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

Masaaki Harada*

March 27, 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 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 $\mathbb{Z}_4$-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 Nordstrom–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 Nordstrom–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.

1All 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 $d_L(C)$ of self-dual $\mathbb{Z}_4$-codes $C$ of length $n$. For even lengths $n = 24k + \ell$, the upper bounds are given as $d_L(C) \leq 8k + g(\ell)$, where $g(\ell)$ is given by the following table:

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

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 $k \geq 154$ (resp. $k \geq 159$). 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 $C$ 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 $C^\perp$ of $C$ is defined
as $C^\perp = \{ x \in \mathbb{Z}_4^n | x \cdot y = 0 \text{ for all } y \in C \}$, where $x \cdot y$ is the standard inner product. A $\mathbb{Z}_4$-code $C$ is self-dual if $C = C^\perp$. The Hamming weight $w_H(x)$, Lee weight $w_L(x)$ and Euclidean weight $w_E(x)$ of a codeword $x$ of $C$ 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 $d_L(C)$ (resp. minimum Euclidean weight $d_E(C)$) of $C$ is the smallest Lee (resp. Euclidean) weight among all non-zero codewords of $C$. The residue code $C^{(i)}$ of $C$ is the binary code defined as $C^{(i)} = \{ c \pmod{2} | c \in C \}$. If $C$ is a self-dual $\mathbb{Z}_4$-code, then $C^{(i)}$ is doubly even [6].

The following characterization of the minimum Lee weights is useful.

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

The Gray map $\phi$ is defined as a map from $\mathbb{Z}_4^n$ to $\mathbb{Z}_2^{2n}$ mapping $(x_1, \ldots, x_n)$ to $(\varphi(x_1), \ldots, \varphi(x_n))$, where $\varphi(0) = (0, 0)$, $\varphi(1) = (0, 1)$, $\varphi(2) = (1, 1)$ and $\varphi(3) = (1, 0)$. The Gray image $\phi(C)$ of a $\mathbb{Z}_4$-code $C$ needs not be linear. Let $C$ be a self-dual $\mathbb{Z}_4$-code of length $n$ and minimum Lee weight $d_L(C)$. Then the Gray image $\phi(C)$ has parameters $(2n, 2^n, d_L(C))$ (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 $d_E(C)$ of a Type II $\mathbb{Z}_4$-code $C$ of length $n$ is bounded by $d_E(C) \leq 8\lfloor \frac{n}{24} \rfloor + 8$. A Type II $\mathbb{Z}_4$-code meeting this bound is called extremal. It was also shown in [19] that the minimum Euclidean weight $d_E(C)$ of a Type I $\mathbb{Z}_4$-code $C$ of length $n$ is bounded by $d_E(C) \leq 8\lfloor \frac{n}{24} \rfloor + 12$ if $n \equiv 23 \pmod{24}$, and $d_E(C) \leq 8\lfloor \frac{n}{24} \rfloor + 12$ 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
A 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 $d(C) \leq 4\lfloor \frac{n}{24} \rfloor + 6$ if $n \equiv 22 \pmod{24}$, $d \leq 4\lfloor \frac{n}{24} \rfloor + 4$ 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 $R(C) \leq \#\{i > 0 \mid B_i \neq 0\}$, 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 $d(S) \leq \frac{n}{2} + 4 - 2d(C)$, 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 $C$. 

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

**Proof.** Since $C^{(1)}$ is doubly even, by Lemma 2.4, there is a binary doubly even self-dual code $C$ satisfying that $C^{(1)} \subseteq C \subseteq C^{(1)\perp}$. Since $C$ has minimum Lee weight $8k + 4$ (resp. $8k + 2$), by Lemma 2.1, $C^{(1)\perp}$ 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 $C \subsetneq C^{(1)\perp}$, then the minimum weight of $C^{(1)\perp}$ is at most $4k$, which is a contradiction. Therefore, $C = C^{(1)}$. □

**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 $C^{(1)}$ is not self-dual. Since $C^{(1)}$ is doubly even, by Lemma 2.4, there is a binary singly even self-dual code $C$ satisfying that $C^{(1)} \subseteq C \subsetneq C^{(1)\perp}$, where $C_0$ denotes the doubly even subcode of $C$. By Lemma 2.1, $C^{(1)\perp}$ 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, $C^{(1)}$ is self-dual, that is, $C^{(1)}$ 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 24\(k\), 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 24\(k\) for \(k \geq 154\) \cite{[21]}. Hence, we immediately have the following:

**Corollary 3.4.** The minimum Lee weight of a self-dual \(Z_4\)-code of length 24\(k\) is at most 8\(k\) for every integer \(k \geq 154\).

### 3.2 Length 24\(k + 8\)

As described in Section 1, the minimum Lee weight of a self-dual \(Z_4\)-code of length 24\(k + 8\) is at most 8\(k + 8\). In this subsection, we consider self-dual \(Z_4\)-codes of length 24\(k + 8\) and minimum Lee weight 8\(k + 8\) or 8\(k + 6\).

**Theorem 3.5.** Let \(C\) be a self-dual \(Z_4\)-code of length 24\(k + 8\). Suppose that the minimum Lee weight of \(C\) is 8\(k + 8\) or 8\(k + 6\). Then \(C^{(1)}\) is a binary extremal doubly even self-dual code of length 24\(k + 8\).

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

\[
C^{(1)} \subseteq C_0 \subsetneq C \subsetneq C_0^\perp \subseteq C^{(1)}_0^\perp,
\]

where \(C_0\) denotes the doubly even subcode of \(C\). By Lemma 2.1, \(C^{(1)}_0^\perp\) has minimum weight at least 4\(k + 3\). Hence, \(C\) has minimum weight 4\(k + 4\). By Lemma 2.3, the minimum weight of the shadow of a binary singly even self-dual [24\(k + 8, 12k + 4, 4k + 4\)] code is at most 4\(k\), which is a contradiction. Hence, \(C^{(1)}\) is self-dual, that is, \(C^{(1)}\) is extremal.

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

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

**Remark 3.7.** Rains \cite[p. 148]{[18]} pointed out that by the linear programing \(d_L(C) \leq 8k + 6\) 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:

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

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

$$
\begin{pmatrix}
    \alpha & \beta & \cdots & \beta \\
    \gamma & \vdots & \ddots & \gamma \\
    I_n & R
\end{pmatrix}
$$

(1)

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:

\[
\begin{pmatrix}
I_{2n} & A & B \\
-B^T & A^T & -B^T \\
\end{pmatrix}
\]

is called a four-negacirculant \(Z_4\)-code of length \(4n\), where \(A\) and \(B\) are \(n \times n\) negacirculant matrices.

Table 1: Bordered double circulant self-dual \(Z_4\)-codes

| Length | Code | First row of \(R\) | \((\alpha, \beta, \gamma)\) | Type | \(d_L\) |
|--------|------|---------------------|-----------------------------|------|-------|
| 24     | \(D_{24,1}\) | (13103303222) | (0, 1, 1) | I | 10 |
| 24     | \(D_{24,2}\) | (01130332322) | (0, 1, 1) | I | 10 |
| 24     | \(D_{24,3}\) | (31030001332) | (0, 1, 1) | I | 10 |
| 32     | \(D_{32}\) | (002210100233312) | (0, 1, 1) | II | 14 |
| 48     | \(D_{48}\) | (11303312013230033212110) | (0, 1, 1) | II | 18 |
| 56     | \(D_{56,1}\) | (022000202022112232101111011) | (2, 1, 1) | II | 18 |
| 56     | \(D_{56,2}\) | (002200202002312010101111011) | (0, 1, 1) | I | 18 |

By considering bordered double circulant codes and four-negacirculant codes, we found self-dual \(Z_4\)-codes of length \(24k\) and minimum Lee weight \(8k + 2\) \((k = 1, 2)\) and self-dual \(Z_4\)-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 \(Z_4\)-codes of length 56 and minimum Lee weight 18 were also found.

For bordered double circulant codes, the first rows of \(R\) and \((\alpha, \beta, \gamma)\) in Table 1 are listed in Table 1. For four-negacirculant codes, the first rows of \(A\) and \(B\) in Table 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 \(Z_4\)-codes

| Length | Code | First row of \(A\) | First row of \(B\) | Type | \(d_L\) |
|--------|------|---------------------|---------------------|------|-------|
| 32     | \(C_{32}\) | (22312012) | (03113022) | II | 14 |
| 56     | \(C_{56}\) | (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 $C$ be a self-dual $\mathbb{Z}_4$-code of length 24 and minimum Lee weight 10. Then $C$ is a Type I $\mathbb{Z}_4$-code having minimum Euclidean weight 12.

**Proof.** Let $x$ be a codeword $x$ of $C$ with $\text{wt}_L(x) = 10$. 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, $C^{(1)} \cong G_{24}$. 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, $\text{wt}_E(x) = 12$. Therefore, $C$ is a Type I $\mathbb{Z}_4$-code having minimum Euclidean weight 12. \qed

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 $\text{wt}_H(x) = t$ in $C$, where $A_t$ denotes the number of such codewords. For an integer $k$ ($1 \leq k \leq n$), let $n_t(j_1, \ldots, j_k)$ be the number of $r$ ($1 \leq r \leq A_t$) such that all $m_{rj_1}, \ldots, m_{rj_k}$ are nonzero for $1 \leq j_1 < \ldots < j_k \leq n$. We consider the set

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

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 $D_{24,i}$ ($i = 1, 2, 3$) 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 $S_k = (\max(S_{9,k}), \min(S_{9,k}), \#S_{9,k})$ ($k = 1, 2, 3, 4$) for the codes. This table shows that the three codes $D_{24,1}, D_{24,2}, D_{24,3}$ are inequivalent.
Table 3: $S_1$, $S_2$, $S_3$, $S_4$ for $D_{24,1}$, $D_{24,2}$, $D_{24,3}$

| Code  | $S_1$     | $S_2$     | $S_3$     | $S_4$     |
|-------|-----------|-----------|-----------|-----------|
| $D_{24,1}$ | (352, 256, 2) | (128, 0, 5) | (48, 0, 11) | (20, 0, 11) |
| $D_{24,2}$ | (352, 256, 2) | (128, 0, 5) | (48, 0, 11) | (18, 0, 10) |
| $D_{24,3}$ | (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 $2^{k(k+1)/2}$ self-dual $\mathbb{Z}_4$-codes $C$ with $C^{(1)} = C$, and an explicit method for construction of these $2^{k(k+1)/2}$ self-dual $\mathbb{Z}_4$-codes $C$ with $C^{(1)} = C$ was given in [15, Section 3]. In our case, there are $2^{78}$ self-dual $\mathbb{Z}_4$-codes $C$ with $C^{(1)} = G_{24}$, 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 $C_{24,i}$ ($i = 1, 2, \ldots, 57$). In Figure 1 we list generator matrices for $C_{24,i}$, 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 $QR_{32}$ and the Reed–Muller $\mathbb{Z}_4$-code $QR.M(2, 5)$, 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 $QR_{32}^{(1)}$ (resp. $QR.M(2, 5)^{(1)}$) 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 $8n$ ($n = 1, 2, \ldots, 8$).
According to the table, the largest minimum Lee weight for length 32 is 14. The code $D_{32}$ 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 $C_{32}$ in Table 2 is a Type II $\mathbb{Z}_4$-code of length 32 and minimum Lee weight 14. We verified by Magma that $C_{32}^{(1)} \cong D_{32}^{(1)} \cong QR_{32}$. 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 $C$ having minimum Lee weight 14 with $C^{(1)} \cong C$ for each $C$ of the remaining three codes.

The extended lifted quadratic residue $\mathbb{Z}_4$-code $QR_{48}$ 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, $QR_{48}^{(1)}$ 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 $D_{48}$ in Table 1 gives an explicit example of such codes. It is unknown whether $D_{48}$ is equivalent to $QR_{48}$ 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 $C_{56}$ in Table 2 is a Type II $\mathbb{Z}_4$-code of length 56 and minimum Lee weight 18. Hence, $C_{56}$ 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 $D_{56,1}$ and $D_{56,2}$ in Table 1 give explicit examples of such codes. We verified by Magma that $D_{56,2}$ has minimum Euclidean weight 20. Since $D_{56,1}$ is Type II, $D_{56,1}$ is extremal. We verified by Magma that $C_{56}^{(1)}$ and $D_{56,1}^{(1)}$ have automorphism groups of orders 28 and 54, respectively. This shows that $C_{56}$ and $D_{56,1}$ 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 $C^{(1)}$ of self-dual $\mathbb{Z}_4$-codes $C$ of length $24k + \alpha$ for $\alpha = 2, 4, 6, 10, 14, 16, 18, 20, 22$.

**Proposition 5.1.** Let $C$ 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 $C^{(1)}$ 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 $C^{(1)} \subseteq C_0 \subset C \subset C_0^\perp \subset C^{(1)}$, where $C_0$ denotes the doubly even subcode of $C$. By Lemma 2.4, $C^{(1)}$ 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 $C^{(1)}$. 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.

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 $C$ 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 $C^{(1)}$. 

12
(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 $\alpha$-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 02011103321 301010131221 |
| :---: | :---: | :---: | :---: | :---: | :---: |
| $M_2$: | 12021003313 313321321222 231310132322 001310313232 023333033010 02011103321 301010131221 |
| $M_3$: | 133223220310 301332220312 210111322321 102122333130 012012013113 110223412301, |
| $M_4$: | 130230213113 311121102120 011132101230 221312130320 323232130323 |
| $M_5$: | 13132003313 303332110320 203332130320 023333303303 023303230130, |
| $M_6$: | 131321102311 311121103202 231330112300 023333033010 02011103321 301010131221 |
| $M_7$: | 13102103131 313321101000 301310312300 203332130320 323232130323, |
| $M_8$: | 311102232300 32323302130 232313320211 322100131110 032203223331 31020132123, |
| $M_9$: | 131120212311 131121301220 011232103201 221312130320 323232130323, |
| $M_{10}$: | 13102103131 313321101000 301310312300 203332130320 323232130323, |
| $M_{11}$: | 311222320111 310110123222 031112323222 023311230132 003201323301 31020132123, |
| $M_{12}$: | 131120212311 131121301220 011232103201 221312130320 323232130323, |
| $M_{13}$: | 131120212311 131121301220 011232103201 221312130320 323232130323, |
| $M_{14}$: | 131120212311 131121301220 011232103201 221312130320 323232130323, |
| $M_{15}$: | 131120212311 131121301220 011232103201 221312130320 323232130323, |
| $M_{16}$: | 131120212311 131121301220 011232103201 221312130320 323232130323, |
| $M_{17}$: | 131120212311 131121301220 011232103201 221312130320 323232130323, |
| $M_{18}$: | 131120212311 131121301220 011232103201 221312130320 323232130323, |
| $M_{19}$: | 131120212311 131121301220 011232103201 221312130320 323232130323, |
| $M_{20}$: | 131120212311 131121301220 011232103201 221312130320 323232130323, |

Figure 1: New self-dual $Z_4$-codes of length 24 and $d_L = 10$.
Figure 1: New self-dual $\mathbb{Z}_4$-codes of length 24 and $d_L = 10$ (continued)
Figure 1: New self-dual $\mathbb{Z}_4$-codes of length 24 and $d_L = 10$ (continued)