An Upper Bound on the Minimum Weight of Type II $\mathbb{Z}_{2k}$-Codes

Masaaki Harada* and Tsuyoshi Miezaki†

February 5, 2010

Abstract

In this paper, we give a new upper bound on the minimum Euclidean weight of Type II $\mathbb{Z}_{2k}$-codes and the concept of extremality for the Euclidean weights when $k = 3, 4, 5, 6$. Together with the known result, we demonstrate that there is an extremal Type II $\mathbb{Z}_{2k}$-code of length $8m$ ($m \le 8$) when $k = 3, 4, 5, 6$.

Key Words: Type II code, Euclidean weight, extremal code, theta series
2000 *Mathematics Subject Classification*. Primary 94B05; Secondary 11F03.

1 Introduction

Let $\mathbb{Z}_{2k}$ be the ring of integers modulo $2k$, where k is a positive integer. In this paper, we take the set $\mathbb{Z}_{2k}$ to be either $\{0, 1, \dots, 2k-1\}$ or $\{0, \pm 1, \dots, \pm(k-1), k\}$. A $\mathbb{Z}_{2k}$-code C of length n (or a code C of length n over $\mathbb{Z}_{2k}$) is a $\mathbb{Z}_{2k}$-submodule of $\mathbb{Z}_{2k}^n$. The Euclidean weight of a codeword $x = (x_1, x_2, \dots, x_n)$ is $\sum_{i=1}^n \min\{x_i^2, (2k - x_i)^2\}$. The minimum Euclidean weight $d_E(C)$ of C is the smallest Euclidean weight among all nonzero codewords of C.

A $\mathbb{Z}_{2k}$-code C is *self-dual* if $C = C^\perp$, where the dual code $C^\perp$ of C is defined as $C^\perp = \{x \in \mathbb{Z}_{2k}^n \mid x \cdot y = 0 \text{ for all } y \in C\}$ under the standard inner

*Department of Mathematical Sciences, Yamagata University, Yamagata 990–8560, Japan and PRESTO, Japan Science and Technology Agency, Kawaguchi, Saitama 332–0012, Japan. email: mharada@sci.kj.yamagata-u.ac.jp. This work was partially supported by JSPS KAKENHI (20540103).

†Research Fellow of the Japan Society for the Promotion of Science and Department of Mathematics, Hokkaido University, Hokkaido 060–0810, Japan. email: miezaki@math.sci.hokudai.ac.jp

product $x \cdot y$. As described in [14], 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 lengths and determine the largest minimum weight among self-dual codes of that length.

A binary doubly even self-dual code is often called Type II. For $\mathbb{Z}_4$-codes, Type II codes were first defined in [2] as self-dual codes containing a (± 1)-vector and with the property that all Euclidean weights are divisible by eight. Then it was shown in [11] that, more generally, the condition of containing a (± 1)-vector is redundant. For general k, Type II $\mathbb{Z}_{2k}$-codes were defined in [1] as self-dual codes with the property that all Euclidean weights are divisible by $4k$. It is known that a Type II $\mathbb{Z}_{2k}$-code of length n exists if and only if n is divisible by eight [1].

The aim of this paper is to show the following theorem.

Theorem 1. *Let C be a Type II $\mathbb{Z}_{2k}$-code of length n. If $k \leq 6$ then the minimum Euclidean weight $d_E(C)$ of C is bounded by*

$$d_E(C) \leq 4k\left\lfloor \frac{n}{24} \right\rfloor + 4k. \tag{1}$$

Remark 2. The upper bound (1) is known for the cases $k = 1$ [13] and $k = 2$ [2]. For $k \geq 3$, the bound (1) is known under the assumption that $\lfloor n/24 \rfloor \leq k - 2$ [1].

We say that a Type II $\mathbb{Z}_{2k}$-code meeting the bound (1) with equality is *extremal* for $k \leq 6$. For the following cases

$$(k, m) = (4, 7), (4, 8), (5, 6), (5, 7), (5, 8), (6, 4), (6, 5), (6, 6), (6, 7) \text{ and } (6, 8),$$

an extremal Type II $\mathbb{Z}_{2k}$-code of length $8m$ is constructed for the first time in Section 4. Together with the known results on the existences of extremal Type II codes, we have the following theorem.

Theorem 3. *If $k \leq 6$ then there is an extremal Type II $\mathbb{Z}_{2k}$-code of length $8m$ for $m \leq 8$.*

The existences of a binary extremal Type II code of length 72 and a 72-dimensional extremal even unimodular (Type II) lattice are long-standing open questions. In this paper, we propose the following question.

Question. Is there an extremal Type II $\mathbb{Z}_{2k}$-code of length 72 for $k \leq 6$?

We remark that if there is an Type II $\mathbb{Z}_{2k}$-code of length 72 ($k = 4, 5, 6$) then a 72-dimensional extremal even unimodular lattice can be obtained by Construction A.

All computer calculations in this paper were done by Magma [3].

2 Preliminaries

An n-dimensional (Euclidean) lattice Λ is a subset of $\mathbb{R}^n$ with the property that there exists a basis $\{e_1, e_2, \dots, e_n\}$ of $\mathbb{R}^n$ such that $\Lambda = \mathbb{Z}e_1 \oplus \mathbb{Z}e_2 \oplus \cdots \oplus \mathbb{Z}e_n$, i.e., Λ consists of all integral linear combinations of the vectors $e_1, e_2, \dots, e_n$. The dual lattice Λ^* of Λ is the lattice $\{x \in \mathbb{R}^n \mid \langle x, y\rangle \in \mathbb{Z} \text{ for all } y \in \Lambda\}$, where $\langle x, y\rangle$ is the standard inner product. A lattice with $\Lambda = \Lambda^*$ is called *unimodular*. The norm of a vector x is $\langle x, x\rangle$. A unimodular lattice with even norms is said to be *even*. A unimodular lattice containing a vector of odd norm is said to be *odd*. An n-dimensional even unimodular lattice exists if and only if $n \equiv 0 \pmod 8$ while an odd unimodular lattice exists for every dimension. The minimum norm $\min(\Lambda)$ of Λ is the smallest norm among all nonzero vectors of Λ. For Λ and a positive integer m, the shell Λ_m of norm m is defined as $\{x \in \Lambda \mid \langle x, x\rangle = m\}$. Two lattices L and L' are *isomorphic*, denoted $L \simeq L'$, if there exists an orthogonal matrix A with $L' = L \cdot A = \{xA \mid x \in L\}$. Two lattices L and L' are *neighbors* if both lattices contain a sublattice of index 2 in common.

The theta series $\Theta_\Lambda(q)$ of Λ is the following formal power series

$$\Theta_\Lambda(q) = \sum_{x\in\Lambda} q^{\langle x,x\rangle} = \sum_{m=0}^{\infty} |\Lambda_m| q^m.$$

For example, when Λ is the E_8-lattice

$$\begin{aligned}\Theta_\Lambda(q) = E_4(q) &= 1 + 240 \sum_{m=1}^{\infty} \sigma_3(m) q^{2m} \\ &= 1 + 240q^2 + 2160q^4 + 6720q^6 + \cdots,\end{aligned}$$

where $\sigma_3(m)$ is a divisor function $\sigma_3(m) = \sum_{0<d|m} d^3$. Moreover, the following theorem is known (see [6, Chap. 7]).

Theorem 4. *If Λ is an even unimodular lattice then*

$$\Theta_\Lambda(q) \in \mathbb{C}[E_4(q), \Delta_{24}(q)],$$

where $\Delta_{24}(q) = q^2 \prod_{m=1}^{\infty}(1 - q^{2m})^{24}$.

We now give a method to construct even unimodular lattices from Type II codes, which is called Construction A [1]. Let ρ be a map from $\mathbb{Z}_{2k}$ to $\mathbb{Z}$ sending $0, 1, \dots, k$ to $0, 1, \dots, k$ and $k+1, \dots, 2k-1$ to $1-k, \dots, -1$, respectively. If C is a self-dual $\mathbb{Z}_{2k}$-code of length n, then the lattice

$$A_{2k}(C) = \frac{1}{\sqrt{2k}}\{\rho(C) + 2k\mathbb{Z}^n\}$$

is an n-dimensional unimodular lattice, where

$$\rho(C) = \{(\rho(c_1), \ldots, \rho(c_n)) \mid (c_1, \ldots, c_n) \in C\}.$$

The minimum norm of $A_{2k}(C)$ is $\min\{2k, d_E(C)/2k\}$. Moreover, if C is Type II then the lattice $A_{2k}(C)$ is an even unimodular lattice [1].

The symmetrized weight enumerator of a $\mathbb{Z}_{2k}$-code C is

$$\mathrm{swe}_C(x_0, x_1, \ldots, x_k) = \sum_{c \in C} x_0^{n_0(c)} x_1^{n_1(c)} \cdots x_{k-1}^{n_{k-1}(c)} x_k^{n_k(c)},$$

where $n_0(c)$, $n_1(c)$, $\ldots$, $n_{k-1}(c)$, $n_k(c)$ are the numbers of $0, \pm 1, \ldots, \pm(k-1), k$ components of c, respectively [1]. Then the theta series of $A_{2k}(C)$ can be found by replacing x_i by

$$f_i = \sum_{x \in 2k\mathbb{Z}+i} q^{x^2/2k},$$

for all $0 \le i \le k$.

3 Proof of Theorem 1

In this section, we give a proof of Theorem 1. Our proof is an analogue of that of [2, Corollary 13] (see also [12]). We remark that in the proof of [2, Corollary 13] $(\Delta/E_8^3 4)$ (p. 973, right, l. -7) should be (tE_4^3/Δ) and $(4\mathbb{Z})^8/2$ (p. 973, right, l. -5) should be $2\mathbb{Z}^8$.

Proof. Let C be a Type II $\mathbb{Z}_{2k}$-code of length n. Then the even unimodular lattice $A_{2k}(C)$ contains a sublattice $\Lambda_0 = \sqrt{2k}\mathbb{Z}^n$ which has minimum norm $2k$. We set $\Theta_{\Lambda_0}(q) = \theta_0$, $n = 8j$ and $j = 3\mu + \nu$ ($\nu = 0, 1, 2$), that is, $\mu = \lfloor n/24 \rfloor$. In this proof, we denote $E_4(q)$ and $\Delta_{24}(q)$ by E_4 and Δ, respectively. By Theorem 4, the theta series of $A_{2k}(C)$ can be written as

$$\Theta_{A_{2k}(C)}(q) = \sum_{s=0}^{\mu} a_s E_4^{j-3s} \Delta^s = \sum_{r \ge 0} |A_{2k}(C)_r| q^r = \theta_0 + \sum_{r \ge 1} \beta_r q^r.$$

Suppose that $d_E(C) \ge 4k(\mu+1)$. We remark that a codeword of Euclidean weight $4km$ gives a vector of norm $2m$ in $A_{2k}(C)$. Then we choose the $a_0, a_1, \ldots, a_\mu$ so that

$$\Theta_{A_{2k}(C)}(q) = \theta_0 + \sum_{r \ge 2(\mu+1)} \beta_r^* q^r.$$

Here, we set b_{2s} as $E_4^{-j}\theta_0 = \sum_{s=0}^{\infty} b_{2s}(\Delta/E_4^3)^s$. That is, $\theta_0 = \sum_{s=0}^{\infty} b_{2s}E_4^{j-3s}\Delta^s$. Then

$$\sum_{s=0}^{\mu} a_s E_4^{j-3s}\Delta^s = \Theta_{A_{2k}(C)}(q) = \sum_{s=0}^{\infty} b_{2s}E_4^{j-3s}\Delta^s + \sum_{r\geq 2(\mu+1)} \beta_r^* q^r.$$

Comparing the coefficients of q^i $(0 \leq i \leq 2\mu)$, we get $a_s = b_{2s}$ $(0 \leq s \leq \mu)$. Hence we have

$$-\sum_{r\geq(\mu+1)} b_{2r}E_4^{j-3r}\Delta^r = \sum_{r\geq 2(\mu+1)} \beta_r^* q^r. \tag{2}$$

In (2), comparing the coefficient of $q^{2(\mu+1)}$, we have

$$\beta^*_{2(\mu+1)} = -b_{2(\mu+1)}.$$

All the series are in $q^2 = t$, and Bürman's formula shows that

$$b_{2s} = \frac{1}{s!}\frac{d^{s-1}}{dt^{s-1}}\left(\left(\frac{d}{dt}(E_4^{-j}\theta_0)\right)(tE_4^3/\Delta)^s\right)_{\{t=0\}}.$$

Using the fact that $\theta_0 = \theta_1^j$, where θ_1 is the theta series of the lattice $\sqrt{2k}\mathbb{Z}^8$,

$$b_{2s} = \frac{-j}{s!}\frac{d^{s-1}}{dt^{s-1}}\left(E_4^{3s-j-1}\theta_1^{j-1}(\theta_1E_4' - \theta_1'E_4)(t/\Delta)^s\right)_{\{t=0\}},$$

where f' is the derivation of f with respect to $t = q^2$.

The condition that there is a codeword of Euclidean weight $4k(\mu+1)$ is equivalent to the condition $\beta^*_{2(\mu+1)} > 0$. It is sufficient to show that the coefficients of $\theta_1^{j-1}(\theta_1E_4' - \theta_1'E_4)$ are positive up to the exponent μ since E_4 and $1/\Delta$ have positive coefficients.

By Proposition 3.4 in [1], there exists a Type II $\mathbb{Z}_{2k}$-code of length 8 for every k. Hence let C_8 be a Type II $\mathbb{Z}_{2k}$-code of length 8. Then $A_{2k}(C_8)$ is the E_8-lattice. In addition, we can write

$$E_4 = \mathrm{swe}_{C_8}(f_0, f_1, \ldots, f_k) \text{ and } \theta_1 = f_0^8.$$

Deriving

$$E_4/\theta_1 = \mathrm{swe}_{C_8}(1, f_1/f_0, \ldots, f_k/f_0),$$

we find

$$\theta_1^{j-1}(\theta_1E_4' - \theta_1'E_4) = \sum_{i=1}^{k} \frac{\partial\,\mathrm{swe}_{C_8}(f_0, f_1, \ldots, f_k)}{\partial x_i} f_0^{8j-1}(f_0f_i' - f_0'f_i)$$

Hence it is sufficient to show that $f_0^{8j-1}(f_0 f_i' - f_0' f_i)$ has positive coefficients up to μ for all $1 \le i \le k$. We only consider the case $f_0^{8j-1}(f_0 f_1' - f_0' f_1)$ and the other cases are similar. We have that

$$t(f_0 f_1' - f_0' f_1) = \sum_{x,y \in \mathbb{Z}} \frac{(1+2ky)^2 - (2kx)^2}{4k} t^{((1+2ky)^2 + (2kx)^2)/4k},$$

then

$$\begin{aligned} & t f_0^s (f_0 f_1' - f_0' f_1) \\ &= \sum_{x,y,x_1,\dots,x_s \in \mathbb{Z}} \frac{(1+2ky)^2 - (2kx)^2}{4k} \cdot t^{((1+2ky)^2 + (2kx)^2 + (2kx_1)^2 + \cdots + (2kx_s)^2)/4k}. \end{aligned} \tag{3}$$

Fix one of the choices y, x, $x_1, \dots x_s \in \mathbb{Z}$ and define ℓ as follows:

$$\ell = (1+2ky)^2 + (2kx)^2 + (2kx_1)^2 + \cdots + (2kx_s)^2. \tag{4}$$

Consider all permutations on the set $\{x,\ x_1, \dots,\ x_s\}$. As the sum of coefficients of $t^{\ell/4k}$ in the right hand side of (3) under these cases, we have that some positive constant multiple by

$$\begin{aligned} & \frac{(s+1)(1+2ky)^2 - (2kx)^2 - (2kx_1)^2 - \cdots - (2kx_s)^2}{4k} \\ & \qquad = \frac{(s+2)(1+2ky)^2 - \ell}{4k}. \end{aligned} \tag{5}$$

If $\ell < s+2$ then (5) is positive. Since we consider the case $s = 8j-1$, $\ell < n+1$. Hence if the exponent $\ell/4k$ of t is less than $(n+1)/4k$ then (5) is positive. This means that if $\mu < (n+1)/4k$ then (5) is positive. This condition $\mu < (n+1)/4k$ is satisfied since $k \le 6$. Thus for any choice y, x, $x_1, \dots x_s$, (5) is positive. The coefficient of $t^{\ell/4k}$ in the right hand side of (3) is the sum of those coefficients (5), that is, positive. This completes the proof of Theorem 1. □

4 Extremal Type II $\mathbb{Z}_{2k}$-codes

An extremal Type II $\mathbb{Z}_{2k}$-code of length $8m$ is currently known for the cases (k, m) listed in the second column of Table 1. In this section, an extremal Type II $\mathbb{Z}_{2k}$-code of length $8m$ is constructed for the first time for the cases (k, m) listed in the last column of Table 1.

Table 1: Existence of extremal Type II $\mathbb{Z}_{2k}$-codes of length $8m$

k	m (known cases)		m (new cases)	
1	$1, 2, \dots, 8, 10, 11, 13, 14, 17$	[6, p. 194], [8]		
2	$1, 2, \dots, 8$	[2], [4], [9]		
3	$1, 2, \dots, 8$	[5], [10]		
4	$1, 2, \dots, 6$	[5], [7]	7, 8	($C_{8,56}$, $C_{8,64}$)
5	$1, 2, \dots, 5$	[5], [7]	6, 7, 8	(Proposition 6, $C_{10,56}$, $C_{10,64}$)
6	$1, 2, 3$	[5]	4, 5, 6, 7, 8	(Proposition 7)

Let A and B be $n \times n$ negacirculant matrices, that is, A and B have the following form

$$\begin{pmatrix} r_0 & r_1 & r_2 & \cdots & r_{n-1} \\ -r_{n-1} & r_0 & r_1 & \cdots & r_{n-2} \\ -r_{n-2} & -r_{n-1} & r_0 & \cdots & r_{n-3} \\ \vdots & \vdots & \vdots & & \vdots \\ -r_1 & -r_2 & -r_3 & \cdots & r_0 \end{pmatrix}.$$

If $AA^T + BB^T = -I_n$, then it is trivial that

$$\left(\begin{array}{ccc} I_{2n} & \begin{array}{cc} A & B \\ -B^T & A^T \end{array} \end{array} \right) \tag{6}$$

generates a self-dual code, where I_n denotes the identity matrix of order n and A^T is the transpose of A.

Table 2: New extremal Type II $\mathbb{Z}_{2k}$-codes

Codes	r_A	r_B
$C_{8,56}$	$(0,0,4,3,4,1,6,3,1,1,1,1,1,2)$	$(1,1,0,0,0,0,0,3,2,0,0,0,0,4)$
$C_{8,64}$	$(0,0,0,2,0,7,3,2,0,0,5,3,1,4,0,2)$	$(0,0,1,0,0,0,0,1,7,1,3,0,1,2,2,0)$
$C_{10,56}$	$(0,0,0,2,5,1,4,1,2,0,5,0,4,1)$	$(0,0,0,0,0,1,0,5,7,0,3,9,1,0)$
$C_{10,64}$	$(0,0,4,3,2,0,0,1,9,0,0,0,9,1,2,0)$	$(1,3,0,1,0,6,9,4,6,2,0,5,0,0,2,3)$
$C_{12,32}$	$(0,0,7,6,0,1,7,10)$	$(0,1,0,4,1,0,3,11)$
$C_{12,40}$	$(0,0,0,2,1,10,5,9,2,10)$	$(0,1,0,1,0,0,11,1,0,4)$
$C_{12,56}$	$(2,11,2,2,4,11,0,5,0,0,6,1,5,7)$	$(1,0,5,3,0,8,0,2,0,7,7,0,0,4)$

Using the above construction method, we have found extremal Type II $\mathbb{Z}_8$-codes $C_{8,56}$ and $C_{8,64}$ of lengths 56 and 64, respectively, and extremal Type II $\mathbb{Z}_{10}$-codes $C_{10,56}$ and $C_{10,64}$ of lengths 56 and 64, respectively. The first rows r_A and r_B of the matrices A and B in their generator matrices (6) are listed in Table 2. Hence we have the following:

Proposition 5. *For lengths* 56 *and* 64*, there is an extremal Type II* $\mathbb{Z}_{2k}$*-code when* $k = 4$ *and* 5.

An n-dimensional even unimodular lattice is called *extremal* if it has minimum norm $2\lfloor n/24 \rfloor + 2$. The existence of an extremal Type II $\mathbb{Z}_{10}$-code of length 48 is established by considering the existence of a 10-frame in some extremal even unimodular lattice. Recall that a set $\{f_1, \dots, f_n\}$ of n vectors $f_1, \dots, f_n$ in an n-dimensional unimodular lattice L with $\langle f_i, f_j \rangle = \ell \delta_{i,j}$ is called an *ℓ-frame* of L, where $\delta_{i,j}$ is the Kronecker delta. It is known that an even unimodular lattice L contains a $2k$-frame if and only if there is a Type II $\mathbb{Z}_{2k}$-code C such that $A_{2k}(C) \simeq L$.

Proposition 6. *There is an extremal Type II* $\mathbb{Z}_{10}$*-code of length* 48.

Proof. Let $C_{5,48}$ be the $\mathbb{F}_5$-code with generator matrix (6), where the first rows r_A and r_B of the matrices A and B are

$$r_A = (2,3,0,2,2,3,2,2,3,2,2,0) \text{ and } r_B = (3,0,4,4,0,1,0,0,4,0,0,1),$$

respectively. Then this code $C_{5,48}$ is a self-dual code and the lattice $A_5(C_{5,48}) = \frac{1}{\sqrt{5}}\{x \in \mathbb{Z}^{48} \mid x \pmod 5 \in C_{5,48}\}$ is an odd unimodular lattice. The lattice has theta series $1 + 393216q^5 + 26201600q^6 + \cdots$. We have verified that $A_5(C_{5,48})$ has an even unimodular neighbor L_{48} which is extremal. Clearly, the lattice $A_5(C_{5,48})$ contains the 5-frame $\{\sqrt{5}e_1, \sqrt{5}e_2, \dots, \sqrt{5}e_{48}\}$, where e_i ($i = 1, 2, \dots, 48$) denotes the i-th unit vector $(\delta_{i,1}, \delta_{i,2}, \dots, \delta_{i,48})$ of length 48. Then the set $F = \{\sqrt{5}(e_{2i-1} \pm e_{2i}) \mid i = 1, 2, \dots, 24\}$ is a 10-frame of the even sublattice of $A_5(C_{5,48})$. Hence F is also a 10-frame of the extremal even unimodular neighbor L_{48}. Therefore there is a Type II $\mathbb{Z}_{10}$-code $C_{10,48}$ of length 48 such that $A_{10}(C_{10,48}) \simeq L_{48}$. Moreover, the code $C_{10,48}$ must be extremal since the lattice L_{48} is extremal. $\square$

Similar to the above proposition, the existence of 12-frames in extremal even unimodular lattices yields that of some extremal Type II $\mathbb{Z}_{12}$-codes.

Proposition 7. *There is an extremal Type II* $\mathbb{Z}_{12}$*-code of length* $8m$ *for* $m = 4, 5, 6, 7$ *and* 8.

Proof. It is known that there is an extremal Type II $\mathbb{Z}_6$-code of length $8m$ for $m = 4, 5, 6, 7$ and 8 (see Table 1). We denote these codes by $C_{6,8m}$ ($m = 4, 5, 6, 7$ and 8), respectively. Since $C_{6,8m}$ is an extremal Type II code, the lattice $A_6(C_{6,8m})$ is an extremal even unimodular lattice for

$m = 4, 5, 6, 7$ and 8. Moreover, clearly the lattice $A_6(C_{6,8m})$ contains the 6-frame $\{\sqrt{6}e_1, \sqrt{6}e_2, \ldots, \sqrt{6}e_{8m}\}$, where e_i denotes the i-th unit vector of length $8m$. Then the set $\{\sqrt{6}(e_{2i-1} \pm e_{2i}) \mid i = 1, 2, \ldots, 4m\}$ is a 12-frame of $A_6(C_{6,8m})$. Hence there is a Type II $\mathbb{Z}_{12}$-code N_{8m} of length $8m$ such that $A_{12}(N_{8m}) \simeq A_6(C_{6,8m})$. Moreover, the code N_{8m} must be extremal since the lattice $A_6(C_{6,8m})$ is extremal. $\square$

Remark 8. Similar to Proposition 5, by considering generator matrices (6), we have found extremal Type II $\mathbb{Z}_{12}$-codes $C_{12,32}$, $C_{12,40}$ and $C_{12,56}$ of lengths $32, 40$ and 56, respectively, where the first rows r_A and r_B of the matrices A and B in (6) are listed in Table 2.

Together with the known results on the existences of extremal Type II codes (see Table 1), Propositions 5, 6 and 7 give Theorem 3.

Acknowledgment. The authors would like to thank Kenichiro Tanabe for useful discussions, and Koichi Betsumiya for helpful conversations on the construction of extremal Type II codes.

References

[1] E. Bannai, S.T. Dougherty, M. Harada and M. Oura, Type II codes, even unimodular lattices, and invariant rings, *IEEE Trans. Inform. Theory* **45** (1999), 1194–1205.

[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 and J. Cannon, Handbook of Magma Functions, Department of Mathematics, University of Sydney, Available online at http://magma.maths.usyd.edu.au/magma/.

[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] R. Chapman, Double circulant constructions of the Leech lattice, *J. Aust. Math. Soc. Ser. A* **69** (2000), 287–297.

[6] J.H. Conway and N.J.A. Sloane, *Sphere Packing, Lattices and Groups (3rd ed.)*, Springer-Verlag, New York, 1999.

[7] T.A. Gulliver and M. Harada, Extremal self-dual codes over $\mathbb{Z}_6, \mathbb{Z}_8$ and $\mathbb{Z}_{10}$, *AKCE Int. J. Graphs Comb.* **2** (2005), 11–24.

[8] M. Harada, An extremal doubly even self-dual code of length 112, *Electron. J. Combin.* **15** (2008), Note 33, 5 pp.

[9] M. Harada, Extremal Type II $\mathbb{Z}_4$-codes of lengths 56 and 64, *J. Combin. Theory Ser. A*, (to appear).

[10] M. Harada, M. Kitazume and M. Ozeki, Ternary code construction of unimodular lattices and self-dual codes over $\mathbb{Z}_6$, *J. Algebraic Combin.* **16** (2002), 209–223.

[11] 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.

[12] C.L. Mallows, A.M. Odlyzko and N.J.A. Sloane, Upper bounds for modular forms, lattices, and codes, *J. Algebra* **36** (1975), 68–76.

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

[14] 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.