AKCE J. Graphs. Combin., 2, No. 1 (2005), pp. 11-24

Extremal Self-Dual Codes over $\mathbb{Z}_6$, $\mathbb{Z}_8$ and $\mathbb{Z}_{10}$

T. Aaron Gulliver
Department of Electrical and Computer Engineering
University of Victoria
P.O. Box 3055, STN CSC, Victoria, B.C.
Canada V8W 3P6.
and
Masaaki Harada
Department of Mathematical Sciences
Yamagata University
Yamagata 990–8560, Japan
E-mail: harada@kdeve.kj.yamagata-u.ac.jp

Communicated by: Mariko Hagita
Received 18 January 2005; revised 13 April 2005; accepted 25 April 2005

Abstract

In this paper, upper bounds on the minimum Euclidean weights of Type I codes over $\mathbb{Z}_6$, and self-dual codes over $\mathbb{Z}_8$ and $\mathbb{Z}_{10}$, are derived for modest lengths. The notion of extremality for Euclidean weights is also introduced. We construct new extremal self-dual codes over these rings. Most of these codes are obtained via the double circulant and quasi-twisted constructions. New extremal odd unimodular lattices are obtained from some of these codes by Construction A.

Keywords: Self-dual code, Extremal code, Construction A, Unimodular lattice.

AMS Subject Classification: 94B05, 11H71

1. Introduction

Let $\mathbb{Z}_{2k}$ $(= \{0,1,2,\dots,2k-1\})$ be the ring of integers modulo $2k$. A code C of length n over $\mathbb{Z}_{2k}$ (or a $\mathbb{Z}_{2k}$-code of length n) is a $\mathbb{Z}_{2k}$-submodule of $\mathbb{Z}_{2k}^n$. Two 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 $C^\perp = \{x \in \mathbb{Z}_{2k}^n \mid x \cdot y = 0$ 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 is $\sum_{i=1}^n \min\{x_i^2, (2k-x_i)^2\}$. The minimum Euclidean weight d_E of C is the smallest Euclidean weight among all nonzero codewords of C. A self-dual code is called *Type II* if it has the property that every Euclidean weight is divisible by $4k$, and is called *Type I* otherwise [1].

Recent work on the construction of unimodular lattices with large minimum norm has motivated the construction of new self-dual $\mathbb{Z}_{2k}$-codes with large minimum Euclidean weights. However, only a few examples of such Type I codes are known for the rings $\mathbb{Z}_6$, $\mathbb{Z}_8$ and $\mathbb{Z}_{10}$. In addition, many examples of such Type II codes are known only for $\mathbb{Z}_4$ and $\mathbb{Z}_6$ (cf., e.g. [1], [4], [7], [8], [10], [12], [13] and [17]). In this paper, we construct extremal self-dual codes over $\mathbb{Z}_6$, $\mathbb{Z}_8$ and $\mathbb{Z}_{10}$

(the definition of extremal self-dual codes is given in Section 3). Most of these self-dual codes are obtained via the double circulant and quasi-twisted constructions.

In Section 2, the double circulant and quasi-twisted constructions are presented, and some basic facts related to these constructions are given. In Section 3, upper bounds on the minimum Euclidean weights of Type I codes over $\mathbb{Z}_6$, Type I and Type II codes over $\mathbb{Z}_8$, and Type I and Type II codes over $\mathbb{Z}_{10}$ are derived for lengths up to 68 , 72 , 88 , 96 and 112 , respectively. The notion of extremality for the Euclidean weights is also introduced. In Section 4, new extremal Type I $\mathbb{Z}_6$ -codes of lengths $32, 36, 40$ and 44 are given. The largest minimum Euclidean weight is also determined for lengths up to 52 . In Section 5, new extremal self-dual $\mathbb{Z}_8$ -codes are given. Finally, in Section 6, we demonstrate that there are extremal Type I $\mathbb{Z}_{10}$ -codes for lengths up to 40 . New extremal odd unimodular lattices are obtained from some of these codes by Construction A.

2. Construction Methods

Let p be an odd prime number. Define the map $\Psi : \mathbb{Z}_{2p} \to \mathbb{Z}_2 \times \mathbb{Z}_p$ by $\Psi(\alpha) = (\alpha \pmod 2), \alpha \pmod p))$. The map Ψ is a ring isomorphism. The map Ψ^{-1} is naturally extended to a map from $\mathbb{Z}_2^n \times \mathbb{Z}_p^n$ to $\mathbb{Z}_{2p}^n$. Let C and C' be a binary code and an $\mathbb{F}_p$ -code of the same length, respectively. We define

$$CRT(C, C') = \{\Psi^{-1}(a, b) \mid a \in C, b \in C'\}.$$

Then $CRT(C, C')$ is a code over $\mathbb{Z}_{2p}$. Here we say that C is the *binary part* and C' is the $\mathbb{F}_p$ *-part* of $CRT(C, C')$. C is a binary doubly-even (resp. singly-even) self-dual code and C' is a self-dual $\mathbb{F}_p$ -code if and only if $CRT(C, C')$ is Type II (resp. Type I) [8]. Note that a self-dual $\mathbb{Z}_6$ -code of length n exists if and only if $n \equiv 0 \pmod 4$, and a self-dual code over $\mathbb{Z}_{2k}$ $(k = 4, 5)$ of length n exists if and only if n is even. It is also known [1] that a Type II code exists if and only if $n \equiv 0 \pmod 8$.

A code C of length $2n$ is *double circulant* if it has generator matrix $(\ I\ ,\ R\ )$, where I is the identity matrix of order n and R is an $n \times n$ circulant matrix. A code C is *quasi-twisted* if it has generator matrix $(\ I\ ,\ M\ )$ where M is an $n \times n$ matrix such that the $(i+1)$ -st row of M is defined as $(-r_n, r_1, \ldots, r_{n-1})$ if the i -th row is $(r_1, r_2, \ldots, r_n)$ for $1 \le i \le n-1$. Many codes with large minimum weights have been obtained via the double circulant and quasi-twisted constructions (cf. [11], [18] and [20]).

Lemma 1. *A $\mathbb{Z}_{2p}$ -code $CRT(C, C')$ is double circulant if and only if both C and C' are double circulant. A $\mathbb{Z}_{2p}$ -code $CRT(C, C')$ is quasi-twisted if and only if C is binary double circulant and C' is quasi-twisted.*

Proof. Follows from the fact that C and C' have generator matrices $(\ I\ ,\ M \pmod 2\ )$ and $(\ I\ ,\ M \pmod p\ )$, respectively, if $CRT(C, C')$ has generator matrix $(\ I\ ,\ M\ )$. □

For a $\mathbb{Z}_{2^m}$ -code C , we say that $C^{(2^k)} = \{x \pmod{2^k} \mid x \in C\}$ is the $\mathbb{Z}_{2^k}$ -residue code for $1 \le k \le m-1$.

Proposition 2. *If a self-dual $\mathbb{Z}_{2^m}$ -code of length n with generator matrix of the form $(\ I\ ,\ A\ )$ exists then n is divisible by eight when $m \ge 2$.*

Proof. Let C be a self-dual $\mathbb{Z}_{2^m}$ -code of length n with generator matrix $(\ I\ ,\ A\ )$. The $\mathbb{Z}_{2^{m-1}}$ -residue code of a self-orthogonal $\mathbb{Z}_{2^m}$ -code is a self-orthogonal code with the property that all

Euclidean weights are divisible by 2^m [7]. Recall that C is self-orthogonal if $C \subset C^\perp$. Since $C^{(2^{m-1})}$ has generator matrix $(I , A \pmod{2^{m-1}})$, $C^{(2^{m-1})}$ is a Type II code. A Type II code of length n exists if and only if n is divisible by eight. □

By the above proposition, self-dual double circulant and quasi-twisted $\mathbb{Z}_8$-codes exist only for lengths divisible by eight. These self-dual $\mathbb{Z}_8$-codes may be used to construct Type II $\mathbb{Z}_4$-codes.

3. Upper Bounds on the Minimum Euclidean Weights

If C is a Type II (resp. Type I) $\mathbb{Z}_{2k}$-code with minimum Euclidean weight d_E then

$$A_{2k}(C) = \frac{1}{\sqrt{2k}}\{(x_1,\dots,x_n) \in \mathbb{Z}^n \mid (x_1 \pmod{2k},\dots,x_n \pmod{2k}) \in C\},$$

is an even (resp. odd) unimodular lattice with minimum norm $\min\{d_E/2k, 2k\}$ [1]. $A_{2k}(C)$ is called the lattice constructed from C by Construction A. It is shown in [21] that an n-dimensional unimodular lattice has minimum norm $\mu \le 2[n/24]+2$ unless $n=23$ when $\mu \le 3$. We say that a unimodular lattice meeting the bound with equality is *extremal*. Gaulter [9] showed that for $n \equiv 0 \pmod{24}$ any n-dimensional unimodular lattice with $\mu = 2[n/24]+2$ has to be even. Let L be an n-dimensional odd unimodular lattice and let L_0 denote the even norm subset of vectors. The set L_0 is a sublattice of L of index 2. Let L_2 be the unique nontrivial coset of L_0 in L. Then the dual lattice L_0^* of L_0 can be written as a union of cosets of L_0: $L_0^* = L_0 \cup L_2 \cup L_1 \cup L_3$. The shadow lattice of L is defined to be $S = L_1 \cup L_3$ [5]. See [6] for undefined terms concerning lattices.

We give upper bounds on the minimum Euclidean weights of Type I $\mathbb{Z}_6$-codes using upper bounds on the minimum norms and the theta series of odd unimodular lattices by Construction A.

Proposition 3. *Any Type I $\mathbb{Z}_6$-code of length $4m \le 68$ has minimum Euclidean weight*

$$\begin{array}{ll} d_{E,6} \le 12\left[\frac{m}{6}\right]+12 & \textit{if } m = 3,4,5,8,9,10,11,14,15,16,17 \\ d_{E,6} \le 12\left[\frac{m}{6}\right]+6 & \textit{otherwise.} \end{array} \qquad (1)$$

Proof. Let μ_n be the largest minimum norm among all odd unimodular lattices in dimension n. Then $\mu_n \le 5$ for $n \le 52$ (cf. [5] and [22]).

If $\mu_n \le 5$, then the upper bounds (1) directly follow from μ_n by considering the minimum norm of the odd unimodular lattices obtained from Type I $\mathbb{Z}_6$-codes by Construction A, as done in [1, Corollary 3.7]. Note that a unimodular lattice in dimensions $8, 24$ and 48 with minimum norms $2, 4$ and 6, respectively, is even (see also [9]). Hence $d_{E,6} \le 6, 18$ and 30 for lengths $8, 24$ and 48, respectively.

If $\mu_n \ge 6$ then we investigate the theta series of odd unimodular lattices with minimum norm 6 and kissing number $2n$, as the largest possible minimum Euclidean weights of Type I codes of lengths 60 and 68 are determined in [17]. Conway and Sloane [5] show that if the theta series of an odd unimodular lattice L is written as

$$\theta_L(q) = \sum_{j=0}^{\lfloor n/8 \rfloor} a_j \theta_3(q)^{n-8j}\Delta_8(q)^j,$$

then the theta series of the shadow lattice S can be written as

$$\theta_S(q) = \sum_{j=0}^{\lfloor n/8 \rfloor} \frac{(-1)^j}{16^j} a_j \theta_2(q)^{n-8j} \theta_4(q^2)^{8j},$$

where $\Delta_8(q) = q \prod_{m=1}^{\infty}(1-q^{2m-1})^8(1-q^{4m})^8$, and $\theta_2(q), \theta_3(q)$ and $\theta_4(q)$ are the Jacobi theta series [6].

Suppose that C is a Type I code of length 56 and minimum Euclidean weight ≥ 42 . Then $A_6(C)$ is an odd unimodular lattice with minimum norm 6 and kissing number 112 . Now we determine the possible theta series of an odd unimodular lattice with minimum norm 6 . From the condition that the minimum norm is 6 , we have that $a_0 = 1$, $a_1 = -112$, $a_2 = 3696$, $a_3 = -35840$, $a_4 = 61040$ and $a_5 = -59136$. In addition, since the shadow does not contain the 0 -vector, we have that $a_7 = 0$. Hence the theta series of an extremal odd unimodular lattice and its shadow lattice are

$$\begin{aligned} \theta_L(q) &= 1 + (8250368 + a_6)q^6 + \cdots , \\ &\text{and} \\ \theta_S(q) &= a_6/65536q^2 + (3696 - 11a_6/8192)q^4 + \cdots , \end{aligned}$$

respectively. Since $A_6(C)$ has kissing number 112 , we have $a_6 = -8250256$. However, the coefficient of q^2 in $\theta_S(q)$ is $-515641/4096$, so there is no odd unimodular lattice with kissing number 112 . Therefore the largest possible minimum Euclidean weight is 36 .

Similarly, the theta series of a 64 -dimensional odd unimodular lattice with minimum norm 6 and its shadow lattice are

$$\begin{aligned} \theta_L(q) &= 1 + (1267712 + a_6)q^6 + \cdots , \\ &\text{and} \\ \theta_S(q) &= -a_7/1048576q^2 + (a_6/256 + 13a_7/131072)q^4 + \cdots , \end{aligned}$$

respectively. If the kissing number is 128 then the shadow has a non-integral coefficient. Therefore the largest possible minimum Euclidean weight is 36 . □

We say that a Type I $\mathbb{Z}_6$ -code of length n (≤ 68) meeting the bound (1) with equality is *extremal.* Since we do not consider the construction of extremal self-dual codes for all lengths, we only derive upper bounds for sufficient lengths.

Proposition 4. *Any Type I $\mathbb{Z}_8$ -code of length $2m \leq 72$ has minimum Euclidean weight*

$$\begin{array}{ll} d_{E,8,I} \leq 16 \left[\frac{m}{12}\right] + 16 & \text{if } m = 6, \ldots, 10, 11, 16, 18, \ldots, 23, 28, \ldots, 35 \\ d_{E,8,I} \leq 16 \left[\frac{m}{12}\right] + 8 & \text{otherwise.} \end{array} \tag{2}$$

Any Type II $\mathbb{Z}_8$ -code of length $8m \leq 88$ has minimum Euclidean weight

$$d_{E,8,II} \leq 16 \left[\frac{m}{3}\right] + 16. \tag{3}$$

Proof. Similar to that of Proposition 3 for the case (2), and the case (3) $8m \leq 64$. We remark that the largest minimum norm among odd unimodular lattices in dimension 72 is at most 7 .

Now suppose that there is a Type II code C of length 72 and minimum Euclidean weight > 64. Then $A_8(C)$ is an extremal even unimodular lattice. However, the kissing number of $A_8(C)$ is 144, which is a contradiction (see Table 1). The cases $8m = 80, 88$ are similar. □

Table 1: Kissing numbers of extremal even unimodular lattices

n	Kissing number	n	Kissing number
72	6218175600	96	565866362880
80	1250172000	104	91508901120
88	168498000	112	10888335360

Remark 5. *The kissing numbers of extremal even unimodular lattices in dimensions* $n = 72, 80, 88, 96, 104$ *and* 112 *are listed in Table 1. These numbers are calculated by [6, Chap. 7, Theorem 17].*

Similarly, one can easily provide upper bounds on the minimum Euclidean weights of self-dual codes over $\mathbb{Z}_{10}$.

Proposition 6. *Any Type I* $\mathbb{Z}_{10}$*-code of length* $2m \leq 96$ *has minimum Euclidean weight*

$$\begin{aligned} d_{E,10,I} &\leq 20\left[\tfrac{m}{12}\right] + 20 \quad \text{if } m = 6,\ldots,10,11,16,18,\ldots,23, \\ &\qquad\qquad\qquad\quad 28,\ldots,35,37,\ldots,47 \\ d_{E,10,I} &\leq 20\left[\tfrac{m}{12}\right] + 10 \quad \text{otherwise.} \end{aligned} \tag{4}$$

Any Type II $\mathbb{Z}_{10}$*-code of length* $8m \leq 112$ *has minimum Euclidean weight*

$$d_{E,10,II} \leq 20\left[\frac{m}{3}\right] + 20. \tag{5}$$

We say that a Type I (resp. Type II) $\mathbb{Z}_8$-code of length $n \leq 72$ (resp. $n \leq 88$) meeting the bound (2) (resp. (3)) with equality is *extremal*, and a Type I (resp. Type II) $\mathbb{Z}_{10}$-code of length $n \leq 96$ (resp. $n \leq 112$) meeting the bound (4) (resp. (5)) with equality is *extremal*.

4. Extremal Type I $\mathbb{Z}_6$-Codes

4.1 Existence of Extremal Type I $\mathbb{Z}_6$-Codes

A set of n orthogonal vectors of norm $2k$ in an n-dimensional lattice L is called a $2k$-frame of L. A lattice L contains a $2k$-frame if and only if L can be constructed from some $\mathbb{Z}_{2k}$-code by Construction A. Hence from the existence of n-dimensional unimodular lattices with large minimum norm which have a $2k$-frame, we can determine the existence of some self-dual $\mathbb{Z}_{2k}$-codes.

If an n-dimensional odd unimodular lattice L can be constructed from some ternary self-dual code by Construction A, then L contains a 6-frame (cf. [17]). Since there is a ternary self-dual code T which determines an odd unimodular lattice with the largest minimum norm for dimensions $n \leq 28$, there is an extremal Type I $\mathbb{Z}_6$-code for $n \leq 28$. Moreover, the construction of unimodular lattices from ternary self-dual codes was studied in [17]. Since a unimodular lattice by this construction has a 6-frame, the lattice can be constructed from some self-dual $\mathbb{Z}_6$-code by Construction A. Hence there is an extremal Type I $\mathbb{Z}_6$-code for lengths $n = 44, 60, 68$ [17] (see [22] for $n = 52$). Recently a 48-dimensional odd unimodular lattice with minimum norm 5 was discovered in [16] via an extremal Type I $\mathbb{Z}_6$-code. Therefore we have the following proposition on known extremal Type I $\mathbb{Z}_6$-codes.

Proposition 7. *There is an extremal Type I $\mathbb{Z}_6$-code for lengths $n \leq 28$ and $n = 44, 48, 52, 60, 68$.*

Explicit examples of extremal Type I $\mathbb{Z}_6$-codes of lengths up to 20 and lengths 44, 48, 60, 68 can be found in [8], [12], [14], [16] and [17]. Here we give examples for lengths 24 and 28. The codes were obtained using the quasi-twisted construction, and the corresponding first rows are listed in Table 2. We have verified that these codes have different Euclidean weight distributions, and so they are inequivalent.

Table 2: Extremal Type I codes of lengths 24 and 28

Length	First row		
24	(404420010000)	(200224010000)	(434220020000)
	(230422020000)	(350211001000)	(135040101000)
	(353022101000)	(323052101000)	(343412301000)
28	(25322140110000)	(52322443110000)	(42024420210000)
	(44344220220000)		

4.2 New Extremal Type I $\mathbb{Z}_6$-Codes

- $n = 32$: By the quasi-twisted construction, we have found extremal Type I codes $C_{32,1}$ and $C_{32,2}$ with first rows

  (4251522022101000) and (1022540032101000),

  respectively. The binary parts of $C_{32,1}$ and $C_{32,2}$ have weight enumerators

  $$1 + 8y^4 + 64y^6 + 316y^8 + \cdots,$$
  and
  $$1 + 24y^4 + 128y^6 + 348y^8 + \cdots,$$

  respectively. The ternary parts of both codes have weight enumerator

  $$1 + 960y^9 + 64512y^{12} + \cdots.$$

  Using MAGMA, we verified that these ternary codes are inequivalent. These ternary codes are extremal self-dual, but a number of such codes are known [20, Table XII].

  There are exactly five extremal odd unimodular lattices up to isomorphism [5]. The lattices $A_6(C_{32,1})$ and $A_6(C_{32,2})$ are included in these five.

- $n = 36$: Let C_{36} be the quasi-twisted code with first row

  (211524402210100000).

C_{36} is an extremal Type I code of length 36.

The binary and ternary parts of C_{36} have the following weight enumerators

$$1+9y^4+72y^6+324y^8+\cdots,$$
and
$$1+288y^9+40248y^{12}+1410624y^{15}+\cdots,$$

respectively. $A_6(C_{36})$ is an extremal odd unimodular lattice with kissing number 42840.

- $n=40$: We have found an extremal Type I code C_{40} using the quasi-twisted construction. This code has first row

(54304422225010001000).

The binary and ternary parts of C_{40} have the following weight enumerators

$$1+10y^4+160y^6+525y^8+\cdots,$$
and
$$1+80y^9+19680y^{12}+\cdots,$$

respectively. $A_6(C_{40})$ is an extremal odd unimodular lattice with theta series

$$1+19120q^4+1376256q^5+43950080q^6+\cdots.$$

Another example of an extremal odd unimodular lattice can be found in [13]. These lattices have different theta series.

The possible theta series of an extremal odd unimodular lattice L and its shadow S are

$$\theta_L(q) = 1+(19120+256\beta)q^4+(1376256-4096\beta)q^5+\cdots,$$
and
$$\theta_S(q) = \beta q^2+(40960-56\beta)q^4+(87818240+1500\beta)q^6+\cdots,$$

respectively, where β is a parameter. The lattice $A_6(C_{40})$ corresponds to $\beta=0$, and the shadow of $A_6(C_{40})$ has minimum norm 4. Hence the two even unimodular neighbors of $A_6(C_{40})$, i.e., $(A_6(C_{40}))_0\cup(A_6(C_{40}))_1$ and $(A_6(C_{40}))_0\cup(A_6(C_{40}))_3$, have minimum norm 4, and so are extremal. Hence the two Type II neighbors of C_{40} are also extremal.

- $n=44$: Using the quasi-twisted construction, we found two extremal Type I $\mathbb{Z}_6$-codes $C_{44,1}$ and $C_{44,2}$. The first rows of the generator matrices of these codes are

(3542203204011000000000) and (3150531002111000000000),

respectively. The lattices $A_6(C_{44,1})$ and $A_6(C_{44,2})$ are extremal odd unimodular lattices. Several extremal Type I codes and extremal odd unimodular lattices are known [14], [17]. The lattices $A_6(C_{44,1})$ and $A_6(C_{44,2})$ have the following theta series

$$\theta_{A_6(C_{44,1})}(q) = 1+6600q^4+811008q^5+\cdots,$$
and
$$\theta_{A_6(C_{44,2})}(q) = 1+9416q^4+788480q^5+\cdots,$$

respectively. Since these lattices have different theta series than those of the known lattices in [14] and [17], the two lattices are new and the two codes are also new.

The binary parts of $C_{44,1}$ and $C_{44,2}$ have the following weight enumerators

$$1 + 11y^4 + 88y^6 + 407y^8 + \cdots,$$
and
$$1 + 220y^8 + 880y^{10} + 9361y^{12} + \cdots,$$

respectively. The binary part of $C_{44,2}$ is an extremal singly-even self-dual code which is equivalent to $P_{44,4}$ in [15]. Using MAGMA, we determined that the ternary parts of the two codes are equivalent and have the following weight enumerator

$$1 + 88y^9 + 8624y^{12} + \cdots.$$

- $n = 56, 64$: Let C and C' be Type I codes of lengths n and n' with minimum Euclidean weights d_E and d'_E, respectively. Then $\{(x, y) \in \mathbb{Z}_6^{n+n'} \mid x \in C, y \in C'\}$ is a Type I code of length $n + n'$ and minimum Euclidean weight $\min\{d_E, d'_E\}$. Hence there is a Type I code with minimum Euclidean weight 18 (resp. 24) for length 56 (resp. 64).

  By considering pairs of binary and ternary self-dual codes, we have found a Type I code C_{56} of length 56 and minimum Euclidean weight 24. C_{56} has a better minimum Euclidean weight than the code obtained via the above construction. C_{56} has generator matrix $(\ I\ ,\ M\ )$ where M is given below using the form $m_1, m_2, \ldots, m_{28}$ where m_j is the j-th row in order to save space.

41333115531311331515333351120, 4140331204344504542330514503
1141000313145545123302142333, 0441133404425021203341123332
3311413044253112303454203351, 0004414115234320001512033514
4000441155043430342453305145, 4135022140001124450031512330
4353224414300414203325453301, 3202511114103312033241230315
5025443344143020335112033424, 0251435301441333024120034245
2541323330144133244230045450, 2110235130044432115300124230
3324210122133314000141343224, 0545130521000144133043405241
5421030210004511143031352440, 4213332130315204441030524401
2103051033155400144405214010, 1033545334254300344145440102
3305154015243010034114404322, 3312213545100023201451400344
3455433451300502014551143031, 1521303543032450445531114033
5510334130021201122353411433, 2100045030215141253533044443
4030122005121312505313004414, 3334521051243322023444333444.

Proposition 8. *There is an extremal Type I $\mathbb{Z}_6$-code for lengths $32, 36$ and 40. The largest minimum Euclidean weight is determined for lengths up to 52.*

The largest minimum Euclidean weight $d(6, n)$ of Type I $\mathbb{Z}_6$-codes of length n is listed in Table 3.

Table 3: The largest minimum Euclidean weight $d(6,n)$

Length n	$d(6,n)$	Length n	$d(6,n)$	Length n	$d(6,n)$
4	6	28	18	52	30
8	6	32	24	56	$24-36$
12	12	36	24	60	36
16	12	40	24	64	$24-36$
20	12	44	24	68	36
24	18	48	30		

5. Extremal Self-Dual $\mathbb{Z}_8$-Codes

5.1 Existence of Extremal Type II $\mathbb{Z}_8$-Codes

We present what is known about the existence of extremal Type II $\mathbb{Z}_8$-codes. The classical construction of the Leech lattice given in [6, Fig. 4.12] gives an extremal Type II $\mathbb{Z}_8$-code L_{24} of length 24 (cf. [1]). In a similar way, extremal even unimodular lattices in dimensions 32 and 40 can be constructed from binary extremal doubly-even self-dual codes of lengths 32 and 40, respectively (cf. [4] and [6]). These constructions provide extremal Type II $\mathbb{Z}_8$-codes. Thus five inequivalent extremal Type II $\mathbb{Z}_8$-codes are known for length 32, and a great number of extremal Type II $\mathbb{Z}_8$-codes are known for length 40. Calderbank (a private communication in [4]), shows that the even unimodular lattice obtained from the extended Hensel lifted quadratic residue $\mathbb{Z}_8$-code QR_{48} is isomorphic to a known extremal even unimodular lattice P_{48q}. Hence QR_{48} is an extremal Type II code of length 48. Therefore extremal Type II $\mathbb{Z}_8$-codes are known for lengths up to 48, and the existence of extremal Type II codes of lengths 56 and 64 is an open problem.

5.2 New Extremal Type II $\mathbb{Z}_8$-Codes

- $n = 24$: By the quasi-twisted construction, we have found an extremal Type II $\mathbb{Z}_8$-code D_{24} of length 24 with first row

  $$(354153703000).$$

  By Construction A, the Leech lattice is obtained from D_{24}. Since the $\mathbb{Z}_2$-residue code of L_{24} consists of only the all-zero vector and the all-one vector, L_{24} and D_{24} are inequivalent. Hence D_{24} gives a new $\mathbb{Z}_8$-code construction of the Leech lattice.

  If D is a Type II $\mathbb{Z}_8$-code with generator matrix of the form $(\ I\ ,\ A\ )$, then $D^{(2)}$ and $D^{(4)}$ are Type II codes over $\mathbb{Z}_2$ and $\mathbb{Z}_4$, respectively. $D_{24}^{(2)}$ is the binary extended Golay $[24,12,8]$ code, which is extremal, however, $D_{24}^{(4)}$ has minimum Euclidean weight 8, which is non-extremal. Recall that a Type II $\mathbb{Z}_4$-code of length n and minimum Euclidean weight $8[n/24]+8$ is called extremal [2]. $A_2(D_{24}^{(2)})$ and $A_4(D_{24}^{(4)})$ are the Niemeier lattices with root systems A_1^{24} and A_3^8, respectively. The Hensel lifted extended Golay code over $\mathbb{Z}_8$ is not extremal, so our code provides an example of a $\mathbb{Z}_8$-lift of the extended Golay code to an extremal Type II code. Note that two other inequivalent extremal Type II codes have recently been found in [10].

- $n = 32$: We give an example of an extremal Type II code D_{32} . D_{32} is a bordered double circulant code with first row $r = (152756011000000)$ and borders $(\alpha, \beta, \gamma) = (4, 1, 1)$, that is, D_{32} has the following generator matrix

$$\left(\begin{array}{ccc} & 4 & 1 \ \cdots \ 1 \\ & 1 & \\ I & \vdots & R' \\ & 1 & \end{array} \right),$$

where R' is the 15×15 circulant matrix with first row r . Similarly to length 24 , it is easy to show that D_{32} is inequivalent to the five known extremal codes. By Construction A, D_{32} gives an example of an extremal even unimodular lattice. $D_{32}^{(2)}$ is equivalent to the extended quadratic residue code of length 32 , which is extremal. $D_{32}^{(4)}$ is also an extremal Type II $\mathbb{Z}_4$ -code. This code gives an extremal $\mathbb{Z}_8$ -lift of the binary extended quadratic residue code of length 32 . Note that the Hensel lifted extended quadratic residue $\mathbb{Z}_8$ -code of length 32 is not extremal.

- $n = 40$: By the quasi-twisted construction, we obtained an extremal Type II code D_{40} of length 40 with first row

$$(53575357521111111111).$$

The $\mathbb{Z}_2$ - and $\mathbb{Z}_4$ -residue codes of D_{40} are not extremal.

5.3 New Extremal Type I $\mathbb{Z}_8$ -Codes

We list in Table 4 extremal Type I codes E_{16} , E_{24} , E_{32} and E_{40} for lengths $16, 24, 32$ and 40 , respectively. These were obtained by the quasi-twisted construction. For each code in the table, we also list if the $\mathbb{Z}_4$ -residue code is extremal.

Table 4: Extremal Type I $\mathbb{Z}_8$ -codes

Code	Length	First row	$\mathbb{Z}_4$-residue
E_{16}	16	(32263450)	extremal
E_{24}	24	(174371501000)	non-extremal
E_{32}	32	(7575715331111110)	extremal
E_{40}	40	(46555315301211111110)	extremal

Note that $A_4(E_{24}^{(4)})$ is the Niemeier lattice with root system A_3^8 , and $A_8(E_{40})$ is an extremal odd unimodular lattice in dimension 40 . Using MAGMA, it was determined that $A_8(E_{40})$ has theta series

$$1 + 19120q^4 + 1376256q^5 + 43950080q^6 + \cdots .$$

6. Extremal Self-Dual $\mathbb{Z}_{10}$ -Codes

It is trivial that there is a Type II $\mathbb{Z}_{10}$ -code with minimum Euclidean weight 20 for lengths divisible by eight since a Type II code of length 8 exists. For lengths $24, 32$ and 40 , extremal Type II codes have been found in [10]. Hence we only consider extremal Type I $\mathbb{Z}_{10}$ -codes. Since there is a Type I $\mathbb{Z}_{10}$-code of length 2, it is trivial that there is a Type I code with minimum Euclidean weight $d_E = 10$ for every length $2n$. For lengths $12, 14, \ldots, 22$, a Type I code with $d_E = 20$ exists [12]. Here we consider extremal Type I codes for lengths $24 \le n \le 40$, as length 40 was the computational limit of the search for extremal codes.

Table 5: Extremal double circulant Type I $\mathbb{Z}_{10}$-codes

Code	Length	First row
G_{26}	26	(6886446100000)
G_{28}	28	(17483243100000)
G_{30}	30	(264626600100000)
G_{32}	32	(4719779011010000)
G_{34}	34	(82042140020000000)
G_{36}	36	(666280004410000000)
G_{38}	38	(4864042944200000000)
$G_{40,1}$	40	(49441516843111111110)

We list in Table 5 extremal double circulant Type I codes for lengths $26, 28, \ldots, 40$. For length 24, by considering pairs of self-dual binary and $\mathbb{F}_5$-codes, we have found an extremal Type I code G_{24}. G_{24} has generator matrix $(\ I\ ,\ M\ )$, where M is given below using the form $m_1, m_2, \ldots, m_{12}$ where m_j is the j-th row in order to save space.

$$
\begin{array}{l}
072222727727, 282383277320, 708788822737, 225878337228,\\
732032883777, 728753238327, 222325323337, 777782582383,\\
787723753288, 233222375873, 283877237532, 278332773708.
\end{array}
$$

Similarly to length 24, we have found one more extremal Type I code $G_{40,2}$ of length 40. $G_{40,2}$ has generator matrix $(\ I\ ,\ M\ )$ where M is given below using the form $m_1, m_2, \ldots, m_{20}$ where m_j is the j-th row in order to save space.

$$
\begin{array}{l}
24422120055055050555, 52442212005505505055, 55244221200550550505,\\
55524422120055055050, 25552442210005505505, 12555244225000550550,\\
21255524420500055055, 77670557440005000550, 97217050795000005000,\\
94776705570000050005, 50505550002492267505, 05505055500244726255,\\
05505505055524422120, 00550550505552442212, 00055055052555244221,\\
50005505501255524422, 05000550552125552442, 00500055057212555244,\\
00050005509721255524, 00005000554972125552.
\end{array}
$$

$A_{10}(G_{40,1})$ and $A_{10}(G_{40,2})$ are extremal odd unimodular lattices with theta series

$$
\begin{array}{l}
1 + 29360q^4 + 1212416q^5 + 44933120q^6 + \cdots,\\
\text{and}\\
1 + 23216q^4 + 1310720q^5 + 44343296q^6 + \cdots,
\end{array}
$$

respectively. Hence the lattice $A_4(C_{40})$ in [13], $A_6(C_{40})$, $A_{10}(G_{40,1})$ and $A_{10}(G_{40,2})$ have different theta series, and so are non-isomorphic.

Table 6: Extremal Type I $\mathbb{Z}_{10}$ -codes

Code	$d(G_i^{(2)})$	$d(G_i^{(5)})$	#	Code	$d(G_i^{(2)})$	$d(G_i^{(5)})$	#
G_{24}	6	9	4096	G_{34}	2	8	544
G_{26}	2	8	3120	G_{36}	2	9	42840
G_{28}	4	6	2240	G_{38}	2	10	29260
G_{30}	2	8	1520	$G_{40,1}$	6	10	29360
G_{32}	6	8	81344	$G_{40,2}$	8	8	23216

Table 6 displays the minimum weights $d(G_i^{(2)})$ and $d(G_i^{(5)})$ of the binary parts $G_i^{(2)}$ and the $\mathbb{F}_5$ -parts $G_i^{(5)}$, respectively, of the codes G_i ($i = 24, 26, \dots, 40$). The fourth and eighth columns give the kissing numbers (#) of the lattices $A_{10}(G_i)$. $G_{24}^{(5)}$ has the largest minimum weight among known $[24, 12]$ $\mathbb{F}_5$ -codes (cf. [3]), however, it was verified by MAGMA that the code is equivalent to Q_{24} in [19]. $G_{40,2}^{(2)}$ is also a binary extremal singly-even self-dual code, however a number of such codes are known. The lattices obtained from the G_i given in the table have the largest minimum norms among odd unimodular lattices for these dimensions. Note that $A_{10}(G_{36})$ and $A_{10}(G_{38})$ have the same kissing numbers as the extremal lattices given in [22].

Table 7: The largest minimum Euclidean weights $d(10, n)$

Length n	$d(10, n)$	Length n	$d(10, n)$	Length n	$d(10, n)$
2	10	16	20	30	30
4	10	18	20	32	40
6	10	20	20	34	30
8	10	22	20	36	40
10	10	24	30	38	40
12	20	26	30	40	40
14	20	28	30		

The largest minimum Euclidean weights $d(10, n)$ of Type I $\mathbb{Z}_{10}$ -codes of length n ($n \leq 40$) are listed in Table 7. Hence we have the following:

Proposition 9. *There is an extremal Type I $\mathbb{Z}_{10}$ -code for each admissible length $n \leq 40$.*

Acknowledgment. The authors would like to thank the anonymous referee for helpful comments, including improvements of Propositions 4 and 6.

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), 257–269.

[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] A.E. Brouwer, Bounds on the size of linear codes, in Handbook of Coding Theory, V.S. Pless and W.C. Huffman, eds., Elsevier, Amsterdam, 1998, 295–461. Also published electronically at `http://www.win.tue.nl/~aeb/voorlincod.html`.

[4] R. Chapman and P. Solé, Universal codes and unimodular lattices, *J. de th. des nombres de Bordeaux,* **8** (1996), 369–376.

[5] J.H. Conway and N.J.A. Sloane, A note on optimal unimodular lattices, *J. Number Theory,* **72** (1998), 357–362.

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

[7] S.T. Dougherty, T.A. Gulliver and M. Harada, Type II self-dual codes over finite rings and even unimodular lattices, *J. Alg. Combin.,* **9** (1999), 233–250.

[8] S.T. Dougherty, M. Harada and P. Solé, Self-dual codes over rings and the Chinese remainder theorem, *Hokkaido Math. J.,* **28** (1999), 253–283.

[9] M. Gaulter, Minima of odd unimodular lattices in dimension $24m$, *J. Number Theory,* **91** (2001), 81–91.

[10] S. Georgiou, M. Harada and C. Koukouvinos, Orthogonal designs and Type II codes over $\mathbb{Z}_{2k}$, *Designs, Codes and Cryptogr.,* **25** (2002), 163–174.

[11] T.A. Gulliver, New optimal ternary linear codes, *IEEE Trans. Inform. Theory,* **41** (1995), 1182–1185.

[12] T.A. Gulliver and M. Harada, Double circulant self-dual codes over $\mathbb{Z}_{2k}$, *IEEE Trans. Inform. Theory,* **44** (1998), 3105–3123.

[13] M. Harada, Self-dual $\mathbb{Z}_4$-codes and Hadamard matrices, *Discrete Math.,* **245** (2002), 273–278.

[14] M. Harada, Extremal odd unimodular lattices in dimensions 44, 46 and 47, *Hokkaido Math. J.,* **32** (2003), 153–159.

[15] M. Harada, T.A. Gulliver and H. Kaneta, Classification of extremal double circulant self-dual codes of length up to 62, *Discrete Math.,* **188** (1998), 127–136.

[16] M. Harada, M. Kitazume, A. Munemasa and B. Venkov, On some self-dual codes and unimodular lattices in dimension 48, *Europ. J. Combin.,* **26** (2005), 543–557.

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

[18] R. Hill and P.P. Greenough, Optimal quasi-twisted codes, *Int. Workshop Algebraic and Comb. Coding Theory*, Bulgaria, (1992), 92–97.

[19] J.S. Leon, V. Pless and N.J.A. Sloane, Self-dual codes over GF (5) , *J. Combin. Theory Ser. A*, **32** (1982), 178–194.

[20] E. Rains and N.J.A. Sloane, Self-dual codes, in Handbook of Coding Theory, V.S. Pless and W.C. Huffman, eds., Elsevier, Amsterdam, 1998, 177–294.

[21] E. Rains and N.J.A. Sloane, The shadow theory of modular and unimodular lattices, *J. Number Theory,* **73** (1998), 359–389.

[22] N.J.A. Sloane and G. Nebe, Unimodular lattices, together with a table of the best such lattices, in A Catalogue of Lattices, published electronically at `http://www.research.att.com/~njas/lattices/`.