |f'(a_1)|_p^2 \cdot t^{2^{\ell-1}} \leq 2^{-2} \cdot (2^{2-r})^{2^{\ell-1}} = 2^{-(2+(r-2)\cdot 2^{\ell-1})}.$$

For a fixed m, we choose k such that $2 + (r-2) \cdot 2^{k-1} \geq m$. Then a_k is a solution of $f(x) \equiv 0 \pmod{2^m}$. □

We are ready to prove the main theorem of this paper.

THEOREM 3.2. *Let $R = GR(2^m, r)$, and n be a positive integer such that $(n-1) \mid (2^r - 1)$ and $8 \mid n$. Then there exists an MDS self-dual code over R with parameters $[n, n/2, n/2+1]$.*

Proof. Let $\xi \in R$ be a primitive $(2^r - 1)$th root of unity. Let $\alpha = \xi^{\frac{2^r-1}{n-1}}$. Then α is a primitive $(n-1)$th root of unity. By Lemma 2.4, $\{0, 1, \alpha, \alpha^2, \ldots, \alpha^{n-2}\}$ is subtractive. Let

$$G0 = \begin{bmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-2} \\ 0 & 1 & \alpha^2 & (\alpha^2)^2 & \cdots & (\alpha^{n-2})^2 \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 0 & 1 & \alpha^{\frac{n}{2}-1} & (\alpha^2)^{\frac{n}{2}-1} & \cdots & (\alpha^{n-2})^{\frac{n}{2}-1} \end{bmatrix}. \tag{3.1}$$

By Theorem 2.6, we know that $G0$ is the generator matrix of the $GRS_{\frac{n}{2}}(\delta, \mathbf{1})$ code which is an $[n, \frac{n}{2}, \frac{n}{2}+1]$ MDS code, where $\delta = (0, 1, \alpha, \alpha^2, \ldots, \alpha^{n-2})$

and $\mathbf{1} = (1, 1, \ldots, 1)$, and we also know that $GRS_{\frac{n}{2}}(\delta, \mathbf{1})^{\perp} = GRS_{\frac{n}{2}}(\delta, w)$, where $w = (w_1, w_2, \ldots, w_n)$,

$$w_i = \prod_{1 \le j \le n, j \ne i} (\delta_i - \delta_j)^{-1},$$

where $\delta_1 = 0, \delta_k = \alpha^{k-2}(k = 2, 3, \ldots, n)$. We have

$$\begin{aligned} w_1^{-1} &= (0-1)(0-\alpha)(0-\alpha^2)\cdots(0-\alpha^{n-2}) \\ &= (-1)\alpha^{1+2+\cdots+n-2} \\ &= (-1)(\alpha^{n-1})^{\frac{n-2}{2}} \\ &= -1. \end{aligned}$$

Using Lemma 2.8, we can calculate w_i, $(2 \le i \le n)$

$$\begin{aligned} w_i^{-1} &= (\alpha^{i-2} - 0) \prod_{0 \le j \le n-2, j \ne i-2} (\alpha^{i-2} - \alpha^j) \\ &= \alpha^{i-2} \cdot \alpha^{(i-2)(n-2)} \cdot (n-1) \\ &= \alpha^{(i-2)(n-1)}(n-1) \\ &= (\alpha^{n-1})^{i-2}(n-1) \\ &= n-1. \end{aligned}$$

Therefore we have

$$w = (w_1, w_2, \ldots, w_n) = (-1, \frac{1}{n-1}, \frac{1}{n-1}, \ldots, \frac{1}{n-1})$$

and

$$(n-1)w = (-(n-1), 1, 1, \ldots, 1).$$

We claim that $-(n-1)$ is a square element in $R = GR(2^m, r)$. More precisely, let $f(x) = x^2 + (n-1)$. Then we claim that $f(x) \equiv 0 \pmod{2^m}$ has a solution for all $m \ge 1$. By Lemma 3.1, we know that there is an integer solution for $f(x) \equiv 0 \pmod{2^m}$. Let β be a solution for $f(x) \equiv 0 \pmod{2^m}$. Then $-(n-1) = \beta^2$ in $R = GR(2^m, r)$. Let $v = (\beta, 1, 1, \ldots, 1)$. Then $GRS_{\frac{n}{2}}(\delta, v)$ is MDS self-dual by Theorem 2.7. The generator matrix of $GRS_{\frac{n}{2}}(\delta, v)$ is given by the following matrix G:

$$G = \begin{bmatrix} \beta & 1 & 1 & 1 & \cdots & 1 \\ 0 & 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-2} \\ 0 & 1 & \alpha^2 & (\alpha^2)^2 & \cdots & (\alpha^{n-2})^2 \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 0 & 1 & \alpha^{\frac{n}{2}-1} & (\alpha^2)^{\frac{n}{2}-1} & \cdots & (\alpha^{n-2})^{\frac{n}{2}-1} \end{bmatrix}. \tag{3.2}$$

TABLE 1. Positive integer pairs $(n, v_2(n))$ such that $(n-1) \mid (2^r - 1)$, $(v_2(n) \geq 2$, $n \geq 8$, $3 \leq r \leq 10)$

r	$(n, v_2(n))$	r	$(n, v_2(n))$
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)

□

In Table 1, we give positive integer pairs $(n, v_2(n))$ such that $(n-1) \mid (2^r - 1)$, $v_2(n) \geq 2$, $n \geq 8$, and $3 \leq r \leq 10$. In Table 1, for the case $n = 8, 16, 32, 64, 128, 256, 512, 1024$, since $v_2(n) \geq 3$, by Theorem 3.2, we know that there exists an MDS self-dual code over $R = GR(2^m, r)$ with parameters $[n, n/2, n/2+1]$. The generator matrix G of the code is given by Equation (3.2). In G, we should determine β. Following the proof of Lemma 3.1, we can determine the value β. We explain this in the following. Let k_0 be the smallest value such that $2+(v_2(n)-2)\cdot 2^{k_0-1} \geq m$. Let $\beta \equiv a_{k_0} \pmod{2^m}$. In Table 2, we give the values, k_0, a_{k_0}, β for $n = 8, 16, 32$, and $1 \leq m \leq 10$. For example, if $n = 8$ and $m = 7$, then since $v_2(n) = 3$, k_0 is the smallest value such that $2+(3-2)\cdot 2^{k_0-1} \geq 7$. So, $k_0 = 4$. By the sequence formula,

$$a_1 = 1,\ a_{\ell+1} = a_\ell - \frac{a_\ell^2 + 7}{2a_\ell}, (\ell \geq 1),$$

we have

$$a_4 = 31/3$$

and

$$\frac{31}{3} \equiv 31 \cdot 3^{-1} \equiv 31 \cdot 43 \equiv 53 \pmod{2^7}.$$

Therefore $\beta = 53$. Note that β is the solution of $f(x) \equiv 0 \pmod{2^7}$, i.e., $53^2 + 7 = 2816 \equiv 0 \pmod{2^7}$.

In Table 1, for the two case $n = 52$ and $n = 12$, we have $v_2(52) = v_2(12) = 2$. By Theorem 1.3, there exists an MDS self-dual code of length 52 and length 12 over $R = GR(2^m, 8)$ and $R = GR(2^m, 10)$, respectively, $(m = 1, 2)$. But we can not apply Theorem 3.2 to this case, therefore we don't know the existence of an MDS self-dual code for $m \geq 3$. The main point of Theorem 3.2 is that $-(n-1)$ should be a square element of $R = GR(2^m, r)$. The following lemma shows that $-(n-1)$ is not a square element in $\mathbb{Z}_{2^m}$, $(m \geq 3)$ if $v_2(n) = 1, 2$.

TABLE 2. (k_0, a_{k_0}, β)

$n\backslash m$	1	2	3	4	5
8	(1,1,1)	(1,1,1)	(1,1,1)	(2,−3,13)	(3,−1/3,21)
16	(1,1,1)	(1,1,1)	(1,1,1)	(1,1,1)	(2,−7,25)
32	(1,1,1)	(1,1,1)	(1,1,1)	(1,1,1)	(1,1,1)
$n\backslash m$	6	7	8	9	10
8	(3,−1/3,21)	(4,31/3,53)	(4,31/3,181)	(4,31/3,181)	(4,31/3,693)
16	(2,−7,57)	(3,−17/7,89)	(3,−17/7,217)	(3,−17/7,217)	(3,−17/7,729)
32	(2,−15,49)	(2,−15,113)	(2,−15,241)	(3,−97/15,369)	(3,−97/15,881)

TABLE 3. Existence of MDS self-dual codes of code length n over $GR(2^m, r), (m \geq 2, 1 \leq r \leq 5, 4 \leq n \leq 32)$

$r\backslash n$	4	8	12	16	20	24	28	32
1								
2	O							
3	X	O						
4	O	?	?	O				
5	X	?	?	?	?	?	?	O

LEMMA 3.3. *Let n be an even positive integer such that $n \not\equiv 0 \pmod 8$. Let $f(x) = x^2 + (n-1)$. Then there is no integer solution for $f(x) \equiv 0 \pmod{2^m}$ for $m \geq 3$.*

Proof. Suppose that β is an integer solution of $f(x) \equiv 0 \pmod{2^m}$, $(m \geq 3)$. Then

$$\beta^2 + (n-1) \equiv 0 \pmod 8.$$

Since $n-1$ is odd, β should be odd and $\beta^2 \equiv 1 \pmod 8$. Therefore $\beta^2 + (n-1) \equiv n \not\equiv 0 \pmod 8$. We conclude that $f(x) \equiv 0 \pmod{2^m}$ has no solution for $m \geq 3$. □

Although $-(n-1)$ is not a square element in $\mathbb{Z}_{2^m}$, $(m \geq 3)$ if $v_2(n) = 2$, it is still possible that $-(n-1)$ is a square element in $R = GR(2^m, r)$. We give the following open problem.

Open Problem: *Let n be a positive integer such that $n \equiv 0 \pmod 4$ and $n \not\equiv 0 \pmod 8$, and $(n-1) \mid (2^r - 1)$. Let $f(x) = x^2 + (n-1)$. Does the equation $f(x) = 0$ have a solution in $GR(2^m, r)$, $(m \geq 3)$?*

In Table 3, we show the existence of MDS self-dual codes of length n over $GR(2^m, r), (m \geq 2, 1 \leq r \leq 5, 4 \leq n \leq 32)$. In this table, 'X', 'O', and '?' represents the nonexistence, existence, and tentatively unknown existence, respectively. Using Theorem 1.2 and Theorem 3.2, the table can be verified.

4. Summary

In this paper, we studied the generalized Reed-Solomon codes over Galois rings and the stronger version of Hensel's lemma. Using these 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 $8 \mid n$. Many aspects remain to be studied in the future, including the open problem presented in the main section. The question marks '?' in Table 3 are also possible research topics in the future.

References

[1] Keith Conrad, *Hensel's lemma,* https://kconrad.math.uconn.edu/blurbs/gradnumthy/hensel.pdf

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

[3] 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.

[4] Fernando Q. Gouvêa, *p-adic Numbers An Introduction,* Second Edition, Springer, 1997, Corrected 3rd printing 2003.

[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] S. Han, *On the construction of MDS self-dual codes over Galois rings,* Journal of Applied and Pure Mathematics, **4** (2022), 211–219.

[9] W.C. Huffman, V.S. Pless, *Fundamentals of Error-correcting Codes,* Cambridge: Cambridge University Press, 2003.

[10] L. Jin and C. Xing, *New MDS Self-Dual Codes From Generalized Reed?Solomon Codes,* IEEE-IT, **63** (2017), 1434–1438.

[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 structure of linear and cyclic codes over a finite chain ring,* Appl. Algebra Engrg. Comm. Comput., **10** (2000), 489–506.

[13] G.H. Norton, A. Salagean, *On the key equation over a commutative ring,* Designs, Codes and Cryptography, **20** (2000), 125–141.

[14] G. Quintin, M. Barbier, C. Chabot, *On Generalized Reed-Solomon Codes Over Commutative and Noncommutative Rings,* IEEE-IT, **59** (2013), 5882–5897.

[15] Z.-X. Wan, *Finite Fields and Galois Rings,* World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2012.

[16] H. Yan, *A note on the constructions of MDS self-dual codes,* Cryptogr. Commun., **11** (2019), 259–268.

Sunghyu Han
School of Liberal Arts
KoreaTec
Cheonan 31253, Republic of Korea
E-mail: sunghyu@koreatech.ac.kr