J. Appl. Math. & Informatics Vol. **42**(2024), No. 6, pp. 1463 - 1474
https://doi.org/10.14317/jami.2024.1463

SQUARE ELEMENTS IN GALOIS RINGS AND MDS SELF-DUAL CODES†

SUNGHYU HAN

Abstract. Let $GR(2^m, r)$ be a Galois ring with even characteristic. We prove that if r is even and $n \equiv 0 \pmod 4$, then $-(n-1)$ is a square element in $GR(2^m, r)$ for all $m \geq 1$. Using this fact we also prove that if $(n-1) \mid (2^r - 1)$, $4 \mid n$, and r is even, then there exists an MDS(Maximum Distance Separable) self-dual code over $GR(2^m, r)$ with parameters $[n, n/2, n/2+1]$.

AMS Mathematics Subject Classification : 94B05, 13B05.
Key words and phrases : Galois ring, MDS code, self-dual code.

1. Introduction

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

Theorem 1.1. [6, 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 $k = 1, \cdots, 2^{r-1}$.*

The study for $\mathbb{F}_{2^r}$ is completed if MDS conjecture over finite fields [11, Section 7.4] is true. For odd prime p, there are numerous papers for MDS self-dual codes over $\mathbb{F}_{p^r}$ (see [4] as an example) and the research has not been completed.

MDS self-dual codes over Galois rings are studied [8]. If p is odd, then the existence of MDS self-dual codes over $GR(p^m, r)$ is equivalent to those over $\mathbb{F}_{p^r}$ [8, Theorem 3.8, Theorem 3.9]. Specifically, 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, if we have an MDS self-dual code

Received March 4, 2024. Revised May 8, 2024. Accepted June 9, 2024.
†This paper was supported by the Education and Research Promotion Program of KOREATECH in 2024.

TABLE 1. Positive integers n such that $(n-1) \mid (2^r-1)$, $4 \mid n$, $n \geq 8$, and $3 \leq r \leq 10$

r	n	r	n
3	8	7	128
4	16	8	16, 52, 256
5	32	9	8, 512
6	8, 64	10	12, 32, 1024

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 difficult. The focus of this paper is about MDS self-dual codes over $GR(2^m, r)$. If $m = 1$, then $GR(2^m, r) = \mathbb{F}_2^r$. 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. [8, 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.*

From the above theorem, we will consider $n \geq 8$ and $4 \mid n$ for code length n. The following theorem gives construction method for some MDS self-dual codes.

Theorem 1.3. [9, 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 above theorem is developed to the following theorem.

Theorem 1.4. [10, 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 $[n, n/2, n/2+1]$.*

In Table 1, we give positive integers n such that $(n-1) \mid (2^r-1)$, $4 \mid n$, $n \geq 8$, and $3 \leq r \leq 10$. In Table 1, for the case $n = 8, 16, 32, 64, 128, 256, 512, 1024$, since $8 \mid n$, by Theorem 1.4, we know that there exists an MDS self-dual code over $R = GR(2^m, r)$ with parameters $[n, n/2, n/2+1]$.

In Table 1, for the two cases $n = 52$ and $n = 12$, we have $8 \nmid 52$ and $8 \nmid 12$. 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, for $m = 1, 2$. But we can not apply Theorem 1.4 to this case, therefore we don't know the existence of an MDS self-dual code for $m \geq 3$. The main point of the proof of Theorem 1.4 is that $-(n-1)$ should be a square element of $R = GR(2^m, r)$. If $8 \mid n$, then we have the following result.

Lemma 1.5. [10, 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 $m \geq 1$.*

The following lemma shows that $-(n-1)$ is not a square element in $\mathbb{Z}_{2^m}$, $(m \geq 3)$ if $8 \nmid n$.

Lemma 1.6. [10, 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 $m \geq 3$.*

Although $-(n-1)$ is not a square element in $\mathbb{Z}_{2^m}$, $(m \geq 3)$ if $8 \nmid n$, it is still possible that $-(n-1)$ is a square element in $R = GR(2^m, r)$. In this paper, we prove that if r is even and $n \equiv 0 \pmod 4$, then $-(n-1)$ is a square element in $GR(2^m, r)$ for all $m \geq 1$. Using this fact we also prove that if $(n-1) \mid (2^r - 1)$, $4 \mid n$, and r is even, then there exists an MDS self-dual code over R with parameters $[n, n/2, n/2 + 1]$.

This paper is organized as follows. In Section 2, we provide basic facts for Galois rings, linear codes, MDS codes, self-dual codes, and generalized Reed-Solomon codes. In Section 3, we describe our main results. In Section 4, we summarize this paper and give some future works. All the computations are made using Magma software [1].

2. Preliminaries

2.1. Galois rings. In this subsection, we present some well-known facts about Galois rings (see [17] as an example). Let p be a fixed prime and m be a positive integer. First, we consider the following canonical projection

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

which is defined by

$$\mu(c) = c \pmod p.$$

The map μ can be extended naturally to the following map

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

which is defined by

$$\mu(a_0 + a_1 x + \cdots + a_n x^n) = \mu(a_0) + \mu(a_1)x + \cdots + \mu(a_n)x^n.$$

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

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

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

$$a_0 + a_1x + \cdots + a_{r-1}x^{r-1} + (f(x)),$$

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

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 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

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

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

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

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

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

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

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 [14, 15]:

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

where the columns are grouped into square blocks of sizes $k_0, k_1, \ldots, k_{m-1}$. The rank of C, denoted by $\text{rank}(C)$, is defined to be the number of nonzero rows of its generator matrix G in a standard form. Therefore $\text{rank}(C) = \sum_{i=0}^{m-1} k_i$. We call k_0 in G the free rank of a code C. If $\text{rank}(C) = k_0$, 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 [13] as an example) that for a (linear or nonlinear) code C of length n over any finite alphabet A,

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

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

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

Codes meeting this bound are called maximum distance with respect to rank (MDR) codes [3, 15]. The following lemma states the necessary and sufficient condition for MDS codes over Galois rings (see [7] 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 $\mathbf{x}, \mathbf{y} \in GR(p^m, r)^n$,

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

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

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

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 $R = GR(p^m, r)$ [15, 16]. We start with the following definition (see [15, Definition 2.2], [16, 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 $s \neq t$.

We have the following result for subtractive subsets of Galois rings.

Lemma 2.3. [10, 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 $|B| \leq |T|$.*

Now we define the generalized Reed-Solomon codes over Galois rings (see [15, Example 3.7], [16, Definition 22] as examples).

Definition 2.4. Let $R = GR(p^m, r)$ and n, k be two positive integers such that $1 \leq k \leq n$. Let P_k be the set of polynomials over R of degree less than k, including the zero polynomial in $R[x]$. Let $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ be a subtractive subset of R, $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in R^n$, and $v = (v_1, v_2, \ldots, v_n) \in R^n$, where v_i is unit for $1 \leq i \leq n$. Then the generalized Reed-Solomon code, $GRS_k(\alpha, v)$ is defined by

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

The following theorem is used in the main section. The proof can be found in [16, Proposition 23, Corollary 24, Proposition 25].

Theorem 2.5. *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*

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

3. Main

We start with the following two definitions.

Definition 3.1. Let t be a non-zero element of $GR(p^m, r)$ with the representation

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

where $t_i \in T, (0 \le i \le m-1)$ and $T = \{0, 1, \xi, \xi^2, \ldots, \xi^{p^r-2}\}$ is the Teichmüller representatives. We define the p-adic valuation of t, $v_p(t)$, by the first i such that $t_i \neq 0$. In other words,

$$v_p(t) = i, \ (t_0 = t_1 = \cdots = t_{i-1} = 0, \ t_i \neq 0).$$

Definition 3.2. Let t be an element of $GR(p^m, r)$. We define the p-adic absolute value of t by

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

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

The two definitions on $GR(p^m, r)$ above are similar to the two definitions, p-adic valuation on $\mathbb{Q}$ and p-adic absolute value on $\mathbb{Q}$ [5, Definition 2.1.2, Definition 2.1.4].

Example 3.3. Consider the Galois ring $GR(2^{10}, 8)$.
Then $GR(2^{10}, 8) = \mathbb{Z}_{2^{10}}[x]/(h(x))$, $h(x) = x^8 + 4x^7 + 2x^6 + 6x^5 + 3x^4 + 5x^3 + 3x^2 + 2x + 1$. $\overline{h}(x) = x^8 + x^4 + x^3 + x^2 + 1$ is a primitive polynomial [12, p. 553] and $h(x)$ is a Hensel lift of $\overline{h}(x)$. Let $\xi = x + (h(x))$ and $p = 2$. If $t = 1 + \xi \cdot p$, then $v_p(t) = 0$ and $|t|_p = p^{-0} = 1$. If $t = \xi^3 \cdot p^2 + \xi^2 \cdot p^3$, then $v_p(t) = 2$ and $|t|_p = p^{-2} = \frac{1}{4}$.

We are ready to prove our main results.

Theorem 3.4. *Let n be an integer with $n \equiv 0 \pmod 4$. If r is even then $-(n-1)$ is a square element in $GR(2^m, r)$ for all $m \geq 1$.*

Proof. Our proof is similar to the first proof of Theorem 4.1 in [2]. For a fixed m, let $R = GR(2^m, r)$. Then $R = \mathbb{Z}_{2^m}[x]/(h(x))$, where $h(x)$ is a basic primitive polynomial of degree r. Let $\xi = x + (h(x))$. Then $|\xi| = 2^r - 1$. Since r is even, $2^r - 1$ is divisible by 3. Let $\alpha = \xi^{\frac{2^r-1}{3}}$. Then $\alpha^3 = 1$ and $1 + \alpha + \alpha^2 = 0$ in R. Let $p = 2$ and $a = 1 + 2\alpha$ in R. Let $f(x) = x^2 + (n-1)$. Then $f'(x) = 2x$. If $n \equiv 0 \pmod 8$, then there is an integer solution for $f(x) \equiv 0 \pmod{2^m}$ for all $m \geq 1$ by Lemma 1.5. Therefore we assume that $n \not\equiv 0 \pmod 8$. If $m = 1$ or $m = 2$, then $-(n-1) = 1$ in R and $-(n-1)$ is a square element in R. So, we assume that $m \geq 3$.

Note that $f(a) = a^2 + (n-1) = (1+2\alpha)^2 + (n-1) = 4(1+\alpha+\alpha^2) - 3 + (n-1) = n - 4$. Therefore $f(a) \equiv 0 \pmod 8$ and $|f(a)|_p \leq 2^{-3}$. $f'(a) = 2(1+2\alpha) = 2 + \alpha \cdot 2^2$ and $|f'(a)|_p^2 = 2^{-2}$. If $|f(a)|_p = 0$, then $f(a) = 0$ and $-(n-1)$ is a square element in R. So, we assume that $|f(a)|_p \neq 0$. Let $t = |f(a)|_p / |f'(a)|_p^2$. Then $t = 2^{-t_1}$ for some $t_1 \geq 1$.

We define a sequence a_k in R. Let $a_1 = a$ and

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

We claim the followings:

(i) a_k is well-defined and a unit in R.
(ii) $|f'(a_k)|_p = |f'(a_1)|_p = 2^{-1}$.
(iii) $|f(a_k)|_p \leq |f'(a_1)|_p^2 \cdot t^{2^{k-1}} = 2^{-2} \cdot 2^{-t_1 \cdot 2^{k-1}}$.

We prove the claim by induction on k. If $k = 1$, then the claim is clearly true. Assume that (i), (ii), and (iii) are true for k. To prove (i) for $k+1$, note that using (ii) and (iii) we have

$$|f(a_k)|_p / |f'(a_k)|_p \leq \frac{2^{-2} \cdot 2^{-t_1 \cdot 2^{k-1}}}{2^{-1}} = 2^{-1} \cdot 2^{-t_1 \cdot 2^{k-1}}.$$

This means that $\frac{f(a_k)}{f'(a_k)}$ is well-defined and a_{k+1} is a unit in R. So, (i) is true for $k+1$. To prove (ii) for $k+1$, note that

$$|f'(a_{k+1})|_p = |2a_{k+1}|_p = 2^{-1}|a_{k+1}|_p.$$

Since a_{k+1} is a unit, $|a_{k+1}|_p = 1$ and $|f'(a_{k+1})|_p = 2^{-1}$. So, (ii) is true for $k+1$. To prove (iii) for $k+1$, note that

$$\begin{aligned}
f(a_{k+1}) &= (a_k - f(a_k)/f'(a_k))^2 + (n-1) \\
&= a_k^2 - 2a_k \frac{f(a_k)}{f'(a_k)} + (f(a_k)/f'(a_k))^2 + (n-1) \\
&= a_k^2 + (n-1) - 2a_k \frac{f(a_k)}{2a_k} + (f(a_k)/f'(a_k))^2 \\
&= f(a_k) - f(a_k) + (f(a_k)/f'(a_k))^2 \\
&= (f(a_k)/f'(a_k))^2.
\end{aligned}$$

Therefore

$$|f(a_{k+1})|_p = |f(a_k)/f'(a_k)|_p^2 = \frac{|f(a_k)|_p^2}{|f'(a_1)|_p^2} \le \frac{|f'(a_1)|_p^4 t^{2k}}{|f'(a_1)|_p^2} = |f'(a_1)|_p^2 \cdot t^{2k}.$$

This completes the induction. We choose the smallest positive integer k_0 such that $2 + t_1 \cdot 2^{k_0-1} \ge m$. Then we have $f(a_{k_0}) = 0$ in R by (iii). This completes the proof. □

For the sequence a_k in the proof of Theorem 3.4, we claim that $a_k = b_k(1+2\alpha)$ for some $b_k \in \mathbb{Z}_{2^m}$. We prove this by induction. Note that $b_1 = 1$. Assume that $a_k = b_k(1+2\alpha)$ for some $b_k \in \mathbb{Z}_{2^m}$. Then,

$$\begin{aligned} a_{k+1} &= a_k - \frac{f(a_k)}{f'(a_k)} \\ &= b_k(1+2\alpha) - \frac{(b_k(1+2\alpha))^2 + (n-1)}{2b_k(1+2\alpha)} \\ &= b_k(1+2\alpha) - \frac{b_k^2(-3) + (n-1)}{2b_k}\Big(-\frac{1+2\alpha}{3}\Big) \\ &= b_k(1+2\alpha) + \frac{-3b_k^2 + (n-1)}{2 \cdot 3 \cdot b_k}(1+2\alpha) \\ &= \Big(b_k + \frac{-3b_k^2 + (n-1)}{2}\Big)(3^{-1})(b_k^{-1})(1+2\alpha) \end{aligned}$$

Therefore

$$b_{k+1} = b_k + \frac{-3b_k^2 + (n-1)}{2}(3^{-1})(b_k^{-1}) \in \mathbb{Z}_{2^m}$$

and $b_{k+1} \in \mathbb{Z}_{2^m}$. This completes the proof.

Using the sequence a_k and b_k, we give a calculation β such that $\beta^2 = -(n-1)$ in $GR(2^m, r)$ for the two cases, $n = 52$, $r = 8$, $m = 10$ and $n = 12$, $r = 10$, $m = 10$. For the first case, $n = 52$, $r = 8$, $m = 10$. Let $R = GR(2^{10}, 8) = \mathbb{Z}_{2^{10}}[x]/(h(x))$, where $h(x)$ is the polynomial in Example 3.3. Let $\xi = x + (h(x))$. $|\xi| = 2^8 - 1 = 255$. Let $\alpha = \xi^{255/3} = \xi^{85}$. Therefore $\alpha^3 = 1$ and $(\alpha-1)(\alpha^2+\alpha+1) = 0$. Since $\alpha \ne 1$, we have $\alpha^2+\alpha+1 = 0$, $(1+2\alpha)^2 = 1+4\alpha+4\alpha^2 = -3+4(1+\alpha+\alpha^2) = -3$, $(1+2\alpha)^{-1} = (1+2\alpha)/(-3)$, and $f(a) = (1+2\alpha)^2 + 51 = 3 \times 2^4$. Therefore $|f(a)|_p = 2^{-4}$ and $|f(a)/f'(a)^2|_p = 2^{-4}/2^{-2} = 2^{-2}$. So, $t_1 = 2$. We choose the smallest positive integer k_0 such that $2 + 2 \cdot 2^{k_0-1} \ge 10$. So, $k_0 = 3$. We have $b_1 = 1$, and

$$\begin{aligned} b_2 &= b_1 + \frac{-3b_1^2 + (n-1)}{2}(3^{-1})(b_1^{-1}) \\ &= 1 + \frac{-3 \cdot 1^2 + (52-1)}{2}(3^{-1})(1^{-1}) \\ &= 1 + \frac{48}{2}(3^{-1})(1^{-1}) \\ &= 1 + 24(3^{-1})(1^{-1}) \end{aligned}$$

$$= \quad 1 + 24(683)(1) = 9,$$

and

$$\begin{aligned} b_3 &= b_2 + \frac{-3b_2^2 + (n-1)}{2}(3^{-1})(b_2^{-1}) \\ &= 9 + \frac{-3 \cdot 9^2 + (52-1)}{2}(3^{-1})(9^{-1}) \\ &= 9 + \frac{-192}{2}(3^{-1})(9^{-1}) \\ &= 9 - 96(3^{-1})(9^{-1}) \\ &= 9 - 96(683)(569) = 233. \end{aligned}$$

Therefore $a_1 = 1 + 2\alpha$, $a_2 = 9(1 + 2\alpha)$, $a_3 = 233(1 + 2\alpha)$, and $\beta = a_3$ is a solution of $f(x) = x^2 + (52-1) = 0$ in $GR(2^{10}, 8)$. Note that β is also a solution of $f(x) = x^2 + (52-1) = 0$ in $GR(2^m, 8)$ for $1 \leq m \leq 9$. More specifically, the solutions are the following: $\beta = 233 + 466\alpha$ in $GR(2^9, 8)$, $\beta = 233 + 210\alpha$ in $GR(2^8, 8)$, $\beta = 105 + 82\alpha$ in $GR(2^7, 8)$, $\beta = 41 + 18\alpha$ in $GR(2^6, 8)$, $\beta = 9 + 18\alpha$ in $GR(2^5, 8)$, $\beta = 9 + 2\alpha$ in $GR(2^4, 8)$, $\beta = 1 + 2\alpha$ in $GR(2^3, 8)$, $\beta = 1 + 2\alpha$ in $GR(2^2, 8)$, $\beta = 1$ in $GR(2^1, 8)$.

For the second case, $n = 12$, $r = 10$, $m = 10$. Let $R = GR(2^{10}, 10) = \mathbb{Z}_{2^{10}}[x]/(h(x))$ and $h(x) = x^{10} + 6x^5 + 4x^4 + 7x^3 + 1$. $\overline{h}(x) = x^{10} + x^3 + 1$ is a primitive polynomial [12, p. 553] and $h(x)$ is a Hensel lift of $\overline{h}(x)$. Let $\xi = x + (h(x))$. Then $|\xi| = 2^{10} - 1 = 1023$. Let $\alpha = \xi^{1023/3} = \xi^{341}$. By similar calculation to the first case, we have $t_1 = 1$, $k_0 = 4$, $b_1 = 1$, $b_2 = 685$, $b_3 = 197$, and $b_4 = 549$. Therefore $a_1 = 1 + 2\alpha$, $a_2 = 685(1 + 2\alpha)$, $a_3 = 197(1 + 2\alpha)$, $a_4 = 549(1 + 2\alpha)$, and $\beta = a_4$ is a solution of $f(x) = x^2 + (12 - 1) = 0$ in $GR(2^{10}, 10)$. Like the first case, β is also a solution of $f(x) = x^2 + (12-1) = 0$ in $GR(2^m, 10)$ for $1 \leq m \leq 9$. More specifically, the solutions are the following: $\beta = 37 + 74\alpha$ in $GR(2^9, 10)$, $\beta = 37 + 74\alpha$ in $GR(2^8, 10)$, $\beta = 37 + 74\alpha$ in $GR(2^7, 10)$, $\beta = 37 + 10\alpha$ in $GR(2^6, 10)$, $\beta = 5 + 10\alpha$ in $GR(2^5, 10)$, $\beta = 5 + 10\alpha$ in $GR(2^4, 10)$, $\beta = 5 + 2\alpha$ in $GR(2^3, 10)$, $\beta = 1 + 2\alpha$ in $GR(2^2, 10)$, $\beta = 1$ in $GR(2^1, 10)$.

We state the main theorem of this paper in the following.

Theorem 3.5. *Let $R = GR(2^m, r)$, and n be a positive integer such that $(n-1) \mid (2^r - 1)$ and $4 \mid n$. If r is even, then there exists an MDS self-dual code over R with parameters $[n, n/2, n/2 + 1]$.*

Proof. By Theorem 3.4, there exists a unit β in R such that $\beta^2 = -(n-1)$. 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. Let $\delta = (0, 1, \alpha, \alpha^2, \ldots, \alpha^{n-2})$ and $v = (\beta, 1, 1, \ldots, 1)$. Let C be the code $GRS_{\frac{n}{2}}(\delta, v)$. Then by Theorem 2.5, C is an $[n, \frac{n}{2}, \frac{n}{2} - 1]$ MDS

Table 2. Integers n such that $(n-1) \mid (2^r-1)$, $2 \mid r$, $4 \mid n$, $8 \nmid n$, $n \geq 8$, $(2 \leq r \leq 20)$

r	n
8	52
10	12
12	36, 92, 196, 316, 820
14	44
16	52, 772, 13108
18	20, 28, 172, 220, 1388, 1972, 12484
20	12, 76, 124, 156, 276, 452, 3076, 5116, 6356, 11276, 209716

code with the following generator matrix G:

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

We prove that C is self-dual by showing that the inner product of two rows of G is zero. Let G_i be the i-th row of G. First, note that

$$G_1 \cdot G_1 = \beta^2 + 1^2 + 1^2 + \cdots + 1^2 = \beta^2 + (n-1) = 0.$$

For the other cases,

$$\begin{aligned} G_i \cdot G_j &= 1 \cdot 1 + \alpha^{i-1}\alpha^{j-1} + (\alpha^2)^{i-1}(\alpha^2)^{j-1} + \cdots + (\alpha^{n-2})^{i-1}(\alpha^{n-2})^{j-1} \\ &= 1 + \alpha^{i+j-2} + (\alpha^2)^{i+j-2} + (\alpha^3)^{i+j-2} + \cdots + (\alpha^{n-2})^{i+j-2} \\ &= 1 + (\alpha^{i+j-2}) + (\alpha^{i+j-2})^2 + (\alpha^{i+j-2})^3 + \cdots + (\alpha^{i+j-2})^{n-2} \\ &= \frac{1-(\alpha^{i+j-2})^{n-1}}{1-\alpha^{i+j-2}}, \end{aligned}$$

where $1 \leq i+j-2 \leq n-2$. Since $1-(\alpha^{i+j-2})^{n-1} = 1-(\alpha^{n-1})^{i+j-2} = 1-1 = 0$. Therefore $G_i \cdot G_j = 0$ and C is MDS self-dual. □

In Table 2, we give integers n such that $(n-1) \mid (2^r-1)$, $2 \mid r$, $4 \mid n$, $8 \nmid n$, $n \geq 8$, $(2 \leq r \leq 20)$. Therefore, for the integers n in Table 2 we can make MDS self-dual codes of code length n using Theorem 3.5.

The remaining problem is that r is odd. In other words, we have the following question: Let $(n-1) \mid (2^r-1)$, $4 \mid n$, $n \geq 8$, $8 \nmid n$, $m \geq 3$, and r be an odd positive integer. Does $-(n-1)$ be a square element in $GR(2^m, r)$? We made a calculation using Magma software and have the following result: There does not exist n such that $(n-1) \mid (2^r-1)$, r is odd, $4 \mid n$, $n \geq 8$, $8 \nmid n$ for $r \leq 673$. So, we give the following conjecture.

Table 3. Current state of the existence of MDS self-dual codes of code length n over $GR(2^m, r), (m \geq 2, 3 \leq r \leq 10)$

r	n : known existence	n : unknown existence
3	8	
4	4, 16	8, 12
5	32	$4k$, $(2 \leq k \leq 7)$
6	4, 8, 64	$4k$, $(3 \leq k \leq 15)$
7	128	$4k$, $(2 \leq k \leq 31)$
8	4, 16, 52, 256	8, 12, $4k$, $(5 \leq k \leq 12, 14 \leq k \leq 63)$
9	8, 512	$4k$, $(3 \leq k \leq 127)$
10	4, 12, 32, 1024	8, $4k$, $(4 \leq k \leq 7, 9 \leq k \leq 255)$

Conjecture : *There does not exist a positive integer* n *such that* $(n-1) \mid (2^r-1)$, r *is odd,* $4 \mid n$, $n \geq 8$, $8 \nmid n$.

If the conjecture is true, then the condition, "r is even", can be removed in Theorem 3.5.

In Table 3, we give the current state of the existence of MDS self-dual codes of code length n over $GR(2^m, r), (n \geq 8, m \geq 2, 3 \leq r \leq 10)$. In Table 3, the second column gives the code length n for which MDS self-dual codes exist, and the third column gives the code length n for which we don't know the existence of such codes.

4. Summary

In this paper, we defined the p-adic valuation and p-adic absolute value in Galois rings, which are similar concepts to those defined in rational numbers. With these concepts we proved that if r is even and $n \equiv 0 \pmod 4$, then $-(n-1)$ is a square element in $GR(2^m, r)$ for all $m \geq 1$. Using this fact we also proved that if $(n-1) \mid (2^r - 1)$, $4 \mid n$, and r is even, then there exists an MDS self-dual code over $GR(2^m, r)$ with parameters $[n, n/2, n/2 + 1]$. Many aspects remain to be studied in the future, including the conjecture presented in the main section. The unknown cases in Table 3 are also possible research topics in the future.

Conflicts of interest : The author declare no conflict of interest.

Data availability : Not applicable

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. Keith Conrad, *Hensel's lemma*, https://kconrad.math.uconn.edu/blurbs/gradnumthy/hensel.pdf
3. S.T. Dougherty and K. Shiromoto, *MDR Codes over* $\mathbb{Z}_k$, IEEE-IT **46** (2000), 265-269.

4. X. Fang, K. Lebed, H. Liu, and J. Luo, *New MDS self-dual codes over finite fields of odd characteristic*, Des. Codes Cryptogr. **88** (2020), 1127-1138.
5. Fernando Q. Gouvêa, *p-adic Numbers An Introduction*, Second Edition, Springer, 1997, Corrected 3rd printing 2003.
6. M. Grassl and T.A. Gulliver, *On self-dual MDS codes*, In: Proceedings of ISIT (2008), 1954-1957.
7. S. Han, *MDS self-dual codes and antiorthogonal matrices over Galois rings*, MDPI Information **10** (2019), 1-12.
8. S. Han, *On the existence of MDS self-dual codes over finite chain rings*, J. Chungcheong Math. Soc. **33** (2020), 255-270.
9. S. Han, *On the construction of MDS self-dual codes over Galois rings*, Journal of Applied and Pure Mathematics **4** (2022), 211-219.
10. S. Han, *MDS self-dual codes over Galois rings with even characteristic*, J. Chungcheong Math. Soc. **36** (2023), 181-194.
11. W.C. Huffman and V.S. Pless, *Fundamentals of Error-correcting Codes*, Cambridge University Press, Cambridge, 2003.
12. R. Lidl, H. Niederreiter, *Finite Fields*, Addison-Wesley Publishing Company, 1983.
13. F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes,* Amsterdam, The Netherlands: North-Holland, 1977.
14. G.H. Norton and A. Salagean, *On the structure of linear and cyclic codes over a finite chain ring*, Appl. Algebra Engrg. Comm. Comput. **10** (2000), 489-506.
15. G.H. Norton and A. Salagean, *On the key equation over a commutative ring*, Designs, Codes and Cryptography **20** (2000), 125-141.
16. G. Quintin, M. Barbier, and C. Chabot, *On Generalized Reed-Solomon Codes Over Commutative and Noncommutative Rings*, IEEE-IT **59** (2013), 5882-5897.
17. 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