Nonexistence for extremal Type II $\mathbb{Z}_{2k}$-Codes

Tsuyoshi Miezaki*

August 23, 2009

Abstract

In this paper, we show that an extremal Type II $\mathbb{Z}_{2k}$-code of length $n$ does not exist for all sufficiently large $n$ when $k = 2, 3, 4, 5, 6$.

Key Words: Type II code, Euclidean weight, extremal code, theta series

2000 Mathematics Subject Classification. Primary 94B05; Secondary 11F03.

1 Introduction

Let $\mathbb{Z}_{2k} (= \{0, 1, 2, \ldots, 2k - 1\})$ be the ring of integers modulo $2k$, where $k$ is a positive integer. 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 $\mathbb{Z}_{2k}^n$. A 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 product $x \cdot y$. The Euclidean weight of a codeword $x = (x_1, x_2, \ldots, x_n)$ 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 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 $(\pm 1)$-vector and with the property that all Euclidean weights are divisible by eight. Then it was shown in [5] that, more generally, the condition of containing a

*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
(±1)-vector is redundant. Type II $\mathbb{Z}_{2k}$-codes was defined in [1] as a self-dual code 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.

In [4], we show the following theorem:

**Theorem 1.1** (cf. [4]). 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

\[ d_E(C) \leq 4k \left\lfloor \frac{n}{24} \right\rfloor + 4k. \]

**Remark 1.1.** The upper bound (1) is known for the cases $k = 1$ [7] and $k = 2$ [2]. For $k \geq 3$, the bound (1) is known under the assumption that $|n/24| \leq k - 2$ [1].

In [4], we define that a Type II $\mathbb{Z}_{2k}$-code meeting the bound (1) with equality is *extremal* for $k \leq 6$.

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

**Theorem 1.2.** For $k \leq 6$, an extremal Type II $\mathbb{Z}_{2k}$-code of length $n$ does not exist for all sufficiently large $n$.

**Remark 1.2.** For the case $k = 1$, the above result in Theorem 1.2 was shown in [7].

## 2 Preliminaries

An $n$-dimensional (Euclidean) lattice $\Lambda$ is a subset of $\mathbb{R}^n$ with the property that there exists a basis \{${e_1, e_2, \ldots, e_n}$\} 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., $\Lambda$ consists of all integral linear combinations of the vectors $e_1, e_2, \ldots, e_n$. The dual lattice $\Lambda^*$ of $\Lambda$ is the lattice \{${x \in \mathbb{R}^n \mid \langle x, y \rangle \in \mathbb{Z}}$ 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 $x$ 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 $\Lambda$ is the smallest norm among all nonzero vectors of $\Lambda$. For $\Lambda$ and a positive integer $m$, the shell $\Lambda_m$ of norm $m$ is defined as \{${x \in \Lambda \mid \langle x, x \rangle = m}$\}. 

2
The theta series of $\Lambda$ is
\[
\Theta_{\Lambda}(z) = \Theta_{\Lambda}(q) = \sum_{x \in \Lambda} q^{(x,x)} = \sum_{m=0}^{\infty} |\Lambda_m| q^m, \quad q = e^{\pi i z}, \quad \text{Im}(z) > 0.
\]

For example, let $\Lambda$ be the $E_8$-lattice. Then,
\[
\Theta_{\Lambda}(q) = E_4(q) = 1 + 240 \sum_{m=1}^{\infty} \sigma_3(m) q^{2m} = 1 + 240q^2 + 2160q^4 + 6720q^6 + 17520q^8 + \cdots,
\]
where $\sigma_3(m)$ is a divisor function $\sigma_3(m) = \sum_{d | m} d^3$.

It is well-known that if $\Lambda$ is an $n$-dimensional even unimodular lattice then $\Theta_{\Lambda}$ is a modular form of weight $n/2$ for the full modular group $SL_2(\mathbb{Z})$ (see [3]). For example, $E_4(q)$ is a modular form of weight 4 for $SL_2(\mathbb{Z})$. Moreover the following theorem is known (see [3, Chap. 7]).

**Theorem 2.1.** If $\Lambda$ is an even unimodular lattice then
\[
\Theta_{\Lambda}(q) \in \mathbb{C}[E_4(q), \Delta_{24}(q)],
\]
where $\Delta_{24}(q) = q^2 \prod_{m=1}^{\infty} (1 - q^{2m})^{24}$ which is a modular form of weight 12 for $SL_2(\mathbb{Z})$.

We now give a method to construct even unimodular lattices from Type II codes, which is called Construction A [1]. Let $\rho$ be a map from $\mathbb{Z}_{2k}$ to $\mathbb{Z}$ sending $0, 1, \ldots, k$ to $0, 1, \ldots, k$ and $k+1, \ldots, 2k-1$ to $1-k, \ldots, -1$, 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.

The symmetrized weight enumerator of a $\mathbb{Z}_{2k}$-code $C$ is
\[
\text{swe}_C(x_0, x_1, \ldots, x_k) = \sum_{c \in C} x_0^{n_0(c)} x_1^{n_1(c)} \cdots x_{k-1}^{n_{k-1}(c)} x_k^{n_k(c)},
\]
where \( n_0(c), n_1(c), \ldots, n_{k-1}(c), n_k(c) \) are the number of 0, ±1, ..., ±(k − 1), k components of \( c \), respectively. Then the theta series of \( A_{2k}(C) \) can be found by replacing \( x_1, x_2, \ldots, x_k \) by

\[
\begin{align*}
\Theta_{A_{2k}(C)}(q) &= \sum_{x \in \mathbb{Z}/2^k} \frac{q^{x^2/2k}}{2^{k}}, \quad \Theta_{A_{2k}(C)}(q) = \sum_{x \in \mathbb{Z}/2^k} \frac{q^{x^2/2k}}{2^k}.
\end{align*}
\]

respectively.

### 3 Review of Theorem 1.1

In this section, we review a proof of Theorem 1.1. For the details, see [4].

**Proof of Theorem 1.1.** Let \( C \) be a Type II \( \mathbb{Z}_{2^k} \)-code of length \( n \). Then the even unimodular lattice \( A_{2k}(C) \) contains the 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 \( \Delta \), respectively.

By Theorem 2.1, the theta series of \( A_{2k}(C) \) can be written as

\[
\Theta_{A_{2k}(C)}(q) = \sum_{s=0}^{\mu} a_s E_4^{j-3s} \Delta^s + \sum_{r \geq 2(\mu+1)} |A_{2k}(C)|_{r} q^{r}.
\]

Suppose that \( d_0(C) \geq 4k(\mu+1) \). 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

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

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

Then

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

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

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

(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

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

Using the fact that $\theta_0 = \theta_1^j$ where $\theta_1$ is the theta series of the lattice $\sqrt{2kZ}_8$, we have

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

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 $\theta_1^{j-1} (\theta_1 E_4' - \theta_1' E_4)$ are positive up to the exponent $\mu$ since $E_4$ and $1/\Delta$ have positive coefficients.

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

$$E_4 = \text{swe}_{C_8}(f_0, f_1, \ldots, f_k)$$

and $\theta_1 = f_0^8$.

Deriving

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

we find

$$\theta_1^{j-1} (\theta_1 E_4' - \theta_1' E_4) = \frac{\partial \text{swe}_{C_8}(f_0, f_1, \ldots, f_k)}{\partial x_1} f_0^{s_j-1}(f_0 f_1' - f_0' f_1) + \cdots + \frac{\partial \text{swe}_{C_8}(f_0, f_1, \ldots, f_k)}{\partial x_k} f_0^{s_j-1}(f_0 f_k' - f_0' f_k).$$

Hence it is sufficient to show that $f_0^{s_j-1}(f_0 f_1' - f_0' f_1), \ldots, f_0^{s_j-1}(f_0 f_k' - f_0' f_k)$ have positive coefficients up to $\mu$. We only consider the case $f_0^{s_j-1}(f_0 f_1' - f_0' f_1)$ 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{equation}
(3) \quad tf_0^s(f_0f_1' - f_0'f_1) = \sum_{x, y, x_1, \ldots, x_s \in \mathbb{Z}} \frac{(1 + 2k)^2 - (2kx)^2}{4k}. \quad t^{(1 + 2k)^2 + (2kx)^2 + (2kx_1)^2 + \cdots + (2kx_s)^2}/4k.
\end{equation}

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

\begin{equation}
(4) \quad l = (1 + 2k)^2 + (2kx)^2 + (2kx_1)^2 + \cdots + (2kx_s)^2.
\end{equation}

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

\begin{equation}
(5) \quad \frac{(s + 1)(1 + 2k)^2 - (2k)^2 - (2kx)^2 - (2kx_1)^2 - \cdots - (2kx_s)^2}{4k} = \frac{(s + 2)(1 + 2k)^2 - l}{4k}.
\end{equation}

If \( l < s + 2 \) then (5) is positive. Since we consider the case \( s = 8j - 1, l < n + 1 \). Hence if the exponent \( l/4k \) 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 \( k \leq 6 \). Thus for any choice \( y, x, x_1, \ldots, x_s, (5) \) is positive. The coefficient of \( t^{l/4k} \) in the right hand side of (3) is the sum of those coefficients (5), that is, positive. This completes the proof of Theorem 1.1. \( \square \)

### 4 Proof of Theorem 1.2

In this section, we give a proof of Theorem 1.1. Our proof is an analogue of that of [6]. Before we give the proof of Theorem 1.2 we quote the following lemma from [6].

**Lemma 4.1** ([6, Lemma 1]). Suppose that \( G(q), H(q) \) are analytic inside the circle \( |q| = 1 \) and satisfy:

(i) \( H(q) = \sum_{s=0}^{\infty} H_s q^s \) with \( H_0 > 0, H_1 > 0 \), and \( H_s \geq 0 \) for \( s \geq 2 \),

(ii) if \( F(y) = e^{2\pi y} H(e^{-2\pi y}) \), then \( F'(y) = 0 \) has a solution \( y = y_0 \) in the range \( y > 0 \), with \( F(y_0) = c_1 > 0, F''(y_0)/F(y_0) = c_2 > 0, G(e^{-2\pi y_0}) \neq 0. \)
Then $\beta_r$, the coefficient of $q^r$ in $G(q)H(q)^r$, satisfies

$$\beta_r \sim \frac{2\pi}{(rc_2)^{1/2}} G(e^{-2\pi y_0})c_1^r, \text{ as } r \to \infty.$$  

Proof of Theorem 1.2. In (2), comparing the coefficient of $q^{2(\mu+1)}$ and $q^{2(\mu+2)}$, we have

$$
\begin{align*}
\left\{ &\begin{array}{ll}
\beta_{2(\mu+1)}^r = -b_{2(\mu+1)}, \\
\beta_{2(\mu+2)}^r = -b_{2(\mu+2)} + b_{2(\mu+1)}(24\mu - 240\nu + 744),
\end{array} \right.
\end{align*}
$$

where

$$b_{2s} = \frac{1}{s!} \frac{d^{s-1}}{dt^{s-1}} \left( \frac{d}{dt}(E_{4}^{-j}(t)(tE_{4}/\Delta)^s) \right)_{t=0},$$

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

$$b_{2s} = -\frac{j}{s!} \frac{d^{s-1}}{dt^{s-1}} (E_{4}^{3s-j-1}\theta_1^{-1}(\theta_1E_4 - \theta_1'E_4)(t/\Delta)^s)_{t=0},$$

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

We show that $\beta_{2(\mu+2)}^r < 0$ for sufficiently large $n$. When we set $h(t) = \Pi_{r=1}^{\infty}(1 - r^2)^{-24}$,

$$b_{2(\mu+1)} = -\frac{j}{(\mu+1)!} \frac{d^{\mu}}{dt^{\mu}} (E_{4}^{2-\nu}\theta_1^{-1}(\theta_1E_4 - \theta_1'E_4)(h(q))^{\mu+1})_{t=0},$$

$$b_{2(\mu+2)} = -\frac{j}{(\mu+2)!} \frac{d^{\mu+1}}{dt^{\mu+1}} (E_{4}^{5-\nu}\theta_1^{-1}(\theta_1E_4 - \theta_1'E_4)(h(q))^{\mu+2})_{t=0}.$$

It was shown in Theorem 1.1 that $\beta_{2(\mu+1)}^r > 0$. We show that $|b_{2(\mu+2)}^r/b_{2(\mu+1)}^r|$ is bounded, which implies that $\beta_{2(\mu+2)}^r < 0$ as $n \to \infty$.

Here, we now apply Lemma 4.4 with $G(t) = G_1(t) = E_{4}^{2-\nu}\theta_1^{-1}(\theta_1E_4 - \theta_1'E_4)h(t)$ and $H(t) = h(t)$. Then, as is shown in [6], hypothesis (i) and (ii) in Lemma 4.4 are satisfied. So,

$$b_{2(\mu+1)} \sim -2\pi j c_2^{-1/2} \mu^{-3/2} G_1(e^{-2\pi y_0})c_1^\mu, \text{ as } r \to \infty,$$

where $c_1$ and $c_2$ are constants. Similarly with $G(q) = G_2(q) = E_{4}^{5-\nu}\theta_1^{-1}(\theta_1E_4 - \theta_1'E_4)h(q)$ and $H(q) = h(q)$.

$$b_{2(\mu+2)} \sim -2\pi j c_2^{-1/2} \mu^{-3/2} G_2(e^{-2\pi y_0})c_1^{\mu+1}, \text{ as } r \to \infty.$$
Hence $|b_{2(\mu+1)}/b_{2(\mu+1)}|$ is bounded (In fact, it approaches a limit of about \(1.64 \times 10^6\) as \(\mu \to \infty\)).

**Remark 4.1.** Using the equations (3), the coefficient $\beta_{2(\mu+2)}^*$ first goes negative when $n$ is about 5200. Namely, for $k \leq 6$, an extremal Type II $\mathbb{Z}_{2k}$-code of length $n$ does not exist for $n \geq 5200$. Hence there are finitely many extremal Type II $\mathbb{Z}_{2k}$-codes for $k \leq 6$.

**Acknowledgment.** The author would like to thank Masaaki Harada and Kenichiro Tanabe for useful discussions.

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

[4] M. Harada and T. Miezaki, An Upper Bound on the Minimum Weight of Type II $\mathbb{Z}_{2k}$-Codes, (submitted).

[5] 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.

[6] 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.

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