Extremal Type II $\mathbb{Z}_4$-codes constructed from binary doubly even self-dual codes of length 40

Masaaki Harada*

June 13, 2017

Abstract

In this note, we demonstrate that every binary doubly even self-dual code of length 40 can be realized as the residue code of some extremal Type II $\mathbb{Z}_4$-code. As a consequence, it is shown that there are at least 94356 inequivalent extremal Type II $\mathbb{Z}_4$-codes of length 40.

1 Introduction

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. A code $C$ is self-dual if $C = C^\perp$, where the dual code $C^\perp$ is defined as $\{x \in \mathbb{Z}_4^n \mid x \cdot y = 0 \text{ for all } y \in C\}$ under the standard inner product $x \cdot y$. The Euclidean weight of a codeword $x = (x_1, \ldots, x_n)$ of $C$ is $n_1(x) + 4n_2(x) + n_3(x)$, where $n_\alpha(x)$ denotes the number of components $i$ with $x_i = \alpha$ ($\alpha = 1, 2, 3$). 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] and [3]. 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 $n \equiv 0 \pmod{8}$. The minimum Euclidean weight $d_E$ of $C$ is the smallest Euclidean

*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.
weight among all nonzero codewords of \( C \). The minimum Euclidean weight \( d_E \) of a Type II \( Z_4 \)-code of length \( n \) is bounded by \( d_E \leq 8\lfloor n/24 \rfloor + 8 \) \cite{2}. A Type II \( Z_4 \)-code meeting this bound with equality is called extremal.

The residue code \( C^{(1)} \) of a \( Z_4 \)-code \( C \) is the binary code \( C^{(1)} = \{ c \mod 2 \mid c \in C \} \). If \( C \) is self-dual, then \( C^{(1)} \) is a binary doubly even code \cite{5}. If \( C \) is Type II, then \( C^{(1)} \) contains the all-ones vector \( 1 \) \cite{8}. It follows that there is a Type II \( Z_4 \)-code \( C \) with \( C^{(1)} = B \) for a given binary doubly even code \( B \) containing \( 1 \) (see \cite{9}). However, it is not known in general whether there is an extremal Type II \( Z_4 \)-code \( C \) with \( C^{(1)} = B \) or not.

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 \( d \leq 4\lfloor n/24 \rfloor + 4 \). A binary doubly even self-dual code meeting this bound with equality is called extremal. Two binary codes \( B \) and \( B' \) are equivalent 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 40 (see \cite{1}). For every binary doubly even self-dual code \( B \) of length 24, there is an extremal Type II \( Z_4 \)-code \( C \) with \( C^{(1)} = B \) \cite{4}. Postscript] (see also \cite{7}). In addition, for every binary doubly even self-dual code \( B \) of length 32, there is an extremal Type II \( Z_4 \)-code \( C \) with \( C^{(1)} = B \) \cite{6}.

In this note, this work is extended to length 40. We demonstrate that there is an extremal Type II \( Z_4 \)-code \( C \) with \( C^{(1)} = B \) for every binary doubly even self-dual code \( B \) of length 40. As a consequence, it is shown that there are at least 94356 inequivalent extremal Type II \( Z_4 \)-codes of length 40. In addition, our result implies that there is an extremal Type II \( Z_4 \)-code \( C \) with \( C^{(1)} = B \) for every binary doubly even self-dual code \( B \) of length \( n \in \{8, 16, 24, 32, 40\} \). Also, there is an extremal Type II \( Z_4 \)-code \( C \) with \( C^{(1)} = B \) for every binary extremal doubly even self-dual code \( B \) of length \( n \in \{8, 16, 24, 32, 40, 48\} \).

All computer calculations in this note were done by Magma \cite{3}.

2 Extremal Type II \( Z_4 \)-codes of length 40

2.1 Construction method

We review the method for constructing Type II \( Z_4 \)-codes, which was given in \cite{9}. Let \( B \) be a binary doubly even self-dual code of length \( n \). Let \( I_n \)
denote the identity matrix of order $n$ and let

$$
\tilde{I}_n = \begin{pmatrix}
1 & \cdots & 1 \\
0 \\
\vdots & & I_{n-1} \\
0 
\end{pmatrix}.
$$

Without loss of generality, we may assume that $B$ has generator matrix of the following form:

(1) $$
G_1 = \begin{pmatrix}
A_1 & \tilde{I}_n
\end{pmatrix},
$$

where $A_1$ is an $n/2 \times n/2$ matrix which has the property that the first row is 1. Then we have a generator matrix of a Type II $\mathbb{Z}_4$-code $C$ as follows:

(2) $$
\begin{pmatrix}
A_1 & \tilde{I}_n + 2A_2
\end{pmatrix},
$$

where $A_2$ is an $n/2 \times n/2$ $(1, 0)$-matrix 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 $A_2$, and the rest is completely determined from the property that $C$ is Type II. Since any Type II $\mathbb{Z}_4$-code is equivalent to some Type II $\mathbb{Z}_4$-code containing 1 [8], without loss of generality, we may assume that the first row of $A_2$ is the zero vector. This reduces our search space for finding extremal Type II $\mathbb{Z}_4$-codes. It is the aim of this work to find a $20 \times 20$ $(1, 0)$-matrix $A_2$ such that the matrix of form (2) generates an extremal Type II $\mathbb{Z}_4$-code from a generator matrix of form (1) for a given binary doubly even self-dual code of length 40.

### 2.2 Extremal Type II $\mathbb{Z}_4$-codes of length 40

There are 94343 inequivalent binary doubly even self-dual codes of length 40 [II]. Let $B$ be one of the 94343 binary codes. Without loss of generality, we may assume that $B$ has generator matrix of form (1). In the above method, we explicitly found a $20 \times 20$ $(1, 0)$-matrix $A_2$ such that the matrix of form (2) generates an extremal Type II $\mathbb{Z}_4$-code $C$. Note that $C^{(1)} = B$. This was done for all the 94343 binary doubly even self-dual codes. Hence, we have the following:

**Proposition 1.** Let $B$ be a binary doubly even self-dual code of length 40. Then there is an extremal Type II $\mathbb{Z}_4$-code $C$ with $C^{(1)} = B$.  


Remark 2. The extremality of the code was verified as follows. Let \( C \) be a Type II \( \mathbb{Z}_4 \)-code of length 40. The following lattice

\[
A_4(C) = \frac{1}{2}\{ (x_1, \ldots, x_n) \in \mathbb{Z}^n \mid (x_1 \mod 4, \ldots, x_n \mod 4) \in C \}
\]

has minimum norm 4 if and only if \( C \) is extremal \([2]\). Instead of calculating the minimum Euclidean weight of \( C \), we calculated the minimum norm of \( A_4(C) \). This speeded up the calculations by MAGMA \([3]\) considerably. As an example, for some five extremal Type II \( \mathbb{Z}_4 \)-codes, the calculations for the minimum Euclidean weights took about 1223 minutes, but the calculations for the minimum norms took about 3 seconds only, using a single core of a PC Intel i7 4 core processor.

By the above proposition, 94343 extremal Type II \( \mathbb{Z}_4 \)-codes are constructed from the 94343 inequivalent binary doubly even self-dual codes of length 40. The 94343 extremal Type II \( \mathbb{Z}_4 \)-codes are inequivalent, since their residue codes are inequivalent. Generator matrices for the 94343 codes can be written in the form \( (I_{20} \ M) \), where \( M \) can be obtained electronically from \url{http://www.math.is.tohoku.ac.jp/~mharada/Paper/Z4-40-II.txt}.

For \( m = 7, 8, \ldots, 19 \), an extremal Type II \( \mathbb{Z}_4 \)-code \( C \) of length 40 such that the residue code \( C^{(1)} \) has dimension \( m \) is known \([6]\). Hence, we have the following:

**Corollary 3.** There are at least 94356 inequivalent extremal Type II \( \mathbb{Z}_4 \)-codes of length 40.

As described above, for every binary doubly even self-dual code \( B \) of length 24 (resp. 32), there is an extremal Type II \( \mathbb{Z}_4 \)-code \( C \) with \( C^{(1)} = B \) \([4]\).\[Postscript\] (resp. \([6]\)). Hence, we have the following:

**Corollary 4.** Suppose that \( n \in \{8, 16, 24, 32, 40\} \). Let \( B \) be a binary doubly even self-dual code of length \( n \). Then there is an extremal Type II \( \mathbb{Z}_4 \)-code \( C \) with \( C^{(1)} = B \).

It is known that the binary extended quadratic residue code \( QR_{48} \) of length 48 is the unique binary extremal doubly even self-dual code of that length. The binary code \( QR_{48} \) is the residue code of the extended lifted quadratic residue \( \mathbb{Z}_4 \)-code of length 48, which is an extremal Type II \( \mathbb{Z}_4 \)-code \([2]\). Hence, we have the following:
Corollary 5. Suppose that $n \in \{8, 16, 24, 32, 40, 48\}$. Let $B$ be a binary extremal doubly even self-dual code of length $n$. Then there is an extremal Type II $\mathbb{Z}_4$-code $C$ with $C^{(1)} = B$.

In this note, 94343 inequivalent extremal Type II $\mathbb{Z}_4$-codes $C_i$ of length 40 were constructed explicitly ($i = 1, 2, \ldots, 94343$). It is a worthwhile problem to determine whether extremal even unimodular lattices $A_4(C_i)$ ($i = 1, 2, \ldots, 94343$) are isomorphic or not.

Acknowledgment. This work was supported by JSPS KAKENHI Grant Number 15H03633.

References

[1] K. Betsumiya, M. Harada and A. Munemasa, A complete classification of doubly even self-dual codes of length 40, Electronic J. Combin. 19 (2012), #P18 (12 pp.).

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

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

[4] A.R. Calderbank and N.J.A. Sloane, Double circulant codes over $\mathbb{Z}_4$ and even unimodular lattices, J. Algebraic Combin. 6 (1997), 119–131.

[5] 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.

[6] M. Harada, On the residue codes of extremal Type II $\mathbb{Z}_4$-codes of lengths 32 and 40, Discrete Math. 311 (2011), 2148–2157.

[7] M. Harada, C.H. Lam and A. Munemasa, Residue codes of extremal Type II $\mathbb{Z}_4$-codes and the moonshine vertex operator algebra, Math. Z. 274 (2013), 685–700.

[8] M. Harada, P. Solé and P. Gaborit, Self-dual codes over $\mathbb{Z}_4$ and unimodular lattices: a survey, Algebras and combinatorics (Hong Kong, 1997), 255–275, Springer, Singapore, 1999.
[9] 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.