MATHEMATICS OF COMPUTATION
Volume 78, Number 267, July 2009, Pages 1787–1796
S 0025-5718(08)02194-7
Article electronically published on October 24, 2008

CLASSIFICATION OF TERNARY EXTREMAL SELF-DUAL CODES OF LENGTH 28

MASAAKI HARADA, AKIHIRO MUNEMASA, AND BORIS VENKOV

Abstract. All 28-dimensional unimodular lattices with minimum norm 3 are known. Using this classification, we give a classification of ternary extremal self-dual codes of length 28. Up to equivalence, there are 6,931 such codes.

1. Introduction

As described in [21], 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 determine the largest minimum weight among self-dual codes of that length. By the Gleason–Pierce theorem, there are nontrivial divisible self-dual codes over $\mathbb{F}_q$ for $q = 2, 3$ and 4 only, where $\mathbb{F}_q$ denotes the finite field of order q; this is one of the reasons why much work has been done concerning self-dual codes over these fields.

A ternary self-dual code C of length n is a code over $\mathbb{F}_3$ satisfying $C = C^\perp$ where the dual code $C^\perp$ of C is defined as $C^\perp = \{x \in \mathbb{F}_3^n \mid x \cdot y = 0 \text{ for all } y \in C\}$ under the standard inner product $x \cdot y$. A ternary self-dual code of length n exists if and only if $n \equiv 0 \pmod 4$. It was shown in [18] that the minimum weight d of a self-dual code of length n is bounded by $d \leq 3[n/12] + 3$. If $d = 3[n/12] + 3$, then the code is called *extremal*.

All ternary self-dual codes of length ≤ 20 have been classified [5, 17, 20]. At length 24, the complete classification has not yet been done, but by showing that every ternary extremal self-dual code is generated by the rows of some Hadamard matrix of order 24, it is shown that there are exactly two inequivalent extremal self-dual codes [16] (see [14] for known results on the classification).

The aim of this paper is to establish the following classification.

Theorem 1. *There are exactly* 6,931 *inequivalent ternary extremal self-dual codes of length* 28.

Generator matrices of all codes can be obtained electronically from [11]. All computer calculations in this paper were done using Magma [4].

Received by the editor January 29, 2008 and, in revised form, June 9, 2008.
2000 *Mathematics Subject Classification.* Primary 94B05; Secondary 11H71.
Key words and phrases. Extremal self-dual code, unimodular lattice, frame.
The work of the first and second authors was partially supported by the Sumitomo Foundation (Grant for Basic Science Research Projects, 050034).

2. Self-dual codes and unimodular lattices

Let $\mathbb{Z}_k$ be the ring of integers modulo k, where k is a positive integer. Although we shall exclusively deal with the special case $k = 3$ (and hence $\mathbb{Z}_k = \mathbb{F}_3$) in later sections, we discuss the general case here since the presentation remains the same for all k. A code C of length n over $\mathbb{Z}_k$ (or a $\mathbb{Z}_k$-code of length n) is a $\mathbb{Z}_k$-submodule of $\mathbb{Z}_k^n$. A code C is *self-dual* if $C = C^\perp$ where the dual code $C^\perp$ of C is defined as $C^\perp = \{x \in \mathbb{Z}_k^n \mid x \cdot y = 0 \text{ for all } y \in C\}$ under the standard inner product $x \cdot y$. Two $\mathbb{Z}_k$-codes C and C' are *equivalent* if there exists a monomial $(\pm 1, 0)$-matrix P with $C' = C \cdot P = \{xP \mid x \in C\}$. The automorphism group $\mathrm{Aut}(C)$ of C is the group of all monomial $(\pm 1, 0)$-matrices P with $C = C \cdot P$.

A (Euclidean) lattice L in dimension n is *integral* if $L \subseteq L^*$, where the dual lattice L^* is defined as $L^* = \{x \in \mathbb{R}^n | (x, y) \in \mathbb{Z} \text{ for all } y \in L\}$ under the standard inner product (x, y). An integral lattice with $L = L^*$ is called *unimodular*. The norm of a vector x is (x, x). The minimum norm of L is the smallest norm among all nonzero vectors of L. The theta series $\theta_L(q)$ of L is the formal power series $\theta_L(q) = \sum_{x \in L} q^{(x,x)} = \sum_{m=0}^{\infty} N_m q^m$, where N_m is the number of vectors of norm m. The kissing number is the second nonzero coefficient of the theta series, that is, the number of vectors of L with minimum norm. Two lattices L and L' are *isomorphic*, denoted $L \cong L'$, if there exists an orthogonal matrix A with $L' = L \cdot A$. The automorphism group $\mathrm{Aut}(L)$ of L is the group of all orthogonal matrices A with $L = L \cdot A$.

For a $\mathbb{Z}_k$-code C of length n,

$$A_k(C) = \frac{1}{\sqrt{k}}\{(x_1, \ldots, x_n) \in \mathbb{Z}^n \mid (x_1 \bmod k, \ldots, x_n \bmod k) \in C\}$$

is a lattice, and $A_k(C)^* = A_k(C^\perp)$ holds (see e.g., [3, Lemma 3.1]). In particular, C is self-dual if and only if $A_k(C)$ is unimodular. This construction of lattices from codes is called Construction A. Clearly, if $\mathbb{Z}_k$-codes C and C' are equivalent, then the lattices $A_k(C)$ and $A_k(C')$ are isomorphic. Indeed, if P is a monomial $(\pm 1, 0)$-matrix and $C' = C \cdot P$, then $A_k(C) \cdot P = A_k(C')$.

A set $\{f_1, \ldots, f_n\}$ of n vectors $f_1, \ldots, f_n$ in an n-dimensional lattice L with $(f_i, f_j) = k\delta_{ij}$ is called a *k-frame* of L, where δ_{ij} is the Kronecker delta. Clearly, $A_k(C)$ has a k-frame. Conversely, self-dual codes over $\mathbb{Z}_k$ correspond to k-frames in unimodular lattices. To state this precisely and more generally, we consider an arbitrary integral lattice L in dimension n, and let $\mathcal{F} = \{f_1, \ldots, f_n\}$ be a k-frame of L. Consider the mapping

$$\pi_{\mathcal{F}} : \frac{1}{k}\bigoplus_{i=1}^{n} \mathbb{Z} f_i \to \mathbb{Z}_k^n,$$
$$\pi_{\mathcal{F}}(x) = ((x, f_i) \bmod k)_{1 \le i \le n}.$$

Then $\mathrm{Ker}\, \pi_{\mathcal{F}} = \bigoplus_{i=1}^{n} \mathbb{Z} f_i \subset L$, so the code $C = \pi_{\mathcal{F}}(L)$ satisfies $\pi_{\mathcal{F}}^{-1}(C) = L$. This implies $A_k(C) \cong L$ and every code C with $A_k(C) \cong L$ is obtained as $\pi_{\mathcal{F}}(L)$ for some k-frame $\mathcal{F}$ of L. In particular, if L is unimodular, then $\pi_{\mathcal{F}}(L)$ is self-dual and every self-dual code C with $A_k(C) \cong L$ is obtained in this way.

Lemma 2. *Let L be an integral lattice in dimension n, and let $\mathcal{F} = \{f_1, \ldots, f_n\}$, $\mathcal{F}' = \{f'_1, \ldots, f'_n\}$ be k-frames of L. Then the codes $\pi_{\mathcal{F}}(L)$ and $\pi_{\mathcal{F}'}(L)$ are equivalent if and only if there exists an orthogonal matrix $P \in \mathrm{Aut}(L)$ such that*

$$\{\pm f_1, \ldots, \pm f_n\} \cdot P = \{\pm f'_1, \ldots, \pm f'_n\}.$$

Proof. Let $C = \pi_{\mathcal{F}}(L)$, $C' = \pi_{\mathcal{F}'}(L)$. Since $A_k(C \cdot Q) = A_k(C) \cdot Q$ for a monomial $(\pm 1, 0)$-matrix Q, the codes C and C' are equivalent if and only if $A_k(C) \cdot Q = A_k(C')$ for some monomial $(\pm 1, 0)$-matrix Q. Let F and F' denote the $n \times n$ matrices whose row vectors consist of the elements of $\mathcal{F}$ and $\mathcal{F}'$, respectively. Then

$$A_k(C) \cdot \frac{1}{\sqrt{k}} F = A_k(C') \cdot \frac{1}{\sqrt{k}} F' = L.$$

This implies that the codes C and C' are equivalent if and only if $\frac{1}{k} F^T Q F' \in \mathrm{Aut}(L)$ for some monomial $(\pm 1, 0)$-matrix Q. This occurs precisely when $FP = QF'$ for some $P \in \mathrm{Aut}(L)$. □

3. Methods of classification

In this section, we describe our approach for classifying ternary extremal self-dual codes of length 28.

The minimum norm of a unimodular lattice in dimension 28 is at most 3 (see [6, Chapter 19]). We say that such a unimodular lattice with minimum norm 3 is optimal. There are 38 non-isomorphic optimal unimodular lattices in dimension 28 [2]. In [2], the 38 optimal unimodular lattices are denoted by $\mathbf{R}_{28,1}(\emptyset)$, $\mathbf{R}_{28,2}(\emptyset), \ldots, \mathbf{R}_{28,36}(\emptyset)$, $\mathbf{R}_{28,37e}(\emptyset)$, $\mathbf{R}_{28,38e}(\emptyset)$. These lattices have the following theta series:

$$\theta_{\mathbf{R}_{28,i}(\emptyset)}(q) = 1 + 2240q^3 + 98280q^4 + \cdots \ (i = 1, 2, \ldots, 36), \tag{1}$$

$$\theta_{\mathbf{R}_{28,i}(\emptyset)}(q) = 1 + 1728q^3 + 106472q^4 + \cdots \ (i = 37e, 38e). \tag{2}$$

In order to distinguish lattices, some polynomial $m_v(x)$ is defined in [2, p. 239]. We remark that the polynomial $m_v(x)$ has a misprint, namely, "$\langle v, \alpha \rangle = 1$" should be "$\langle v, \alpha \rangle = -1$".

If C is a self-dual code with minimum weight d, then $A_3(C)$ is a unimodular lattice with minimum norm $\min\{3, d/3\}$. Thus, if C is an extremal self-dual code of length 28, then $A_3(C)$ is an optimal unimodular lattice. An extremal self-dual code C of length 28 has the following weight enumerator:

$$1 + 2184y^9 + 78624y^{12} + 768096y^{15} + 2159976y^{18} + \cdots.$$

Since a codeword of weight 9 gives a vector of norm 3 in the lattice $A_3(C)$, $A_3(C)$ has exactly $2184 + 2 \cdot 28$ vectors of norm 3. Hence we have the following:

Lemma 3. *Let C be a ternary extremal self-dual code of length 28. Then the lattice $A_3(C)$ has theta series (1).*

Lemma 4. *Let L be an optimal unimodular lattice in dimension 28 having a 3-frame $\{u_1, \ldots, u_{28}\}$. Let L_0 be the even sublattice of the lattice L. If $u \in L_0^* \setminus L$, then*

$$u = \frac{1}{6} \sum_{i=1}^{28} \lambda_i u_i \tag{3}$$

for some odd integers $\lambda_1, \ldots, \lambda_{28}$.

Proof. Follows from [10, Lemma 2]. □

Lemma 5. *Let C be a ternary extremal self-dual code of length 28. Let $\{u_1, \dots, u_{28}\}$ be a 3-frame of $L = A_3(C)$ coming from C. Let L_0 be the even sublattice of the lattice L. Then L_0^* has minimum norm 3. Moreover, for any vector $u \in L_0^* \setminus L$ of norm 3, there exists a unique $i_0 \in \{1, \dots, 28\}$ such that*

$$|(u, u_i)| = \begin{cases} \frac{3}{2} & \text{if } i = i_0, \\ \frac{1}{2} & \text{otherwise.} \end{cases}$$

Proof. Since C has minimum weight 9, L has minimum norm 3. Hence L_0 has minimum norm 4 (see also [10, Lemma 1]). Let $u \in L_0^* \setminus L$ and write u as in (3). Then by Lemma 4, we have

$$\begin{aligned} 28 &\le \sum_{i=1}^{28} \lambda_i^2 \\ &= \frac{1}{3} \sum_{i=1}^{28} (\lambda_i u_i, \lambda_i u_i) \\ &= \frac{1}{3}(6u, 6u) \\ &= 12(u, u). \end{aligned}$$

Since $(u, u) \in \mathbb{Z}$ we have $(u, u) \ge 3$, and equality holds if and only if there exists a unique $i_0 \in \{1, \dots, 28\}$ such that

$$|\lambda_i| = \begin{cases} 3 & \text{if } i = i_0, \\ 1 & \text{otherwise,} \end{cases}$$

and the assertion follows. □

Remark 6. By Lemma 3, L has theta series (1). From [6, p. xlv], the shadow $L_0^* \setminus L$ has minimum norm 3. This gives an alternative proof of the assertion that L_0^* has minimum norm 3.

For a lattice L, a vector u not necessarily in L, an integer m and a real number c, set

$$L_{m,c}(u) = \{v \mid v \in L,\ (v, v) = m,\ (u, v) = \pm c\}. \tag{4}$$

Lemma 7. *Let L be an optimal unimodular lattice in dimension 28. Let S_3 be the set of vectors of norm 3 in $L_0^* \setminus L$. Let u_1, u_2 be orthogonal vectors of norm 3 in L. If there exists a 3-frame containing u_1 and u_2, then*

$$\{u_1, u_2\} \not\subset L_{3,3/2}(u) \quad \text{for all } u \in S_3. \tag{5}$$

Proof. Immediate from Lemma 5. □

Let L be a 28-dimensional optimal unimodular lattice with kissing number 2240. Let L_3 be the set $\{\{x, -x\} | (x, x) = 3, x \in L\}$ and let S_3 be the set $\{x | (x, x) = 3, x \in L_0^* \setminus L\}$. We define the simple undirected graph Γ, whose set of vertices is the set of 1120 pairs in L_3 and two vertices $\{x, -x\}, \{y, -y\} \in L_3$ are adjacent if $(x, y) = 0$ and $\{x, y\} \not\subset L_{3,3/2}(u)$ for any $u \in S_3$. It follows that the 3-frames are precisely the 28-cliques in the graph Γ. We could have defined Γ as the "orthogonality graph," by simply joining two vertices $\{x, -x\}, \{y, -y\} \in L_3$ whenever $(x, y) = 0$. The effect

of Lemma 7 is to remove those edges from the "orthogonality graph" which cannot be contained in 3-frames. This speeds up the computations considerably. It is clear that $\mathrm{Aut}(L)$ acts on the graph Γ as automorphisms, and Lemma 2 implies that the $\mathrm{Aut}(L)$-orbits on the set of 28-cliques in Γ are in one-to-one correspondence with the equivalence classes of codes C satisfying $A_3(C) \cong L$. Therefore, the classification of such codes reduces to finding a set of representatives of 28-cliques in Γ up to the action of $\mathrm{Aut}(L)$. This computation was performed using Magma, the results were then converted to 3-frames, and then to ternary extremal self-dual codes of length 28. In this way, by considering all 28-dimensional optimal unimodular lattices with kissing number 2240, we have all inequivalent extremal self-dual codes of length 28 by Lemma 3.

Remark 8. From the odd Leech lattice which is the unique odd unimodular lattice with minimum norm 3 in dimension 24, we can define the "orthogonality graph" as above. Classifying 24-cliques up to the automorphism group of the odd Leech lattice, we have verified that there are exactly two 3-frames in the odd Leech lattice up to conjugacy under the automorphism group. This confirms the known classification (see [16]) of ternary extremal self-dual codes of length 24.

4. Results of classification

By the approach described in Section 3, we completed the classification of ternary extremal self-dual codes of length 28. The number F_i $(i = 1, 2, \ldots, 36)$ of 3-frames in $\mathbf{R}_{28,i}(\emptyset)$ is listed in Table 1. The number N_i $(i = 1, 2, \ldots, 36)$ of inequivalent extremal self-dual codes C with $A_3(C) \cong \mathbf{R}_{28,i}(\emptyset)$ is also listed in Table 1. The last column $(\#\,\mathrm{Aut}, N_i(\#\,\mathrm{Aut}))$ in Table 1 lists the number $N_i(\#\,\mathrm{Aut})$ of the codes whose automorphism groups have order $\#\,\mathrm{Aut}$. Therefore, we have Theorem 1. As a corollary, we have the following:

Corollary 9. *A 28-dimensional optimal unimodular lattice L can be constructed from some ternary extremal self-dual code of length 28 by Construction A if and only if L is isomorphic to $\mathbf{R}_{28,i}(\emptyset)$ for some $i = 1, 2, \ldots, 27, 29, \ldots, 33, 35, 36$.*

We investigate the previously known extremal self-dual codes of length 28. Huffman [13] showed that there are 14 and 5 inequivalent extremal self-dual $[28, 14, 9]$ codes with automorphisms of orders 7 and 13, respectively. Denote the 14 codes with automorphisms of order 7 by $H_{7,1}, \ldots, H_{7,14}$, and the 5 codes with automorphisms of order 13 by $H_{13,1}, \ldots, H_{13,5}$, according to the order in [13, Theorem 4]. However, he did not check if there is a pair of equivalent codes $H_{7,i}$ and $H_{13,j}$ among these codes. We have verified that the codes $H_{7,2}$ and $H_{13,2}$ are equivalent and the codes $H_{7,14}$ and $H_{13,3}$ are equivalent.

In [8], 16 inequivalent extremal self-dual codes which are inequivalent to any of the codes in [13] are constructed and these codes are denoted by $C_{28,1}, \ldots, C_{28,16}$ in [8]. We remark that the existence of some extremal ternary self-dual code of length 28 with trivial automorphism group is announced in [9] and one example of such a code is given. However, we have verified that the code with generator matrix G_{28} given in [9] is equivalent to $C_{28,1}$. Hence 33 inequivalent extremal self-dual codes are previously known explicitly. We have verified that all of these 33 codes appear in the present classification, and we list the order $\#\,\mathrm{Aut}(C)$ of the automorphism group and the lattice $\mathbf{R}_{28,i}(\emptyset)$ with $A_3(C) \cong \mathbf{R}_{28,i}(\emptyset)$ in Table 2.

TABLE 1. Ternary extremal self-dual codes of length 28

i	F_i	N_i	$(\#\operatorname{Aut}, N_i(\#\operatorname{Aut}))$
1	4144	1036	$(2,1036)$
2	4804	735	$(2,501),(4,166),(8,64),(16,4)$
3	4218	589	$(2,474),(4,98),(8,17)$
4	4088	575	$(2,448),(4,125),(8,2)$
5	4728	667	$(2,516),(4,149),(8,2)$
6	3896	558	$(2,417),(4,139),(8,2)$
7	4420	376	$(2,364),(4,3),(6,8),(12,1)$
8	4296	333	$(2,213),(4,102),(8,18)$
9	4768	298	$(2,298)$
10	3328	208	$(2,208)$
11	4480	328	$(2,237),(4,81),(8,10)$
12	4184	166	$(2,102),(4,51),(8,13)$
13	5268	154	$(2,83),(4,40),(6,6),(8,13),(12,6),(16,1),(24,4),(48,1)$
14	5656	180	$(2,64),(4,102),(6,2),(8,4),(12,6),(24,2)$
15	5744	176	$(2,56),(4,74),(8,35),(16,5),(56,5),(112,1)$
16	4720	76	$(2,44),(4,28),(8,4)$
17	5080	84	$(2,30),(4,40),(6,3),(8,2),(12,8),(24,1)$
18	5968	83	$(2,49),(4,15),(6,13),(8,5),(24,1)$
19	3360	37	$(2,19),(4,11),(8,7)$
20	4608	57	$(2,18),(4,33),(8,6)$
21	5360	44	$(2,25),(4,15),(8,4)$
22	3100	16	$(2,15),(4,1)$
23	6336	36	$(2,16),(4,15),(8,5)$
24	5568	22	$(2,9),(4,9),(8,4)$
25	9432	36	$(2,3),(4,7),(6,1),(8,11),(12,2),(16,3),(24,6),(48,3)$
26	18688	26	$(4,4),(6,5),(8,3),(12,6),(16,1),(24,6),(48,1)$
27	5120	4	$(6,4)$
28	0	0	
29	5472	3	$(6,2),(54,1)$
30	41856	9	$(4,1),(6,1),(12,1),(16,1),(18,1),(24,3),(72,1)$
31	14400	6	$(24,2),(48,3),(336,1)$
32	16960	5	$(28,3),(52,2)$
33	36864	4	$(24,2),(48,1),(336,1)$
34	0	0	
35	230400	1	$(3024,1)$
36	12908160	3	$(2184,1),(4212,1),(117936,1)$

For those lattices $\mathbf{R}_{28,i}(\emptyset)$ which are not listed in Table 2, we list a code C_i with $\mathbf{R}_{28,i}(\emptyset) \cong A_3(C_i)$ where the rows of the matrix M_i in a generator matrix $(I,\ M_i)$ of C_i are given in Table 3. The order $\#\operatorname{Aut}(C_i)$ of the automorphism group of C_i is also listed.

The lattice $\mathbf{R}_{28,35}(\emptyset)$ was constructed by Nebe [19], and it can be given simply as

$$\Lambda = E_8 \wedge E_8,$$

where E_8 denotes the root lattice of type E_8. The unique code C with $A_3(C) \cong \Lambda$ can be constructed from a 3-frame of the lattice Λ, which we shall now describe.

Let $e_1, \ldots, e_9$ denote an orthonormal basis of the vector space $\mathbb{R}^9$. The $\mathbb{Z}$-linear span of $\{e_i - e_j \mid 1 \le i < j \le 9\}$ is known as the A_8-lattice. For a subset T of $\{1, \ldots, 9\}$, we denote by e_T the vector$\sum_{i \in T} e_i$, and by $\bar{T}$ the complementary set of T in $\{1, \ldots, 9\}$. Let $\mathcal{T}$ denote the set of all 3-subsets of the set $\{1, \ldots, 9\}$. Then, together with the 72 roots of A_8, the $2\binom{9}{3} = 168$ roots $\{\pm\frac{1}{3}(2e_T - e_{\bar{T}}) \mid T \in \mathcal{T}\}$ form the root system E_8. The group $\mathrm{PSL}(2,8)$ acts triply transitively on the

TABLE 2. The automorphism groups and lattices of known codes

Codes C	$\#\operatorname{Aut}(C)$	$\mathbf{R}_{28,i}(\emptyset)$	Codes C	$\#\operatorname{Aut}(C)$	$\mathbf{R}_{28,i}(\emptyset)$
$H_{7,1}$	56	$\mathbf{R}_{28,15}(\emptyset)$	$C_{28,1}$	2	$\mathbf{R}_{28,16}(\emptyset)$
$H_{7,2}$	2184	$\mathbf{R}_{28,36}(\emptyset)$	$C_{28,2}$	4	$\mathbf{R}_{28,12}(\emptyset)$
$H_{7,3}$	28	$\mathbf{R}_{28,32}(\emptyset)$	$C_{28,3}$	2	$\mathbf{R}_{28,11}(\emptyset)$
$H_{7,4}$	56	$\mathbf{R}_{28,15}(\emptyset)$	$C_{28,4}$	24	$\mathbf{R}_{28,17}(\emptyset)$
$H_{7,5}$	28	$\mathbf{R}_{28,32}(\emptyset)$	$C_{28,5}$	2	$\mathbf{R}_{28,9}(\emptyset)$
$H_{7,6}$	28	$\mathbf{R}_{28,32}(\emptyset)$	$C_{28,6}$	4	$\mathbf{R}_{28,5}(\emptyset)$
$H_{7,7}$	56	$\mathbf{R}_{28,15}(\emptyset)$	$C_{28,7}$	2	$\mathbf{R}_{28,2}(\emptyset)$
$H_{7,8}$	112	$\mathbf{R}_{28,15}(\emptyset)$	$C_{28,8}$	4	$\mathbf{R}_{28,6}(\emptyset)$
$H_{7,9}$	3024	$\mathbf{R}_{28,35}(\emptyset)$	$C_{28,9}$	2	$\mathbf{R}_{28,2}(\emptyset)$
$H_{7,10}$	56	$\mathbf{R}_{28,15}(\emptyset)$	$C_{28,10}$	2	$\mathbf{R}_{28,6}(\emptyset)$
$H_{7,11}$	56	$\mathbf{R}_{28,15}(\emptyset)$	$C_{28,11}$	4	$\mathbf{R}_{28,5}(\emptyset)$
$H_{7,12}$	336	$\mathbf{R}_{28,33}(\emptyset)$	$C_{28,12}$	8	$\mathbf{R}_{28,2}(\emptyset)$
$H_{7,13}$	336	$\mathbf{R}_{28,31}(\emptyset)$	$C_{28,13}$	8	$\mathbf{R}_{28,13}(\emptyset)$
$H_{7,14}$	117936	$\mathbf{R}_{28,36}(\emptyset)$	$C_{28,14}$	2	$\mathbf{R}_{28,3}(\emptyset)$
$H_{13,1}$	4212	$\mathbf{R}_{28,36}(\emptyset)$	$C_{28,15}$	2	$\mathbf{R}_{28,2}(\emptyset)$
$H_{13,4}$	52	$\mathbf{R}_{28,32}(\emptyset)$	$C_{28,16}$	4	$\mathbf{R}_{28,3}(\emptyset)$
$H_{13,5}$	52	$\mathbf{R}_{28,32}(\emptyset)$			

projective line $\mathbb{F}_8 \cup \{\infty\}$. Identifying $\mathbb{F}_8 \cup \{\infty\}$ with $\{1, \ldots, 9\}$, we regard $\mathrm{PSL}(2,8)$ as a permutation group on the set $\{1, \ldots, 9\}$. The group $\mathrm{PSL}(2,8)$ has a unique conjugacy class $\mathcal{C}$ of fixed-point-free elements of order 3. This conjugacy class $\mathcal{C}$ contains 28 pairs of elements and their inverses. Let $x \in \mathcal{C}$, and let T_1, T_2, T_3 be the $\langle x \rangle$-orbits on $\{1, \ldots, 9\}$. Define $f_x \in \Lambda$ by

$$f_x = \frac{1}{3}(e_{T_1} \wedge e_{T_2} + e_{T_2} \wedge e_{T_3} + e_{T_3} \wedge e_{T_1}).$$

Note that f_x is not uniquely determined by x, but determined up to sign. The set $\{\pm f_x \mid x \in \mathcal{C}\}$ forms a 3-frame in the lattice Λ. One obtains an extremal ternary self-dual code of length 28 from this 3-frame of Λ.

Finally, we remark that the lattice $\mathbf{R}_{28,36}(\emptyset)$ was first constructed in [1], and 3-frames of the lattice $\mathbf{R}_{28,36}(\emptyset)$ correspond to symplectic spreads in $\mathbb{F}_3^6$, as pointed out in [2, Remark 2.1]. Consequently, our classification gives an alternative proof of the classification of symplectic spreads in $\mathbb{F}_3^6$, given in [7].

TABLE 3. Some generator matrices of extremal self-dual codes

i	M_i	$\#\operatorname{Aut}(C_i)$
1	12211011201012, 10210021121122, 11102212101220, 10002220012101, 00212001122200, 02222011011000, 21022211212001, 22222221220200, 02010102210102, 22202122120011, 01212120122022, 12221120120120, 02121021200020, 01210002020222	2
4	22222002021111, 01012111210222, 12101200211221, 20221222012011, 12000020211012, 20201121222210, 20202101200022, 11222221222111, 01211000210201, 00102111212000, 02122011001001, 20110001222020, 02000102201222, 00222022122212	8
7	00001210210122, 22121101220202, 00220222212222, 02012002211001, 01122210010100, 10102000022221, 01212012020002, 22222210102101, 00101101110012, 20120000101121, 11010012200201, 21222122112211, 20212202211210, 22211010112210	12
8	00122221211210, 22210220110221, 20102111111202, 01122010200220, 00022121112122, 20210121121022, 22012200212122, 11121020222021, 20222121201101, 02211111220012, 02212112001111, 21200110112122, 00011002012222, 11202200012100	8

TABLE 3. Some generator matrices of extremal self-dual codes (continued)

i	M_i	$\#\operatorname{Aut}(C_i)$
10	02010220110021, 21201022112201, 00110120101101, 21210001211211, 21122022100222, 20221100212221, 01022111112110, 01220112101122, 00122212012000, 21120011202112, 02112002002220, 22201111211001, 12012222012201, 22200021200202	2
14	02220020101110, 00121002102210, 22210202112022, 12221100121101, 21011111210102, 00211021100011, 22110021121012, 21102211022220, 01002002111110, 21011002201200, 00212211022111, 11122201110210, 11101210102212, 01121212002121	24
18	21211122212212, 02221000210120, 22102201111210, 02111210220221, 21211220101102, 11012122111002, 20220100110021, 10020001210222, 00221122012121, 02110000202111, 21222222111221, 11001112021212, 02212101110000, 02201220000111	24
19	10102002022202, 21220200100021, 00002011012211, 02102220111000, 02012212202221, 11100210210001, 00111201002201, 21120210012122, 20010022011011, 20120112211101, 20200201120110, 22222100111201, 02201201012010, 01121110111021	8
20	20222002202200, 02000220120212, 02212222102202, 20001112200201, 00202202101120, 10001212111000, 11010221222202, 20120221212220, 12201002111111, 21202022221110, 22211120002122, 20022022020101, 12212020112021, 11021011001020	8
21	11011212011220, 10002202120102, 12010100022102, 10110221221011, 10112021120222, 21110210110222, 12111020020001, 21211121001120, 10212222102012, 01100000111121, 00220220221200, 00211210010201, 21100122112201, 11222121000212	8
22	02211201222021, 10011021200102, 12221111112121, 00121200211001, 21201111210102, 01020021201120, 00221222011212, 20021221000220, 20202102020101, 12220100000111, 02111100020201, 11122021202012, 12210211022110, 00102101101201	4
23	01110221001020, 11101211001111, 10010110011202, 01121221012102, 22111010112021, 21012220020010, 12102000220102, 20110222102221, 01211122210101, 22210012222220, 02202101011020, 02000102121011, 00202210111200, 21100220112000	8
24	00111220000122, 00220011012110, 10100022222002, 00121212012221, 22122111001110, 12112001100010, 11200122200100, 00121022210100, 11201012001002, 12112122210001, 01212010222111, 12202101112021, 20202200211020, 01202221000202	8
25	21222200220000, 12011220000021, 20020122101010, 20102102121211, 00012002212022, 01120200110220, 20221112010000, 10200221101100, 22121000112211, 02012110100101, 22021112201102, 21120210121011, 20110021200110, 11000102022201	48
26	20002202001122, 11100202121112, 00221102212212, 21010012012010, 10010101210202, 00110011002111, 12021011201111, 20011020222020, 21121120102120, 11001120212222, 00111212100001, 22220100122112, 22211010221102, 21220000100221	48
27	01121210201122, 12212010222110, 11201111001121, 12121111020201, 01200202121010, 20012201221221, 10201222212202, 20111100021200, 22101110110000, 21222020122101, 10221012211120, 10100010201111, 11020021210020, 00001021122102	6
29	12021100210100, 10102100012102, 21022101101222, 22220111100211, 21001220122111, 02202022101100, 22011011201212, 20011022222122, 22110110012212, 10122001002220, 11001020010122, 12102021221210, 02201202002220, 02120100022120	54
30	00202020211102, 20001201001121, 01120020210110, 22020102002120, 21002011010021, 20011012021001, 22200210222211, 02200022021201, 10102121221012, 12121120122002, 20022011120200, 01010220202011, 00110121022001, 01112200212122	72

5. Covering radii and 3-designs

The covering radius $R(C)$ of a code C of length n is the smallest integer R such that spheres of radius R around codewords of C cover the space $\mathbb{F}_3^n$. For linear codes, the covering radius is the largest weight of all coset leaders of the code. The covering radius is a basic and important geometric parameter of a code. Let C be an extremal self-dual code of length 28. Then, by the sphere-covering bound and the Delsarte bound, it is known that $R(C) = 6$ or 7 (see [12, Table 1]). Using our classification, explicit calculations show the following:

Proposition 10. *Every extremal self-dual code of length* 28 *has covering radius* 7.

A t-(v, k, λ) design is a set X of v points together with a collection $\mathcal{B}$ of k-subsets of X called blocks such that every t-subset of X is contained in exactly λ blocks. Two designs with the same parameters are isomorphic if there is a bijection between their point sets that maps the blocks of the first design into blocks of the second design. The automorphism group $\mathrm{Aut}(D)$ of a t-design D is the group of all isomorphisms of D with itself. If a 3-$(28, 9, \lambda)$ design exists, then λ must be divisible by 28 (see [15, p. 57]). Hence 3-$(28, 9, 28)$ designs have the smallest λ among 3-$(28, 9, \lambda)$ designs.

By the Assmus–Mattson theorem, the supports of the codewords of minimum weight in an extremal self-dual code of length 28 form a 3-$(28, 9, 28)$ design. We have verified that the 6,931 3-$(28, 9, 28)$ designs obtained from the extremal self-dual codes are non-isomorphic. Thus we have the following:

Proposition 11. *There are at least* 6,931 *non-isomorphic* 3-$(28, 9, 28)$ *designs.*

Remark 12. We have verified that every extremal self-dual code of length 28 is generated by the codewords of minimum weight.

For every extremal self-dual code C of length 28, we have verified that the order of the automorphism group of the 3-$(28, 9, 28)$ design obtained from C is half of the order of the automorphism group of C.

Acknowledgment

The authors would like to thank Gabriele Nebe for helpful discussions.

References

[1] R. Bacher and B. Venkov, Lattices and association schemes: a unimodular example without roots in dimension 28, *Ann. Inst. Fourier (Grenoble)* **45** (1995), 1163–1176. MR1370742 (96j:11093)

[2] R. Bacher and B. Venkov, Réseaux entiers unimodulaires sans racines en dimensions 27 et 28, Réseaux euclidiens, designs sphériques et formes modulaires, 212–267, Monogr. Enseign. Math., 37, Enseignement Math., Geneva, 2001. MR1878751 (2003a:11082)

[3] C. Bachoc, T.A. Gulliver and M. Harada, Isodual codes over $\mathbb{Z}_{2k}$ and isodual lattices, *J. Algebraic Combin.* **12** (2000), 223–240. MR1803233 (2001j:94052)

[4] 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/.

[5] J.H. Conway, V. Pless and N.J.A. Sloane, Self-dual codes over GF(3) and GF(4) of length not exceeding 16, *IEEE Trans. Inform. Theory* **25** (1979), 312–322. MR528009 (80h:94026)

[6] J.H. Conway and N.J.A. Sloane, *Sphere Packing, Lattices and Groups (3rd ed.)*, Springer-Verlag, New York, 1999. MR1662447 (2000b:11077)

[7] U. Dempwolff, Translation planes of order 27, *Des. Codes Cryptogr.* **4** (1994), 105–121. MR1268564 (95a:51012)

[8] M. Harada, New extremal ternary self-dual codes, *Australas. J. Combin.* **17** (1998), 133–145. MR1626295 (99c:94043)
[9] M. Harada, An extremal ternary self-dual $[28, 14, 9]$ code with a trivial automorphism group, *Discrete Math.* **239** (2001), 121–125. MR1850990 (2002m:94058)
[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. MR1943589 (2004b:11099)
[11] M. Harada and A. Munemasa, Database of Self-Dual Codes, Available online at http://www.math.is.tohoku.ac.jp/~munemasa/selfdualcodes.htm.
[12] M. Harada, M. Ozeki and K. Tanabe, On the covering radius of ternary extremal self-dual codes, *Des. Codes Cryptogr.* **33** (2004), 149–158. MR2080361 (2005d:94214)
[13] W.C. Huffman, On extremal self-dual ternary codes of lengths 28 to 40, *IEEE Trans. Inform. Theory* **38** (1992), 1395–1400. MR1168760 (93b:94030)
[14] W.C. Huffman, On the classification and enumeration of self-dual codes, *Finite Fields Appl.* **11** (2005), 451–490. MR2158773 (2006h:94253)
[15] D.L. Kreher, "t-Designs, $t \geq 3$," The CRC Handbook of Combinatorial Designs, C.J. Colbourn and J.H. Dinitz (Editors), CRC Press, Boca Raton, 1996, pp. 47–66. MR1392993 (97a:05001)
[16] J.S. Leon, V. Pless and N.J.A. Sloane, On ternary self-dual codes of length 24, *IEEE Trans. Inform. Theory* **27** (1981), 176–180. MR633414 (83c:94020)
[17] C.L. Mallows, V. Pless and N.J.A. Sloane, Self-dual codes over $GF(3)$, *SIAM J. Appl. Math.* **31** (1976), 649–666. MR0441541 (55:14404)
[18] C.L. Mallows and N.J.A. Sloane, An upper bound for self-dual codes, *Inform. Control* **22** (1973), 188–200. MR0414223 (54:2326)
[19] G. Nebe, Finite subgroups of $\mathrm{GL}_n(\mathbf{Q})$ for $25 \leq n \leq 31$, *Comm. Algebra* **24** (1996), 2341–2397. MR1390378 (97e:20066)
[20] V. Pless, N.J.A. Sloane and H.N. Ward, Ternary codes of minimum weight 6 and the classification of length 20, *IEEE Trans. Inform. Theory* **26** (1980), 305–316. MR570014 (81b:94033)
[21] 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. MR1667939

Department of Mathematical Sciences, Yamagata University, Yamagata 990–8560, Japan

Graduate School of Information Sciences, Tohoku University, Sendai 980–8579, Japan

Steklov Institute of Mathematics at St. Petersburg, St. Petersburg 191011, Russia