Note on the residue codes of self-dual $\mathbb{Z}_4$-codes having large minimum Lee weights

Masaaki Harada*

March 26, 2014

Abstract

It is shown that the residue code of a self-dual $\mathbb{Z}_4$-code of length $24k$ (resp. $24k+8$) and minimum Lee weight $8k+4$ or $8k+2$ (resp. $8k+8$ or $8k+6$) is a binary extremal doubly even self-dual code for every positive integer k. A number of new self-dual $\mathbb{Z}_4$-codes of length 24 and minimum Lee weight 10 are constructed using the above characterization.

1 Introduction

Self-dual codes are an important class of (linear) codes[1] for both theoretical and practical reasons. It is a fundamental problem to classify self-dual codes of modest length and determine the largest minimum weight among self-dual codes of that length. Among self-dual $\mathbb{Z}_k$-codes, self-dual $\mathbb{Z}_4$-codes have been widely studied because such codes have nice applications to unimodular lattices and (non-linear) binary codes, where $\mathbb{Z}_k$ denotes the ring of integers modulo k and k is a positive integer with $k \geq 2$. It is well known that the Nordstorm–Robinson, Kerdock and Preparata codes, which are some best known non-linear binary codes, can be constructed as the Gray images of some $\mathbb{Z}_4$-codes [8]. We emphasize that the Nordstorm–Robinson code can be

*Research Center for Pure and Applied Mathematics, Graduate School of Information Sciences, Tohoku University, Sendai 980–8579, Japan. email: mharada@m.tohoku.ac.jp. This work was partially carried out at Yamagata University.

[1]All codes in this note are linear unless otherwise noted.

constructed as the Gray image of the unique self-dual $\mathbb{Z}_4$-code of length 8 and minimum Lee weight 6. In this note, we pay attention to the minimum Lee weight from the viewpoint of a connection with the minimum distance of binary (non-linear) codes obtained as the Gray images. Rains [18] gave upper bounds on the minimum Lee weights $d_L(\mathcal{C})$ of self-dual $\mathbb{Z}_4$-codes $\mathcal{C}$ of length n. For even lengths $n = 24k + \ell$, the upper bounds are given as $d_L(\mathcal{C}) \le 8k + g(\ell)$, where $g(\ell)$ is given by the following table:

ℓ	0	2	4	6	8	10	12	14	16	18	20	22
$g(\ell)$	4	2	4	4	8	4	4	6	8	8	8	8

In this note, we study residue codes of self-dual $\mathbb{Z}_4$-codes having large minimum Lee weights. According to the above upper bounds, the minimum Lee weights of self-dual $\mathbb{Z}_4$-codes of lengths $24k$ and $24k + 8$ are at most $8k + 4$ and $8k + 8$, respectively. It is shown that the residue code of a self-dual $\mathbb{Z}_4$-code of length $24k$ and minimum Lee weight $8k + 4$ or $8k + 2$ is a binary extremal doubly even self-dual code of length $24k$ for every positive integer k. It is also shown that the residue code of a self-dual $\mathbb{Z}_4$-code of length $24k+8$ and minimum Lee weight $8k+8$ or $8k+6$ is a binary extremal doubly even self-dual code of length $24k + 8$. As a consequence, we show that the minimum Lee weight of a self-dual $\mathbb{Z}_4$-code of length $24k$ (resp. $24k + 8$) is at most $8k$ (resp. $8k + 4$) for every integer $k \ge 154$ (resp. $k \ge 159$). A number of new self-dual $\mathbb{Z}_4$-codes of length 24 and minimum Lee weight 10 are constructed using the above characterization. Some self-dual $\mathbb{Z}_4$-codes of length n and minimum Lee weight d_L are also constructed for the cases $(n, d_L) = (32, 14), (48, 18), (56, 18)$. Finally, we give a certain characterization of binary self-dual codes containing the residue codes of self-dual $\mathbb{Z}_4$-codes for some other lengths.

All computer calculations in this note were done by Magma [4].

2 Preliminaries

2.1 Self-dual $\mathbb{Z}_4$-codes

Let $\mathbb{Z}_4$ $(= \{0, 1, 2, 3\})$ denote the ring of integers modulo 4. A $\mathbb{Z}_4$-*code* $\mathcal{C}$ of length n is a $\mathbb{Z}_4$-submodule of $\mathbb{Z}_4^n$. Two $\mathbb{Z}_4$-codes are *equivalent* if one can be obtained from the other by permuting the coordinates and (if necessary) changing the signs of certain coordinates. The *dual code* $\mathcal{C}^\perp$ of $\mathcal{C}$ is defined as $\mathcal{C}^\perp = \{x \in \mathbb{Z}_4^n \mid x \cdot y = 0$ for all $y \in \mathcal{C}\}$, where $x \cdot y$ is the standard inner product. A $\mathbb{Z}_4$-code $\mathcal{C}$ is *self-dual* if $\mathcal{C} = \mathcal{C}^\perp$. The *Hamming weight* $\mathrm{wt}_H(x)$, *Lee weight* $\mathrm{wt}_L(x)$ and *Euclidean weight* $\mathrm{wt}_E(x)$ of a codeword x of $\mathcal{C}$ are defined as $n_1(x)+n_2(x)+n_3(x)$, $n_1(x)+2n_2(x)+n_3(x)$ and $n_1(x)+4n_2(x)+n_3(x)$, respectively, where $n_i(x)$ is the number of components of x which are equal to i. The *minimum Lee weight* $d_L(\mathcal{C})$ (resp. *minimum Euclidean weight* $d_E(\mathcal{C})$) of $\mathcal{C}$ is the smallest Lee (resp. Euclidean) weight among all non-zero codewords of $\mathcal{C}$. The *residue code* $\mathcal{C}^{(1)}$ of $\mathcal{C}$ is the binary code defined as $\mathcal{C}^{(1)} = \{c \pmod 2 \mid c \in \mathcal{C}\}$. If $\mathcal{C}$ is a self-dual $\mathbb{Z}_4$-code, then $\mathcal{C}^{(1)}$ is doubly even [6].

The following characterization of the minimum Lee weights is useful.

Lemma 2.1 (Rains [17])**.** *Let $\mathcal{C}$ be a self-dual $\mathbb{Z}_4$-code. Then $d(\mathcal{C}^{(1)}) \le d_L(\mathcal{C}) \le 2d({\mathcal{C}^{(1)}}^\perp)$.*

The *Gray map* ϕ is defined as a map from $\mathbb{Z}_4^n$ to $\mathbb{Z}_2^{2n}$ mapping $(x_1, \dots, x_n)$ to $(\varphi(x_1), \dots, \varphi(x_n))$, where $\varphi(0) = (0,0)$, $\varphi(1) = (0,1)$, $\varphi(2) = (1,1)$ and $\varphi(3) = (1,0)$. The Gray image $\phi(\mathcal{C})$ of a $\mathbb{Z}_4$-code $\mathcal{C}$ needs not be linear. Let $\mathcal{C}$ be a self-dual $\mathbb{Z}_4$-code of length n and minimum Lee weight $d_L(\mathcal{C})$. Then the Gray image $\phi(\mathcal{C})$ has parameters $(2n, 2^n, d_L(\mathcal{C}))$ (as a non-linear code).

A self-dual $\mathbb{Z}_4$-code which has the property that all Euclidean weights are divisible by eight, is called *Type II*. A self-dual $\mathbb{Z}_4$-code which is not Type II, is called *Type I*. A Type II $\mathbb{Z}_4$-code of length n exists if and only if $n \equiv 0 \pmod 8$, while a Type I $\mathbb{Z}_4$-code exists for every length. It was shown in [3] that the minimum Euclidean weight $d_E(\mathcal{C})$ of a Type II $\mathbb{Z}_4$-code $\mathcal{C}$ of length n is bounded by $d_E(\mathcal{C}) \le 8\lfloor \frac{n}{24} \rfloor + 8$. A Type II $\mathbb{Z}_4$-code meeting this bound is called *extremal*. It was also shown in [19] that the minimum Euclidean weight $d_E(\mathcal{C})$ of a Type I $\mathbb{Z}_4$-code $\mathcal{C}$ of length n is bounded by $d_E(\mathcal{C}) \le 8\lfloor \frac{n}{24} \rfloor + 8$ if $n \not\equiv 23 \pmod{24}$, and $d_E(\mathcal{C}) \le 8\lfloor \frac{n}{24} \rfloor + 12$ if $n \equiv 23 \pmod{24}$.

2.2 Binary self-dual codes, covering radii and shadows

A binary code C is called *self-dual* if $C = C^\perp$, where $C^\perp$ is the dual code of C under the standard inner product. Two binary self-dual codes C and C' are *equivalent*, denoted $C \cong C'$, if one can be obtained from the other by permuting the coordinates. A binary self-dual code C is *doubly even* if all codewords of C have weight divisible by four, and *singly even* if there is at least one codeword of weight congruent to 2 modulo 4. It is known that a binary self-dual code of length n exists if and only if n is even, and a binary doubly even self-dual code of length n exists if and only if $n \equiv 0 \pmod 8$. The minimum weight $d(C)$ of a binary self-dual code C of length n is bounded by $d(C) \le 4\lfloor \frac{n}{24} \rfloor + 6$ if $n \equiv 22 \pmod{24}$, $d \le 4\lfloor \frac{n}{24} \rfloor + 4$ otherwise [14] and [16]. A binary self-dual code meeting the bound is called *extremal*.

The *covering radius* $R(C)$ of a binary code C is the smallest integer R such that spheres of radius R around codewords of C cover the space $\mathbb{Z}_2^n$. The covering radius is a basic and important geometric parameter of a code. A vector a of a coset U is called a coset leader of U if the weight of a is minimal in U and the weight of a coset U is defined as the weight of a coset leader. The covering radius is the same as the largest weight of all the coset leaders of the code (see [1]). The following bound is known as the Delsarte bound (see [1, Theorem 1]).

Lemma 2.2. *Let C be a binary code. Then $R(C) \le \#\{i > 0 \mid B_i \neq 0\}$, where B_i is the number of vectors of weight i in $C^\perp$.*

Let C be a binary singly even self-dual code and let C_0 denote the subcode of codewords having weight congruent to 0 modulo 4. Then C_0 is a subcode of codimension 1. The *shadow* S of C is defined to be $C_0^\perp \setminus C$. Shadows were introduced by Conway and Sloane [5], in order to provide restrictions on the weight enumerators of singly even self-dual codes. A binary self-dual code meeting the following bound is called *s-extremal*.

Lemma 2.3 (Bachoc and Gaborit [2])**.** *Let C be a binary self-dual code of length n and let S be the shadow of C. Let $d(C)$ and $d(S)$ denote the minimum weights of C and S, respectively. Then $d(S) \le \frac{n}{2} + 4 - 2d(C)$, except in the case that $n \equiv 22 \pmod{24}$ and $d(C) = 4\lfloor \frac{n}{24} \rfloor + 6$, where $d(S) = \frac{n}{2} + 8 - 2d(C)$.*

We end this section by proposing the following lemma, which is obtained from [13, Theorems 2.1 and 2.2].

Lemma 2.4. *Let C be a binary self-orthogonal code of length n.*

(i) *If n is even, then there is a binary self-dual code containing C.*

(ii) *If $n \equiv 0 \pmod 8$ and C is doubly even which is not self-dual, then there is a binary doubly even self-dual code containing C, and there is a binary singly even self-dual code containing C.*

3 Characterization of the residue codes for lengths $24k$ and $24k+8$

3.1 Length $24k$

As described in Section 1, the minimum Lee weight of a self-dual $\mathbb{Z}_4$-code of length $24k$ is at most $8k+4$. In this subsection, we consider self-dual $\mathbb{Z}_4$-codes of length $24k$ and minimum Lee weight $8k+4$ or $8k+2$.

Theorem 3.1. *Let $\mathcal{C}$ be a self-dual $\mathbb{Z}_4$-code of length $24k$. Suppose that the minimum Lee weight of $\mathcal{C}$ is $8k+4$ or $8k+2$. Then $\mathcal{C}^{(1)}$ is a binary extremal doubly even self-dual code of length $24k$.*

Proof. Since $\mathcal{C}^{(1)}$ is doubly even, by Lemma 2.4, there is a binary doubly even self-dual code C satisfying that $\mathcal{C}^{(1)} \subseteq C \subseteq {\mathcal{C}^{(1)}}^{\perp}$. Since $\mathcal{C}$ has minimum Lee weight $8k+4$ (resp. $8k+2$), by Lemma 2.1, ${\mathcal{C}^{(1)}}^{\perp}$ has minimum weight at least $4k+2$ (resp. $4k+1$). Hence, C is extremal.

Now consider the covering radius $R(C)$ of C. By Lemma 2.2, $R(C) \leq 4k$. Hence, if $C \subsetneq {\mathcal{C}^{(1)}}^{\perp}$, then the minimum weight of ${\mathcal{C}^{(1)}}^{\perp}$ is at most $4k$, which is a contradiction. Therefore, $C = \mathcal{C}^{(1)}$. □

Remark 3.2. Recently, the nonexistence of a self-dual $\mathbb{Z}_4$-code of length 36 and minimum Lee weight 16 has been shown in [10]. This result can be directly obtained by the bound in [18], which is given in Section 1, however, the approach in [10] can be generalized to the following alternative proof of the above theorem. Suppose that $\mathcal{C}^{(1)}$ is not self-dual. Since $\mathcal{C}^{(1)}$ is doubly even, by Lemma 2.4, there is a binary singly even self-dual code C satisfying that

$$\mathcal{C}^{(1)} \subseteq C_0 \subsetneq C \subsetneq C_0^{\perp} \subseteq {\mathcal{C}^{(1)}}^{\perp},$$

where C_0 denotes the doubly even subcode of C. By Lemma 2.1, ${\mathcal{C}^{(1)}}^{\perp}$ has minimum weight at least $4k+1$. By [16, Theorem 5], C has minimum weight $4k+2$. By Lemma 2.3, the minimum weight of the shadow of a binary singly even self-dual $[24k, 12k, 4k+2]$ code is at most $4k$, which is a contradiction. Hence, $\mathcal{C}^{(1)}$ is self-dual, that is, $\mathcal{C}^{(1)}$ is extremal. This completes the alternative proof.

Remark 3.3. For lengths up to 24, optimal self-dual $\mathbb{Z}_4$-codes with respect to the minimum Hamming and Lee weights were widely studied in [17]. At length 24, the above theorem follows from [17, Theorem 2 and Corollary 5].

For length $24k$, the only known binary extremal doubly even self-dual codes are the extended Golay code G_{24} and the extended quadratic residue code QR_{48} of length 48. The existence of a binary extremal doubly even self-dual code of length 72 is a long-standing open question. In addition, there is no binary extremal doubly even self-dual code of length $24k$ for $k \geq 154$ [21]. Hence, we immediately have the following:

Corollary 3.4. *The minimum Lee weight of a self-dual $\mathbb{Z}_4$-code of length $24k$ is at most $8k$ for every integer $k \geq 154$.*

3.2 Length $24k + 8$

As described in Section 1, the minimum Lee weight of a self-dual $\mathbb{Z}_4$-code of length $24k + 8$ is at most $8k + 8$. In this subsection, we consider self-dual $\mathbb{Z}_4$-codes of length $24k + 8$ and minimum Lee weight $8k + 8$ or $8k + 6$.

Theorem 3.5. *Let $\mathcal{C}$ be a self-dual $\mathbb{Z}_4$-code of length $24k + 8$. Suppose that the minimum Lee weight of $\mathcal{C}$ is $8k + 8$ or $8k + 6$. Then $\mathcal{C}^{(1)}$ is a binary extremal doubly even self-dual code of length $24k + 8$.*

Proof. Suppose that $\mathcal{C}^{(1)}$ is not self-dual. Since $\mathcal{C}^{(1)}$ is doubly even, by Lemma 2.4, there is a binary singly even self-dual code C satisfying that

$$\mathcal{C}^{(1)} \subseteq C_0 \subsetneq C \subsetneq C_0^{\perp} \subseteq \mathcal{C}^{(1)\perp},$$

where C_0 denotes the doubly even subcode of C. By Lemma 2.1, $\mathcal{C}^{(1)\perp}$ has minimum weight at least $4k + 3$. Hence, C has minimum weight $4k + 4$. By Lemma 2.3, the minimum weight of the shadow of a binary singly even self-dual $[24k+8, 12k+4, 4k+4]$ code is at most $4k$, which is a contradiction. Hence, $\mathcal{C}^{(1)}$ is self-dual, that is, $\mathcal{C}^{(1)}$ is extremal. $\square$

Remark 3.6. (i) The case that the minimum Lee weight $d_L(\mathcal{C})$ is $8k + 8$ follows immediately from [18, Theorem 1].

(ii) The above theorem can be proved by a similar argument to the proof of Theorem 3.1.

Remark 3.7. Rains [18, p. 148] pointed out that by the linear programing $d_L(\mathcal{C}) \leq 8k + 6$ for $k \leq 4$.

It is known that there is a binary extremal doubly even self-dual code of length $24k+8$ for $k \leq 4$. In addition, since there is no binary extremal doubly even self-dual code of length $24k+8$ for $k \geq 159$ [21], we immediately have the following:

Corollary 3.8. *The minimum Lee weight of a self-dual $\mathbb{Z}_4$-code of length $24k+8$ is at most $8k+4$ for every integer $k \geq 159$.*

4 Self-dual $\mathbb{Z}_4$-codes having large minimum Lee weights

By using the characterizations of the residue codes, which are given in the previous section, a number of self-dual $\mathbb{Z}_4$-codes having large minimum Lee weights are constructed in this section.

4.1 Double circulant and four-negacirculant codes

Throughout this note, let A^T denote the transpose of a matrix A and let I_k denote the identity matrix of order k. An $n \times n$ matrix is *circulant* and *negacirculant* if it has the following form:

$$\begin{pmatrix} r_0 & r_1 & \cdots & r_{n-2} & r_{n-1} \\ cr_{n-1} & r_0 & \cdots & r_{n-3} & r_{n-2} \\ cr_{n-2} & cr_{n-1} & \ddots & r_{n-4} & r_{n-3} \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ cr_1 & cr_2 & \cdots & cr_{n-1} & r_0 \end{pmatrix},$$

where $c = 1$ and -1, respectively. A $\mathbb{Z}_4$-code with generator matrix of the form:

$$(1) \qquad \left(\begin{array}{c|cccc} & \alpha & \beta & \cdots & \beta \\ & \gamma & & & \\ I_n & \vdots & & R & \\ & \gamma & & & \end{array}\right)$$

is called a *bordered double circulant* $\mathbb{Z}_4$-code of length $2n$, where R is an $(n-1) \times (n-1)$ circulant matrix and $\alpha, \beta, \gamma \in \mathbb{Z}_4$. A $\mathbb{Z}_4$-code with generator matrix of the form:

$$
\left(\begin{array}{ccc} I_{2n} & \begin{array}{cc} A & B \\ -B^T & A^T \end{array} \end{array}\right) \tag{2}
$$

is called a *four-negacirculant* $\mathbb{Z}_4$-code of length $4n$, where A and B are $n \times n$ negacirculant matrices.

Table 1: Bordered double circulant self-dual $\mathbb{Z}_4$-codes

Length	Code	First row of R	(α, β, γ)	Type	d_L
24	$\mathcal{D}_{24,1}$	(13103303222)	$(0, 1, 1)$	I	10
	$\mathcal{D}_{24,2}$	(01130332322)	$(0, 1, 1)$	I	10
	$\mathcal{D}_{24,3}$	(31030001332)	$(0, 1, 1)$	I	10
32	$\mathcal{D}_{32}$	(002210100233312)	$(0, 1, 1)$	II	14
48	$\mathcal{D}_{48}$	(11303312013230033212110)	$(0, 1, 1)$	II	18
56	$\mathcal{D}_{56,1}$	(022000202022112232101111011)	$(2, 1, 1)$	II	18
	$\mathcal{D}_{56,2}$	(002202002002312010101111011)	$(0, 1, 1)$	I	18

By considering bordered double circulant codes and four-negacirculant codes, we found self-dual $\mathbb{Z}_4$-codes of length $24k$ and minimum Lee weight $8k+2$ $(k = 1, 2)$ and self-dual $\mathbb{Z}_4$-codes of length 32 and minimum Lee weight 14. These codes were found under the condition that the residue codes are binary extremal doubly even self-dual codes, by Theorems 3.1 and 3.5. Self-dual $\mathbb{Z}_4$-codes of length 56 and minimum Lee weight 18 were also found.

For bordered double circulant codes, the first rows of R and (α, β, γ) in (1) are listed in Table 1. For four-negacirculant codes, the first rows of A and B in (2) are listed in Table 2. The minimum Lee weights d_L determined by Magma are also listed. The 5th column in both tables indicates the Type of the code.

Table 2: Four-negacirculant self-dual $\mathbb{Z}_4$-codes

Length	Code	First row of A	First row of B	Type	d_L
32	$\mathcal{C}_{32}$	(22312012)	(03113022)	II	14
56	$\mathcal{C}_{56}$	(11130213112212	(30101110001000)	II	18

4.2 Length 24

For length 24, there are 13 self-dual $\mathbb{Z}_4$-codes having minimum Lee weight 12, up to equivalence [17, Theorem 11]. Note that these self-dual $\mathbb{Z}_4$-codes are extremal Type II $\mathbb{Z}_4$-codes [17, Theorem 9].

In this subsection, we consider self-dual $\mathbb{Z}_4$-codes having minimum Lee weight 10.

Lemma 4.1. *Let $\mathcal{C}$ be a self-dual $\mathbb{Z}_4$-code of length 24 and minimum Lee weight 10. Then $\mathcal{C}$ is a Type I $\mathbb{Z}_4$-code having minimum Euclidean weight 12.*

Proof. Let x be a codeword x of $\mathcal{C}$ with $\mathrm{wt}_L(x) = 10$. Then

$$(n_1(x) + n_3(x), n_2(x)) = (10, 0), (8, 1), (6, 2), (4, 3), (2, 4), (0, 5).$$

By Theorem 3.1, $\mathcal{C}^{(1)} \cong G_{24}$. Thus, $n_1(x) + n_3(x) = 8$ or $n_1(x) + n_3(x) = 0$. In addition, if $n_1(x) + n_3(x) = 0$, then $n_2(x) \equiv 0 \pmod 4$ with $n_2(x) \geq 8$. This gives

$$(n_1(x) + n_3(x), n_2(x)) = (8, 1).$$

Hence, $\mathrm{wt}_E(x) = 12$. Therefore, $\mathcal{C}$ is a Type I $\mathbb{Z}_4$-code having minimum Euclidean weight 12. $\square$

We use the following method in order to verify that given two $\mathbb{Z}_4$-codes are inequivalent (see [7]). Let C be a self-dual $\mathbb{Z}_4$-code of length n. Let $M_t = (m_{ij})$ be the $A_t \times n$ matrix with rows composed of the codewords x with $\mathrm{wt}_H(x) = t$ in C, where A_t denotes the number of such codewords. For an integer k $(1 \leq k \leq n)$, let $n_t(j_1, \dots, j_k)$ be the number of r $(1 \leq r \leq A_t)$ such that all $m_{rj_1}, \dots, m_{rj_k}$ are nonzero for $1 \leq j_1 < \dots < j_k \leq n$. We consider the set

$$S_{t,k} = \{n_t(j_1, \dots, j_k) \mid \text{ for any distinct } k \text{ columns } j_1, \dots, j_k\ \}.$$

In [7], the authors claimed that there are two inequivalent bordered double circulant Type I $\mathbb{Z}_4$-codes of length 24 and minimum Lee weight 10. Unfortunately, this is not true. In fact, the number of such codes should be three not two. The codes $\mathcal{D}_{24,i}$ $(i = 1, 2, 3)$ given in Table 1 are bordered double circulant Type I $\mathbb{Z}_4$-codes of length 24 and minimum Lee weight 10. In Table 3, we list $\mathcal{S}_k = (\max(S_{9,k}), \min(S_{9,k}), \#S_{9,k})$ $(k = 1, 2, 3, 4)$ for the codes. This table shows that the three codes $\mathcal{D}_{24,1}, \mathcal{D}_{24,2}, \mathcal{D}_{24,3}$ are inequivalent.

Table 3: $\mathcal{S}_1$, $\mathcal{S}_2$, $\mathcal{S}_3$, $\mathcal{S}_4$ for $\mathcal{D}_{24,1}$, $\mathcal{D}_{24,2}$, $\mathcal{D}_{24,3}$

Code	$\mathcal{S}_1$	$\mathcal{S}_2$	$\mathcal{S}_3$	$\mathcal{S}_4$
$\mathcal{D}_{24,1}$	$(352, 256, 2)$	$(128, 0, 5)$	$(48, 0, 11)$	$(20, 0, 11)$
$\mathcal{D}_{24,2}$	$(352, 256, 2)$	$(128, 0, 5)$	$(48, 0, 11)$	$(18, 0, 10)$
$\mathcal{D}_{24,3}$	$(352, 256, 2)$	$(128, 0, 5)$	$(48, 0, 11)$	$(16, 0, 9)$

Proposition 4.2. *There are three inequivalent bordered double circulant Type I* $\mathbb{Z}_4$*-codes of length* 24 *and minimum Lee weight* 10*.*

For a given binary doubly even code C of dimension k, there are $2^{\frac{k(k+1)}{2}}$ self-dual $\mathbb{Z}_4$-codes $\mathcal{C}$ with $\mathcal{C}^{(1)} = C$, and an explicit method for construction of these $2^{\frac{k(k+1)}{2}}$ self-dual $\mathbb{Z}_4$-codes $\mathcal{C}$ with $\mathcal{C}^{(1)} = C$ was given in [15, Section 3]. In our case, there are 2^{78} self-dual $\mathbb{Z}_4$-codes $\mathcal{C}$ with $\mathcal{C}^{(1)} = G_{24}$, and it seems infeasible to find all such codes. Using the above method, we tried to construct many self-dual $\mathbb{Z}_4$-codes. Then we stopped our search after we found 57 self-dual $\mathbb{Z}_4$-codes having minimum Lee weight 10 satisfying that the 57 codes and the three codes in Table 3 have distinct $S_{9,k}$ $(k = 1, 2, 3, 4)$. Hence, we have the following proposition.

Proposition 4.3. *There are at least* 60 *inequivalent self-dual* $\mathbb{Z}_4$*-codes of length* 24 *and minimum Lee weight* 10*.*

We denote the new codes by $\mathcal{C}_{24,i}$ $(i = 1, 2, \dots, 57)$. In Figure 1, we list generator matrices for $\mathcal{C}_{24,i}$, where we consider generator matrices in standard form $(\ I_{12}\ ,\ M_i\ )$ and only 12 rows in M_i are listed, to save space.

4.3 Lengths 32, 48, 56 and 80

The extended lifted quadratic residue $\mathbb{Z}_4$-code $\mathcal{QR}_{32}$ and the Reed–Muller $\mathbb{Z}_4$-code $\mathcal{QRM}(2, 5)$, which are given in [3, Table I], are self-dual $\mathbb{Z}_4$-codes of length 32 and minimum Lee weight 14. Both codes are extremal Type II $\mathbb{Z}_4$-codes [3]. It is known that $\mathcal{QR}_{32}^{(1)}$ (resp. $\mathcal{QRM}(2, 5)^{(1)}$) is the extended quadratic residue code QR_{32} (resp. a second-order the Reed–Muller code $RM(2, 5)$) of length 32, which is a binary extremal doubly even self-dual code. The largest minimum Lee weight among bordered double circulant self-dual $\mathbb{Z}_4$-codes is listed in the table in [11] for length $8n$ $(n = 1, 2, \dots, 8)$.

According to the table, the largest minimum Lee weight for length 32 is 14. The code $\mathcal{D}_{32}$ in Table 2 is a Type II $\mathbb{Z}_4$-code of length 32 and minimum Lee weight 14, which gives an explicit example of such codes. In addition, the code $\mathcal{C}_{32}$ in Table 2 is a Type II $\mathbb{Z}_4$-code of length 32 and minimum Lee weight 14. We verified by MAGMA that $\mathcal{C}_{32}^{(1)} \cong \mathcal{D}_{32}^{(1)} \cong QR_{32}$. It is unknown whether the three codes are equivalent or not. There are five inequivalent binary extremal doubly even self-dual codes of length 32, two of which are QR_{32} and $RM(2,5)$ (see [20, Table IV]). It is worthwhile to determine whether there is a self-dual $\mathbb{Z}_4$-code $\mathcal{C}$ having minimum Lee weight 14 with $\mathcal{C}^{(1)} \cong C$ for each C of the remaining three codes.

The extended lifted quadratic residue $\mathbb{Z}_4$-code $\mathcal{QR}_{48}$ of length 48 is a self-dual $\mathbb{Z}_4$-code having minimum Lee weight 18, which is an extremal Type II $\mathbb{Z}_4$-code. This is the only known self-dual $\mathbb{Z}_4$-code of length 48 and minimum Lee weight at least 18. Of course, $\mathcal{QR}_{48}^{(1)}$ is QR_{48}. According to the table in [11], the largest minimum Lee weight among bordered double circulant self-dual $\mathbb{Z}_4$-codes of length 48 is 18. The code $\mathcal{D}_{48}$ in Table 1 gives an explicit example of such codes. It is unknown whether $\mathcal{D}_{48}$ is equivalent to $\mathcal{QR}_{48}$ or not.

At length 56, under the condition that the residue code is a binary extremal doubly even self-dual code, we tried to construct a self-dual $\mathbb{Z}_4$-code having minimum Lee weight 20 or 22, but our search failed to do this. In this process, however, we found extremal Type II $\mathbb{Z}_4$-codes. The code $\mathcal{C}_{56}$ in Table 2 is a Type II $\mathbb{Z}_4$-code of length 56 and minimum Lee weight 18. Hence, $\mathcal{C}_{56}$ is extremal. According to the table in [11], the largest minimum Lee weight among bordered double circulant self-dual $\mathbb{Z}_4$-codes of length 56 is 18. The codes $\mathcal{D}_{56,1}$ and $\mathcal{D}_{56,2}$ in Table 1 give explicit examples of such codes. We verified by MAGMA that $\mathcal{D}_{56,2}$ has minimum Euclidean weight 20. Since $\mathcal{D}_{56,1}$ is Type II, $\mathcal{D}_{56,1}$ is extremal. We verified by MAGMA that $\mathcal{C}_{56}^{(1)}$ and $\mathcal{D}_{56,1}^{(1)}$ have automorphism groups of orders 28 and 54, respectively. This shows that $\mathcal{C}_{56}$ and $\mathcal{D}_{56,1}$ are inequivalent. An extremal Type II $\mathbb{Z}_4$-code of length 56 given in [9] has the residue code of dimension 14. Hence, we have the following:

Proposition 4.4. *There are at least three inequivalent extremal Type II $\mathbb{Z}_4$-codes of length* 56*.*

It is unknown whether there is a self-dual $\mathbb{Z}_4$-code having minimum Lee weight $20, 22$ or not.

At length 80, the minimum Lee weight of the extended lifted quadratic residue $\mathbb{Z}_4$-code was determined in [12] as 26. It is unknown whether there is a self-dual $\mathbb{Z}_4$-code having minimum Lee weight $28, 30$ or not.

5 Characterization of the residue codes for other lengths

Finally, in this section, we give a certain characterization of binary self-dual codes containing the residue codes $\mathcal{C}^{(1)}$ of self-dual $\mathbb{Z}_4$-codes $\mathcal{C}$ of length $24k+\alpha$ for $\alpha = 2, 4, 6, 10, 14, 16, 18, 20, 22$.

Proposition 5.1. *Let $\mathcal{C}$ be a self-dual $\mathbb{Z}_4$-code of length $24k+\alpha$ and minimum Lee weight $8k+\beta$, where $(\alpha,\beta) = (2,2), (4,4), (6,4), (10,4)$. Then any binary self-dual code C containing $\mathcal{C}^{(1)}$ is an s-extremal self-dual code having minimum weight $4k+2$.*

Proof. Since all cases are similar, we only give the details for the case $(\alpha,\beta) = (6,4)$. By Lemma 2.4, there is a binary self-dual code C satisfying that

$$\mathcal{C}^{(1)} \subseteq C_0 \subsetneq C \subsetneq C_0^{\perp} \subseteq {\mathcal{C}^{(1)}}^{\perp},$$

where C_0 denotes the doubly even subcode of C. By Lemma 2.1, ${\mathcal{C}^{(1)}}^{\perp}$ has minimum weight at least $4k+2$. Hence, C has minimum weight $4k+2$ or $4k+4$.

Suppose that C has minimum weight $4k+4$. By Lemma 2.3, the minimum weight of the shadow $C_0^{\perp} \setminus C$ of C is at most $4k-1$, which contradicts the minimum weight of ${\mathcal{C}^{(1)}}^{\perp}$. Now, suppose that C has minimum weight $4k+2$. The weight of every vector of the shadow $C_0^{\perp} \setminus C$ is congruent to 3 modulo 4 [5]. Since $C_0^{\perp}$ has minimum weight at least $4k+2$, the shadow has minimum weight at least $4k+3$. By Lemma 2.3, the minimum weight of the shadow $C_0^{\perp} \setminus C$ of C is at most $4k+3$. Hence, C is s-extremal. $\square$

The situations in the following proposition are slightly different to that in the above proposition. However, a similar argument to the proof of the above proposition establishes the following proposition, and their proofs are omitted.

Proposition 5.2. *Let $\mathcal{C}$ be a self-dual $\mathbb{Z}_4$-code of length $24k+\alpha$ and minimum Lee weight $8k+\beta$. Let C be a binary self-dual code containing $\mathcal{C}^{(1)}$.*

(i) *Suppose that* $(\alpha, \beta) = (14, 6), (18, 8), (20, 8)$. *Then* C *is an s-extremal self-dual code having minimum weight* $4k + 4$.

(ii) *Suppose that* $(\alpha, \beta) = (16, 8)$. *If* C *is singly even, then* C *is an s-extremal self-dual code having minimum weight* $4k + 4$. *If* C *is doubly even, then* C *is extremal.*

(iii) *Suppose that* $(\alpha, \beta) = (22, 8)$. *Then* C *is an s-extremal self-dual code having minimum weight* $4k + 4$ *or* $4k + 6$.

Acknowledgment. This work is supported by JSPS KAKENHI Grant Number 23340021.

References

[1] E.F. Assmus, Jr. and V. Pless, On the covering radius of extremal self-dual codes, *IEEE Trans. Inform. Theory* **29** (1983), 359–363.

[2] C. Bachoc and P. Gaborit, Designs and self-dual codes with long shadows, *J. Combin. Theory Ser. A* **105** (2004), 15–34.

[3] A. Bonnecaze, P. Solé, C. Bachoc and B. Mourrain, Type II codes over $\mathbb{Z}_4$, *IEEE Trans. Inform. Theory* **43** (1997), 969–976.

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

[5] J.H. Conway and N.J.A. Sloane, A new upper bound on the minimal distance of self-dual codes, *IEEE Trans. Inform. Theory* **36** (1990), 1319–1333.

[6] J.H. Conway and N.J.A. Sloane, Self-dual codes over the integers modulo 4, *J. Combin. Theory Ser. A* **62** (1993), 30–45.

[7] T.A. Gulliver and M. Harada, Certain self-dual codes over $\mathbb{Z}_4$ and the odd Leech lattice, *Lecture Notes in Comput. Sci.* **1255** (1997), 130–137.

[8] A.R. Hammons, Jr., P.V. Kumar, A.R. Calderbank, N.J.A. Sloane and P. Solé, The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals and related codes, *IEEE Trans. Inform. Theory* **40** (1994), 301–319.

[9] M. Harada, Extremal type II $\mathbb{Z}_4$-codes of lengths 56 and 64, *J. Combin. Theory Ser. A* **117** (2010), 1285–1288.

[10] M. Kiermaier, There is no self-dual $\mathbb{Z}_4$-linear code whose Gray image has the parameters $(72, 2^{36}, 16)$, *IEEE Trans. Inform. Theory* **59** (2013), 3384–3386.

[11] M. Kiermaier and A. Wassermann, Double and bordered α-circulant self-dual codes over finite commutative chain rings, Proceedings of Eleventh Intern. Workshop on Alg. and Combin. Coding Theory, June, 2008, Pamporovo, Bulgaria, pp. 144–150.

[12] M. Kiermaier and A. Wassermann, Minimum weights and weight enumerators of $\mathbb{Z}_4$-linear quadratic residue codes, *IEEE Trans. Inform. Theory* **58** (2012), 4870–4883.

[13] F.J. MacWilliams, N.J.A. Sloane and J.G. Thompson, Good self dual codes exist, *Discrete Math.* **3** (1972), 153–162.

[14] C.L. Mallows and N.J.A. Sloane, An upper bound for self-dual codes, *Inform. Control* **22** (1973), 188–200.

[15] V. Pless, J. Leon and J. Fields, All $\mathbb{Z}_4$ codes of Type II and length 16 are known, *J. Combin. Theory Ser. A* **78** (1997), 32–50.

[16] E.M. Rains, Shadow bounds for self-dual codes, *IEEE Trans. Inform. Theory* **44** (1998), 134–139.

[17] E. Rains, Optimal self-dual codes over $\mathbb{Z}_4$, *Discrete Math.* **203** (1999), 215–228.

[18] E. Rains, Bounds for self-dual codes over $\mathbb{Z}_4$, *Finite Fields Appl.* **6** (2000), 146–163.

[19] E. Rains and N.J.A. Sloane, The shadow theory of modular and unimodular lattices, *J. Number Theory* **73** (1998), 359–389.

[20] E. Rains and N.J.A. Sloane, Self-dual codes, Handbook of Coding Theory, V.S. Pless and W.C. Huffman (Editors), Elsevier, Amsterdam, 1998, pp. 177–294.

[21] S. Zhang, On the nonexistence of extremal self-dual codes, *Discrete Appl. Math.* **91** (1999), 277–286.

M_1: 301203221111 131321121202 031330112300 023333033010 020111103321 301010131221
313322212031 330331002332 213211120231 320120311112 230012013313 132223130321,

M_2: 123021003313 313321321222 231310132322 001313013232 002331103321 321012113201
133322232033 330113222132 211011322231 102122333130 010212011313 110223112301,

M_3: 123023021313 331121101022 011132310120 221313213030 220111121323 323232313203
113302210033 330331220112 011011302231 120100113310 012012231311 130223110303,

M_4: 323023003133 131321121222 213310130302 003333033212 002331303303 303230313023
311320032013 110333200132 213033122231 100302111312 212012213311 112203310303,

M_5: 103203003333 333321101000 031130132300 203333211212 220111303323 303230333001
111320012031 330113002130 013033320033 122122133332 032232013311 132023112101,

M_6: 101201201331 333321101000 031130132300 203333211210 222113101321 301232131003
113322210033 330113002132 011031122031 122122133332 030230211313 130021310101,

M_7: 103223003113 131121301220 013132130320 021311031012 200311123323 301032111001
331102210233 332333002130 233213320211 322100131110 032210233333 310021332123,

M_8: 321223001111 131101103222 013112332322 023311231032 222113123121 301032111001
113320012211 130311022110 011211302231 320122111312 210210233133 132203310301,

M_9: 123223001111 113121103220 211332312302 023111213212 002331301321 323030313223
131120032011 310311002110 033013120231 122100331330 012212011133 330003332103,

M_{10}: 321023201133 111103103202 231112312120 223133031212 002133323323 303012311223
311122230011 132131202112 213013300031 302300133330 210010231311 332221330121,

M_{11}: 121021023131 313321321022 213332132100 003311211210 200331101121 121030311021
311102030211 330331220330 031213302031 122100113130 030230033331 112201110323,

M_{12}: 123223203113 111121121022 033112132322 203133213012 020313321103 321012111223
133120032231 332113000130 213033120031 302100313132 232032231333 132021312303,

M_{13}: 103203203333 331321103222 011332312300 003311213232 020313101121 303232111003
311120232033 330311220130 031031122033 120100313110 212010013113 312223312321,

M_{14}: 121201001313 111301123020 233130330302 023131031230 222131123101 101210311003
133320010231 330113022132 231231302231 102300313312 212032231331 130021312303,

M_{15}: 323023203111 313103321200 031112110302 003133013210 202111103103 323212133201
331322230233 310331002312 033231100213 320322131310 010212013113 312201110123,

M_{16}: 103021201131 113323103002 031332110300 201113231210 200311321323 101232333201
333300012233 112311002312 211013322233 122102311312 212030233311 130201312101,

M_{17}: 121223023111 333301101022 211310330302 203113031032 022113301303 303030311201
311102010013 132333222332 231033122213 122120133332 232012213111 130201112321,

M_{18}: 301221023133 333101321222 211332130320 223133231010 222333121301 103232333023
131322032031 112131022312 011211302231 102120313112 012012031113 330223312101,

M_{19}: 101203003133 311103121200 231132112102 223333033010 202131323103 323032313023
333320010211 330131200312 231033322011 300322333132 030232011331 110023330301,

M_{20}: 323021021133 313301321020 033330112102 023331231012 222111301321 101210311003
311102230033 330133222332 213213122211 302120113110 212012011313 132203132103,

Figure 1: New self-dual $\mathbb{Z}_4$-codes of length 24 and $d_L = 10$

M_{21}: 323203201311 133303121000 011112330120 003113213230 222111301321 123212313023
113320232231 330331020110 211211102011 122100111332 030210033311 312201110301,
M_{22}: 103023023311 131323103200 213132112102 201133011210 000111301321 301212113021
113122010213 112113220130 031211300233 320120113112 032232013333 310203332101,
M_{23}: 323221023131 111121303202 213132110120 221131233032 220111321321 123012113221
311302212211 112131002130 031233120031 302102131110 230230213131 130201330103,
M_{24}: 301001221131 133123321000 231110112300 023131213230 000313321321 103030311203
331322032011 312331020312 011033120211 120100311312 230030031131 130201332321,
M_{25}: 103223023131 331301123000 233312332322 021331013230 200331323101 101232331003
111300012031 312331222310 213211302211 302300133112 010230231111 130201330321,
M_{26}: 103221223133 313123321020 033132132120 021133013032 000331323303 321230131003
331300210213 312113022112 211033102011 300300131312 030010211333 112023312101,
M_{27}: 101003201311 313301321000 233132312102 203111013212 022133103123 121010311003
111102012033 112331202110 011213120031 122320113330 012010211111 110021132321,
M_{28}: 123023003333 331101101222 233130112320 201313233212 222111321301 323030331203
333102232011 310113202110 213231120033 102102331332 010212033313 310021112123,
M_{29}: 323203223111 131321303000 033312332322 023331031212 020111321321 121012331001
311102010013 330113020312 031013122033 120100313110 230010031111 112001132103,
M_{30}: 123201023133 113323301220 013130312322 201313233212 020333303301 301012133003
311122012031 312331222132 031013320031 100300331312 032010233333 130223130321,
M_{31}: 121223223331 131321323022 213332112322 221113213012 220133303323 303032333221
133302012031 330333020132 011213320033 322302313330 210232233311 110021130103,
M_{32}: 321201221113 333323321222 031312130320 003131033212 200113323321 101010333223
113102012213 312331000130 031031322213 322100331132 012212031333 310223110121,
M_{33}: 323201201133 313323101022 033330130302 203131013032 002133121323 123210311021
313122232231 332111000110 033013322011 320320131310 030012031313 132201332321,
M_{34}: 321023023131 111303303022 211112332120 021333231212 000311323123 103212333021
131302010211 312333022332 011213322033 320122311110 210032213313 110221312301,
M_{35}: 101023021333 133123301200 213332330322 201133231230 202333101301 323210311003
131100032033 310131200112 011233320013 120300333110 230210231313 312001110321,
M_{36}: 103023201133 113323321020 211312312120 221113231212 022111101121 303230133223
133300012031 130313022310 213013120233 322320313112 210210213113 332001130103,
M_{37}: 123003001313 331121303200 031312310322 203311033012 020131321323 323210111221
333302210011 132131222112 213033120013 322102333112 210012231131 330023310101,
M_{38}: 301201001311 131103323000 031332332322 201333233032 020113301323 123232133001
331300230233 112333200130 011213102213 102320331312 032232031113 330221330323,
M_{39}: 103023203311 311103121022 011312112322 001313013230 202131303123 123232331001
111322030011 110313200110 033211120233 320322311130 230032231113 332223112301,
M_{40}: 303223021311 331321103202 213332332302 021131233032 202333123303 301030331021
113300010211 130333202332 211031120231 122120333312 210230233311 130221110321,

Figure 1: New self-dual $\mathbb{Z}_4$-codes of length 24 and $d_L = 10$ (continued)

M_{41}: 101001021133 333323301222 031110132120 201333213012 020331121323 103012113201
133120010033 330311020312 211213100213 122322113332 210230031313 332001132301,
M_{42}: 323223023111 313121121202 011110130302 203111033232 020133123321 123012313203
311102212231 130333202332 213011320033 322102113110 232030011133 332021330101,
M_{43}: 321021201333 111321301020 011130330322 223113013230 202113323321 123012311221
131320232013 310131020330 233231122231 302322133110 232010011333 112223312101,
M_{44}: 121201221133 331103321002 211110312322 223131033010 002333303123 303210133221
133120212233 310113022110 031011102013 122122111110 032032211133 132021130121,
M_{45}: 323201023311 333101301002 213330332300 003311013230 222133303323 303210311203
311102010013 130311222112 231031100233 120120331112 210210231333 312221112301,
M_{46}: 321221201333 333303123000 011130332322 201333233032 000111103321 123230113203
113302030031 312313020130 011213122031 102300313130 210012031333 110203332301,
M_{47}: 321001023313 111123103222 011312312100 201133011010 202313301321 101030113201
313100232013 312311220112 211231322011 102100111112 210010211133 132201110321,
M_{48}: 103023223311 333103101002 233112332122 003311011212 200131301101 323012133201
113322032031 112333202132 213213302213 300122133310 012230211333 132023132103,
M_{49}: 323021223333 111123103222 031110310120 223131231030 222333323301 321232331021
113322230213 112313022330 031033120013 120102311130 032232031333 310203332323,
M_{50}: 121223003313 131301303020 213332132102 023131231232 022111123123 123012113001
331120012233 310331220132 211013320011 100120313110 230212011113 310023130123,
M_{51}: 103023223113 113123303222 233130310102 023131231230 000131303321 103212313003
131300012011 312111000132 231033102213 320120111132 012030013313 310221312303,
M_{52}: 103221003331 113323103220 213112132102 223311011210 002111101121 321210131001
111320010013 330133222112 013013302231 122122113130 012010031311 310201110321,
M_{53}: 303221221313 313303303022 033330130302 023311233212 002311123323 121012133001
333122230033 110131202130 211211122033 300322333312 030032031113 312001332321,
M_{54}: 103023221133 313103301202 011312330302 023331013210 220331103123 121210111201
313122030031 132111220312 013213320231 120100313110 010032011113 310001332321,
M_{55}: 303023003313 111301123002 233110310320 201111233010 202133121303 323010131003
311300210033 110111200330 211033102211 120302333112 212232213331 110201310123,
M_{56}: 103023203113 133123123222 031310330122 001133231030 002111303323 123012333221
333100232233 110113202132 233011320013 320102113332 010210231333 330003312101,
M_{57}: 321003003131 311323123002 211310112320 223333233210 222133123321 103230113203
313300210031 132333222112 031033122031 122120313332 030212233333 112203132303

Figure 1: New self-dual $\mathbb{Z}_4$-codes of length 24 and $d_L = 10$ (continued)