Discrete Mathematics 311 (2011) 2148–2157

Contents lists available at SciVerse ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

On the residue codes of extremal Type II $\mathbb{Z}_4$-codes of lengths 32 and 40

Masaaki Harada *

Department of Mathematical Sciences, Yamagata University, Yamagata 990–8560, Japan
PRESTO, Japan Science and Technology Agency, Kawaguchi, Saitama 332–0012, Japan

A R T I C L E I N F O

Article history:
Received 30 August 2010
Received in revised form 17 May 2011
Accepted 20 June 2011
Available online 23 July 2011

Keywords:
Extremal Type II $\mathbb{Z}_4$-code
Residue code
Binary doubly even code

A B S T R A C T

In this paper, we determine the dimensions of the residue codes of extremal Type II $\mathbb{Z}_4$-codes of lengths 32 and 40. We demonstrate that every binary doubly even self-dual code of length 32 can be realized as the residue code of some extremal Type II $\mathbb{Z}_4$-code. It is also shown that there is a unique extremal Type II $\mathbb{Z}_4$-code of length 32 whose residue code has the smallest dimension 6 up to equivalence. As a consequence, many new extremal Type II $\mathbb{Z}_4$-codes of lengths 32 and 40 are constructed.

1. Introduction

As described in [19], 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 construct self-dual codes with 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 applications to unimodular lattices and nonlinear binary codes, where $\mathbb{Z}_k$ denotes the ring of integers modulo k and k is a positive integer.

A $\mathbb{Z}_4$-code C is Type II if C is self-dual and the Euclidean weights of all codewords of C are divisible by 8 [2,14]. This is a remarkable class of self-dual $\mathbb{Z}_4$-codes related to even unimodular lattices. A Type II $\mathbb{Z}_4$-code of length n exists if and only if $n \equiv 0 \pmod 8$, and the minimum Euclidean weight d_E of a Type II $\mathbb{Z}_4$-code of length n is bounded by $d_E \le 8\lfloor n/24 \rfloor + 8$ [2]. A Type II $\mathbb{Z}_4$-code meeting this bound with equality is called extremal. If C is a Type II $\mathbb{Z}_4$-code, then the residue code $C^{(1)}$ is a binary doubly even code containing the all-ones vector $\mathbf{1}$ [7,14].

It follows from the mass formula in [8] that for a given binary doubly even code B containing $\mathbf{1}$ there is a Type II $\mathbb{Z}_4$-code C with $C^{(1)} = B$. However, it is not known in general whether there is an extremal Type II $\mathbb{Z}_4$-code C with $C^{(1)} = B$ or not. Recently, at length 24, binary doubly even codes which are the residue codes of extremal Type II $\mathbb{Z}_4$-codes have been classified in [13]. In particular, there is an extremal Type II $\mathbb{Z}_4$-code whose residue code has dimension k if and only if $k \in \{6, 7, \dots, 12\}$ [13, Table 1]. It is shown that there is a unique extremal Type II $\mathbb{Z}_4$-code with residue code of dimension 6 up to equivalence [13]. Also, every binary doubly even self-dual code of length 24 can be realized as the residue code of some extremal Type II $\mathbb{Z}_4$-code [5, Postscript] (see also [13]). Since extremal Type II $\mathbb{Z}_4$-codes of length 24 and their residue codes are related to the Leech lattice [2,5] and structure codes of the moonshine vertex operator algebra [13], respectively, this length is of special interest. For the next two lengths, $n = 32$ and 40, a number of extremal Type II $\mathbb{Z}_4$-codes are known (see [15]). However, only a few extremal Type II $\mathbb{Z}_4$-codes which have residue codes of dimension less than $n/2$ are known for these lengths n. This motivates us to study the dimensions of the residue codes of extremal Type II $\mathbb{Z}_4$-codes for these lengths.

* Corresponding address: Department of Mathematical Sciences, Yamagata University, Yamagata 990–8560, Japan.
E-mail address: mharada@sci.kj.yamagata-u.ac.jp.

0012-365X/$ – see front matter
doi:10.1016/j.disc.2011.06.022

In this paper, it is shown that there is an extremal Type II $\mathbb{Z}_4$-code of length 32 whose residue code has dimension k if and only if $k \in \{6, 7, \dots, 16\}$. In particular, we study two cases $k = 6$ and 16. We demonstrate that every binary doubly even self-dual code of length 32 can be realized as the residue code of some extremal Type II $\mathbb{Z}_4$-code. It is also shown that there is a unique extremal Type II $\mathbb{Z}_4$-code of length 32 with residue code of dimension 6 up to equivalence. Finally, it is shown that there is an extremal Type II $\mathbb{Z}_4$-code of length 40 whose residue code has dimension k if and only if $k \in \{7, 8, \dots, 20\}$. As a consequence, many new extremal Type II $\mathbb{Z}_4$-codes of lengths 32 and 40 are constructed. Extremal Type II $\mathbb{Z}_4$-codes of lengths 32 and 40 are used to construct extremal even unimodular lattices by Construction A (see [2]). All computer calculations in this paper were done by Magma [3].

2. Preliminaries

2.1. Extremal Type II $\mathbb{Z}_4$-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 $C^\perp = \{x \in \mathbb{Z}_4^n \mid x \cdot y = 0 \text{ for all } y \in C\}$, where $x \cdot y = x_1y_1 + \cdots + x_ny_n$ for $x = (x_1, \dots, x_n)$ and $y = (y_1, \dots, y_n)$. A code C is *self-dual* if $C = C^\perp$.

The *Euclidean weight* of a codeword $x = (x_1, \dots, x_n)$ of C is $n_1(x) + 4n_2(x) + n_3(x)$, where $n_\alpha(x)$ denotes the number of components i with $x_i = \alpha$ ($\alpha = 1, 2, 3$). The *minimum Euclidean weight* d_E of C is the smallest Euclidean weight among all nonzero codewords of C. A $\mathbb{Z}_4$-code C is *Type II* if C is self-dual and the Euclidean weights of all codewords of C are divisible by 8 [2,14]. A Type II $\mathbb{Z}_4$-code of length n exists if and only if $n \equiv 0 \pmod 8$, and the minimum Euclidean weight d_E of a Type II $\mathbb{Z}_4$-code of length n is bounded by $d_E \le 8\lfloor n/24 \rfloor + 8$ [2]. A Type II $\mathbb{Z}_4$-code meeting this bound with equality is called *extremal*.

The classification of Type II $\mathbb{Z}_4$-codes has been done for lengths 8 and 16 [7,16]. At lengths 24, 32 and 40, a number of extremal Type II $\mathbb{Z}_4$-codes are known (see [15]). At length 48, only two inequivalent extremal Type II $\mathbb{Z}_4$-codes are known [2,12]. At lengths 56 and 64, recently, an extremal Type II $\mathbb{Z}_4$-code has been constructed in [11].

2.2. Binary doubly even self-dual codes

Throughout this paper, we denote by $\dim(B)$ the dimension of a binary code B. Also, for a binary code B and a binary vector v, we denote by $\langle B, v \rangle$ the binary code generated by the codewords of B and v. A binary code B is called doubly even if $\mathrm{wt}(x) \equiv 0 \pmod 4$ for any codeword $x \in B$, where $\mathrm{wt}(x)$ denotes the weight of x. A binary doubly even self-dual code of length n exists if and only if $n \equiv 0 \pmod 8$, and the minimum weight d of a binary doubly even self-dual code of length n is bounded by $d \le 4\lfloor n/24 \rfloor + 4$ (see [15,19]). A binary doubly even self-dual code meeting this bound with equality is called extremal.

Two binary codes B and B' are equivalent, denoted $B \cong B'$, if B can be obtained from B' by permuting the coordinates. The classification of binary doubly even self-dual codes has been done for lengths up to 32 (see [6,15,19]). There are 85 inequivalent binary doubly even self-dual codes of length 32, five of which are extremal [6].

2.3. Residue codes of $\mathbb{Z}_4$-codes

Every $\mathbb{Z}_4$-code C of length n has two binary codes $C^{(1)}$ and $C^{(2)}$ associated with C:

$$C^{(1)} = \{c \bmod 2 \mid c \in C\} \quad \text{and} \quad C^{(2)} = \left\{c \bmod 2 \mid c \in \mathbb{Z}_4^n, 2c \in C\right\}.$$

The binary codes $C^{(1)}$ and $C^{(2)}$ are called the *residue* and *torsion* codes of C, respectively. If C is self-dual, then $C^{(1)}$ is a binary doubly even code with $C^{(2)} = C^{(1)\perp}$ [7]. If C is Type II, then $C^{(1)}$ contains the all-ones vector $\mathbf{1}$ [14].

The following two lemmas can be easily shown (see [13] for length 24).

Lemma 2.1. *Let B be the residue code of an extremal Type II $\mathbb{Z}_4$-code of length $n \in \{24, 32, 40\}$. Then B satisfies the following conditions:*

$$B \text{ is doubly even;} \tag{1}$$

$$\mathbf{1} \in B; \tag{2}$$

$$B^\perp \text{ has minimum weight at least } 4. \tag{3}$$

Proof. The assertions (1) and (2) follow from [7,14], respectively, as described above. If C is an extremal Type II $\mathbb{Z}_4$-code of length n, then $C^{(2)}$ has minimum weight at least $2\lfloor n/24 \rfloor + 2$ (see [11]). The assertion (3) follows. □

Lemma 2.2. *Let B be the residue code of an extremal Type II $\mathbb{Z}_4$-code of length n. Then, $6 \le \dim(B) \le 16$ if $n = 32$, and $7 \le \dim(B) \le 20$ if $n = 40$.*

Proof. Since a binary doubly even code is self-orthogonal, $\dim(B) \le n/2$. From (3), $B^{\perp}$ has minimum weight at least 4. It is known that a $[32, k, 4]$ code exists only if $k \le 26$ and a $[40, k, 4]$ code exists only if $k \le 33$ (see [4]). The result follows. □

In this paper, we consider the existence of an extremal Type II $\mathbb{Z}_4$-code with residue code of dimension k for a given k. To do this, the following lemma is useful, and it was shown in [13] for length 24. Since its modification to lengths 32 and 40 is straightforward, we omit the proof.

Lemma 2.3. *Let C be an extremal Type II $\mathbb{Z}_4$-code of length $n \in \{24, 32, 40\}$. Let v be a binary vector of length n and weight 4 such that $v \notin C^{(1)}$ and the code $\langle C^{(1)}, v\rangle$ is doubly even. Then there is an extremal Type II $\mathbb{Z}_4$-code C' such that $C'^{(1)} = \langle C^{(1)}, v\rangle$.*

2.4. Construction method

In this subsection, we review the method of construction of Type II $\mathbb{Z}_4$-codes, which was given in [16]. Let C_1 be a binary code of length $n \equiv 0 \pmod 8$ and dimension k satisfying conditions (1) and (2). Without loss of generality, we may assume that C_1 has generator matrix of the following form:

$$G_1 = \begin{pmatrix} A & \tilde{I_k} \end{pmatrix}, \tag{4}$$

where A is a $k \times (n-k)$ matrix which has the property that the first row is $\mathbf{1}$, $\tilde{I_k} = \begin{pmatrix} 1 & \cdots & 1 \\ 0 & & \\ \vdots & I_{k-1} & \\ 0 & & \end{pmatrix}$, and I_{k-1} denotes the identity matrix of order $k-1$. Since C_1 is self-orthogonal, the matrix G_1 can be extended to a generator matrix $\begin{pmatrix} G_1 \\ D \end{pmatrix}$ of $C_1^{\perp}$. Then we have a generator matrix of a Type II $\mathbb{Z}_4$-code C as follows:

$$\begin{pmatrix} A & \tilde{I_k} + 2B \\ \multicolumn{2}{c}{2D} \end{pmatrix}, \tag{5}$$

where B is a $k \times k$ (1, 0)-matrices and we regard the matrices as matrices over $\mathbb{Z}_4$. Here, we can choose freely the entries above the diagonal elements and the (1, 1)-entry of B, and the rest is completely determined from the property that C is Type II. Hence, there are $2^{1+k(k-1)/2}$ $k \times k$ (1, 0)-matrices B in (5), and there are $2^{1+k(k-1)/2}$ Type II $\mathbb{Z}_4$-codes C with $C^{(1)} = C_1$ [8,16].

Since any Type II $\mathbb{Z}_4$-code is equivalent to some Type II $\mathbb{Z}_4$-code containing $\mathbf{1}$ [14], without loss of generality, we may assume that the first row of B is the zero vector. This reduces our search space for finding extremal Type II $\mathbb{Z}_4$-codes. In fact, there are only $2^{(k-1)(k-2)/2}$ Type II $\mathbb{Z}_4$-codes C with $C^{(1)} = C_1$ containing $\mathbf{1}$ (see also [1]).

3. Extremal Type II $\mathbb{Z}_4$-codes of length 32

3.1. Known extremal Type II $\mathbb{Z}_4$-codes of length 32

Currently, 57 inequivalent extremal Type II $\mathbb{Z}_4$-codes of length 32 are known (see [9,15]). Among the 57 known codes, 54 codes have residue codes which are extremal doubly even self-dual codes. In particular, for every binary extremal doubly even self-dual code B of length 32, there is an extremal Type II $\mathbb{Z}_4$-code C with $C^{(1)} \cong B$ [9].

Only $C_{5,1}$ in [2] and $\tilde{C}_{31,2}$, $\tilde{C}_{31,3}$ in [17] are known extremal Type II $\mathbb{Z}_4$-codes whose residue codes are not extremal doubly even self-dual codes (see [9]). The residue codes of $\tilde{C}_{31,2}$, $\tilde{C}_{31,3}$ in [17] have dimension 11. The residue code of $C_{5,1}$ in [2] is the first order Reed–Muller code $RM(1, 5)$ of length 32, thus, $\dim(C_{5,1}^{(1)}) = 6$. In Section 3.4, we show that there is a unique extremal Type II $\mathbb{Z}_4$-code of length 32 with residue code of dimension 6, up to equivalence.

3.2. Determination of dimensions of residue codes

By Lemma 2.2, if C is an extremal Type II $\mathbb{Z}_4$-code of length 32, then $6 \le \dim(C^{(1)}) \le 16$. In this subsection, we show the converse assertion using Lemma 2.3. To do this, we first fix the coordinates of $RM(1, 5)$ by considering the following matrix as a generator matrix of $RM(1, 5)$:

$$\begin{pmatrix}
11111111 & 11111111 & 11111111 & 11111111 \\
11111111 & 11111111 & 00000000 & 00000000 \\
11111111 & 00000000 & 11111111 & 00000000 \\
11110000 & 11110000 & 11110000 & 11110000 \\
11001100 & 11001100 & 11001100 & 11001100 \\
10101010 & 10101010 & 10101010 & 10101010
\end{pmatrix}. \tag{6}$$

Table 1
Supports $\mathrm{supp}(v_i)$ and weight distributions of $B_{32,i}$.

i	$\mathrm{supp}(v_i)$	A_4	A_8	A_{12}	A_{16}
7	{1, 2, 3, 4}	1	0	7	110
8	{1, 2, 5, 6}	3	0	21	206
9	{1, 2, 7, 8}	6	4	42	406
10	{1, 2, 9, 10}	10	12	102	774
11	{1, 2, 11, 12}	16	36	208	1526
12	{1, 2, 13, 14}	28	84	420	3030
13	{1, 2, 17, 18}	36	196	924	5878
14	{1, 2, 19, 20}	48	428	1936	11558
15	{1, 2, 21, 22}	72	892	3960	22918

It is well known that $RM(1,5)$ has the following weight enumerator:

$$1 + 62y^{16} + y^{32}. \tag{7}$$

For $i = 7, 8, \dots, 15$, we define $B_{32,i}$ to be the binary code $\langle B_{32,i-1}, v_i\rangle$, where $B_{32,6} = RM(1,5)$ and the support $\mathrm{supp}(v_i)$ of the vector v_i is listed in Table 1. The weight distributions of $B_{32,i}$ ($i = 7, 8, \dots, 15$) are also listed in the table, where A_j denotes the number of codewords of weight j ($j = 4, 8, 12, 16$). From the weight distributions, one can easily verify that $v_i \notin B_{32,i-1}$ and $B_{32,i}$ is doubly even for $i = 7, 8, \dots, 15$. Note that the code $C_{5,1}$ in [2] is an extremal Type II $\mathbb{Z}_4$-code with residue code $RM(1,5)$, and there are extremal Type II $\mathbb{Z}_4$-codes with residue codes of dimension 16. By Lemma 2.3, we have the following:

Proposition 3.1. *There is an extremal Type II $\mathbb{Z}_4$-code of length 32 whose residue code has dimension k if and only if $k \in \{6, 7, \dots, 16\}$.*

Remark 3.2. In the next two subsections, we study two cases $k = 6$ and 16.

As another approach to Proposition 3.1, we explicitly found an extremal Type II $\mathbb{Z}_4$-code $C_{32,i}$ with $C_{32,i}^{(1)} \cong B_{32,i}$ for $i = 7, 8, \dots, 15$, using the method given in Section 2.4. Any $\mathbb{Z}_4$-code with residue code of dimension k is equivalent to a code with generator matrix of the form:

$$\begin{pmatrix} I_k & A \\ O & 2B \end{pmatrix}, \tag{8}$$

where A is a matrix over $\mathbb{Z}_4$ and B is a $(1,0)$-matrix. For these codes $C_{32,i}$, we give generator matrices of the form (8), by only listing in Fig. 1 the $i \times (32 - i)$ matrices A in (8) to save space. Note that the lower part in (8) can be obtained from the matrices $\begin{pmatrix} I_k & A \end{pmatrix}$, since $C^{(2)} = C^{(1)\perp}$ and $\begin{pmatrix} I_k & A \bmod 2 \end{pmatrix}$ is a generator matrix of $C^{(1)}$, where $A \bmod 2$ denotes the binary matrix whose (i,j)-entry is $a_{ij} \bmod 2$ for $A = (a_{ij})$.

3.3. Residue codes of dimension 16

As described above, there are 85 inequivalent binary doubly even self-dual codes of length 32. These codes are denoted by C1, C2, …, C85 in [6, Table A], where C81, …, C85 are extremal. For each B of the 5 extremal ones, there is an extremal Type II $\mathbb{Z}_4$-code C with $C^{(1)} \cong B$ [9].

Using the method given in Section 2.4, we explicitly found an extremal Type II $\mathbb{Z}_4$-code $D_{32,i}$ with $D_{32,i}^{(1)} \cong Ci$ for $i = 1, 2, \dots, 80$. Generator matrices for $D_{32,i}$ can be written in the form $\begin{pmatrix} I_{16} & M_i \end{pmatrix}$ ($i = 1, 2, \dots, 80$), where M_i can be obtained electronically from http://sci.kj.yamagata-u.ac.jp/~mharada/Paper/z4-32.txt. Hence, we have the following:

Proposition 3.3. *Every binary doubly even self-dual code of length 32 can be realized as the residue code of some extremal Type II $\mathbb{Z}_4$-code.*

Among known 57 inequivalent extremal Type II $\mathbb{Z}_4$-codes of length 32, the residue codes of 54 codes are extremal doubly even self-dual codes and the residue codes of the other three codes $C_{5,1}$ in [2] and $\tilde{C}_{31,2}$, $\tilde{C}_{31,3}$ in [17] have dimensions 6, 11 and 11, respectively. In particular, $\tilde{C}_{31,2}^{(1)}$ and $\tilde{C}_{31,3}^{(1)}$ have the following identical weight enumerators:

$$1 + 496y^{12} + 1054y^{16} + 496y^{20} + y^{32}.$$

Hence, by Table 1, none of $\tilde{C}_{31,2}$ and $\tilde{C}_{31,3}$ is equivalent to $C_{32,11}$. The code $C_{32,i}^{(1)}$ has dimension i for $i = 7, 8, \dots, 15$, and $D_{32,i}^{(1)}$ is a non-extremal doubly even self-dual code for $i = 1, 2, \dots, 80$. Since equivalent $\mathbb{Z}_4$-codes have equivalent residue codes, we have the following:

$$\begin{pmatrix} 000000000000000020033322 \\ 110011110011000112111101 2 \\ 101010101010101101101011 1 \\ 011001100110011011010111 1 \\ 001111000011110000112220 3 \\ 001111111100000113002220 0 \\ 111111111111111100000000 0 \end{pmatrix} \quad \begin{pmatrix} 0000000000000000003332220 \\ 0000000000000000001321202 \\ 1010101010101011010 11111 \\ 1010100101010111003 31331 \\ 1111001100001101102 00300 \\ 1100111100110001102 02230 \\ 0011111111000001122 02223 \\ 1111111111111111000 000000 \end{pmatrix}$$

$$\begin{pmatrix} 000000200000002003300032 \\ 000000000000000001322021 \\ 101010110101011010111 11 \\ 101010110101031003131 31 \\ 111100211110021122203 00 \\ 110011211001101122320 02 \\ 001111200111121102032 20 \\ 000000011111110020022 02 \\ 111111100000000000222 20 \end{pmatrix} \quad \begin{pmatrix} 000000200000033322200 2 \\ 000000200000013212000 0 \\ 000000200000013201202 2 \\ 000000200000013220122 0 \\ 001111000111133200232 0 \\ 110011211001133202203 2 \\ 101010110101010111111 1 \\ 010110301011003311133 3 \\ 000000011111120020220 1 \\ 111111000000020000020 0 \end{pmatrix}$$

$$\begin{pmatrix} 00000020000013120200 0 \\ 00000020020013010220 2 \\ 00000000020033003200 2 \\ 00000000020013002120 0 \\ 00000020020013200010 0 \\ 11001121101133020002 3 \\ 10101011011010111111 1 \\ 01100130110103113111 3 \\ 00111100021100000001 2 \\ 00111121110000022222 0 \\ 11111110020020002200 0 \end{pmatrix} \quad \begin{pmatrix} 00000020033202002230 \\ 00000000033002022223 \\ 00000020013220202122 \\ 00000020013022001022 \\ 00000020033020030020 \\ 00000020033000320222 \\ 10101011010111111111 \\ 10101011003113331133 \\ 11110021120021220200 \\ 11001101100012022200 \\ 00111101100100000220 \\ 11111110000002222220 \end{pmatrix}$$

$$\begin{pmatrix} 000000113022002222 2 \\ 000000310120020202 2 \\ 000000330230220002 2 \\ 000000132201200002 2 \\ 000000332002300200 0 \\ 000000332200232200 0 \\ 000000132202021220 2 \\ 000000110220002302 2 \\ 001111330020222210 2 \\ 110011132020002223 2 \\ 101010103311111333 3 \\ 010110013113113331 3 \\ 111111222222002222 1 \end{pmatrix} \quad \begin{pmatrix} 00000113020022200 2 \\ 00000112300220220 0 \\ 00200132010022020 0 \\ 00000310021202002 2 \\ 00000130220120202 0 \\ 00000132202010220 0 \\ 00000312000221000 0 \\ 00000312222002102 2 \\ 00200332020020032 0 \\ 11011132020222002 3 \\ 10110301131331133 1 \\ 01101031113113331 3 \\ 00011202220022003 2 \\ 11300220020000020 2 \end{pmatrix} \quad \begin{pmatrix} 0011022202220002 3 \\ 0013000220202001 2 \\ 0033220222200030 2 \\ 0031220222200102 0 \\ 0011002300022202 0 \\ 0011020230220202 2 \\ 0033022223220200 0 \\ 0031000022102020 2 \\ 0011220000030020 0 \\ 0031020200001200 0 \\ 1030133113111133 1 \\ 1001333331131113 3 \\ 1100003202000000 2 \\ 1100232022022220 2 \\ 1102302222202002 2 \end{pmatrix}$$

Fig. 1. Matrices A in generator matrices of $C_{32,i}$.

Corollary 3.4. *There are at least* 146 *inequivalent extremal Type II* $\mathbb{Z}_4$*-codes of length* 32*.*

Remark 3.5. The torsion codes of all of the 9 codes $C_{32,i}$ $(i = 7, 8, \ldots, 15)$ have minimum weight 4, since their residue codes have minimum weight 4 and the torsion code of an extremal Type II $\mathbb{Z}_4$-code contains no codeword of weight 2. The torsion codes of all of the 80 codes $D_{32,i}$ $(i = 1, 2, \ldots, 80)$ have minimum weight 4. By Theorem 1 in [18], all of the 89 codes $C_{32,i}$ and $D_{32,i}$ have minimum Hamming weight 4. In addition, all of the codes have minimum Lee weight 8, since the minimum Lee weight of an extremal Type II $\mathbb{Z}_4$-code with minimum Hamming weight 4 is 8 (see [2] for the definitions).

3.4. Residue codes of dimension 6

At length 24, the smallest dimension among codes satisfying conditions (1)–(3) is 6. There is a unique binary [24, 6] code satisfying (1)–(3), and there is a unique extremal Type II $\mathbb{Z}_4$-code with residue code of dimension 6 up to equivalence [13]. In this subsection, we show that a similar situation holds for length 32.

Lemma 3.6. *Up to equivalence, $RM(1, 5)$ is the unique binary* [32, 6] *code satisfying conditions* (1)–(3)*.*

Proof. Let B_{32} be a binary $[32, 6]$ code satisfying (1)–(3). From (1) and (2), the weight enumerator of B_{32} is written as:

$$1 + ay^4 + by^8 + cy^{12} + (62 - 2a - 2b - 2c)y^{16} + cy^{20} + by^{24} + ay^{28} + y^{32},$$

where a, b and c are nonnegative integers. By the MacWilliams identity, the weight enumerator of $B_{32}^{\perp}$ is given by:

$$1 + (9a + 4b + c)y^2 + (294a + 24b - 10c + 1240)y^4 + \cdots.$$

From (3), $9a + 4b + c = 0$. This gives $a = b = c = 0$, since all a, b and c are nonnegative. Hence, the weight enumerator of B_{32} is uniquely determined as (7).

Let G be a generator matrix of B_{32} and let r_i be the ith row of G ($i = 1, 2, \ldots, 6$). From the weight enumerator (7), we may assume without loss of generality that the first three rows of G are as follows:

$$\begin{aligned} r_1 &= (11111111 \quad 11111111 \quad 11111111 \quad 11111111),\\ r_2 &= (11111111 \quad 11111111 \quad 00000000 \quad 00000000),\\ r_3 &= (11111111 \quad 00000000 \quad 11111111 \quad 00000000).\end{aligned}$$

Put $r_4 = (v_1, v_2, v_3, v_4)$, where v_i ($i = 1, 2, 3, 4$) are vectors of length 8 and let n_i denote the number of 1's in v_i. Since the binary code B_4 generated by the four rows r_1, r_2, r_3, r_4 has weight enumerator $1 + 14y^{16} + y^{32}$, we have the following system of equations:

$$\begin{aligned} &\mathrm{wt}(r_4) = n_1 + n_2 + n_3 + n_4 = 16,\\ &\mathrm{wt}(r_2 + r_4) = (8 - n_1) + (8 - n_2) + n_3 + n_4 = 16,\\ &\mathrm{wt}(r_3 + r_4) = (8 - n_1) + n_2 + (8 - n_3) + n_4 = 16,\\ &\mathrm{wt}(r_2 + r_3 + r_4) = n_1 + (8 - n_2) + (8 - n_3) + n_4 = 16.\end{aligned}$$

This system of the equations has a unique solution $n_1 = n_2 = n_3 = n_4 = 4$. Hence, we may assume without loss of generality that

$$r_4 = (11110000 \quad 11110000 \quad 11110000 \quad 11110000).$$

Similarly, put $r_5 = (v_1, v_2, \ldots, v_8)$, where v_i ($i = 1, \ldots, 8$) are vectors of length 4 and let n_i denote the number of 1's in v_i. Since the binary code $B_5 = \langle B_4, r_5\rangle$ has weight enumerator $1 + 30y^{16} + y^{32}$, we have the following system of the equations:

$$\sum_{a\in\Gamma_t} n_a + \sum_{b\in\{1,\ldots,8\}\setminus\Gamma_t} (4 - n_b) = 16 \quad (t = 1, \ldots, 8),$$

where Γ_t ($t = 1, \ldots, 8$) are $\{1, \ldots, 8\}$, $\{5, 6, 7, 8\}$, $\{3, 4, 7, 8\}$, $\{2, 4, 6, 8\}$, $\{1, 2, 7, 8\}$, $\{1, 3, 6, 8\}$, $\{1, 4, 5, 8\}$ and $\{2, 3, 5, 8\}$. This system of the equations has a unique solution $n_i = 2$ ($i = 1, \ldots, 8$). Hence, we may assume without loss of generality that

$$r_5 = (11001100 \quad 11001100 \quad 11001100 \quad 11001100).$$

Finally, put $r_6 = (v_1, v_2, \ldots, v_{16})$, where v_i ($i = 1, \ldots, 16$) are vectors of length 2 and let n_i denote the number of 1's in v_i. Similarly, since the binary code $\langle B_5, r_6\rangle$ has weight enumerator (7), we have $n_i = 1$ ($i = 1, \ldots, 16$). Hence, we may assume without loss of generality that

$$r_6 = (10101010 \quad 10101010 \quad 10101010 \quad 10101010).$$

Therefore, a generator matrix G is uniquely determined up to permutation of columns. □

Using a classification method similar to that described in [13, Section 4.3], we verified that all Type II $\mathbb{Z}_4$-codes with residue codes $RM(1, 5)$ are equivalent. Therefore, we have the following:

Proposition 3.7. *Up to equivalence, there is a unique extremal Type II $\mathbb{Z}_4$-code of length* 32 *with residue code of dimension* 6.

By Proposition 3.3 and Lemma 3.6, all binary $[32, k]$ codes satisfying (1)–(3) can be realized as the residue codes of some extremal Type II $\mathbb{Z}_4$-codes for $k = 6$ and 16. The binary $[32, 7]$ code $N_{32} = \langle RM(1, 5), v\rangle$ satisfies (1)–(3), where $RM(1, 5)$ is defined by (6) and

$$\mathrm{supp}(v) = \{1, 2, 3, 4, 5, 9, 17, 29\}.$$

However, we verified that none of the Type II $\mathbb{Z}_4$-codes C with $C^{(1)} = N_{32}$ is extremal, using the method in Section 2.4. Therefore, there is a binary code satisfying (1)–(3) which cannot be realized as the residue code of an extremal Type II $\mathbb{Z}_4$-code of length 32.

Table 2
Supports $\mathrm{supp}(w_i)$ and weight distributions of $B_{40,i}$.

i	$\mathrm{supp}(w_i)$	A_4	A_8	A_{12}	A_{16}	A_{20}
8	{1, 2, 4, 29}	1	0	1	35	180
9	{1, 2, 5, 33}	3	0	3	75	348
10	{1, 2, 7, 31}	6	1	10	150	688
11	{1, 2, 9, 10}	10	6	22	313	1344
12	{1, 2, 11, 17}	15	21	48	634	2658
13	{1, 2, 12, 39}	22	56	102	1271	5288
14	{1, 2, 13, 27}	29	99	280	2620	10326
15	{1, 2, 14, 37}	37	175	688	5296	20374
16	{1, 2, 15, 35}	47	313	1548	10694	40330
17	{1, 2, 20, 36}	57	509	3436	21698	79670
18	{1, 2, 21, 28}	68	845	7344	43826	157976
19	{1, 2, 24, 32}	84	1533	15184	87938	314808

4. Extremal Type II $\mathbb{Z}_4$-codes of length 40

4.1. Determination of dimensions of residue codes

Currently, 23 inequivalent extremal Type II $\mathbb{Z}_4$-codes of length 40 are known [5,9,10,17]. Among these 23 known codes, the 22 codes have residue codes which are doubly even self-dual codes and the other code is given in [17]. Using an approach similar to that used in the previous section, we determine the dimensions of the residue codes of extremal Type II $\mathbb{Z}_4$-codes of length 40.

By Lemma 2.2, if C is an extremal Type II $\mathbb{Z}_4$-code of length 40, then $7 \le \dim(C^{(1)}) \le 20$. Using the method given in Section 2.4, we explicitly found an extremal Type II $\mathbb{Z}_4$-code from some binary doubly even [40, 7, 16] code. This binary code was found as a subcode of some binary doubly even self-dual code. We denote the extremal Type II $\mathbb{Z}_4$-code by $C_{40,7}$. The weight enumerators of $C_{40,7}^{(1)}$ and ${C_{40,7}^{(1)}}^{\perp}$ are given by:

$$
\begin{aligned}
&1 + 15y^{16} + 96y^{20} + 15y^{24} + y^{40},\\
&1 + 1510y^{4} + 59\,520y^{6} + 1203\,885y^{8} + 13\,235\,584y^{10} + 87\,323\,080y^{12}\\
&\quad + 362\,540\,160y^{14} + 982\,189\,650y^{16} + 1771\,386\,240y^{18} + 2154\,055\,332y^{20} + \cdots + y^{40},
\end{aligned}
$$

respectively. For the code $C_{40,7}$, we give a generator matrix of the form (5), by only listing the 7×40 matrix G_{40} which has form $(\ A\ \ \tilde{I_7} + 2B)$ in (5):

$$
G_{40} = \begin{pmatrix}
111111111111111111111111111111111 & 1111111\\
101101001011110000011001100000101 & 0100000\\
100000101011011000100010001111011 & 2210000\\
100110011011001101111111101000100 & 0203000\\
011110110111111001011010010001010 & 0002300\\
110100101111000011100110000010100 & 0202010\\
010111101001111110010110110100010 & 0002003
\end{pmatrix}.
$$

Note that the lower part in (5) can be obtained from G_{40}.

Using the generator matrix $G_{40} \bmod 2$ of the binary code $C_{40,7}^{(1)}$, we establish the existence of some extremal Type II $\mathbb{Z}_4$-codes, by Lemma 2.3, as follows. For $i = 8, 9, \ldots, 19$, we define $B_{40,i}$ to be the binary code $\langle B_{40,i-1}, w_i\rangle$, where $B_{40,7} = C_{40,7}^{(1)}$ and $\mathrm{supp}(w_i)$ is listed in Table 2. The weight distributions of $B_{40,i}$ $(i = 8, 9, \ldots, 19)$ are also listed in the table, where A_j denotes the number of codewords of weight j $(j = 4, 8, 12, 16, 20)$. From the weight distributions, one can easily verify that $w_i \notin B_{40,i-1}$ and $B_{40,i}$ is doubly even for $i = 8, 9, \ldots, 19$. There are extremal Type II $\mathbb{Z}_4$-codes with residue codes of dimension 20. By Lemma 2.3, we have the following:

Proposition 4.1. *There is an extremal Type II $\mathbb{Z}_4$-code of length 40 whose residue code has dimension k if and only if $k \in \{7, 8, \ldots, 20\}$.*

As another approach to Proposition 4.1, we explicitly found an extremal Type II $\mathbb{Z}_4$-code $C_{40,i}$ with $C_{40,i}^{(1)} \cong B_{40,i}$ for $i = 8, 9, \ldots, 19$. To save space, we only list in Fig. 2 the $i \times (40 - i)$ matrices A in generator matrices of the form (8).

Remark 4.2. Similar to Remark 3.5, all of the codes $C_{40,i}$ $(i = 7, 8, \ldots, 19)$ have minimum Hamming weight 4 and minimum Lee weight 8.

$$\begin{pmatrix}
11211101101110100310100112102303 \\
01311010010110010300111111130210 \\
01100100001110100111011112012220 \\
11001111011010001201110113003301 \\
11001000111101000210000010131312 \\
11200100010001011101001103021013 \\
00011111111111111100000000022000 \\
11300000000000000000000002000202
\end{pmatrix}
\quad
\begin{pmatrix}
101111010010110010301111111 0102 \\
10131100110000000001111100332213 \\
00020111101101000121110112012 10 \\
00201010101001110010100102131 31 \\
11000010001000101111001110211 12 \\
00221110110111010010100103022 31 \\
00001111111111111111000000020020 \\
11300000000000000000000000020202 \\
11230000000000000000000000020020
\end{pmatrix}$$

$$\begin{pmatrix}
103110111100010111001011023131 \\
011330110011001110001103313323 \\
002221101000100110110111133012 \\
000220010001000101011100310332 \\
002220100011110100101101202003 \\
110021010101001110101111102220 \\
000201111111111111010000102220 \\
113020000000000000000002002220 \\
110230000000000000000000020002 \\
112300000000000000000000200002
\end{pmatrix}
\quad
\begin{pmatrix}
1200110110111101010301110 1331 \\
010011011011110101010311211 33 \\
000000011110101110200031212 00 \\
020100100011011010010323320 00 \\
021000001111001101021002130 22 \\
131101010101000110320101332 22 \\
020111100111011110101112202 00 \\
001001111111011111032103022002 \\
110000000000000000000002200023 \\
110000000000000000200022023 02 \\
130000000000000000220220220 12
\end{pmatrix}$$

$$\begin{pmatrix}
1120000000000000000220023020 \\
0022011110101110000033030222 \\
0111111111111000110130231312 2 \\
0022201111001101001002312221 \\
0133101110110011110230103311 \\
1120200000000000000202002322 \\
1100011000000000000322022013 \\
1011311011110101010333211300 \\
0133111100101011111201213332 \\
1132200000000000000202200000 \\
1102300000000000000202022000 \\
1103000000000000000202202200
\end{pmatrix}
\quad
\begin{pmatrix}
1102000000000000000022203222 \\
0111310101011011010000003101 \\
1102200100000100311113020 03 \\
0002201111001101001203102 12 \\
0113111110110011110321031 10 \\
1100200000000000000022020302 \\
0111130011110101010112313 11 \\
0022020111011110101322200 21 \\
0111331011110101210132133 21 \\
1130020000000000000002222202 \\
1122320000000000020000002022 \\
1123000000000000020002020200 \\
1102030000000000020022222202
\end{pmatrix}$$

$$\begin{pmatrix}
110222000000000000032220020 \\
110200300000000000202000202 \\
101131310110011001132311 31 \\
101311110111001012133313 01 \\
112200000000000000203020222 \\
002220201010111003223323 13 \\
101333300101111102132003 00 \\
000002001010111001203113 32 \\
112200000100111111223102 00 \\
013113311111101111331200 22 \\
113020200000000000220202200 \\
110032200000000000202002000 \\
112320000000000000200200222 \\
112203200000000000222220002
\end{pmatrix}
\quad
\begin{pmatrix}
110002200000000000232222022 \\
101131310110010233333311 33 \\
011131310111010103133132 3 \\
110220000000000000203022000 \\
110202001010110032223011 3 \\
101133100101111201110012 0 \\
110200001010110232001133 0 \\
000020200100111310023002 0 \\
103333111111111111333202 20 \\
110020000000000000202302020 \\
113022200000000002022222022 \\
110032000000000000220000220 \\
112320000000000002020220020 \\
110220300000000000002220000 \\
110203200000000002002220222
\end{pmatrix}$$

Fig. 2. Matrices A in generator matrices of $C_{40,i}$.

4.2. Residue codes of dimension 7

At lengths 24 and 32, the smallest dimensions among binary codes satisfying (1)–(3) are both 6, and there is a unique extremal Type II $\mathbb{Z}_4$-code with residue code of dimension 6, up to equivalence, for both lengths (see [13] and Proposition 3.7).

At length 40, we found an extremal Type II $\mathbb{Z}_4$-code $C'_{40,7}$ with residue code $C'^{(1)}_{40,7} = \langle C^{(1)}_{40,7} \cap \langle v \rangle^{\perp}, v \rangle$, where

$$\mathrm{supp}(v) = \{1, 3, 4, 6, 8, 9, 10, 11, 12, 13, 18, 20\}.$$

The weight enumerators of $C'^{(1)}_{40,7}$ and ${C'^{(1)}_{40,7}}^{\perp}$ are given by:

$$1 + y^{12} + 11y^{16} + 102y^{20} + 11y^{24} + y^{28} + y^{40},$$

$$1 + 1542y^4 + 59264y^6 + 1204\,653y^8 + 13\,234\,816y^{10} + 87\,321\,928y^{12} \\
+ 362\,544\,000y^{14} + 982\,186\,834y^{16} + 1771\,383\,424y^{18} + 2154\,061\,668y^{20} + \cdots + y^{40},$$

$$\begin{pmatrix}
1120200000002002220302220\\
1100202000030020220200020\\
0002000000000000333020002\\
1120020000000002222232002\\
0111333011130012311111331\\
1011131111031022203131020\\
1013311111011002203132120\\
0000222001001111322002030\\
1120020010101122310023130\\
1033331111131133103312000\\
1122220000020022200030020\\
1130020000020002020000020\\
1122320000000000220200200\\
1123020000020002222202000\\
1122203000000000000222002\\
1100032000020000000200022
\end{pmatrix}
\begin{pmatrix}
1120200220000022023202 0\\
0000022220002003330202 0\\
1122000000000202200032 02\\
1031313310111032131113 1\\
1011133131110020001333 2\\
1031331131112022003132 1\\
1122002020012111122222 0\\
0022222000101102330001 1\\
1031131131113111303130 2\\
1120002200000200220203 22\\
1132200200000002022000 20\\
1102302020000020000222 0\\
1103020020000022022020 0\\
1102200320002020020200 0\\
1120022030000022000220 0\\
1122003200002020202200 2\\
1120232200000200200222 00
\end{pmatrix}$$

$$\begin{pmatrix}
11002002200222022222302\\
00102103002022020022222\\
13002200200222200001202\\
01112310333313133331313\\
13103013300202220222220\\
13101003120100000000002\\
02110011132322200020222\\
13110112002320200022000\\
13000000002202222122020\\
12110310131331131311130\\
13000202220220122000200\\
13002002022202012022000\\
13011303203220202020000\\
13002002222222222000201\\
11002200222030200020220\\
13000002220220020220120\\
11000200202223020220020\\
11000000022022223200000
\end{pmatrix}
\begin{pmatrix}
0130020200020212020020\\
0023300220000300000220\\
0112002022020023200000\\
1130300021000302023020\\
1132122201202322212220\\
0031333130111213302130\\
1132300222220120033020\\
0132222202002222120220\\
0112222222020002220300\\
0130022020122220220000\\
1012331131311131131130\\
0132002002021020020020\\
0130020022220000022010\\
0132200222010202200200\\
0132020120202200020220\\
0110220232220200020020\\
0132201202020222020220\\
1023122000220020222220\\
0110030202200222220020
\end{pmatrix}$$

Fig. 2. (*continued*)

respectively. In order to give a generator matrix of $C'_{40,7}$ of the form (8), we only list the 7×33 matrix A in (8):

$$A = \begin{pmatrix}
100000000000001011111111111030232\\
011011011101000001011000101230302\\
011100001110011110001110100311332\\
100000111111113101101010010201033\\
010110010110101100111101000312111\\
010001111010000010000001011311013\\
111111111111111000000000000020200
\end{pmatrix}.$$

Hence, at length 40, there are at least two inequivalent extremal Type II $\mathbb{Z}_4$-codes whose residue codes have the smallest dimension among binary codes satisfying (1)–(3).

Among these 23 known codes, the 22 codes have residue codes which are doubly even self-dual codes and the residue code of the other code given in [17] has dimension 13 and the following weight enumerator:

$$1 + 156y^{12} + 1911y^{16} + 4056y^{20} + 1911y^{24} + 156y^{28} + y^{40}.$$

It turns out that the code in [17] and $C_{40,13}$ are inequivalent. Hence, none of the codes $C_{40,i}$ ($i = 7, 8, \ldots, 19$) and $C'_{40,7}$ is equivalent to any of the known codes. Thus, we have the following:

Corollary 4.3. *There are at least* 37 *inequivalent extremal Type II $\mathbb{Z}_4$-codes of length* 40.

The binary [40, 8] code $N_{40} = \langle C^{(1)}_{40,7}, w\rangle$ satisfies (1)–(3), where

$$\mathrm{supp}(w) = \{4, 8, 13, 22, 23, 34, 36, 39\}.$$

However, we verified that none of the Type II $\mathbb{Z}_4$-codes C with $C^{(1)} = N_{40}$ is extremal, using the method in Section 2.4. Therefore, there is a binary code satisfying (1)–(3) which cannot be realized as the residue code of an extremal Type II $\mathbb{Z}_4$-code of length 40. It is not known whether there is a binary [40, 7] code B satisfying (1)–(3) such that none of the Type II $\mathbb{Z}_4$-codes C with $C^{(1)} = B$ is extremal.

Acknowledgments

The author would like to thank Akihiro Munemasa for his help in the classification given in Proposition 3.7. Thanks are also due to the anonymous referee for useful comments.

References

[1] R.A.L. Betty, A. Munemasa, Mass formula for self-orthogonal codes over $\mathbf{Z}_{p^2}$, J. Combin. Inform. System Sci. 34 (2009) 51–66.
[2] A. Bonnecaze, P. Solé, C. Bachoc, B. Mourrain, Type II codes over $\mathbb{Z}_4$, IEEE Trans. Inform. Theory 43 (1997) 969–976.
[3] W. Bosma, J. Cannon, Handbook of Magma Functions, Department of Mathematics, University of Sydney. Available online at http://magma.maths.usyd.edu.au/magma/.
[4] A.E. Brouwer, Bounds on the size of linear codes, in: V.S. Pless, W.C. Huffman (Eds.), Handbook of Coding Theory, Elsevier, Amsterdam, 1998, pp. 295–461.
[5] A.R. Calderbank, N.J.A. Sloane, Double circulant codes over $\mathbb{Z}_4$ and even unimodular lattices, J. Algebraic Combin. 6 (1997) 119–131.
[6] J.H. Conway, V. Pless, N.J.A. Sloane, The binary self-dual codes of length up to 32: a revised enumeration, J. Combin. Theory Ser. A 60 (1992) 183–195.
[7] J.H. Conway, N.J.A. Sloane, Self-dual codes over the integers modulo 4, J. Combin. Theory Ser. A 62 (1993) 30–45.
[8] P. Gaborit, Mass formulas for self-dual codes over Z_4 and $F_q + uF_q$ rings, IEEE Trans. Inform. Theory 42 (1996) 1222–1228.
[9] P. Gaborit, M. Harada, Construction of extremal Type II codes over $\mathbb{Z}_4$, Des. Codes Cryptogr. 16 (1999) 257–269.
[10] M. Harada, New extremal Type II codes over $\mathbb{Z}_4$, Des. Codes Cryptogr. 13 (1998) 271–284.
[11] M. Harada, Extremal Type II $\mathbb{Z}_4$-codes of lengths 56 and 64, J. Combin. Theory Ser. A 117 (2010) 1285–1288.
[12] M. Harada, M. Kitazume, A. Munemasa, B. Venkov, On some self-dual codes and unimodular lattices in dimension 48, Eur. J. Comb. 26 (2005) 543–557.
[13] M. Harada, C.H. Lam, A. Munemasa, On the structure codes of the moonshine vertex operator algebra (submitted for publication) ArXiv:math.QA/1005.1144.
[14] M. Harada, P. Solé, P. Gaborit, Self-dual codes over $\mathbb{Z}_4$ and unimodular lattices: a survey, in: Algebras and Combinatorics (Hong Kong, 1997), Springer, Singapore, 1999, pp. 255–275.
[15] W.C. Huffman, On the classification and enumeration of self-dual codes, Finite Fields Appl. 11 (2005) 451–490.
[16] V. Pless, J. Leon, J. Fields, All $\mathbb{Z}_4$ codes of Type II and length 16 are known, J. Combin. Theory Ser. A 78 (1997) 32–50.
[17] V. Pless, P. Solé, Z. Qian, Cyclic self-dual $\mathbb{Z}_4$-codes, Finite Fields Appl. 3 (1997) 48–69.
[18] E. Rains, Optimal self-dual codes over $\mathbb{Z}_4$, Discrete Math. 203 (1999) 215–228.
[19] E. Rains, N.J.A. Sloane, Self-dual codes, in: V.S. Pless, W.C. Huffman (Eds.), Handbook of Coding Theory, Elsevier, Amsterdam, 1998, pp. 177–294.