AN EVEN EXTREMAL LATTICE OF RANK 64

ICHIRO SHIMADA

Abstract. We construct an even extremal lattice of rank 64 by means of a generalized quadratic residue code.

1. Introduction

A *lattice* is a free $\mathbb{Z}$-module L of finite rank with a symmetric bilinear form

$$\langle\ ,\ \rangle\colon L \times L \to \mathbb{Z}$$

that makes $L \otimes \mathbb{R}$ a positive-definite real quadratic space. Let L be a lattice. The group of automorphisms of L is denoted by $\mathrm{O}(L)$. For simplicity, we write x^2 instead of $\langle x, x\rangle$ for $x \in L$. We say that L is *even* (or of type II) if $x^2 \in 2\mathbb{Z}$ holds for all $x \in L$. In this paper, we treat only even lattices. Since $\langle\ ,\ \rangle$ is non-degenerate, the mapping $x \mapsto \langle x, -\rangle$ embeds L into the *dual lattice*

$$L^\vee := \{\ x \in L \otimes \mathbb{Q}\ \mid\ \langle x, y\rangle \in \mathbb{Z}\ \text{ for all }\ y \in L\ \}.$$

We say that L is *unimodular* if this embedding is an isomorphism. We put

$$\min(L) := \min\{x^2 \,|\, x \in L \setminus \{0\}\}.$$

It is well-known that, if L is an even unimodular lattice, then its rank n is divisible by 8 and $\min(L)$ satisfies

$$\min(L) \le 2 + 2\left\lfloor \frac{n}{24} \right\rfloor. \tag{1.1}$$

Definition 1.1. We say that an even unimodular lattice L of rank n is *extremal* if the equality holds in (1.1).

Extremal lattices are important and interesting, because they give rise to dense sphere-packings. Extremal lattices of rank ≤ 24 are completely classified. The famous Leech lattice is characterized as the unique (up to isomorphism) extremal lattice of rank 24. On the other hand, the classification of extremal lattices of rank ≥ 32 seems to be very difficult. The known examples of extremal lattices are listed in the website [12] administrated by Nebe and Sloane, in Conway and Sloane [4, Chapter 1], or in Gaborit [5, Table 3].

As is extensively described in Conway and Sloane [4], there exist various methods of constructing a lattice from a code. The binary extended quadratic residue codes play an important role in these constructions. The most classical examples are that the extended Hamming code yields the extremal lattice E_8 of rank 8, and that the extended Golay code yields the Niemeier lattice of type $24A_1$. Various generalizations of quadratic residue codes are investigated. In particular, in Bonnecaze, Solé and Calderbank [1], the Leech lattice is constructed by a generalized

2010 *Mathematics Subject Classification.* 11H31, 94B05, 11H56.

This work was supported by JSPS KAKENHI Grant Number 16H03926 and 16K13749.

quadratic residue code of length 24 with components in $\mathbb{Z}/4\mathbb{Z}$. See also Chapman and Solé [2] and Harada and Kitazume [7].

In this paper, we consider a quadratic residue code with components in the *discriminant group* $D_R := R^\vee/R$ of an even lattice R of small rank, and construct a lattice L of large rank as an even overlattice of the orthogonal direct-sum of copies of R by using the code as the gluing data. As an application, we obtain the following:

Theorem 1.2. *There exists an extremal lattice $L_{\mathcal{Q}}$ of rank 64 whose automorphism group $\mathrm{O}(L_{\mathcal{Q}})$ is of order 119040. This group $\mathrm{O}(L_{\mathcal{Q}})$ contains a subgroup $\Gamma_{\mathcal{Q}}$ of index 2 that fits in the exact sequence*

$$0 \to (\mathbb{Z}/2\mathbb{Z})^2 \to \Gamma_{\mathcal{Q}} \to \mathrm{PSL}_2(31) \to 1. \tag{1.2}$$

The code $\mathcal{Q}$ that is used in the construction of $L_{\mathcal{Q}}$ is a generalized quadratic residue code of length 32 with components in the discriminant group $D_R \cong \mathbb{Z}/35\mathbb{Z}$ of the lattice

$$R = \begin{bmatrix} 6 & 1 \\ 1 & 6 \end{bmatrix}.$$

In [14], Quebbemann constructed (possibly several) extremal lattices of rank 64 as overlattices of the orthogonal direct-sum $E_8(3)^8$ of 8 copies of $E_8(3)$. (See also [4, Chapter 8.3].) Here $E_8(3)$ denotes the lattice obtained from the lattice E_8 by multiplying the intersection form by 3. We have the following:

Proposition 1.3. *The lattice $L_{\mathcal{Q}}$ does not contain $E_8(3)$ as a sublattice.*

Corollary 1.4. *The lattice $L_{\mathcal{Q}}$ cannot be obtained by Quebbemann's construction.*

In [11], Nebe discovered an extremal lattice

$$N_{64} := L_{8,2} \otimes L_{32,2}$$

of rank 64, and showed that $\mathrm{O}(N_{64})$ contains a subgroup of order 587520 generated by 6 elements. (See the website [12].) Since $|\mathrm{O}(L_{\mathcal{Q}})| < 587520$, we obtain the following:

Corollary 1.5. *The lattices $L_{\mathcal{Q}}$ and N_{64} are not isomorphic.*

In Harada, Kitazume and Ozeki [8] and Harada and Miezaki [9], they also constructed several extremal lattices of rank 64. The relation of these lattices with our lattice has not yet been clarified.

We found the lattice $L_{\mathcal{Q}}$ by an experimental search. We hope that several more extremal lattices can be obtained by the same method.

This paper is organized as follows. In Section 2.1, we fix notions and notation about codes with components in a finite abelian group. In Section 2.2, we explain how to construct an even unimodular lattice from a code with components in the discriminant group D_R of an even lattice R. In Section 3, we give the definition of a generalized quadratic residue code, and investigate its automorphisms. In Section 4, we construct the lattice $L_{\mathcal{Q}}$, and prove that $L_{\mathcal{Q}}$ is extremal and that $\mathrm{O}(L_{\mathcal{Q}})$ contains a subgroup $\Gamma_{\mathcal{Q}}$ of order 59520 that fits in the exact sequence (1.2). In particular, a brute-force method of the proof of $\min(L_{\mathcal{Q}}) = 6$ is explained in detail. In Section 5, we calculate the set $\mathcal{S}$ of vectors of square-norm 6 in $L_{\mathcal{Q}}$. Using this set, we prove Proposition 1.3, and calculate the order of $\mathrm{O}(L_{\mathcal{Q}})$. In the last section, we give another construction of $L_{\mathcal{Q}}$.

The computational data obtained in this article is available from the author's website [17]. In particular, the Gram matrix of $L_{\mathcal{Q}}$ is found in [17]. A generating set of $\mathrm{O}(L_{\mathcal{Q}})$ is available from in [12], though it is not minimal. For the computation, we used `GAP` [6].

Thanks are due to Professor Masaaki Harada for informing us of the extremal lattices of rank 64 in [8] and [9]. We also thank Professor Masaaki Kitazume and Professor Gabriele Nebe for the comments.

Conventions. The action of a group on a set is from the *right*, unless otherwise stated.

2. Preliminaries

2.1. Codes over a finite abelian group.

Definition 2.1. Let A be a finite abelian group. A *code of length m over A* is a subgroup of A^m.

Let G be a group. Then the symmetric group $\mathfrak{S}_m$ acts on G^m by permutations of components. We denote by $G \wr \mathfrak{S}_m$ the wreath product $G^m \rtimes \mathfrak{S}_m$. Then we have a splitting exact sequence

$$1 \to G^m \to G \wr \mathfrak{S}_m \to \mathfrak{S}_m \to 1. \tag{2.1}$$

Suppose that G acts on a set X. Since $\mathfrak{S}_m$ acts on X^m by permutations of components and G^m acts on X^m by

$$(x_1, \dots, x_m)^{(g_1,\dots,g_m)} = (x_1^{g_1}, \dots, x_m^{g_m}), \quad \text{where} \quad x_i \in X, \quad g_i \in G,$$

the group $G \wr \mathfrak{S}_m$ acts on X^m in a natural way.

Let H be a subgroup of the automorphism group $\mathrm{Aut}(A)$ of a finite abelian group A. Then $H \wr \mathfrak{S}_m$ acts on A^m. For a code $\mathcal{C}$ of length m over A, we put

$$\mathrm{Aut}_H(\mathcal{C}) := \{\, g \in H \wr \mathfrak{S}_m \mid \mathcal{C}^g = \mathcal{C} \,\}.$$

2.2. Discriminant forms and overlattices.

Let R be an even lattice. We define the *dual lattice* of R by

$$R^\vee := \{\, x \in R \otimes \mathbb{Q} \mid \langle x, v \rangle \in \mathbb{Z} \text{ for all } v \in R \,\},$$

and the *discriminant group* D_R of R by

$$D_R := R^\vee / R.$$

Note that $R^\vee$ has a natural $\mathbb{Q}$-valued symmetric bilinear form that extends the $\mathbb{Z}$-valued symmetric bilinear form of R. Hence D_R is naturally equipped with a quadratic form

$$q_R \colon D_R \to \mathbb{Q}/2\mathbb{Z}$$

defined by $q_R(x \bmod R) := x^2 \bmod 2\mathbb{Z}$. We call q_R the *discriminant form* of R. We denote by $\mathrm{O}(q_R)$ the automorphism group of the finite quadratic form (D_R, q_R). Then we have a natural homomorphism

$$\eta_R \colon \mathrm{O}(R) \to \mathrm{O}(q_R).$$

Remark 2.2. The notion of discriminant forms was introduced by Nikulin [13] for the study of $K3$ surfaces, and it has been widely used in the investigation of $K3$ surfaces and Enriques surfaces. (See, for example, [16].)

The discriminant form of the orthogonal direct-sum R^m of m copies of R is the orthogonal direct-sum (D_R^m, q_R^m) of m copies of (D_R, q_R). Let $\mathcal{C}$ be a code of length m over D_R that is totally isotropic with respect to the quadratic form

$$q_R^m \colon D_R^m \to \mathbb{Q}/2\mathbb{Z}.$$

Then the pull-back

$$L_{\mathcal{C}} := \mathrm{pr}^{-1}(\mathcal{C}) \tag{2.2}$$

of $\mathcal{C}$ by the natural projection $\mathrm{pr}\colon R^{\vee m} \to D_R^m$ with the restriction of the natural $\mathbb{Q}$-valued symmetric bilinear form of $R^{\vee m}$ is an even lattice that contains R^m as a sublattice of finite index; that is, $L_{\mathcal{C}}$ is an even *overlattice* of R^m. Moreover, since the index of R^m in $L_{\mathcal{C}}$ is equal to $|\mathcal{C}|$, if $\mathcal{C}$ satisfies

$$|\mathcal{C}|^2 = |D_R|^m,$$

then $L_{\mathcal{C}}$ is unimodular.

Let $\mathcal{C}$ be a code of length m over D_R totally isotropic with respect to q_R^m. We put

$$H(R) := \mathrm{Im}(\eta_R \colon \mathrm{O}(R) \to \mathrm{O}(q_R)) \quad \subset \quad \mathrm{Aut}(D_R),$$

and consider the group $\mathrm{Aut}_{H(R)}(\mathcal{C})$. Each element g of $\mathrm{Aut}_{H(R)}(\mathcal{C})$ is uniquely written as

$$g = \sigma \cdot (h_1, \dots, h_m) \qquad (\ \sigma \in \mathfrak{S}_m,\ h_i \in H(R)\ ).$$

By the definition of $H(R)$, there exist elements $\tilde{h}_i \in \mathrm{O}(R)$ such that $\eta_R(\tilde{h}_i) = h_i$ for $i = 1, \dots, m$. Since g preserves the code $\mathcal{C}$, the action of

$$\tilde{g} := \sigma \cdot (\tilde{h}_1, \dots, \tilde{h}_m) \quad \in \quad \mathrm{O}(R) \wr \mathfrak{S}_m$$

on $(R^\vee)^m$ preserves the submodule $L_{\mathcal{C}} \subset (R^\vee)^m$, and hence we obtain a lift $\tilde{g} \in \mathrm{O}(L_{\mathcal{C}})$ of g. If η_R is injective, then the lift $\tilde{g}$ of g is unique. Therefore we have the following:

Lemma 2.3. *Let $\mathcal{C}$ and $L_{\mathcal{C}}$ be as above. If the natural homomorphism η_R is injective, then we have an injective homomorphism $\mathrm{Aut}_{H(R)}(\mathcal{C}) \hookrightarrow \mathrm{O}(L_{\mathcal{C}})$.*

3. Generalized quadratic residue codes

3.1. **Definition.** Let A be a finite abelian group, and p an odd prime. We consider the set of rational points

$$\mathbb{P}^1(\mathbb{F}_p) = \mathbb{F}_p \cup \{\infty\} = \{0, 1, \dots, p-1, \infty\}$$

of the projective line over $\mathbb{F}_p$, and let A^{p+1} denote the abelian group of all mappings

$$\boldsymbol{v} \colon \mathbb{P}^1(\mathbb{F}_p) \to A$$

from $\mathbb{P}^1(\mathbb{F}_p)$ of A. Let $\chi_p \colon \mathbb{F}_p^\times \to \{\pm 1\}$ denote the Legendre character of the multiplicative group $\mathbb{F}_p^\times := \mathbb{F}_p \setminus \{0\}$.

Definition 3.1. Let a, b, d, s, t, e be elements of A. A *generalized quadratic residue code* of length $p+1$ over A with parameter (a, b, d, s, t, e) is the subgroup $\mathcal{Q}$ of A^{p+1} generated by the elements $\boldsymbol{v}_\infty$, $\boldsymbol{v}_0, \boldsymbol{v}_1, \dots, \boldsymbol{v}_{p-1} \in A^{p+1}$ defined as follows:

$$\boldsymbol{v}_\infty(\nu) = \begin{cases} a & \text{if } \nu \in \mathbb{F}_p, \\ b & \text{if } \nu = \infty, \end{cases}$$

and, for $\mu \in \mathbb{F}_p$,

$$\boldsymbol{v}_\mu(\nu) = \begin{cases} d & \text{if } \nu = \mu, \\ s & \text{if } \nu \in \mathbb{F}_p \setminus \{\mu\} \text{ and } \chi_p(\mu - \nu) = 1, \\ t & \text{if } \nu \in \mathbb{F}_p \setminus \{\mu\} \text{ and } \chi_p(\mu - \nu) = -1, \\ e & \text{if } \nu = \infty. \end{cases}$$

3.2. **Automorphisms of a generalized quadratic residue code.** Let A and p be as above. For simplicity, we put

$$\mathfrak{S} := \mathfrak{S}(\mathbb{P}^1(\mathbb{F}_p)) \cong \mathfrak{S}_{p+1}.$$

The linear fractional transformation embeds $\mathrm{PSL}_2(p)$ into $\mathfrak{S}$. Let α be a generator of $\mathbb{F}_p^\times$. Then $\mathrm{PSL}_2(p)$ is generated by the three elements

$$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{bmatrix},$$

which correspond respectively to the permutations of $\mathbb{P}^1(\mathbb{F}_p)$ defined as follows:

$$\xi\colon \nu \mapsto -1/\nu, \quad \eta\colon \nu \mapsto \nu + 1, \quad \zeta\colon \nu \mapsto \alpha^2\nu,$$

with the understanding that $-1/0 = \infty, -1/\infty = 0, \infty + 1 = \infty$, and $\alpha^2\infty = \infty$. Let $\mathcal{Q} \subset A^{p+1}$ be a generalized quadratic residue code of length $p+1$ over A, and H a subgroup of $\mathrm{Aut}(A)$. Let $f_{\mathcal{Q}}$ be the composite homomorphism of the natural inclusion $\mathrm{Aut}_H(\mathcal{Q}) \hookrightarrow H \wr \mathfrak{S}$ and the surjection $H \wr \mathfrak{S} \twoheadrightarrow \mathfrak{S}$ in (2.1):

$$f_{\mathcal{Q}}\colon \mathrm{Aut}_H(\mathcal{Q}) \hookrightarrow H \wr \mathfrak{S} \twoheadrightarrow \mathfrak{S}$$

Lemma 3.2. *The image of $f_{\mathcal{Q}}$ contains η and ζ.*

Proof. The permutation of components given by η (resp. by ζ) preserves the generating set $\{\boldsymbol{v}_\infty, \boldsymbol{v}_0, \dots, \boldsymbol{v}_{p-1}\}$ of $\mathcal{Q}$. □

4. An extremal lattice $L_{\mathcal{Q}}$ of rank 64

We construct an extremal lattice $L_{\mathcal{Q}}$ of rank 64. Let R be the lattice of rank 2 with a basis e_1, e_2 such that the Gram matrix of R with respect to e_1, e_2 is

$$\begin{bmatrix} \langle e_1, e_1\rangle & \langle e_1, e_2\rangle \\ \langle e_2, e_1\rangle & \langle e_2, e_2\rangle \end{bmatrix} = \begin{bmatrix} 6 & 1 \\ 1 & 6 \end{bmatrix}. \tag{4.1}$$

Let $e_1^\vee, e_2^\vee$ be the basis of $R^\vee$ dual to e_1, e_2. Then D_R is a cyclic group of order 35 generated by

$$u := 6e_1^\vee + 2e_2^\vee = \frac{1}{35}(34e_1 + 6e_2).$$

For simplicity, we denote by $n \in \mathbb{Z}/35\mathbb{Z}$ the element

$$n\,(6e_1^\vee + 2e_2^\vee) \in D_R.$$

Then the discriminant form $q_R\colon D_R \to \mathbb{Q}/2\mathbb{Z}$ is given by

$$q_R(n) = 6n^2/35 \bmod 2\mathbb{Z}.$$

We have

$$\mathrm{O}(q_R) = \{\, k \in (\mathbb{Z}/35\mathbb{Z})^\times \mid 6k^2 \equiv 6 \bmod 70 \,\} = \{\pm 1, \pm 6\}.$$

$$\left[\begin{array}{cccccccccccccccc}
32 & 30 & 15 & 11 & 7 & 29 & 19 & 10 & 26 & 11 & 31 & 33 & 28 & 22 & 22 & 12 \\
16 & 13 & 23 & 21 & 19 & 30 & 25 & 3 & 11 & 21 & 31 & 32 & 12 & 9 & 9 & 4 \\
34 & 6 & 30 & 22 & 22 & 19 & 20 & 32 & 17 & 30 & 30 & 24 & 10 & 33 & 0 & 20 \\
34 & 26 & 1 & 17 & 9 & 6 & 4 & 17 & 14 & 12 & 25 & 19 & 34 & 8 & 33 & 20 \\
34 & 26 & 21 & 23 & 4 & 28 & 26 & 1 & 34 & 9 & 7 & 14 & 29 & 32 & 8 & 18 \\
34 & 24 & 21 & 8 & 10 & 23 & 13 & 23 & 18 & 29 & 4 & 31 & 24 & 27 & 32 & 28 \\
34 & 34 & 19 & 8 & 30 & 29 & 8 & 10 & 5 & 13 & 24 & 28 & 6 & 22 & 27 & 17 \\
34 & 23 & 29 & 6 & 30 & 14 & 14 & 5 & 27 & 0 & 8 & 13 & 3 & 4 & 22 & 12 \\
34 & 18 & 18 & 16 & 28 & 14 & 34 & 11 & 22 & 22 & 30 & 32 & 23 & 1 & 4 & 7 \\
34 & 13 & 13 & 5 & 3 & 12 & 34 & 31 & 28 & 17 & 17 & 19 & 7 & 21 & 1 & 24 \\
34 & 30 & 8 & 0 & 27 & 22 & 32 & 31 & 13 & 23 & 12 & 6 & 29 & 5 & 21 & 21 \\
34 & 27 & 25 & 30 & 22 & 11 & 7 & 29 & 13 & 8 & 18 & 1 & 16 & 27 & 5 & 6 \\
34 & 12 & 22 & 12 & 17 & 6 & 31 & 4 & 11 & 8 & 3 & 7 & 11 & 14 & 27 & 25 \\
34 & 31 & 7 & 9 & 34 & 1 & 26 & 28 & 21 & 6 & 3 & 27 & 17 & 9 & 14 & 12 \\
34 & 18 & 26 & 29 & 31 & 18 & 21 & 23 & 10 & 16 & 1 & 27 & 2 & 15 & 9 & 34 \\
34 & 5 & 13 & 13 & 16 & 15 & 3 & 18 & 5 & 5 & 11 & 25 & 2 & 0 & 15 & 29
\end{array}\right]$$

TABLE 4.1. The matrix B

On the other hand, the group $\mathrm{O}(R)$ is of order 4 and is generated by

$$g_1 := \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad g_2 := \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}.$$

The natural homomorphism $\eta_R \colon \mathrm{O}(R) \to \mathrm{O}(q_R)$ maps g_1 to -6 and g_2 to -1. Hence η_R is an isomorphism. In particular, the image $H(R)$ of η_R is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

We investigate the generalized quadratic residue code $\mathcal{Q}$ of length 32 over D_R with parameter

$$(a, b, d, s, t, e) = (0, 0, 1, 7, 3, 2).$$

Note that $\mathbb{F}_{31}^{\times}$ is generated by 3. We arrange the elements of $\mathbb{P}^1(\mathbb{F}_{31})$ as

$$[\,\infty, 0 \mid 1, 3^2, 3^4, \dots, 3^{28}, \mid 3, 3^3, 3^5, \dots, 3^{29}\,], \tag{4.2}$$

and write elements of D_R^{32}, $H(R)^{32}$, and $(R \otimes \mathbb{Q})^{32}$ as row vectors according this arrangement.

Proposition 4.1. *The code $\mathcal{Q}$ is totally isotropic with respect to q_R^{32}, and satisfies $|\mathcal{Q}| = 35^{16}$.*

Proof. The code $\mathcal{Q}$ is generated by the row vectors of the matrix $[I_{16}|B]$, where I_{16} is the identity matrix of size 16, and B is the 16×16 matrix in Table 4.1. (The components of B are in $D_R = \mathbb{Z}/35\mathbb{Z}$.) It is easy to confirm that $\mathcal{Q}$ is totally isotropic with respect to q_R^{32}, and that $|\mathcal{Q}| = 35^{16}$ holds. □

Hence we obtain an even unimodular overlattice $L_{\mathcal{Q}} = \mathrm{pr}^{-1}(\mathcal{Q})$ of R^{32} by (2.2). We will show that $L_{\mathcal{Q}}$ is extremal, and that $\mathrm{O}(L_{\mathcal{Q}})$ contains a subgroup $\Gamma_{\mathcal{Q}}$ with the properties stated in Theorem 1.2.

Proposition 4.2. *The kernel of the homomorphism $f_{\mathcal{Q}} \colon \mathrm{Aut}_{H(R)}(\mathcal{Q}) \to \mathfrak{S}$ is equal to the image of the diagonal homomorphism $\delta \colon H(R) \hookrightarrow H(R)^{32}$. The image of $f_{\mathcal{Q}}$ contains the permutation $\xi \in \mathfrak{S}$.*

n	0	±1	±2	±3	±4	±5	±6	±7	±8	±9	±10
$35\lambda(n)$	0	6	24	54	26	10	6	14	34	66	40

n	±11	±12	±13	±14	±15	±16	±17
$35\lambda(n)$	26	24	34	56	90	66	54

TABLE 4.2. $\lambda(n)$

Proof. Let σ be an element of $\mathfrak{S}$. Let Z be the 32×32 matrix

$$\left[\begin{array}{c|c} I_{16} & B \\ \hline O & 35\, I_{16} \end{array}\right],$$

where B is regarded as a matrix with components, not in $\mathbb{Z}/35\mathbb{Z}$, but in $\mathbb{Z}$, and we put $Z^* := 35Z^{-1}$, which is a matrix with components in $\mathbb{Z}$. Let Z^σ be the matrix obtained by applying the permutation σ of components to the row vectors of Z. For

$$\boldsymbol{x} = (x_1, \ldots, x_{32}) \in H(R)^{32} \subset H(R) \wr \mathfrak{S},$$

let $\Delta(\boldsymbol{x})$ denote the diagonal matrix with components being the representatives in $\mathbb{Z}$ of $x_1, \ldots, x_{32} \in H(R) = \{\pm1, \pm6\} \subset (\mathbb{Z}/35\mathbb{Z})^\times$. Then we have $\mathcal{Q}^{\sigma \boldsymbol{x}} = \mathcal{Q}$ only when

$$Z^\sigma \cdot \Delta(\boldsymbol{x}) \cdot Z^* \equiv O \mod 35. \tag{4.3}$$

We can calculate the set

$$\Lambda(\sigma) := \{\, \gamma \in H(R)^{32} \mid \mathcal{Q}^{\sigma\gamma} = \mathcal{Q} \,\}$$

by solving the congruence linear equation (4.3) with unknowns $x_1, \ldots, x_{32}$. By this method, we obtain $\Lambda(\mathrm{id}) = \delta(H(R))$, and hence $\operatorname{Ker} f_\mathcal{Q} = \delta(H(R))$. On the other hand, we have $\Lambda(\xi) \neq \emptyset$. Indeed, we see that $\Lambda(\xi)$ contains the element

$$(\,1, -1, -6, \ldots, -6, 6, \ldots, 6\,) \in H(R)^{32} \quad (15 \text{ times of } -6 \text{ and } 15 \text{ times of } 6).$$

Hence $\operatorname{Im} f_\mathcal{Q}$ contains ξ. □

Combining Proposition 4.2 with Lemma 3.2, we see that the image of $f_\mathcal{Q}$ includes the subgroup $\mathrm{PSL}_2(31) \subset \mathfrak{S}$. We put

$$\overline{\Gamma}_\mathcal{Q} := f_\mathcal{Q}^{-1}(\mathrm{PSL}_2(31)).$$

By Lemma 2.3, we have a natural embedding $\overline{\Gamma}_\mathcal{Q} \hookrightarrow \mathrm{O}(L_\mathcal{Q})$ of the subgroup $\overline{\Gamma}_\mathcal{Q}$ of $\mathrm{Aut}_{H(R)}(\mathcal{Q})$ into $\mathrm{O}(L_\mathcal{Q})$. Let $\Gamma_\mathcal{Q}$ be the image of this embedding. Then $\Gamma_\mathcal{Q}$ satisfies the exact sequence (1.2) in Theorem 1.2. In particular, $\Gamma_\mathcal{Q}$ is of order 59520.

Proposition 4.3. *We have* $\min(L_\mathcal{Q}) = 6$.

Proof. It is easy to calculate a basis of $L_\mathcal{Q}$ and the associated Gram matrix. Therefore the minimal norm $\min(L_\mathcal{Q})$ can be calculated by, for example, the function `ShortestVectors` of `GAP` [6]. However, this method did not give an answer in reasonable time. Hence we adopt the following method.

For $n \in D_R = \mathbb{Z}/35\mathbb{Z}$, we put

$$\lambda(n) := \min \{\, x^2 \mid x \in R^\vee,\ x \bmod R = n \,\}.$$

Then the values of $\lambda(n)$ are calculated as in Table 4.2. For a codeword

$$w = [\, n_\infty, n_0 \mid n_1, n_{3^2}, \dots, n_{3^{28}} \mid n_3, n_{3^3}, n_{3^5}, \dots, n_{3^{29}} \,] \ \in \ (\mathbb{Z}/35\mathbb{Z})^{32},$$

we put

$$\mu(w) := \lambda(n_\infty) + \lambda(n_0) + \sum_{k=0}^{14} \lambda(n_{3^{2k}}) + \sum_{k=0}^{14} \lambda(n_{3^{2k+1}}).$$

In order to prove Proposition 4.3, it is enough to show that there exists no non-zero codeword w in $\mathcal{Q}$ with $\mu(w) \leq 4$.

We introduce an ordering $\prec$ on $\mathbb{Z}/35\mathbb{Z}$ by

$$m \prec m' \iff \tilde{m} < \tilde{m}',$$

where $\tilde{m} \in \mathbb{Z}$ is the representative of $m \in \mathbb{Z}/35\mathbb{Z}$ satisfying $0 \leq \tilde{m} < 35$. For $n \in \mathbb{Z}/35\mathbb{Z}$, we denote by $\mathrm{Stab}(n)$ the stabilizer subgroup of n in $H(R) = \{\pm 1, \pm 6\} \subset (\mathbb{Z}/35\mathbb{Z})^\times$. Then, for each codeword w of $\mathcal{Q}$, the orbit

$$w^{\overline{\Gamma}_{\mathcal{Q}}} := \{\, w^\gamma \ \mid \ \gamma \in \overline{\Gamma}_{\mathcal{Q}} \,\}$$

of w under the action of $\overline{\Gamma}_{\mathcal{Q}}$ contains at least one element

$$[\, n_\infty, n_0, n_1, n_9, \dots, n_3, n_{27}, \dots \,]$$

with the following properties:

(i) $\lambda(n_\infty) \geq \lambda(n_\nu)$ for any $\nu \in \mathbb{F}_p$,
(ii) $n_\infty \succeq k n_\infty$ for any $k \in H(R) = \{\pm 1, \pm 6\}$,
(iii) $\lambda(n_0) \geq \lambda(n_\nu)$ for any $\nu \in \mathbb{F}_p^\times$,
(iv) $n_0 \succeq k n_0$ for any $k \in \mathrm{Stab}(n_\infty)$,
(v) $\lambda(n_1) \geq \lambda(n_{3^{2k}})$ for $k = 1, \dots, 14$, and if $\lambda(n_1) = \lambda(n_{3^{2k}})$, then $n_1 \succeq n_{3^{2k}}$,
(vi) $n_1 \succeq k n_1$ for any $k \in \mathrm{Stab}(n_\infty) \cap \mathrm{Stab}(n_0)$.

By backtrack searching, we look for a non-zero codeword satisfying $\mu(w) \leq 4$ and the properties (i)-(vi), and confirm that there exist no such codewords in $\mathcal{Q}$. (The arrangement (4.2) of the points of $\mathbb{P}^1(\mathbb{F}_p)$ is convenient for this backtrack searching.) This task was carried out by distributed computation on eight CPUs of 3 GHz. It took us about 75 days. □

Thus Theorem 1.2 is proved, except for the fact that $\Gamma_{\mathcal{Q}}$ is of index 2 in $\mathrm{O}(L_{\mathcal{Q}})$.

5. Short vectors of $L_{\mathcal{Q}}$

In this section, we prove Proposition 1.3, and complete the proof of Theorem 1.2 by showing $|\mathrm{O}(L_{\mathcal{Q}})| = 119040$.

By the theory of modular forms (see, for example, [15, Chapter 7]), we see that the theta function of $L_{\mathcal{Q}}$ is equal to

$$\sum_{v \in L_{\mathcal{Q}}} q^{v^2/2} = 1 + 2611200\, q^3 + 19525860480\, q^4 + 19715393260800\, q^5 + \cdots .$$

In particular, the size of the set $\mathcal{S}$ of vectors $v \in L_{\mathcal{Q}}$ of square-norm $v^2 = 6$ is 2611200. We calculate the set $\mathcal{S}$ and its orbit decomposition by $\Gamma_{\mathcal{Q}}$ by the following random search method. The result is given in Table 5.1, and presented more explicitly in [17].

Random search method. Let G be the Gram matrix of $L_{\mathcal{Q}}$. We set

$$\mathcal{S} = \{\,\}, \quad \mathcal{O} = \{\,\}.$$

size of an orbit	128	3968	11904	19840	59520
number of orbits	2	4	3	6	41

TABLE 5.1. Orbit decomposition of $\mathcal{S}$ by $\Gamma_{\mathcal{Q}}$

While $|\mathcal{S}| \leq 2611200$, we do the following calculation. Let $U \in \mathrm{GL}_{64}(\mathbb{Z})$ be a random unimodular matrix of size 64 with integer components. We apply the LLL algorithm by Lenstra, Lenstra and Lovász [10] (see also [3, Chapter 2]) to

$$ {}^{U}G := U \cdot G \cdot {}^{T}U $$

with the sensitivity parameter 1. Suppose that we find a vector $v' \in \mathbb{Z}^{64}$ such that $v' \cdot {}^{U}G \cdot {}^{T}v' = 6$. Then $v := v' \cdot U$ is a vector of square-norm 6 in $L_{\mathcal{Q}}$. If v is not yet in $\mathcal{S}$, then we append its orbit $o := \{v^{\gamma} \,|\, \gamma \in \Gamma_{\mathcal{Q}}\}$ to $\mathcal{S}$, and add the set o to $\mathcal{O}$. When $|\mathcal{S}|$ reaches 2611200, the set $\mathcal{S}$ is equal to the set of vectors in $L_{\mathcal{Q}}$ of square-norm 6 and $\mathcal{O}$ gives the orbit decomposition of $\mathcal{S}$ by $\Gamma_{\mathcal{Q}}$.

The set $\mathcal{S}$ is decomposed into 56 orbits by $\Gamma_{\mathcal{Q}}$. We choose an element $v^{(i)}$ from each orbit o_i for $i = 1, \ldots, 56$. Let $\varepsilon_1, \ldots, \varepsilon_8$ be the standard basis of $E_8(3)$. We have $\varepsilon_i^2 = 6$ for $i = 1, \ldots, 8$. If $L_{\mathcal{Q}}$ contained a sublattice isomorphic to $E_8(3)$, then there would exist an embedding

$$ \iota \colon \{\varepsilon_1, \ldots, \varepsilon_8\} \hookrightarrow \mathcal{S} $$

that preserves the intersection form. By the action of $\Gamma_{\mathcal{Q}}$, we can assume that $\iota(\varepsilon_1)$ is equal to the representative element $v^{(i)}$ of some orbit o_i. By backtrack searching, we confirm that there exists no such embedding ι. Thus Proposition 1.3 is proved.

For $v \in \mathcal{S}$, we define its *type* $\tau(v)$ by

$$ \tau(v) := [\, t_0(v),\ t_1(v),\ t_2(v),\ t_3(v),\ t_6(v)\,], $$

where $t_m(v)$ is the size of the set

$$ \{\ x \in \mathcal{S}\ \mid\ \langle x, v\rangle = m\ \}. $$

Then we have $t_6(v) = 1$ and

$$ t_0(v) + 2(\, t_1(v) + t_2(v) + t_3(v) + t_6(v)\,) = 2611200 $$

for any $v \in \mathcal{S}$. The set $\mathcal{S}$ is decomposed into the disjoint union

$$ \mathcal{S} \ = \bigsqcup \mathcal{S}_{\tau}, \quad \text{where } \mathcal{S}_{\tau} := \{v \in \mathcal{S} \,|\, \tau(v) = \tau\}, $$

according to the types, and each $\mathcal{S}_{\tau}$ is a disjoint union of orbits o_i of the action of $\Gamma_{\mathcal{Q}}$. In Table 5.2, we give the list of all possible types τ and the size of each set $\mathcal{S}_{\tau}$. Note that the action of $\mathrm{O}(L_{\mathcal{Q}})$ preserves each $\mathcal{S}_{\tau}$. Let $\mathcal{S}_0$ be the set of vectors of type

$$ [\ 1377392,\ 578256,\ 38343,\ 304,\ 1\ ]. $$

The size 23808 of $\mathcal{S}_0$ is minimal among all $\mathcal{S}_{\tau}$. (See the last line of Table 5.2.) This subset $\mathcal{S}_0$ is a union of two orbits o_{k_1} and o_{k_2} of size 11904. By direct calculation, we confirm the following fact:

(5.1) For each $v \in \mathcal{S}_0$, there exist exactly seven vectors v' in $\mathcal{S}_0$ such that $\langle v, v'\rangle = -3$.

We find a sequence $V_0 = [v_1, \ldots, v_{64}]$ of vectors v_i of $\mathcal{S}_0$ satisfying the following:

t_0	t_1	t_2	t_3	t_6	the size of $\mathcal{S}_\tau$
1368552	583866	37323	134	1	39680
1370112	582876	37503	164	1	39680
1371152	582216	37623	184	1	119040
1371880	581754	37707	198	1	59520
1372088	581622	37731	202	1	476160
1372192	581556	37743	204	1	119040
1372504	581358	37779	210	1	119040
1372608	581292	37791	212	1	119040
1372816	581160	37815	216	1	59520
1372920	581094	37827	218	1	158720
1373128	580962	37851	222	1	59520
1373232	580896	37863	224	1	59520
1373440	580764	37887	228	1	59520
1373648	580632	37911	232	1	119040
1373752	580566	37923	234	1	119040
1373960	580434	37947	238	1	59520
1374168	580302	37971	242	1	119040
1374272	580236	37983	244	1	59520
1374480	580104	38007	248	1	75648
1374584	580038	38019	250	1	59520
1374688	579972	38031	252	1	59520
1374896	579840	38055	256	1	178560
1375000	579774	38067	258	1	59520
1375104	579708	38079	260	1	119040
1376872	578586	38283	294	1	71424
1377392	578256	38343	304	1	23808

TABLE 5.2. Decomposition of $\mathcal{S}$ by types

(i) $\langle v_i, v_j \rangle = -3$ if and only if $|i-j| = 1$, and
(ii) $v_1, \ldots, v_{64}$ form a basis of $L_{\mathcal{Q}}$.

See [17] for the explicit vector representations of these vectors $v_1, \ldots, v_{64}$. We then enumerate all the sequences $V' = [v'_1, \ldots, v'_{64}]$ of vectors of $\mathcal{S}_0$ such that

(a) v'_1 is either $v^{(k_1)}$ or $v^{(k_2)}$, where $v^{(k_\nu)}$ is the fixed representative of the orbit o_{k_ν} contained in $\mathcal{S}_0$, and
(b) $\langle v_i, v_j \rangle = \langle v'_i, v'_j \rangle$ for $i, j = 1, \ldots, 64$.

Then we obtain exactly 10 sequences $V_1, \ldots, V_{10}$ with these properties. Since the action of $\mathrm{O}(L_{\mathcal{Q}})$ preserves $\mathcal{S}_0 = o_{k_1} \sqcup o_{k_2}$ and the action of $\Gamma_{\mathcal{Q}}$ is transitive on each of o_{k_1} and o_{k_2}, we see that, for each $g \in \mathrm{O}(L_{\mathcal{Q}})$, there exists an element $h \in \Gamma_{\mathcal{Q}}$ such that

$$V_0^{gh} = [v_1^{gh}, \ldots, v_{64}^{gh}] \in \{V_1, \ldots, V_{10}\}.$$

For each $i = 1, \ldots, 10$, we calculate the matrix $g_i \in \mathrm{O}(L_{\mathcal{Q}} \otimes \mathbb{Q})$ such that $V_0^{g_i} = V_i$. It turns out that these g_i preserve $L_{\mathcal{Q}} \subset L_{\mathcal{Q}} \otimes \mathbb{Q}$, and hence we have $g_i \in \mathrm{O}(L_{\mathcal{Q}})$. By construction, the group $\mathrm{O}(L_{\mathcal{Q}})$ is generated by $\Gamma_{\mathcal{Q}}$ together with $g_1, \ldots, g_{10}$.

We calculate the order of $|\mathrm{O}(L_{\mathcal{Q}})|$. It turns out that

$$|\mathrm{O}(L_{\mathcal{Q}})| = 119040 = 2|\Gamma_{\mathcal{Q}}|.$$

Thus the proof of Theorem 1.2 is completed.

Remark 5.1. If $g \in \mathrm{O}(L_{\mathcal{Q}})$ is not contained in $\Gamma_{\mathcal{Q}}$, then g does not preserve the sublattice $R^{32} \subset L_{\mathcal{Q}}$, and hence does not induce an automorphism of the code $\mathcal{Q}$.

6. Another construction of $L_{\mathcal{Q}}$

Let o_1 and o_2 be the two orbits of size 128 in $\mathcal{S}$ (see Table 5.1). Let $\langle o_1\rangle$ and $\langle o_2\rangle$ be the sublattices of $L_{\mathcal{Q}}$ generated by o_1 and by o_2, respectively. It is easily confirmed that both $\langle o_1\rangle$ and $\langle o_2\rangle$ are of rank 64 and that

$$\langle o_1\rangle + \langle o_2\rangle = L_{\mathcal{Q}}. \tag{6.1}$$

For simplicity, we put

$$E := \{e_1^{(1)}, e_2^{(1)}, \dots, e_1^{(32)}, e_2^{(32)}\},$$

where $e_1^{(i)}$ and $e_2^{(i)}$ are the standard basis of the ith component of R^{32} satisfying (4.1). One of the two orbits of size 128, say o_1, is equal to the union of E and $-E$. For each $e_\nu^{(i)} \in E \subset o_1$, there exists a unique vector $f_{+\nu}^{(i)} \in o_2$ (resp. $f_{-\nu}^{(i)} \in o_2$) such that $\langle e_\nu^{(i)}, f_{+\nu}^{(i)}\rangle = 2$ (resp. $\langle e_\nu^{(i)}, f_{-\nu}^{(i)}\rangle = -2$). The mapping

$$e_1^{(i)} \mapsto f_{+1}^{(i)}, \quad e_2^{(i)} \mapsto f_{-1}^{(i)}$$

induces an isometry

$$\rho\colon \langle o_1\rangle \xrightarrow{\sim} \langle o_2\rangle,$$

and hence gives rise to $\rho \otimes \mathbb{Q} \in \mathrm{O}(R^{32} \otimes \mathbb{Q})$.

Remark 6.1. The orthogonal transformation $\rho \otimes \mathbb{Q}$ of $R^{32} \otimes \mathbb{Q}$ does not preserve $L_{\mathcal{Q}} \subset R^{32} \otimes \mathbb{Q}$. Indeed, the order of $\rho \otimes \mathbb{Q} \in \mathrm{O}(R^{32} \otimes \mathbb{Q})$ is infinite.

The matrix representation M_ρ of $\rho \otimes \mathbb{Q}$ with respect to the basis E of $R^{32} \otimes \mathbb{Q}$ is related to generalized quadratic residue codes as follows. Let T be the 32×32 matrix whose rows and columns are indexed by $\mathbb{P}^1(\mathbb{F}_{31})$ sorted as in (4.2), and whose (μ, ν)th component is the string

$$\begin{cases} \texttt{"a"} & \text{if } \mu = \infty \text{ and } \nu \neq \infty, \\ \texttt{"b"} & \text{if } \mu = \infty \text{ and } \nu = \infty, \\ \texttt{"d"} & \text{if } \mu = \nu \neq \infty, \\ \texttt{"s"} & \text{if } \mu \neq \infty,\ \nu \neq \infty,\ \mu \neq \nu, \text{ and } \chi_{31}(\mu - \nu) = 1, \\ \texttt{"t"} & \text{if } \mu \neq \infty,\ \nu \neq \infty,\ \mu \neq \nu, \text{ and } \chi_{31}(\mu - \nu) = -1, \\ \texttt{"e"} & \text{if } \mu \neq \infty \text{ and } \nu = \infty\,; \end{cases}$$

that is, T is the template matrix of quadratic residue codes of length 32. We put

$$m_a := \frac{1}{35}\begin{bmatrix} 1 & -6 \\ 6 & -1 \end{bmatrix}, \quad m_b := \frac{1}{35}\begin{bmatrix} 12 & -2 \\ 2 & -12 \end{bmatrix}, \quad m_d := \frac{1}{35}\begin{bmatrix} 12 & -2 \\ 2 & -12 \end{bmatrix},$$
$$m_s := \frac{1}{35}\begin{bmatrix} -6 & 1 \\ -1 & 6 \end{bmatrix}, \quad m_t := \frac{1}{35}\begin{bmatrix} 6 & -1 \\ 1 & -6 \end{bmatrix}, \quad m_e := \frac{1}{35}\begin{bmatrix} -1 & 6 \\ -6 & 1 \end{bmatrix}.$$

Proposition 6.2. *The matrix representation M_ρ of $\rho \otimes \mathbb{Q}$ with respect to the basis E of $R^{32} \otimes \mathbb{Q}$ is obtained from the template matrix T by substituting* `"a"` *with m_a,* `"b"` *with m_b,* `"d"` *with m_d,* `"s"` *with m_s,* `"t"` *with m_t, and* `"e"` *with m_e.*

By (6.1), we obtain another method of construction of $L_{\mathcal{Q}}$ as follows.

Proposition 6.3. *The lattice $L_{\mathcal{Q}}$ is generated by E and E^ρ in $R^{32} \otimes \mathbb{Q}$.*

Note added on 2018/05/04: Masaaki Harada confirmed $\min(L_{\mathcal{Q}}) = 6$ by a direct computation using `Magma`. It took about 27 days. We thank Professor Masaaki Harada for this heavy computation.

References

[1] Alexis Bonnecaze, Patrick Solé, and A. R. Calderbank. Quaternary quadratic residue codes and unimodular lattices. *IEEE Trans. Inform. Theory*, 41(2):366–377, 1995.

[2] Robin Chapman and Patrick Solé. Universal codes and unimodular lattices. *J. Théor. Nombres Bordeaux*, 8(2):369–376, 1996.

[3] Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.

[4] J. H. Conway and N. J. A. Sloane. *Sphere packings, lattices and groups*, volume 290 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, New York, third edition, 1999.

[5] Philippe Gaborit. Construction of new extremal unimodular lattices. *European J. Combin.*, 25(4):549–564, 2004.

[6] The GAP Group. GAP - Groups, Algorithms, and Programming. Version 4.7.9; 2015 (http://www.gap-system.org).

[7] Masaaki Harada and Masaaki Kitazume. $\mathbb{Z}_4$-code constructions for the Niemeier lattices and their embeddings in the Leech lattice. *European J. Combin.*, 21(4):473–485, 2000.

[8] Masaaki Harada, Masaaki Kitazume, and Michio Ozeki. Ternary code construction of unimodular lattices and self-dual codes over $\mathbb{Z}_6$. *J. Algebraic Combin.*, 16(2):209–223, 2002.

[9] Masaaki Harada and Tsuyoshi Miezaki. On the existence of extremal Type II $\mathbb{Z}_{2k}$-codes. *Math. Comp.*, 83(287):1427–1446, 2014.

[10] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász. Factoring polynomials with rational coefficients. *Math. Ann.*, 261(4):515–534, 1982.

[11] Gabriele Nebe. Some cyclo-quaternionic lattices. *J. Algebra*, 199(2):472–498, 1998.

[12] Gabriele Nebe and Neil Sloane. A Catalogue of Lattices. `http://www.math.rwth-aachen.de/~Gabriele.Nebe/LATTICES/`. Accessed: 2017-03-01.

[13] V. V. Nikulin. Integer symmetric bilinear forms and some of their geometric applications. *Izv. Akad. Nauk SSSR Ser. Mat.*, 43(1):111–177, 238, 1979. English translation: Math USSR-Izv. 14 (1979), no. 1, 103–167 (1980).

[14] H.-G. Quebbemann. A construction of integral lattices. *Mathematika*, 31(1):137–140, 1984.

[15] J.-P. Serre. *A course in arithmetic*. Springer-Verlag, New York-Heidelberg, 1973. Translated from the French, Graduate Texts in Mathematics, No. 7.

[16] Ichiro Shimada. On elliptic $K3$ surfaces. *Michigan Math. J.*, 47(3):423–446, 2000.

[17] Ichiro Shimada. An even extremal lattices of rank 64: computational data. `http://www.math.sci.hiroshima-u.ac.jp/~shimada/lattices`, 2017.

Department of Mathematics, Graduate School of Science, Hiroshima University, 1-3-1 Kagamiyama, Higashi-Hiroshima, 739-8526 JAPAN

E-mail address: `ichiro-shimada@hiroshima-u.ac.jp`