JOURNAL OF THE
CHUNGCHEONG MATHEMATICAL SOCIETY
Volume **31**, No. 2, May 2018
http://dx.doi.org/10.14403/jcms.2018.31.1.269

SELF-DUAL CODES AND ANTIORTHOGONAL MATRICES OVER GALOIS RINGS

Sunghyu Han*

Abstract. We study self-dual codes over Galois rings using the building-up construction method. In the construction, the existence of an antiorthogonal matrix is very important. In this study, we examine the existence problem of an antiorthogonal matrix over Galois rings.

1. Introduction

In this study, we are interested in self-dual codes. Self-dual codes are interesting, because they are closely related to other areas of mathematics, such as block designs, lattices, modular forms, and sphere packings [4]. Moreover, they are of interest in their own right (see [18], for example).

There are several approaches to constructing self-dual codes, such as the gluing vectors approach [3], the balance principle approach [9], the double circulant approach [5], and the building-up approach [13]. In this study, we adopt the building-up approach, in which short self-dual codes are used to construct longer codes.

The first appearance of building-up construction is in Harada's paper [8]. Kim [10] extended this method and called it "building-up construction." He also made the converse statement: any binary self-dual code can be constructed from a shorter self-dual code. Kim and Lee [11] described the building-up approach for finite fields $\mathbb{F}_q$, where q is a power of 2 or $q \equiv 1 \pmod 4$. Later, they described the building-up approach for finite fields $\mathbb{F}_q$, $q \equiv 3 \pmod 4$ [13].

Received January 05, 2018; Accepted May 01, 2018.
2010 Mathematics Subject Classification: 94B05.
Key words and phrases: antiorthogonal matrix, building-up construction, Galois rings, self-dual codes.
*Supported by the 2018 Professor Education and Research Promotion Program of KoreaTech.

For $\mathbb{Z}_{p^m}$, the building-up construction for $p \equiv 1 \pmod 4$ is given by Lee and Lee [14]. Then, $p \equiv -1 \pmod 4$ is given by Kim and Lee [13], and $p = 2$ is given by Han [6, 7].

Thus, the building-up construction method is completely described for the finite field $\mathbb{F}_{p^r}$ and integer modulo ring $\mathbb{Z}_{p^m}$.

The natural next step is the study of Galois rings $GR(p^m, r)$. In $GR(p^m, r)$, if $m = 1$, then $GR(p^1, r) = \mathbb{F}_{p^r}$, and if $r = 1$, then $GR(p^m, 1) = \mathbb{Z}_{p^m}$. Therefore, we already have the building-up construction of $GR(p^m, r)$ for $m = 1$ or $r = 1$.

For $GR(p^m, r)$, $p \equiv 1 \pmod 4$ with any r, and $p \equiv -1 \pmod 4$ with even r, the building-up construction method is described, with examples, in [12]. For $GR(p^m, r)$, $p \equiv -1 \pmod 4$ with odd r, the building-up construction method is described in [13].

The remaining case is $GR(2^m, r)$ with $m \geq 2, r \geq 2$, and is the focus of this study. This paper is organized as follows. In Sect. 2, we state the basic definitions and facts for self-dual codes over finite chain rings. We also give the building-up construction method for finite chain rings and explain Galois rings. The important part of the building-up construction is the existence of a square matrix U such that $UU^T = -I$, which is called antiorthogonal. In Sect. 3, we study the existence problem of antiorthogonal matrices over Galois rings. In Sect. 4, we give examples of self-dual codes over $GR(2^m, r)$ using the building-up construction method. All computations are performed using Magma [2].

2. Preliminaries

Throughout this paper, let R be a finite commutative ring with identity $1 \neq 0$. An R-submodule $C \leq R^n$ is called a linear code of length n over R. Unless otherwise specified, all codes are assumed to be linear.

We define the usual inner product: for $\mathbf{x}, \mathbf{y} \in R^n$,

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

For a code C of length n over R, let

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

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.

A principal ideal ring is a ring in which each ideal is generated by a single element. A chain ring is a ring in which the ideals are linearly ordered. Thus, it follows immediately that a chain ring R is necessarily a principal ideal ring and that the ideals of the ring R are

$$\{0\} = \langle \gamma^e \rangle \subseteq \langle \gamma^{e-1} \rangle \subseteq \cdots \subseteq \langle \gamma^2 \rangle \subseteq \langle \gamma \rangle \subseteq R,$$

for some element γ and some natural number e. The number e is said to be the nilpotency index of γ.

It is well known [17] that a generator matrix for a code C over a finite chain ring is permutation-equivalent to the matrix of the form

(2.1)

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

where e is the nilpotency index of γ. The generator matrix G is said to be in *standard form*. All generator matrices in standard form for a code C over a finite chain ring have the same parameters $k_0, k_1, k_2, \ldots, k_{e-1}$ [17, Theorem 3.3]. We define $k_i(C) = k_i, (i = 0, 1, 2, \ldots, e-1)$ and $k(C) = \sum_{i=0}^{e-1} k_i$.

Now, we describe the building-up construction for a finite chain ring [6].

THEOREM 2.1. [6] *Let R be a finite chain ring, let C_0 be a self-dual code over R of length n with $k(C_0) = k$, and let G_0 be a $k \times n$ generator matrix for C_0. Let $a \geq 1$ be an integer and let X be an $a \times n$ matrix over R such that $XX^T = -I$. Let U be an $a \times a$ matrix over R such that $UU^T = -I$, and let 0 be an $a \times a$ zero matrix. Then, the matrix*

$$G = \left(\begin{array}{c|c|c} I & 0 & X \\ \hline -G_0 X^T & G_0 X^T U & G_0 \end{array} \right)$$

generates a self-dual code C of length $n + 2a$ over R.

The purpose of this study is to investigate the building-up construction for Galois rings. Therefore, we first provide some basic facts about Galois rings. Let p be a fixed prime and m be a positive integer. Let f be a polynomial in $\mathbb{Z}_{p^m}[x]$ and $\bar{f}$ be the image of f under the projection $\mathbb{Z}_{p^m}[x] \to \mathbb{Z}_p[x]$. Then, f is called basic irreducible if $\bar{f}$ is irreducible. Let r be the degree of f. A Galois ring is constructed as $GR(p^m, r) = \mathbb{Z}_{p^m}[x]/(f)$, where f is a monic basic irreducible polynomial in $\mathbb{Z}_{p^m}[x]$ of degree r.

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

$$\{0\} = \langle p^m \rangle \subset \langle p^{m-1} \rangle \subset \cdots \subset \langle p^2 \rangle \subset \langle p \rangle \subset GR(p^m, r). \tag{2.2}$$

The following lemma is needed in our study.

LEMMA 2.2. [1, Proposition 6.1.7] *Let $GR(p^m, r)$ be a Galois ring, where p is a prime and n, r are positive integers. Then:*

1. *Every subring is of the form $GR(p^m, s)$ for some divisor s of r. Conversely, for every positive divisor s of r there exists a unique subring of R that is isomorphic to $GR(p^m, s)$.*
2. *Any homomorphic image ($\neq (0)$) of $GR(p^m, r)$ is a ring of the form $GR(p^\ell, r)$ for some integer $1 \leq \ell \leq m$. Conversely, for each integer $1 \leq \ell \leq m$, there are exactly r homomorphisms of $GR(p^m, r)$ onto $GR(p^\ell, r)$.*

To apply Theorem 2.1 to self-dual codes over $GR(p^m, r)$, we should have an $a \times a$ matrix U and an $a \times n$ matrix X such that $UU^T = -I$ and $XX^T = -I$. For $1 \leq a \leq n$, if there exists an $a \times a$ matrix U, then there exists an $a \times n$ matrix X such that $XX^T = -I$. The proof is given below. Let $X = [U|O]$. Then, $XX^T = UU^T + OO^T = -I$. Therefore, the important part of the building-up construction is the existence of the matrix U.

The square matrix U such that $UU^T = -I$ over finite fields is considered by Massey [15]. He called the matrix U antiorthogonal. Using the antiorthogonal matrix, he characterized the self-dual codes and constructed linear codes with complementary duals (LCD codes). In [16], Massey considered the existence problem of antiorthogonal matrices over finite fields. Following Massey's terminology, we provide the following definition.

DEFINITION 2.3. A square matrix U over a finite chain ring R is said to be antiorthogonal if

$$UU^T = -I. \tag{2.3}$$

3. On the problem of the existence of antiorthogonal matrices over $GR(p^m, r)$

In this section, we examine the existence of an $a \times a$ antiorthogonal matrix U over $GR(p^m, r)$. We begin with the following lemmas.

LEMMA 3.1. [12] *Let p be an odd prime. Then -1 is a square in $GR(p^m, r)$ if and only if either $p \equiv 1 \pmod 4$ with any r or $p \equiv -1 \pmod 4$ with even r.*

LEMMA 3.2. [13] *Let $p \equiv -1 \pmod 4$ and r be an odd integer. Then -1 is a two square sum in $GR(p^m, r)$.*

Proof. See the proof of Proposition 3.3 in [13]. □

THEOREM 3.3. *Let p be an odd prime. For the existence of an $a \times a$ antiorthogonal matrix U over $GR(p^m, r)$, we have the following.*

1. *If $p \equiv 1 \pmod 4$ with any r or $p \equiv -1 \pmod 4$ with even r, then there exists an $a \times a$ antiorthogonal matrix U for all $a \geq 1$.*
2. *If $p \equiv -1 \pmod 4$ with odd r, then there exists an $a \times a$ antiorthogonal matrix U if and only if a is even.*

Proof. We assume that $p \equiv 1 \pmod 4$ with any r or $p \equiv -1 \pmod 4$ with even r. By Lemma 3.1, there is an element c in $GR(p^m, r)$ such that $c^2 = -1$. Let U be an $a \times a$ diagonal matrix with all diagonal elements c, that is,

$$U = \begin{pmatrix} c & & 0 \\ & \ddots & \\ 0 & & c \end{pmatrix}.$$

Then, $UU^T = -I$. This proves the first statement.

We now assume that $p \equiv -1 \pmod 4$ with odd r. By Lemma 3.2, there exist α, β such that $\alpha^2 + \beta^2 = -1$ in $GR(p^m, r)$. Let

$$U_2 = \begin{pmatrix} \alpha & \beta \\ \beta & -\alpha \end{pmatrix}.$$

Then, $U_2 U_2^T = -I$. This proves that there is a 2×2 matrix U such that $UU^T = -I$. For $a = 2t$, where $t \geq 1$, let

$$U_a = \begin{pmatrix} U_2 & & 0 \\ & \ddots & \\ 0 & & U_2 \end{pmatrix}.$$

Then, $U_a U_a^T = -I$.

Finally, we assume that there is an $a \times a$ matrix U such that $UU^T = -I$. Then, $\det(UU^T) = \det(-I)$, and so $(\det U)^2 = (-1)^a$. Therefore, a should be even by Lemma 3.1. This completes the proof. □

Therefore, the odd prime case is solved completely for the existence of an antiorthogonal matrix. Now, we consider the case of $p = 2$.

LEMMA 3.4. [12] *Let $p = 2$. Then -1 is a square in $GR(2^m, r)$ if and only if $m = 1$.*

THEOREM 3.5. *For the existence of an $a \times a$ antiorthogonal matrix U over $GR(2^m, r)$, we have the following.*

1. *If $m = 1$, then there exists an $a \times a$ antiorthogonal matrix U for all $a \geq 1$.*
2. *If $m \geq 2$ and $r = 1$, then there exists an $a \times a$ antiorthogonal matrix U if and only if a is a multiple of 4.*

Proof. Suppose that $m = 1$. Then, $GR(2, r) = GF(2^r)$. Since the $a \times a$ identity matrix I is the antiorthogonal matrix, the first state statement is true. Suppose $m \geq 2$ and $r = 1$. Then, $GR(2^m, 1) = \mathbb{Z}_{2^m}$. The second statements is proved in [7, Theorem 4], $\square$

By Theorem 3.5, we next consider the case $m \geq 2$ and $r \geq 2$.

THEOREM 3.6. *Let $m \geq 2$ and $r \geq 2$. For the existence of an $a \times a$ matrix U over $GR(2^m, r)$ such that $UU^T = -I$, we have the following.*

1. *If there exists an $a \times a$ antiorthogonal matrix U, then a should be even.*
2. *If a is a multiple of 4, then there exists an $a \times a$ antiorthogonal matrix U.*

Proof. Suppose there exists an $a \times a$ matrix U such that $UU^T = -I$. Then $\det(UU^T) = \det(-I)$, $(\det U)^2 = (-1)^a$. Therefore, a should be even, by Lemma 3.4. This completes the first statement. For the second statement, note that $\mathbb{Z}_{2^m} \leq GR(2^m, r)$. It is proved that there is a $4t \times 4t$ antiorthogonal matrix U over $\mathbb{Z}_{2^m}$ for all $t \geq 1$ in [7, Theorem4]. This completes the proof. $\square$

Now, the remaining case is that of $m \geq 2$, $r \geq 2$, and $a = 4t+2 (t \geq 0)$.

LEMMA 3.7. *-1 is a two square sum in $GR(2^m, 2k)$ for all $k \geq 1$ and for all $m \geq 1$.*

Proof. First, we prove the theorem for the $k = 1$ case. Let $f(x) = x^2 + x + 1$ in $\mathbb{Z}_{2^m}[x]$. Then, $f(x)$ is a basic irreducible polynomial. Therefore, $GF(2^m, 2) = \mathbb{Z}_{2^m}[x]/(f(x))$. Let $w = x + (f(x))$. Let $\alpha = w, \beta = w + 1$. Then, $\alpha^2 + \beta^2 = w^2 + (w+1)^2 = w^2 + (w^2 + 2w + 1) = (w^2 + w + 1) + (w^2 + w) = 0 + (-1) = -1$. Therefore, -1 is a two square sum in $GF(2^m, 2)$. Let $k \geq 2$. By Lemma 2.2 (i), $GR(2^m, 2k)$ contains a unique subring R that is isomorphic to $GR(2^m, 2)$. Therefore, -1 is a two square sum in $GR(2^m, 2k)$. This completes the proof. $\square$

TABLE 1. Values of α, β such that $\alpha^2 + \beta^2 = -1$ in $GR(2^2, r) = \mathbb{Z}_{2^2}[x]/(f(x))$

r	$f(x)$	α, β $(w = x + (f(x)))$
2	$x^2 + x + 1$	$w, w + 1$
3	$x^3 + x + 1$	-
4	$x^4 + x + 1$	$w^2 + w, w^2 + w + 1$
5	$x^5 + x^2 + 1$	-
6	$x^6 + x^4 + x^3 + x + 1$	$w^3 + w^2 + w, w^3 + w^2 + w + 1$
7	$x^7 + x + 1$	-
8	$x^8 + x^4 + x^3 + x^2 + 1$	$w^7 + w^6 + w^4 + w^2 + w, w^7 + w^6 + w^4 + w^2 + w + 1$

In Table 1, we give our computational results. By the computation, we can see that -1 is a two square sum in $GR(2^2, r), r = 2, 4, 6, 8$. For example, if $r = 4$, then $GR(2^2, 4)$ is $\mathbb{Z}_{2^2}[x]/(x^4 + x + 1)$ and $(w^2 + w)^2 + (w^2 + w + 1)^2 = -1$, where $w = x + (x^4 + x + 1)$. This result is consistent with Lemma 3.7. In addition, we find that -1 is not a two square sum in $GR(2^2, r), r = 3, 5, 7$.

THEOREM 3.8. *Let $m \geq 1$ and $k \geq 1$. Then, there exists an $a \times a$ antiorthogonal matrix U over $GR(2^m, 2k)$ if and only if a is even.*

Proof. Suppose there is an $a \times a$ antiorthogonal matrix U over $GR(2^m, 2k)$. By Theorem 3.6, a should be even. For the converse statement, by Lemma 3.7, there exist α, β such that $\alpha^2 + \beta^2 = -1$ in $GR(2^m, 2k)$. Let

$$U_2 = \begin{pmatrix} \alpha & \beta \\ \beta & -\alpha \end{pmatrix}.$$

Then, $U_2 U_2^T = -I$. This proves that there is a 2×2 matrix U such that $UU^T = -I$. For $a = 2t$, where $t \geq 1$, let

$$U_a = \begin{pmatrix} U_2 & & 0 \\ & \ddots & \\ 0 & & U_2 \end{pmatrix}.$$

Then, $U_a U_a^T = -I$. This completes the proof. □

Now, the remaining case is that of $m \geq 2$, $r = 2k + 1 (k \geq 1)$, and $a = 4t + 2 (t \geq 0)$ for the existence of $a \times a$ antiorthogonal matrix U over $GR(2^m, r)$.

LEMMA 3.9. *If -1 is a two square sum in $GR(2^m, r)$, then -1 is a two square sum in $GR(2^\ell, r)$, for all $1 \leq \ell \leq m$.*

TABLE 2. Values of α, β such that $\alpha^2 + \beta^2 = -1$ in $GR(2^3, r) = \mathbb{Z}_{2^3}[x]/(f(x))$

r	$f(x)$	α, β $(w = x + (f(x)))$
2	$x^2 + x + 1$	$w, w + 1$
3	$x^3 + x + 1$	-
4	$x^4 + x + 1$	$w^2 + w, w^2 + 3w + 3$
5	$x^5 + x^2 + 1$	-
6	$x^6 + x^4 + x^3 + x + 1$	$w^3 + w^2 + w + 1, 2w^5 + w^3 + w^2 + 3w + 2$

Proof. By Lemma 2.2 (ii), there is a homomorphism of $GR(2^m, r)$ onto $GR(2^\ell, r)$. In fact, we can construct a natural surjective ring homomorphism as follows. Let $f(x)$ be a monic basic irreducible polynomial in $\mathbb{Z}_{p^m}[x]$ of degree r. Let

$$\phi : \mathbb{Z}_{p^m}[x] \to \mathbb{Z}_{p^\ell}[x]$$

be a natural projection. We define

$$\Phi : \mathbb{Z}_{p^m}[x]/(f(x)) \to \mathbb{Z}_{p^\ell}[x]/(f(x))$$

by

$$\Phi(g(x) + (f(x))) = \phi(g(x)) + (f(x)).$$

Clearly, Φ is a surjective ring homomorphism. Suppose that $\alpha^2 + \beta^2 = -1$ in $GR(2^m, r)$. Then, $\Phi(\alpha^2 + \beta^2) = \phi(-1)$ in $GR(2^\ell, r)$. Therefore, $\Phi(\alpha)^2 + \Phi(\beta)^2 = -1$ in $GR(2^\ell, r)$. This completes the proof. □

In Table 2, we give the computational results. Here, we can see that -1 is a two square sum in $GR(2^3, r), r = 2, 4, 6$ and -1 is not a two square sum in $GR(2^3, r), r = 3, 5$. This result is consistent with Lemma 3.9 and the results shown in Table 1.

LEMMA 3.10. *-1 is not a two square sum in $GR(2^2, 2k + 1)$ for $k = 1, 2, 3$.*

Proof. We conducted an exhaustive search. In other words, we checked whether there is α, β such that $\alpha^2+\beta^2 = -1$ for all $\alpha, \beta \in GR(2^2, 2k+1)$. We found that -1 is not a two square sum in $GR(2^2, 2k + 1)$ for $k = 1, 2, 3$. □

COROLLARY 3.11. *-1 is not a two square sum in $GR(2^m, 2k + 1)$ for $k = 1, 2, 3$ and for all $m \geq 2$.*

Proof. The proof follows from Lemma 3.9 and Lemma 3.10. □

TABLE 3. Existence of $a \times a$ antiorthogonal matrix U over $GR(p^m, r)$

p	m	r	$-1:$ SQ	$-1:$ TSQ	Existence of U
$1 \pmod 4$			Yes		$\exists\ (a \geq 1)$
$-1 \pmod 4$		Even	Yes		$\exists\ (a \geq 1)$
		Odd	No	Yes	$\exists \Leftrightarrow a$ is even
2	1		Yes		$\exists\ (a \geq 1)$
	≥ 2	1	No	No	$\exists \Leftrightarrow a = 4t (t \geq 1)$
		$2k (k \geq 1)$	No	Yes	$\exists \Leftrightarrow a$ is even
		$2k+1 (k \geq 1)$	No	?	a is odd $\Rightarrow \nexists$
					$a = 4t \Rightarrow \exists (t \geq 1)$
					$a = 4t+2 (t \geq 1) \Rightarrow ?$

COROLLARY 3.12. *There is no* 2×2 *matrix* U *such that* $UU^T = -I$ *in* $GR(2^m, 2k+1)$ *for* $k = 1, 2, 3$ *and for all* $m \geq 2$.

Proof. By Corollary 3.11. □

From Corollary 3.12, we have the following conjecture.

CONJECTURE 3.13. *There is no* 2×2 *matrix* U *such that* $UU^T = -I$ *in* $GR(2^m, 2k+1)$ *for all* $k \geq 1$ *and for all* $m \geq 2$.

In Table 3, we summarize the existence problem of an $a \times a$ antiorthogonal matrix U over $GR(p^m, r)$. In Table 3 "SQ" means square and "TSQ" means two square sum. For example, if $p \equiv -1 \pmod 4$ and r is odd, then -1 is not a square, but is a two square sum, and there exists an $a \times a$ antiorthogonal matrix U if and only if a is even. We completed Table 3 except in two places, where we place question marks. One represents the problem, "Is -1 a two square sum in $GR(2^m, r), (m \geq 2, r = 2k+1 (k \geq 1))$?" The other represents the problem, "Is there an $a \times a$ antiorthogonal matrix U over $GR(2^m, r), (m \geq 2, r = 2k+1 (k \geq 1), a = 4t+2 (t \geq 0))$?" We finish this section by stating our research problem.

Research Problem: Determine the existence of an $a \times a$ matrix U such that $UU^T = -I$ in $GR(p^m, r)$, where $p = 2$, $m \geq 2$, $r = 2k+1 (k \geq 1)$, and $a = 4t+2 (t \geq 0)$.

4. Examples

In this section, we give examples of self-dual codes over $GR(2^m, r)$ using the building-up construction.

Example 4.1. *Let* C_0 *be a self-dual code of length four over* $GR(2^2, 2) = Z_{2^2}[x]/(f(x))$, *where* $f(x) = x^2 + x + 1$, *with generator matrix*

$$G_0 = \begin{pmatrix} 1 & 0 & w & w+1 \\ 0 & 1 & w+1 & 3w \end{pmatrix}, \tag{4.1}$$

where $w = x + (f(x))$. *The minimum weight of* C_0 *is* 3 *and the weight enumerator for* C_0 *is*

$$W(C_0) = 1 + 60x^3 + 195x^4. \tag{4.2}$$

Let

$$U = \begin{pmatrix} w & w+1 \\ w+1 & 3w \end{pmatrix} \tag{4.3}$$

and

$$X = \begin{pmatrix} 3 & 2w+2 & 1 & 1 \\ 2w+3 & 3 & 2w & 2w+1 \end{pmatrix}. \tag{4.4}$$

Then, $UU^T = -I$ *and* $XX^T = -I$. *By the building-up construction in Theorem 2.1, we have*

(4.5)
$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 3 & 2w+2 & 1 & 1 \\ 0 & 1 & 0 & 0 & 2w+3 & 3 & 2w & 2w+1 \\ 2w & 3w & 2w+1 & w+3 & 1 & 0 & w & w+1 \\ 2w+1 & 3w+1 & 0 & w+2 & 0 & 1 & w+1 & 3w \end{pmatrix},$$

which generates a self-dual code C *of length eight over* $GR(2^2, 2)$. *The minimum weight of* C *is* 4 *and the weight enumerator for* C *is*

$$W(C) = 1 + 90x^4 + 480x^5 + 5160x^6 + 20640x^7 + 39165x^8. \tag{4.6}$$

Example 4.2. *Let* C_0 *be a self-dual code of length four over* $GR(2^2, 4) = Z_{2^2}[x]/(f(x))$, *where* $f(x) = x^4 + x + 1$, *with generator matrix*

$$G_0 = \begin{pmatrix} 1 & 0 & w^2+w & w^2+w+1 \\ 0 & 1 & w^2+w+1 & 3w^2+3w \end{pmatrix}, \tag{4.7}$$

and $w = x + (f(x))$. *The minimum weight of* C_0 *is* 3 *and the weight enumerator for* C_0 *is*

$$W(C_0) = 1 + 1020x^3 + 64515x^4. \tag{4.8}$$

Let

$$U = \begin{pmatrix} w^2+w & w^2+w+1 \\ w^2+w+1 & 3w^2+3w \end{pmatrix} \tag{4.9}$$

and

(4.10)
$$X = \begin{pmatrix} 3w^3+3w & 2w^3+3w^2+2w & 3w^2+2w & w^3+2w^2+3w+1 \\ w^2+2w+1 & 3w^3+w^2 & 3w^2+2w+3 & w^3+w^2+2w+3 \end{pmatrix}.$$

Then, $UU^T = -I$ *and* $XX^T = -I$. *By the building-up construction in Theorem 2.1, we have a self-dual code* C *of length eight over* $GR(2^2, 4)$. *The minimum weight of* C *is* 3 *and the weight enumerator for* C *is*

(4.11)
$$W(C) = 1+15x^3+75x^4+17670x^5+1781370x^6+130601595x^7+4162566570x^8.$$

EXAMPLE 4.3. *Let* C_0 *be a self-dual code of length four over* $GR(2^3, 2) = Z_{2^3}[x]/(f(x))$, *where* $f(x) = x^2 + x + 1$, *with generator matrix*

$$G_0 = \begin{pmatrix} 1 & 0 & w & w+1 \\ 0 & 1 & w+1 & 7w \end{pmatrix}, \tag{4.12}$$

where $w = x + (f(x))$. *The minimum weight of* C_0 *is* 3 *and the weight enumerator for* C_0 *is*

$$W(C) = 1 + 252x^3 + 3843x^4. \tag{4.13}$$

Let

$$U = \begin{pmatrix} w & w+1 \\ w+1 & 7w \end{pmatrix} \tag{4.14}$$

and

$$X = \begin{pmatrix} 6w+7 & 5 & 4w+1 & 4w+4 \\ 6 & 4w+3 & 3 & 4w+7 \end{pmatrix}. \tag{4.15}$$

Then, $UU^T = -I$ *and* $XX^T = -I$. *By the building-up construction in Theorem 2.1, we have*

(4.16)
$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 6w+7 & 5 & 4w+1 & 4w+4 \\ 0 & 1 & 0 & 0 & 6 & 4w+3 & 3 & 4w+7 \\ w+5 & 6w+7 & 5w & 4w+6 & 1 & 0 & w & w+1 \\ 7w+2 & 4w+6 & 7w+5 & 1 & 0 & 1 & w+1 & 7w \end{pmatrix},$$

which generates a self-dual code C *of length eight over* $GR(2^3, 2)$. *The minimum weight of* C *is* 4 *and the weight enumerator for* C *is*

(4.17)
$$W(C) = 1 + 234x^4 + 2592x^5 + 105480x^6 + 1877472x^7 + 14791437x^8.$$

Acknowledgements

The author wishes to thank the reviewers for valuable remarks which helped to improve this article.

References

[1] G. Bini and F. Flamini, *Finite Commutative Rings and Their Applications*, Springer US, Boston, 2002.
[2] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system I: The user language*, J. Symbolic Comput. **24** (1997), 235-265.
[3] J. H. Conway and V. Pless, *On the enumeration of self-dual codes*, J. Combin. Theory ser. A, **28** (1980), 26-53.
[4] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups, third ed.* Springer, New York, 1999.
[5] M. Grassl and T. A. Gulliver, *On circulant self-dual codes over small fields*, Des. Codes Cryptogr. **52** (2009), 57-81.
[6] S. Han, *A method for costructing self-dual codes over* $\mathbb{Z}_{2^m}$, Des. Codes Cryptogr. **75** (2015), 253-262.
[7] S. Han, *On the problem of the existence of a square matrix* U *such that* $UU^T = -I$ *over* $\mathbb{Z}_{p^m}$, MDPI Information, **8** (2017), 1-8.
[8] M. Harada, *The existence of a self-dual* $[70, 35, 12]$ *code and formally self-dual codes*, Finite Fields Appl. **3** (1997), 131-139.
[9] W. C. Huffman and V. S. Pless, *Fundamentals of Error-correcting Codes*, Cambridge, Cambridge University Press, 2003.
[10] J.-L. Kim, *New extremal self-dual codes of lengths* 36*,* 38*, and* 58, IEEE Trans. Inform. Theory **47** (2001), 386-393.
[11] J.-L. Kim and Y. Lee, *Euclidean and Hermitian self-dual MDS codes over large finite fields*, J. Combin. Theory Ser. A **105** (2004), 79-95.
[12] J.-L. Kim and Y. Lee, *Construction of MDS self-dual codes over Galois rings*, Des. Codes Cryptogr. **45** (2007), 247-258.
[13] J.-L. Kim and Y. Lee, *An Efficient Construction of Self Dual Codes*, Bull. Korean Math. Soc. **52** (2015), 915-923.
[14] H. Lee H. and Y. Lee, *Construction of self-dual codes over finite rings* $\mathbb{Z}_p^m$, J. Combin. Theory Ser. A **115**, (2008), 407-422 .
[15] J. L. Massey, *Orthogonal, antiorthogonal and self-orthogonal matrices and their codes*, 1998. (http://citeseerx.ist.psu.edu/viewdoc/versions?doi=10.1.1.36.3608)
[16] J. L. Massey, *On Antiorthogonal Matrices and Their Codes*, ISIT, Cambridge, MA, USA, 1998.
[17] G. H. Norton and A. Sălăgean, *On the Hamming distance of linear codes over a finite chain ring*, IEEE Trans. Inform. Theory, **46** (2000), 1060-1067.
[18] E. Rains and N. J. A. Sloane, *Self-dual codes. in: Pless V.S. Huffman W.C. (Eds.) Handbook of Coding Theory*, Elsevier, Amsterdam, The Netherlands, 1998.

*
School of Liberal Arts
Korea University of Technology and Education
Cheonan 31253, Republic of Korea
E-mail: `sunghyu@koreatech.ac.kr`