LECTURE NOTES
"COMPUTATIONAL TOOLS IN THE STUDY OF $K3$ SURFACES"

ICHIRO SHIMADA

Abstract. We present various computational tools that are useful in the study of $K3$ surfaces.

1. An example

We work over the complex number field $\mathbb{C}$. A $K3$ surface is a compact complex surface X such that

(i) $\pi_1(X) = 1$, and
(ii) there exists a nowhere vanishing holomorphic 2-form ω_X on X.

$K3$ surfaces form an important class in the Enriques-Kodaira classification of compact complex surfaces, a role that is parallel to the role played by elliptic curves in the classification of compact Riemann surfaces. $K3$ surfaces are studied from various points of view, not only in algebraic and arithmetic geometry, but also in, for example, theoretical physics.

In this lecture, we study *algebraic* $K3$ surface, that is, $K3$ surfaces that admit embeddings in projective spaces. We study the geometry of this $K3$ surface X by means of lattice theory and with the aid of a computer. During this investigation, we introduce some computational tools in lattice theory that are also useful in other contexts. In particular, we are interested in the automorphism group

$$\mathrm{Aut}(X) = \mathrm{Bir}(X),$$

where $\mathrm{Bir}(X)$ is the group of self-birational maps of X. The equality follows from the fact that X is minimal, that is, X contains no (-1)-curves.

We start with a concrete example. Let $\overline{X} \to \mathbb{P}^2$ be the double covering of the projective plane $\mathbb{P}^2$ defined by

$$w^2 = f(x, y, z)^2 + g(x, y, z)^3,$$

where f and g are general homogeneous polynomials on $\mathbb{P}^2$ of degree 3 and 2, respectively. The branch curve

$$B := \{f^2 + g^3 = 0\} \subset \mathbb{P}^2$$

of the double covering is a curve of degree 6. The singularities of B consists of six ordinary cusps $\bar{p}_1, \dots, \bar{p}_6$, which are located at the intersection of the cubic curve $f = 0$ and the conic $g = 0$. Hence the singular locus of $\overline{X}$ consists of six rational double points $p_1, \dots, p_6$ of type A_2. Therefore the minimal resolution $X \to \overline{X}$ of $\overline{X}$ is a $K3$ surface.

By a *lattice*, we mean a free $\mathbb{Z}$-module L of finite rank with a non-degenerate symmetric bilinear form

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

We sometimes call this symmetric bilinear form the *intersection paring* or the *intersection form*. We use the same notation

$$\langle\ ,\ \rangle\colon (L\otimes\mathbb{Q}) \times (L\otimes\mathbb{Q}) \to \mathbb{Q}, \qquad \langle\ ,\ \rangle\colon (L\otimes\mathbb{R}) \times (L\otimes\mathbb{R}) \to \mathbb{R}$$

for the scalar extensions of $\langle\ ,\ \rangle$, and, for $x, y \in L\otimes\mathbb{R}$, we call the number $\langle x, y\rangle$ the *intersection number* of x and y

Let L be a lattice of rank n, and let $b_1, \dots, b_n$ be a basis of the underlying $\mathbb{Z}$-module of L. Then the lattice L is expressed by the *Gram matrix*

$$\mathrm{Gram}(L) := (\langle b_i, b_j\rangle)_{i,j=1,\dots,n}.$$

The *discriminant* of L is defined to be $|\det(\mathrm{Gram}(L))|$. Note that the discriminant does not depend on the choice of the basis $b_1, \dots, b_n$. The *signature* (s_+, s_-) of L is the signature of the real quadratic space $L\otimes\mathbb{R}$, that is, s_+ and s_- are the numbers of positive eigenvalues and negative eigenvalues of the symmetric matrix $\mathrm{Gram}(L)$.

We consider the *numerical Néron-Severi lattice*

$$S_X = H^2(X, \mathbb{Z}) \cap H^{1,1}(X)$$

of X, that is, the $\mathbb{Z}$-module of cohomology classes $[D]$ of divisors D on X equipped with the cup product.

Proposition 1.1. *The lattice S_X is of rank 13 with signature $(1, 12)$, and its discriminant is $2\cdot 3^4 = 162$.*

Remark 1.2. The fact that $s_+ = 1$ follows from Hodge index theorem, and holds for the numerical Néron-Severi lattice of any algebraic surface.

We can write generators of S_X explicitly. Let

$$\boldsymbol{h} \in S_X$$

denote the class of the pull-back of a general line of $\mathbb{P}^2$ by the double covering $X \to \overline{X} \to \mathbb{P}^2$. We have

$$\langle \boldsymbol{h}, \boldsymbol{h}\rangle = 2.$$

Recall that the singular locus of $\overline{X}$ consists of six rational double points $p_1, \dots, p_6$ of type A_2. Let $E_i^{(+)}$ and $E_i^{(-)}$ denote the exceptional curves that are contracted to the point $p_i \in \mathrm{Sing}(\overline{X})$ by the desingularization $X \to \overline{X}$. We denote their classes as follows:

$$\boldsymbol{e}_i^{(+)} := [E_i^{(+)}] \in S_X, \quad \boldsymbol{e}_i^{(-)} := [E_i^{(-)}] \in S_X.$$

Then we have

$$\langle \boldsymbol{h}, \boldsymbol{e}_i^{(\pm)}\rangle = 0,$$

and the 12 classes $\boldsymbol{e}_i^{(\pm)}$ form the dual graph of type $6A_2$. Let $\overline{\Gamma} \subset \mathbb{P}^2$ be the conic defined by $g = 0$. Then $\overline{\Gamma}$ passes through all the six cusps of B. The strict transform of $\overline{\Gamma}$ in X is a disjoint union of two smooth rational curves $\Gamma^{(+)}$ and $\Gamma^{(-)}$. We denote their classes as follows:

$$\boldsymbol{\gamma}^{(+)} := [\Gamma^{(+)}] \in S_X, \quad \boldsymbol{\gamma}^{(-)} := [\Gamma^{(-)}] \in S_X.$$

Then we have

$$\langle \boldsymbol{h}, \boldsymbol{\gamma}^{(\pm)}\rangle = 2.$$

For each $i = 1, \dots, 6$, the curve $\Gamma^{(+)}$ intersects one of $E_i^{(+)}$ or $E_i^{(-)}$, and is disjoint from the other. Interchanging the signs in $E_i^{(+)}$ and $E_i^{(-)}$ if necessary, we can assume that

$$\langle \boldsymbol{\gamma}^{(+)}, \boldsymbol{e}_i^{(+)} \rangle = 1, \quad \langle \boldsymbol{\gamma}^{(+)}, \boldsymbol{e}_i^{(-)} \rangle = 0$$

hold for $i = 1, \dots, 6$. Then we have the following:

Proposition 1.3. *The $\mathbb{Q}$-vector space $S_X \otimes \mathbb{Q}$ is generated by the classes*

$$\boldsymbol{h}, \ \ \boldsymbol{e}_1^{(+)}, \boldsymbol{e}_1^{(-)}, \quad \dots \quad, \boldsymbol{e}_6^{(+)}, \boldsymbol{e}_6^{(-)}.$$

The lattice S_X is generated by these classes and the class $\boldsymbol{\gamma}^{(+)}$.

Therefore a vector v of $S_X \otimes \mathbb{Q}$ is specified by the intersection numbers

$$\langle v, \boldsymbol{h} \rangle, \ \ \langle v, \boldsymbol{e}_1^{(+)} \rangle, \ \ \langle v, \boldsymbol{e}_1^{(-)} \rangle, \quad \dots \quad, \langle v, \boldsymbol{e}_6^{(+)} \rangle, \ \ \langle v, \boldsymbol{e}_6^{(-)} \rangle. \tag{1.1}$$

Our main result is as follows:

Theorem 1.4. *The automorphism group* $\mathrm{Aut}(X)$ *of X is generated by* 283 *involutions and* 180 *elements of infinite order.*

We can describe these generators explicitly and geometrically.

Note that, for a $K3$ surface X, we have a natural identification $\mathrm{Pic}(X) \cong S_X$. Hence an isomorphism class of a line bundle $\mathcal{L}$ on X is specified by the intersection numbers (1.1) with $v = c_1(\mathcal{L})$.

A *double covering* $\pi \colon X \to \mathbb{P}^2$ is a generically finite morphism of degree 2. The $K3$ surface X has many double coverings other than the orininal defining double covering $\pi_0 \colon X \to \mathbb{P}^2$ given by the equation $w^2 = f^2 + g^3$. We put

$$h(\pi) := [\pi^*(\mathcal{O}_{\mathbb{P}^2}(1))] \ \in \ S_X.$$

(For example, we have $h(\pi_0) = \boldsymbol{h}$.) The complete linear system $|\mathcal{L}_{h(\pi)}|$ of the line bundle $\mathcal{L}_{h(\pi)}$ whose class is $h(\pi)$ gives the morphism $\pi \colon X \to \mathbb{P}^2$. Hence the double covering π is specified by the class $h(\pi)$. Since a $K3$ surface is minimal, the birational involution of X over $\mathbb{P}^2$ associated with a double covering $\pi \colon X \to \mathbb{P}^2$ induces an involution, which we will denote by

$$i(\pi) \ \in \ \mathrm{Aut}(X).$$

An *elliptic fibration* is a morphism $\phi \colon X \to \mathbb{P}^1$ whose general fiber is a curve of genus 1. A *Jacobian fibration* is an elliptic fibration $\phi \colon X \to \mathbb{P}^1$ with a distinguished section $s \colon \mathbb{P}^1 \to X$, which is called the *zero section*. The generic fiber of a Jacobian fibration is an elliptic curve over the function field $\mathbb{C}(\mathbb{P}^1)$ of the base curve with the origin given by the zero section. Hence the set of sections of a Jacobian fibration form an abelian group $\mathrm{MW}(\phi, s)$, which is called the *Mordell-Weil group*. A Jacobian fibration $\phi \colon X \to \mathbb{P}^1$ with the zero section $s \colon \mathbb{P}^1 \to X$ is specified by the classes

$$f = [\text{a fiber of } \phi] \in S_X, \quad z = [s(\mathbb{P}^1)] \in S_X,$$

and an element $\tau \in \mathrm{MW}(\phi, s)$ is specified by the class

$$t = [\tau(\mathbb{P}^1)] \in S_X.$$

The Mordell-Weil group $\mathrm{MW}(\phi, s)$ acts on X by translations $x \mapsto x + \tau$ on the generic fiber. We can specify the automorphism $x \mapsto x + \tau$ by giving the triple (f, z, t) of vectors of S_X.

Theorem 1.5. *The automorphism group* $\mathrm{Aut}(X)$ *of* X *is generated by*

$$1+90+2\times 6+30\times 6$$

involutions associated with double coverings $X \to \mathbb{P}^2$*, and* 30×6 *elements of infinite order obtained as translations of Jacobian fibrations* $X \to \mathbb{P}^1$*.*

Remark 1.6. The generators given in Theorem 1.5 are described explicitly by giving the vectors $h(\pi)$ and the triples (f, z, t) of vectors that specify the automorphisms. For example, one of the 283 involutions associated with double coverings $X \to \mathbb{P}^2$ is $i(\pi_0)$. One of the 30×6 involutions is equal to $i(\pi)$, where the double covering $\pi\colon X \to \mathbb{P}^2$ is given by the class $h = h(\pi)$ satisfying $\langle h, \boldsymbol{h}\rangle = 14$ and

$$(\langle h, \boldsymbol{e}_i^{(+)}\rangle, \langle h, \boldsymbol{e}_i^{(-)}\rangle) = \begin{cases} (5,4) & \text{if } i=1,\\ (1,0) & \text{if } i=2,\\ (0,5) & \text{if } i\in\{3,4\},\\ (4,0) & \text{if } i\in\{5,6\}.\end{cases}$$

One of the 30×6 elements of infinite order is associated with

$$(f, z, t) = (\ \boldsymbol{e}_1^{(-)} + \boldsymbol{e}_2^{(-)} + \boldsymbol{e}_5^{(-)} + \boldsymbol{e}_6^{(-)} + 2\boldsymbol{\gamma}^{(-)},\ \ \boldsymbol{e}_1^{(+)},\ \ \boldsymbol{e}_2^{(+)}\ ).$$

We also prove the following.

Corollary 1.7. *The automorphism group* $\mathrm{Aut}(X)$ *acts on the set of smooth rational curves on* X *transitively.*

2. An algorithm on a graph

We prove these results by the following standard algorithm in combinatorial group theory.

Remark 2.1. Strictly speaking, the term "algorithm" means a computational procedure that terminates for every input. By abuse of language, we use this term to denote a computational procedure that may fail to terminate.

Let (V, E) be a simple non-oriented connected graph, where V is the set of vertices and E is the set of edges, which is a set of non-ordered pairs of distinct elements of V:

$$E \subset \binom{V}{2}.$$

(Hence (V, E) has no loops and no multiple edges.) The set V may be infinite. The assumption that (V, E) be connected is important.

Suppose that a group G acts on (V, E) from the right. We assume that (V, E) and G have the following *local effectiveness properties.*

(VE-1) For any vertex $v \in V$, the set $\{\, v' \in V \mid \{v, v'\} \in E \,\}$ of vertices adjacent to v is finite, and can be calculated effectively.

(VE-2) For any vertices $v, v' \in V$, we can determine effectively whether the set

$$T_G(v, v') := \{\, g \in G \mid v^g = v' \,\}$$

is empty or not, and when it is non-empty, we can calculate an element of $T_G(v, v')$.

(VE-3) For any vertex $v \in V$, the stabilizer subgroup $T_G(v, v)$ of v in G is finitely generated, and a finite set of generators of $T_G(v, v)$ can be calculated effectively.

We define the *G-equivalence relation* $\sim$ on V by

$$v \sim v' \iff T_G(v, v') \neq \emptyset.$$

Therefore we have two relations on V, the adjacency relation of the graph and the G-equivalence relation.

Suppose that V_0 is a non-empty finite subset of V with the following properties.

(V_0-1) If $v, v' \in V_0$ are distinct, then v and v' are not G-equivalent.
(V_0-2) If a vertex $v \in V$ is adjacent to a vertex in V_0, then v is G-equivalent to a vertex in V_0.

We put

$$\widetilde{V}_0 := \{\, v \in V \mid v \text{ is adjacent to a vertex in } V_0 \,\}.$$

Then, for each $v \in \widetilde{V}_0$, there exists a unique vertex $v' \in V_0$ that is G-equivalent to v, and we choose an element $h(v) \in T_G(v, v')$. (If $v \in V_0$, then we have $v' = v$ and we can choose $1 \in G$ as $h(v)$.) We then put

$$\mathcal{H} := \{\, h(v) \mid v \in \widetilde{V}_0 \,\}.$$

We fix an element $v_0 \in V_0$.

Proposition 2.2. *The natural mapping*

$$V_0 \hookrightarrow V \twoheadrightarrow V/\!\sim\, = V/G \tag{2.1}$$

is a bijection, and the group G is generated by the union of $\mathcal{H}$ and the stabilizer subgroup $T_G(v_0, v_0)$.

Proof. The injectivity of (2.1) follows from property (V_0-1) of V_0. The surjectivity follows from the claim below.

Let $\langle \mathcal{H} \rangle$ be the subgroup of G generated by $\mathcal{H}$. First we prove that, for any $v \in V$, there exists an element $h \in \langle \mathcal{H} \rangle$ such that $v^h \in V_0$, that is, every $\langle \mathcal{H} \rangle$-orbit $v^{\langle \mathcal{H} \rangle}$ in V intersects V_0. Let an element $v \in V$ be fixed. A sequence

$$v_{(0)}, v_{(1)}, \dots, v_{(l)} \tag{2.2}$$

of vertices is said to be a *path from V_0 to $v^{\langle \mathcal{H} \rangle}$* if $v_{(i-1)}$ and $v_{(i)}$ are adjacent for $i = 1, \dots, l$, the starting vertex $v_{(0)}$ is in V_0, and the ending vertex $v_{(l)}$ belongs to the orbit $v^{\langle \mathcal{H} \rangle}$ of the fixed vertex v under the action of $\langle \mathcal{H} \rangle$. Since (V, E) is connected and V_0 is non-empty, there exists at least one path from V_0 to $v^{\langle \mathcal{H} \rangle}$. Suppose that the sequence (2.2) is a path from V_0 to $v^{\langle \mathcal{H} \rangle}$ of length $l > 0$. Since $v_{(1)}$ is adjacent to the vertex $v_{(0)}$ in V_0, we have $v_{(1)} \in \widetilde{V}_0$ and there exists an element $h_1 := h(v_{(1)}) \in \mathcal{H}$ that maps $v_{(1)}$ to an element of V_0. Then

$$v_{(1)}^{h_1}, \dots, v_{(l)}^{h_1}$$

is a path from V_0 to $v^{\langle \mathcal{H} \rangle}$ of length $l - 1$. Thus we obtain a path from V_0 to $v^{\langle \mathcal{H} \rangle}$ of length 0, which implies the claim.

Suppose that $g \in G$. By the claim, there exists an element $h \in \langle \mathcal{H} \rangle$ such that $v_0^{gh} \in V_0$. By property (V_0-1) of V_0, we have $v_0 = v_0^{gh}$ and hence $gh \in T_G(v_0, v_0)$. Therefore G is generated by the union of $\mathcal{H}$ and $T_G(v_0, v_0)$. $\square$

To obtain V_0 and $\mathcal{H}$, we employ Procedure 2.1. This procedure terminates if and only if $|V/G| < \infty$.

```
Initialize V_0 := [v_0], H := {}, and i := 0.
while i < |V_0| do
    Let v_i be the (i+1)st entry of the list V_0.
    Let A(v_i) be the set of vertices adjacent to v_i.
    for each vertex v' in A(v_i) do
        Set flag := true.
        for each v'' in V_0 do
            if T_G(v', v'') ≠ ∅ then
                Add an element h of T_G(v', v'') to H.
                Replace flag by false.
                Break from the innermost for–loop.
        if flag = true then
            Append v' to the list V_0 as the last entry.
    Replace i by i + 1.
```

PROCEDURE 2.1. A computational procedure on a graph

3. Calculation of orthogonal groups

In this section, to introduce some important algorithms, we consider the following problem:

Problem 3.1. Let a lattice L be given by means of the Gram matrix with respect to a certain basis $b_1, \dots, b_n$. Suppose that L is positive-definite, that is, we have $\langle v, v\rangle > 0$ for all non-zero vectors $v \in L$. Calculate the finite group $\mathrm{O}(L)$ of all isometries of L.

3.1. **backtrack search.** A naive method to calculate $\mathrm{O}(L)$ is as follows. We compute the sets

$$V_i := \{\, v \in L \mid \langle v, v\rangle = \langle b_i, b_i\rangle \,\}$$

for $i = 1, \dots, n$, and let V be the union of $V_1, \dots, V_n$. The isometries of L are in one-to-one correspondence with the set of mappings φ from $\{b_1, \dots, b_n\}$ to V such that $\varphi(b_i) \in V_i$ and that

$$\langle \varphi(b_i), \varphi(b_j)\rangle = \langle b_i, b_j\rangle \qquad \text{for all } i, j \text{ with } i < j.$$

We enumerate all these mappings by the *backtrack search*.

Definition 3.2. For k with $0 \le k \le n$, a *partial solution* of size k is a mapping ϕ from $\{b_1, \dots, b_k\}$ to V that preserve the intersection numbers, that is, we have $\phi(b_i) \in V_i$ for $i \le k$ and that

$$\langle \phi(b_i), \phi(b_j)\rangle = \langle b_i, b_j\rangle \qquad \text{for all } i, j \text{ with } i < j \le k.$$

A *full solution* is a partial solution of size n.

We set the list `OL` of all full solutions to be the empty list:

$$\texttt{OL} := [\ ].$$

We then input the partial solution ϕ_0 of size 0 to the procedure `Extend` given in 3.1, which takes a partial solution as an input: When the whole procedure terminates, the list `OL` gives the set of all elements of the group $\mathrm{O}(L)$.

```
procedure Extend (a partial solution φ of size k)
    if k = n then
        Add φ to the list OL;
    else
        for each v in V_{k+1} do
            if ⟨φ(b_i), v⟩ = ⟨b_i, b_{k+1}⟩ for i = 1, ..., k then
                Extend φ to a partial solution φ' of size k + 1 by
                    φ'(b_i) = φ(b_i) for i ≤ k,   φ'(b_{k+1}) = v,
                and input φ' to Extend
```

PROCEDURE 3.1. Backtrack search

Remark 3.3. All partial solutions form a tree such that ϕ' is a descendant of ϕ if and only if ϕ' is an extension of ϕ. The backtrack search above collects the full solutions by walking through all over this tree.

We have two difficulties.

(1) In general, the enumeration of vectors v with a fixed norm $\langle v, v\rangle$ in a positive-definite lattice is difficult.
(2) The tree of partial solutions can be very large, and usually contains many branches that do not extend to a full solution.

3.2. LLL**-reduced basis.** Let $\mathbb{R}^n$ be the n-dimensional real vector space with the standard inner product. A subset L of $\mathbb{R}^n$ is called an $\mathbb{R}$-*lattice* if there exist linearly independent vectors $b_1, \dots, b_n$ of $\mathbb{R}^n$ such that

$$L = \mathbb{Z}b_1 + \cdots + \mathbb{Z}b_n.$$

These vectors $b_1, \dots, b_n$ are called a basis of L. The restriction of the standard inner product of $\mathbb{R}^n$ to L gives a non-degenerate symmetric bilinear form

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

Remark 3.4. A positive-definite lattice L of rank n can be embedded in $\mathbb{R}^n$ in such a way that the original $\mathbb{Z}$-valued intersection paring on L coincides with the restriction of the standard inner product of $\mathbb{R}^n$. Hence the notion of $\mathbb{R}$-lattices is an extension of the notion of positive-definite lattices.

Let L be an $\mathbb{R}$-lattice with a basis $b_1, \dots, b_n$. Then we have

$$\mathrm{vol}(\mathbb{R}^n/L) = |\det(B)|,$$

where B is the matrix whose row vectors are $b_1, \dots, b_n$. If L is a positive-definite lattice, then we have

$$\mathrm{vol}(\mathbb{R}^n/L) = \sqrt{\det(\mathrm{Gram}(L))}.$$

For a positive real number r, let $B_r \subset \mathbb{R}^n$ denote the closed ball of radius r with the center 0, and put

$$\omega_n := (\text{the volume of } B_1) = \frac{\pi^{n/2}}{\Gamma(1+n/2)}.$$

We define the *minimal length* $\lambda_1(L)$ of vectors of L by

$$\lambda_1(L) := \min\{\ \sqrt{\langle v, v\rangle}\ \mid v \in L \setminus \{0\}\ \} = \min\{\ r \mid B_r \cap L \supsetneq \{0\}\ \}.$$

When r is large, we have a rough approximation

$$|B_r \cap L| \;\approx\; \omega_n r^n / \operatorname{vol}(\mathbb{R}^n/L).$$

This leads to the Gaussian heuristic:

$$\lambda_1(L) \approx \left(\frac{\operatorname{vol}(\mathbb{R}^n/L)}{\omega_n}\right)^{1/n} \approx \sqrt{\frac{n}{2\pi e}}\operatorname{vol}(\mathbb{R}^n/L)^{1/n}. \tag{3.1}$$

In fact, we have the following:

Theorem 3.5.

$$\lambda_1(L) \le 2\left(\frac{\operatorname{vol}(\mathbb{R}^n/L)}{\omega_n}\right)^{1/n}.$$

Proof. This is an easy consequence of Minkowski's convex body theorem. Consider the projection $\pi\colon \mathbb{R}^n \to \mathbb{R}^n/L$. Suppose that $\operatorname{vol}(B_r) = \omega_n r^n$ is larger than $\operatorname{vol}(\mathbb{R}^n/L)$. Then the restriction $\pi|B_r\colon B_r \to \mathbb{R}^n/L$ of π cannot be injective, and we have $x, y \in B_r$ with $x \neq y$ and $\pi(x) = \pi(y)$. Since both of $2x$ and $-2y$ belong to B_{2r}, and B_{2r} is convex, we have a non-zero lattice point $x-y \in L$ in B_{2r}. Therefore $\omega_n r^n \ge \operatorname{vol}(\mathbb{R}^n/L)$ implies $2r \ge \lambda_1(L)$. □

The following problem is called the *shortest vector problem* (SVP):

Problem 3.6. Find a non-zero vector v of L with $\sqrt{\langle v, v\rangle} = \lambda_1(L)$.

Remark 3.7. It is widely believed that SVP is computationally very hard, and many cryptosystems based on this hardness (and the hardness of related problems) have been proposed. Many people think that the main stream of the post-quantum cryptosystems will be based on SVP or related problems.

The LLL-*reduced basis* is a very useful tool in the enumeration of vectors of a given length in a positive-definite lattice.

Definition 3.8. Let $b_1, \dots, b_n$ be a basis of $\mathbb{R}^n$. The *Gram-Schmidt orthogonalization* of $b_1, \dots, b_n$ is a basis $b_1^*, \dots, b_n^*$ of $\mathbb{R}^n$ such that

$$b_i^* = b_i - \sum_{j=1}^{i-1} \mu_{ij} b_j^*, \quad \text{where} \quad \mu_{ij} = \frac{\langle b_i, b_j^*\rangle}{\langle b_j^*, b_j^*\rangle}.$$

Starting from $b_1^* = b_1$, we can easily compute the Gram-Schmidt orthogonalization of a given basis.

Definition 3.9. Let α be a parameter with $1/4 < \alpha < 1$. (Usually, we take $\alpha = 3/4$.) A basis $b_1, \dots, b_n$ of an $\mathbb{R}$-lattice L is said to be LLL-*reduced with parameter* α if the following hold:

(i) $|\mu_{ij}| \le 1/2$ for all i, j with $1 \le j < i \le n$, and
(ii) $|b_i^* + \mu_{i,i-1} b_{i-1}^*|^2 \ge \alpha\, |b_{i-1}^*|^2$.

Theorem 3.10. *Suppose that a basis $b_1, \dots, b_n$ of an $\mathbb{R}$-lattice L is given. Then we can find an* LLL*-reduced basis of L by an algorithm* (LLL-algorithm) *that terminates in polynomial-time.*

Theorem 3.11. *If a basis $b_1, \dots, b_n$ of an $\mathbb{R}$-lattice L is* LLL*-reduced with parameter α, then we have*

$$|b_1| \le \beta^{(n-1)/4} \operatorname{vol}(\mathbb{R}^n/L),$$

where $\beta := 4/(4\alpha - 1)$.

Thus an LLL-reduced basis is useful in finding relatively short vectors in a positive-definite lattice. (Compare the multiplicative factor $\beta^{(n-1)/4}$ with $\sqrt{n/(2e\pi)}$ in Gaussian heuristic.) Let Q be a positive-definite symmetric matrix of size n with integer entries, $b \in \mathbb{Z}^n$ a vector, and $c \in \mathbb{Z}$ a constant. We put

$$E_n(Q,b,c) := \{\, x \in \mathbb{R}^n \mid x\,Q\,{}^t x + 2\,x\,{}^t b + c \le 0 \,\},$$

which is a compact subset of $\mathbb{R}^n$, because Q is positive-definite. We consider the problem to calculate the set $E_n(Q,b,c) \cap \mathbb{Z}^n$.

Proposition 3.12. *Let* $\mathrm{pr}\colon \mathbb{R}^n \to \mathbb{R}^{n-1}$ *be the projection*

$$(x_1,\dots,x_n) \mapsto (x_1,\dots,x_{n-1}).$$

Then there exist a positive-definite symmetric matrix Q' of size $n-1$ with integer entries, a vector $b' \in \mathbb{Z}^{n-1}$, and a constant $c' \in \mathbb{Z}$ such that

$$\mathrm{pr}(E_n(Q,b,c)) = E_{n-1}(Q',b',c').$$

The data Q', b', c' can be calculated effectively from the data Q, b, c. □

Therefore we can calculate $E_n(Q,b,c) \cap \mathbb{Z}^n$ by induction on n. This algorithm is called the *Fincke-Pohst algorithm*.

For this algorithm to be fast, it is desirable that the set $E_n(Q,b,c)$ is not "elongated". Let L denote the positive-definite lattice generated by the standard basis $e_1,\dots,e_n$ of $\mathbb{Z}^n \subset \mathbb{R}^n$ and with the Gram matrix Q with respect to this basis $e_1,\dots,e_n$. Changing the basis $e_1,\dots,e_n$ of $L = \mathbb{Z}^n$ to an LLL-reduced basis of L and transforming the data Q, b, c defining $E_n(Q,b,c)$ accordingly, we can calculate $E_n(Q,b,c) \cap \mathbb{Z}^n$ much faster. This algorithm is called *Fincke-Pohst algorithm with* LLL-*preprocessing*.

Remark 3.13. The LLL stands for Lenstra–Lenstra–Lovász [4]. This notion was first introduced in developing a polynomial-time algorithm for the factorization of polynomials of one variable with coefficients in $\mathbb{Q}$. There are many other applications of LLL-reduced bases. See the books [1], [2] or [5] on details and applications of LLL-algorithm.

3.3. **The method of stabilizer-chain.** In many interesting cases, the group $\mathrm{O}(L)$ is very large, and it is practically impossible to enumerate all the elements of $\mathrm{O}(L)$. For example, the order of the orthogonal group of the Leech lattice (the Conway group Co_0) is

$$8315553613086720000 = 2^{22}\cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23 \quad\approx\quad 8.3 \times 10^{18}.$$

An idea to overcome this difficulty is to calculate only a generating set of $\mathrm{O}(L)$. Let $b_1,\dots,b_n$ be a basis of L. We put

$$b_0 := 0,$$

and consider the stabilizer subgroups

$$G_k := \{\, g \in \mathrm{O}(L) \mid b_i^g = b_i \ \text{ for } \ i = 0,\dots,k \,\}$$

for $k = 0,\dots,n$. Then we obtain a sequence of subgroups

$$\mathrm{O}(L) = G_0 \ \supset\ G_1 \ \supset\ G_2 \ \supset\ \dots\ \supset\ G_{n-1} \ \supset\ G_n = \{1\}$$

Let $\Gamma_k \subset G_k$ be a complete set of representatives of the cosets $G_{k+1}\backslash G_k$, that is, a section of the quotient mapping $G_k \to G_{k+1}\backslash G_k$. By $g \mapsto b_{k+1}^g$, the set Γ_k is canonically identified with the orbit

$$o_k := \{\, b_{k+1}^g \mid g \in G_k \,\}$$

of b_{k+1} by the stabilizer subgroup G_k of $b_1, \dots, b_k$.

Proposition 3.14. *Each element $g \in \mathrm{O}(L)$ is uniquely written as*

$$g = \gamma_{n-1} \cdots \gamma_1 \gamma_0, \tag{3.2}$$

where $\gamma_k \in \Gamma_k$ for $k = 0, \dots, n-1$. In particular, we have

$$|\mathrm{O}(L)| = \prod_{k=0}^{n-1} |\Gamma_k| = \prod_{k=0}^{n-1} |o_k|.$$

Proof. We put $g_0 := g$. Then the sequence $\gamma_0, \dots, \gamma_{n-1}$ satisfying (3.2) and $\gamma_k \in \Gamma_k$ is defined inductively by $b_{k+1}^{g_k} = b_{k+1}^{\gamma_k}$ and $g_{k+1} := g_k \gamma_k^{-1} \in G_{k+1}$. □

Definition 3.15. For $k = 0, \dots, n-1$, we denote by id_k the trivial partial solution of size k defined by $\mathrm{id}(b_i) = b_i$ for $i = 1, \dots, k$. For $v \in V_{k+1}$, let $\phi(k, v)$ denote the extension of id_k to size $k+1$ given by $\phi(k, v)(b_{k+1}) = v$.

Then $v \in V_{k+1}$ belongs to the orbit $o_{k+1} = b_{k+1}^{G_k}$ if and only if the partial solution $\phi(k, v)$ of size $k+1$ extends to a full solution, and this full solution gives a representative in G_k of the coset $G_{k+1}\backslash G_k$ corresponding to $v \in o_{k+1}$.

Remark 3.16. We have a few tricks to make the calculation faster.

(a) Let $W \subset L$ be a finite subset of small size that is invariant under the action of $\mathrm{O}(L)$. (For example, we can take as W the set of vectors $v \in L$ with $\langle v, v\rangle = l$ for a small l.) For a partial solution ϕ of size k, we define a function

$$F_{W,\phi} \colon \mathbb{Z}^k \to \mathbb{Z}_{\geq 0}$$

with a finite support by

$$F_{W,\phi}(\nu_1, \dots, \nu_k) := \text{the size of } \{\, w \in W \mid \langle w, \phi(b_i)\rangle = \nu_i \text{ for } i = 1, \dots, k \,\}.$$

Then, for a partial solution ϕ of size k to extend to a full solution, it is necessary that $F_{W,\phi} = F_{W,\mathrm{id}_k}$ holds. By this criterion, we can discard many partial solutions that do not extend to full solutions without searching for the extensions.

(b) Suppose that a subset S of Γ_k is obtained, and $v \in V_{k+1}$ a candidate. If the extension $\phi(k, v)$ of size $k+1$ of the partial solution id_k by v extends to the full solution (resp. fails to extend to the full solution), then so doses $\phi(k, v')$ for any element v' in the orbit $v^{\langle S\rangle}$ of v by the subgroup $\langle S\rangle$ of G_k. Hence, when $\langle S\rangle$ is large, we can skip many calculations.

3.4. **Application: Niemeier's classification.** A lattice L is said to be *even* if $\langle v, v\rangle \in 2\mathbb{Z}$ holds for all $v \in L$, and L is said to be *unimodular* if the Gram matrix of L is of determinant ± 1.

Theorem 3.17. *An even positive-definite unimodular lattice of rank n exists if and only if $n \equiv 0 \bmod 8$.*

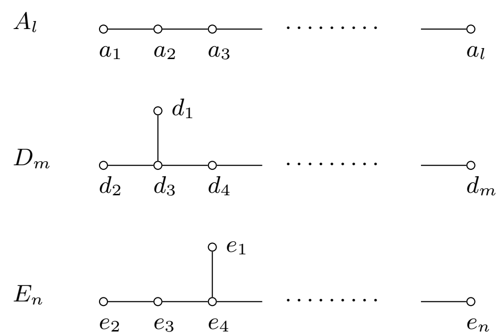

FIGURE 3.1. Connected Dynkin diagrams of type A_l, D_m, or E_n

Let $\mathcal{I}_n$ be the set of isomorphism classes of even positive-definite unimodular lattices of rank n. Then we have the *mass formula*

$$\operatorname{mass}(\mathcal{I}_n) := \sum_{L \in \mathcal{I}_n} \frac{1}{|\mathrm{O}(L)|} = \frac{|B_{n/2}|}{n} \prod_{1 \le j < n/2} \frac{|B_{2j}|}{4j},$$

which is a special case of a more general *Siegel-Minkowski mass formula*. Here B_k is the kth Bernoulli number;

$$\frac{x}{e^x - 1} = \sum_{n=0}^{\infty} \frac{B_n}{n!} x^n.$$

Using this formula and the method of calculating $|\mathrm{O}(L)|$ above, we confirm the classification of even positive-definite unimodular lattices of rank ≤ 24 computationally. (See the last chapter of the text book by Serre [10].)

Let L be an even lattice. A *root* of L is a vector $r \in L$ with $|\langle r, r\rangle| = 2$. Let L_{roots} denote the sublattice of L generated by the roots of L. We say that L is a *root lattice* if $L_{\mathrm{roots}} = L$.

Theorem 3.18. *A positive-definite root lattice has a basis consisting of roots $b_1, \dots, b_n$ such that*

(i) *if $i \ne j$, then $\langle b_i, b_j\rangle$ is either 0 or -1, and*
(ii) *the dual graph of $b_1, \dots, b_n$ is a union of connected Dynkin diagrams of type A_l, D_m, or E_n.*

Here the dual graph of the set of roots $b_1, \dots, b_n$ with $\langle b_i, b_j\rangle \in \{0, -1\}$ for $i \ne j$ is the non-oriented simple graph whose nodes are $b_1, \dots, b_n$ and whose edges are the pairs $\{b_i, b_j\}$ with $\langle b_i, b_j\rangle = -1$. The connected Dynkin diagrams of type A_l, D_m, or E_n are given in Figure 3.1. An *ADE-type* is a finite formal sum of symbols A_l, D_m, or E_n. For an ADE-type τ, we denote by $R(\tau)$ the positive-definite root lattice generated by a set of roots whose dual graph is the Dynkin diagram of type τ, where the sum of ADE-types corresponds to the disjoint union of Dynkin diagrams.

The case $n = 8$. The root lattice $R(E_8)$ is even unimodular of rank 8. We have

$$\operatorname{mass}(\mathcal{I}_8) = \frac{1}{696729600} = \frac{1}{|\mathrm{O}(R(E_8))|}.$$

Hence $\mathcal{I}_8$ consists of only one element, the isomorphism class of $R(E_8)$.

The case $n = 16$. We have

$$\mathrm{mass}(\mathcal{I}_{16}) = \frac{691}{277667181515243520000}.$$

The root lattice $R(2E_8)$ is even unimodular with

$$|\mathrm{O}(R(2E_8))| = 970864271032320000.$$

There exists another even unimodular lattice L of rank 16 such that $L_{\mathrm{roots}} \cong R(D_{16})$, that $L/L_{\mathrm{roots}} \cong \mathbb{Z}/2\mathbb{Z}$, and that

$$|\mathrm{O}(L)| = 685597979049984000.$$

By the mass formula, we see that $\mathcal{I}_{16}$ consists of the isomorphism classes of these two lattices.

The case $n = 24$. We have

$$\mathrm{mass}(\mathcal{I}_{24}) = \frac{1027637932586061520960267}{129477933340026851560636148613120000000}.$$

We can confirm the following result computationally.

Theorem 3.19 (Niemeier)**.** *The set $\mathcal{I}_{24}$ consists of 24 isomorphism classes of lattices. For 23 isomorphism classes, the lattice L contains the root lattice L_{roots} as a sublattice of finite index, and for the remaining one isomorphism class, the lattice contains no roots.*

The ADE-types of L_{roots} and the orders of $\mathrm{O}(L)$ for these 24 lattices $L = N_i$ are given in Table 3.1. Theorem 3.19 implies in particular that an even unimodular positive-definite lattice of rank 24 with no roots is unique up to isomorphism. This lattice is called the *Leech lattice*.

Remark 3.20. We can rediscover these 24 unimodular lattices from one of them (for example, the root lattice of type $3E_8$) by Kneser's p-neibors method.

4. An algorithm on a hyperbolic lattice

A lattice L of rank $n > 1$ is said to be *hyperbolic* if the signature of the real quadratic space $L \otimes \mathbb{R}$ is $(1, n-1)$.

Remark 4.1. Usually, a hyperbolic lattice is defined to be a lattice of signature $(n-1, 1)$. Our convension is suitable for the study of algebraic surfaces.

Let L be a hyperbolic lattice of rank n. Then the set

$$\{\, x \in L \otimes \mathbb{R} \mid \langle x, x\rangle > 0 \,\}.$$

has two connected components. A *positive cone* of L is one of these two connected components. Let $\mathcal{P}$ be a positive cone of L, and $\overline{\mathcal{P}}$ the closure of $\mathcal{P}$ in $L \otimes \mathbb{R}$. We will investigate the group

$$\mathrm{O}(L, \mathcal{P}) := \{\, g \in \mathrm{O}(L) \mid \mathcal{P}^g = \mathcal{P} \,\}.$$

Note that $\mathrm{O}(L) = \mathrm{O}(L, \mathcal{P}) \times \{\pm 1\}$.

Remark 4.2. The space $\mathbb{H}^{n-1} := \mathcal{P}/\mathbb{R}^{\times}_{>0}$ is a model of the hyperbolic space of dimension $n-1$, and $\mathrm{O}(L, \mathcal{P})$ is a discrete subgroup of the group of isometries of this hyperbolic space: $\mathrm{O}(L, \mathcal{P}) \subset \mathrm{Isom}(\mathbb{H}^{n-1})$.

No.	root type	$\lvert \mathrm{O}(N_i) \rvert$
1	0	$2^{22} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23$
2	$3E_8$	$2^{43} \cdot 3^{16} \cdot 5^6 \cdot 7^3$
3	$E_8 + D_{16}$	$2^{44} \cdot 3^{11} \cdot 5^5 \cdot 7^3 \cdot 11 \cdot 13$
4	$2E_7 + D_{10}$	$2^{38} \cdot 3^{12} \cdot 5^4 \cdot 7^3$
5	$E_7 + A_{17}$	$2^{27} \cdot 3^{12} \cdot 5^4 \cdot 7^3 \cdot 11 \cdot 13 \cdot 17$
6	$4E_6$	$2^{32} \cdot 3^{17} \cdot 5^4$
7	$E_6 + D_7 + A_{11}$	$2^{28} \cdot 3^{11} \cdot 5^4 \cdot 7^2 \cdot 11$
8	$D_9 + A_{15}$	$2^{31} \cdot 3^{10} \cdot 5^4 \cdot 7^3 \cdot 11 \cdot 13$
9	$3D_8$	$2^{43} \cdot 3^7 \cdot 5^3 \cdot 7^3$
10	$4D_6$	$2^{39} \cdot 3^9 \cdot 5^4$
11	$D_6 + 2A_9$	$2^{27} \cdot 3^{10} \cdot 5^5 \cdot 7^2$
12	$2D_5 + 2A_7$	$2^{31} \cdot 3^6 \cdot 5^4 \cdot 7^2$
13	$6D_4$	$2^{40} \cdot 3^9 \cdot 5$
14	$D_4 + 4A_5$	$2^{26} \cdot 3^{10} \cdot 5^4$
15	D_{24}	$2^{45} \cdot 3^{10} \cdot 5^4 \cdot 7^3 \cdot 11^2 \cdot 13 \cdot 17 \cdot 19 \cdot 23$
16	$2D_{12}$	$2^{43} \cdot 3^{10} \cdot 5^4 \cdot 7^2 \cdot 11^2$
17	$3A_8$	$2^{23} \cdot 3^{13} \cdot 5^3 \cdot 7^3$
18	$4A_6$	$2^{19} \cdot 3^9 \cdot 5^4 \cdot 7^4$
19	$6A_4$	$2^{22} \cdot 3^7 \cdot 5^7$
20	$8A_3$	$2^{31} \cdot 3^9 \cdot 7$
21	A_{24}	$2^{23} \cdot 3^{10} \cdot 5^6 \cdot 7^3 \cdot 11^2 \cdot 13 \cdot 17 \cdot 19 \cdot 23$
22	$12A_2$	$2^{19} \cdot 3^{15} \cdot 5 \cdot 11$
23	$2A_{12}$	$2^{22} \cdot 3^{10} \cdot 5^4 \cdot 7^2 \cdot 11^2 \cdot 13^2$
24	$24A_1$	$2^{34} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$

TABLE 3.1. Niemeier's list

For $v \in L \otimes \mathbb{R}$ with $\langle v, v \rangle < 0$, we put

$$(v)^{\perp} := \{\, x \in \mathcal{P} \mid \langle x, v \rangle = 0 \,\},$$

which is a real hyperplane of $\mathcal{P}$.

Definition 4.3. By a *chamber*, we mean a closed subset D of $\mathcal{P}$ such that

- D contains a non-empty open subset of $\mathcal{P}$, and
- D is defined by linear inequalities $\langle x, v_i \rangle \geq 0$ $(i \in I)$, where v_i $(i \in I)$ are vectors of $L \otimes \mathbb{Q}$ with negative norm such that the family $\{\, (v_i)^{\perp} \mid i \in I \,\}$ of hyperplanes in $\mathcal{P}$ is locally finite.

Let D be a chamber. A *wall* of D is a closed subset of D of the form $D \cap (v)^{\perp}$, where $v \in L \otimes \mathbb{R}$ is a vector with $\langle v, v \rangle < 0$, such that $(v)^{\perp}$ is disjoint from the interior of D and that $D \cap (v)^{\perp}$ contains a non-empty open subset of $(v)^{\perp}$. We say that a vector $v \in L \otimes \mathbb{R}$ defines a wall w of D if $w = D \cap (v)^{\perp}$ and $\langle x, v \rangle > 0$ for an interior point x of D. A defining vector of a wall is unique up to positive multiplicative constant.

A (-2)-*vector* is a lattice vector $r \in L$ with $\langle r, r \rangle = -2$. A (-2)-vector r defines a reflection

$$s_r \colon x \mapsto x + \langle x, r \rangle r$$

into the mirror $(r)^\perp$. We have $s_r \in \mathrm{O}(L, \mathcal{P})$. Let $W(L)$ denote the subgroup of $\mathrm{O}(L, \mathcal{P})$ generated by all the reflections s_r with respect to (-2)-vectors r. We call $W(L)$ the *Weyl group of* L. The family of hyperplanes

$$\{\, (r)^\perp \mid r \in L, \langle r, r\rangle = -2 \,\}$$

is locally finite in $\mathcal{P}$.

Definition 4.4. A *standard fundamental domain of the Weyl group* $W(L)$ is the closure of a connected component of

$$\mathcal{P} \setminus \bigcup (r)^\perp,$$

where r runs through the set of (-2)-vectors.

For explicit examples of standard fundamental domains of the Weyl groups, see Section 6.

A standard fundamental domain is a chamber, and its walls are defined by (-2)-vectors. Then $W(L)$ acts on the set of standard fundamental domains simple transitively (whence the name "fundamental domains"). Let D be a standard fundamental domain of $W(L)$, and we put

$$\mathrm{O}(L, D) := \{\, g \in \mathrm{O}(L) \mid D^g = D \,\}.$$

Then we have

$$\mathrm{O}(L, \mathcal{P}) = W(L) \rtimes \mathrm{O}(L, D).$$

Therefore it is important to study D. Usually, a standard fundamental domain of $W(L)$ has infinitely many walls, and $\mathrm{O}(L, D)$ is an infinite group.

We consider the following:

Problem 4.5. Let v_1, v_2 be vectors in $(L \otimes \mathbb{Q}) \cap \mathcal{P}$. Determine whether they belong to the same standard fundamental domain of $W(L)$ or not.

For this purpose, it is enough to calculate the set

$$\mathrm{Sep}(v_1, v_2) := \{\, r \in L \mid \langle r, v_1\rangle > 0, \;\; \langle r, v_2\rangle < 0, \;\; \langle r, r\rangle = -2 \,\}$$

of (-2)-vectors *separating* v_1 *and* v_2. For a vector $x \in \mathcal{P}$, we denote by $\langle x\rangle$ the 1-dimensional linear space $\mathbb{R}x$, and $\langle x\rangle^\perp$ the orthogonal complement of $\langle x\rangle$. Note that

$$\left(\bigcup_{t \in \mathbb{R}_{\geq 0} \cup \{\infty\}} \langle v_1 + t v_2\rangle^\perp \right) \quad \cap \quad \{\, y \in L \otimes \mathbb{R} \mid \langle y, y\rangle = -2 \,\}$$

is a compact subset of $L \otimes \mathbb{R}$, and hence the set $\mathrm{Sep}(v_1, v_2)$ of lattice points in this compact subset is finite. (Here we understand $\langle v_1 + \infty v_2\rangle$ as $\langle v_2\rangle$.)

A method to calculate $\mathrm{Sep}(v_1, v_2)$. Note that, if $x \in \mathcal{P}$, then the restriction of $\langle\ ,\ \rangle$ to $\langle x\rangle^\perp$ is negative-definite. We denote by

$$\mathrm{pr} \colon L \otimes \mathbb{R} \to \langle v_1\rangle^\perp$$

the orthogonal projection, and put

$$W := \mathrm{pr}(L).$$

Then we see that $W \subset L \otimes \mathbb{Q}$, and that W is a free $\mathbb{Z}$-module of rank $n-1$. We denote by

$$\langle\ ,\ \rangle_W \;\;:\;\; W \times W \to \mathbb{Q}$$

the restriction of $\langle\ ,\ \rangle$ to W. Suppose that $x \in \mathcal{P}$. Then the composite

$$\langle x\rangle^{\perp} \hookrightarrow L \otimes \mathbb{R} \xrightarrow{\mathrm{pr}} \langle v_1\rangle^{\perp} = W \otimes \mathbb{R} \tag{4.1}$$

is an isomorphism of $\mathbb{R}$-vector spaces. Let $\varphi_x \colon \langle v_1\rangle^{\perp} \xrightarrow{\sim} \langle x\rangle^{\perp}$ denote the inverse of the isomorphism (4.1), that is,

$$\varphi_x(y) = y - \frac{\langle y, x\rangle}{\langle v_1, x\rangle} v_1 \quad \text{for} \quad y \in \langle v_1\rangle^{\perp}.$$

We then define $f_x : \langle v_1\rangle^{\perp} \to \mathbb{R}$ by

$$f_x(y) := \langle \varphi_x(y), \varphi_x(y)\rangle = \langle y, y\rangle_W + \frac{\langle y, x\rangle^2}{\langle v_1, x\rangle^2} \langle v_1, v_1\rangle \quad \text{for} \quad y \in \langle v_1\rangle^{\perp} = W \otimes \mathbb{R}.$$

Since the real quadratic form $\langle\ ,\ \rangle$ restricted to $\langle x\rangle^{\perp}$ is negative-definite, so is f_x. Therefore $f_{v_1+tv_2}$ is negative-definite on $W \otimes \mathbb{R} = \langle v_1\rangle^{\perp}$ for any $t \in \mathbb{R}_{\geq 0} \cup \{\infty\}$. (Here we understand that $f_{v_1+\infty v_2} = f_{v_2}$.) For simplicity, we put

$$c_1 := \langle v_1, v_1\rangle, \quad b := \langle v_1, v_2\rangle, \quad v_W := \mathrm{pr}(v_2) \in W.$$

Let x' be a vector in $\langle v_1\rangle^{\perp} = W \otimes \mathbb{R}$. Since $v_2 - v_W \in \langle v_1\rangle$, we have

$$f_{v_1+tv_2}(x') = \langle x', x'\rangle_W + \frac{t^2\langle x', v_W\rangle_W^2}{(c_1 + tb)^2} c_1. \tag{4.2}$$

We have $c_1/b > 0$, and hence, for a fixed $x' \in \langle v_1\rangle^{\perp}$, $f_{v_1+tv_2}(x')$ is a non-decreasing function with respect to $t \in \mathbb{R}_{\geq 0}$ bounded from above by

$$f_{v_1+\infty v_2}(x') = \langle x', x'\rangle_W + \frac{\langle x', v_W\rangle_W^2}{b^2} c_1.$$

Note that $f_{v_1+\infty v_2}$ restricted to $W \subset W \otimes \mathbb{R}$ is $\mathbb{Q}$-valued, and hence $f_{v_1+\infty v_2}$ is a inhomogeneous quadratic function on $W \otimes \mathbb{Q}$ whose homogeneous part of degree 2 is negative-definite. Applying Fincke-Pohst algorithm with LLL-preprocessing to the positive inhomogeneous $\mathbb{Z}$-valued quadratic function $-M \cdot f_{v_1+\infty v_2}$, where M is an appropriate positive integer, we can calculate the finite set

$$S_W := \{\, r' \in W \mid f_{v_1+\infty v_2}(r') \geq -2 \,\}.$$

Suppose that r is an element of the set $\mathrm{Sep}(v_1, v_2)$. We put

$$t_r := -\frac{\langle r, v_1\rangle}{\langle r, v_2\rangle} \quad \in \quad \mathbb{R}_{>0}.$$

Then we have $r \in \langle v_1 + t_r v_2\rangle^{\perp}$. We put $r' := \mathrm{pr}(r) \in W$. Since $\varphi_{v_1+t_r v_2}(r') = r$, we have

$$-2 = \langle r, r\rangle = f_{v_1+t_r v_2}(r') \leq f_{v_1+\infty v_2}(r').$$

Therefore $r' \in S_W$ holds. Selecting from the finite set S_W all elements r' that lift to elements $r = \alpha v_1 + r' \in \mathrm{Sep}(v_1, v_2)$ by some $\alpha \in \mathbb{Q}$, we obtain $\mathrm{Sep}(v_1, v_2)$. $\square$

5. The nef-and-big cone of a $K3$ surface

Let X be an algebraic $K3$ surface, and let S_X be the lattice of numerical equivalence classes of divisors on X:

$$S_X = H^2(X, \mathbb{Z}) \cap H^{1,1}(X).$$

Suppose that S_X is of rank $n > 1$. Then S_X is an even hyperbolic lattice. Let $\mathcal{P}_X$ be the positive cone of S_X containing an ample class of X. We put

$$\begin{aligned} N_X &:= \{\, x \in \mathcal{P}_X \mid \langle x, [C] \rangle \ge 0 \text{ for all curves } C \text{ on } X \,\}, \\ N_X^{\circ} &:= \text{the interior of } N_X, \\ \overline{N}_X &:= \text{the closure of } N_X \text{ in } \overline{\mathcal{P}}_X. \end{aligned}$$

The cone N_X is called the *nef-and-big cone* of the $K3$ surface X. For a lattice vector $v \in S_X$, we have

$$v \text{ is ample} \iff v \in N_X^{\circ}.$$

We put

$$\mathrm{Rats}(X) := \{\, [C] \in S_X \mid C \text{ is a smooth rational curve on } X \,\}.$$

By the adjunction formula on X, every $r \in \mathrm{Rats}(X)$ is a (-2)-vector of S_X. We have the following:

Theorem 5.1. (1) *The cone N_X is a standard fundamental domain of $W(S_X)$.*
(2) *A (-2)-vector of $r \in S_X$ is in* $\mathrm{Rats}(X)$ *if and only if r defines a wall of N_X.*

We show how to obtain geometric data of X from the lattice-theoretic data S_X and N_X by the computational tools explained so far.

For $v \in \mathcal{P}_X \cap S_X$, we put

$$[v]^{\perp} := \{\, x \in S_X \mid \langle x, v \rangle = 0 \,\}.$$

Then $[v]^{\perp}$ is a negative-definite lattice, and hence we can calculate the set

$$\mathrm{Roots}(\,[v]^{\perp}) := \{\, r \in S_X \mid \langle r, v \rangle = 0, \;\; \langle r, r \rangle = -2 \,\},$$

by Fincke-Pohst algorithm with LLL-preprocessing.

5.1. **Find an ample class of X.** Let $\overline{X}$ be a normal surface birational to X, and $h \in S_X$ the pull-back of an ample class of $\overline{X}$ by the minimal resolution $X \to \overline{X}$. Then we have $h \in N_X$. It is known that $\overline{X}$ has only rational double points as its singularities and hence the exceptional locus of $X \to \overline{X}$ is a union of smooth rational curves whose dual graph is a union of Dynkin diagrams of type ADE. Let $r_1, \dots, r_\mu$ be the classes of smooth rational curves contracted by $X \to \overline{X}$. Then, *locally around* h, the cone N_X is defined by $\langle x, r_i \rangle \ge 0$ for $i = 1, \dots, \mu$. Therefore a lattice vector $\boldsymbol{a} \in \mathcal{P}_X \cap S_X$ is ample if and only if

$$\mathrm{Sep}(h, \boldsymbol{a}) = \emptyset, \quad \mathrm{Roots}(\,[\boldsymbol{a}]^{\perp}) = \emptyset, \quad \text{and} \quad \langle \boldsymbol{a}, r_i \rangle > 0 \;\text{ for }\; i = 1, \dots, \mu.$$

If $a' \in S_X$ satisfies $\langle a', r_i \rangle > 0$ for $i = 1, \dots, \mu$, then $\boldsymbol{a} := Mh + a'$ is ample for sufficiently large integer $M \in \mathbb{Z}$.

Example 5.2. Let $X = X_{f,g}$ be the minimal resolution of the double covering $\overline{X}$ of $\mathbb{P}^2$ defined by $w^2 = f^2 + g^3$ with f and g being general. Recall that $\boldsymbol{h}$ is the pullback of the class of a line on $\mathbb{P}^2$ by the double covering $\pi_0 \colon X \to \overline{X} \to \mathbb{P}^2$. Hence we have $\boldsymbol{h} \in N_X$. The exceptional locus of $X \to \overline{X}$ consists of 12 smooth rational curves of type $6A_2$, and their classes are $\boldsymbol{e}_i^{(\pm)}$ for $i = 1, \dots, 6$. We can confirm that the class $\boldsymbol{a} \in S_X$ satisfying

$$\langle \boldsymbol{a}, \boldsymbol{h} \rangle = 8, \quad \langle \boldsymbol{a}, \boldsymbol{e}_i^{(\pm)} \rangle = 1 \quad (i = 1, \dots, 6),$$

is an ample class of X.

In the following, we suppose that we have obtained an ample class $\boldsymbol{a} \in S_X$.

5.2. **Is a vector with positive norm nef/ample?** Once we obtain an ample class $\boldsymbol{a}$, we can characterize N_X as the unique standard fundamental domain of $W(S_X)$ containing $\boldsymbol{a}$.

Let $v \in S_X$ be a vector with $\langle v, v \rangle > 0$. Then we have

$$v \in \mathcal{P}_X \iff \langle \boldsymbol{a}, v \rangle > 0.$$

When this is the case, we have

$$v \in N_X \iff \mathrm{Sep}(\boldsymbol{a}, v) = \emptyset.$$

When this is the case, we have

$$v \in N_X^{\circ} \iff \mathrm{Roots}(\,[v]^{\perp}) = \emptyset.$$

5.3. **Does an isometry preserve N_X?** Let g be an element of $\mathrm{O}(S_X)$. Then we have

$$g \in \mathrm{O}(S_X, \mathcal{P}_X) \iff \langle \boldsymbol{a}, \boldsymbol{a}^g \rangle > 0.$$

When this is the case, we have

$$g \in \mathrm{O}(S_X, N_X) \iff \mathrm{Sep}(\boldsymbol{a}, \boldsymbol{a}^g) = \emptyset.$$

Remark 5.3. Suppose that we have a set $\{\boldsymbol{a}_1, \dots, \boldsymbol{a}_M\}$ of many ample classes of X. Then, for $g \in \mathrm{O}(S_X, \mathcal{P}_X)$, we have

$$\begin{aligned} g \in \mathrm{O}(S_X, N_X) \quad &\iff \quad \forall\, i, j \quad \text{we have} \quad \mathrm{Sep}(\boldsymbol{a}_i, \boldsymbol{a}_j^g) = \emptyset \\ &\iff \quad \exists\, i, j \;\; \text{such that} \;\; \mathrm{Sep}(\boldsymbol{a}_i, \boldsymbol{a}_j^g) = \emptyset. \end{aligned}$$

Choosing i, j such that $\langle \boldsymbol{a}_i, \boldsymbol{a}_j^g \rangle$ is small, we can make the computation of $\mathrm{Sep}(\boldsymbol{a}_i, \boldsymbol{a}_j^g)$ faster.

This criterion has the following important application. We consider the natural homomorphism

$$\mathrm{Aut}(X) \to \mathrm{O}(S_X).$$

Let $\mathrm{aut}(X)$ denote the image of this homomorphism. As a corollary of Torelli theorem for $K3$ surfaces due to Piatetski-Shapiro and Shafarevich [8], we have the following:

Theorem 5.4. *An isometry $g \in \mathrm{O}(S_X)$ is in $\mathrm{aut}(X)$ if and only if g belongs to $\mathrm{O}(S_X, N_X)$ and satisfies the period condition.*

Remark 5.5. We explain the term "period condition". First, we have to define the notion of *discriminant forms*, which was introduced by Nikulin [6]. Let L be an even lattice. Then the *dual lattice* $L^{\vee}$ of L is defined to be

$$\{\, v \in L \otimes \mathbb{Q} \mid \langle x, v \rangle \in \mathbb{Z} \;\text{ for all }\; v \in L \,\}.$$

The abelian group $A(L) := L^{\vee}/L$ is of order $|\det(\mathrm{Gram}(L))|$. This group $A(L)$ is called the *discriminant group* of L. We then define the quadratic form

$$q(L) \colon A(L) \to \mathbb{Q}/2\mathbb{Z}$$

by $q(x \bmod L) := \langle x, x\rangle \bmod 2\mathbb{Z}$. This finite quadratic form is called the *discriminant form* of L.

Recall that S_X is a primitive sublattice of the even unimodular lattice $H^2(X,\mathbb{Z})$ of rank 22 and signature $(3,19)$. Let T_X denote the orthogonal complement of S_X in $H^2(X,\mathbb{Z})$. Note that $H^2(X,\mathbb{Z})$ is a submodule of $S_X^\vee \oplus T_X^\vee$ containing $S_X \oplus T_X$. Since $H^2(X,\mathbb{Z})$ is unimodular, the submodule $H^2(X,\mathbb{Z})$ of $S_X^\vee \oplus T_X^\vee$ modulo $S_X \oplus T_X$ is the graph

$$H^2(X,\mathbb{Z})/(S_X \oplus T_X) \quad \subset \quad (S_X^\vee \oplus T_X^\vee)/(S_X \oplus T_X) = A(S_X) \times A(T_X)$$

of an isomorphism of $A(S_X)$ and $A(T_X)$, which induces an isomorphism

$$q(S_X) \cong -q(T_X). \tag{5.1}$$

Consider a pair (g_S, g_T) of isometries $g_S \in \mathrm{O}(S_X)$ and $g_T \in \mathrm{O}(T_X)$. Then the action of this pair on $S_X^\vee \oplus T_X^\vee$ preserves the submodule $H^2(X,\mathbb{Z})$ if and only if the action of g_S on $q(S_X)$ is equal to the action of g_T on $q(T_X)$ via the isomorphism (5.1).

Note that T_X is the minimal primitive submodule of $H^2(X,\mathbb{Z})$ such that $T_X \otimes \mathbb{C}$ contains the period $H^{2,0}(X) = \mathbb{C}\omega_X \subset H^2(X,\mathbb{C})$ of X, where ω_X is a nonzero holomorphic 2-form on X. We put

$$\mathrm{O}(T_X, \omega_X) := \{\, g_T \in \mathrm{O}(T_X) \mid g_T \otimes \mathbb{C} \text{ preserves } H^{2,0}(X)\,\}.$$

Then we say that $g_S \in \mathrm{O}(S_X)$ satisfies the *period condition* if the action of g_S on $q(S_X)$ is equal to the action on $q(T_X)$ of some of $g_T \in \mathrm{O}(T_X, \omega_X)$ via the isomorphism (5.1).

Thus we have the following:

Proposition 5.6. *An isometry $g_S \in \mathrm{O}(S_X)$ extends to an isomoetry of $H^2(X,\mathbb{Z})$ preserving the period $H^{2,0}(X)$ if and only if g satisfies the period condition.*

Therefore every $g_S \in \mathrm{aut}(X)$ statisfies the period condition. It is obvious that every $g_S \in \mathrm{aut}(X)$ preserves N_X. Torelli theorem says that these two conditions are sufficient for $g_S \in \mathrm{O}(S_X)$ to be in $\mathrm{aut}(X)$.

Example 5.7. Let X be $X_{f,g}$, where the polynomials f and g are general. Then the natural homomorphism $\mathrm{Aut}(X) \to \mathrm{O}(S_X)$ is injective, and we have $\mathrm{Aut}(X) \cong \mathrm{aut}(X)$. Since f and g are general, we see that $\mathrm{O}(T_X, \omega_X)$ is equal to $\{\pm 1\}$. Hence an isometry $g_S \in \mathrm{O}(S_X)$ satisfies the period condition if and only if the action of g_S on the discriminant group $A(S_X)$ is ± 1.

Therefore, for a given isomoetry g of S_X, we can determine effectively whether g belongs to $\mathrm{aut}(X)$ or not.

5.4. **Does a (-2)-vector belong to $\mathrm{Rats}(X)$?** Let $r \in S_X$ be a (-2)-vector such that $\langle \boldsymbol{a}, r\rangle > 0$. By Riemann-Roch theorem, there exists an effective divisor D of X such that $r = [D]$. Then $r \in \mathrm{Rats}(X)$ if and only if D is irreducible.

Proposition 5.8. *We put*

$$a'_r := \boldsymbol{a} + \frac{\langle \boldsymbol{a}, r\rangle}{2} r.$$

Then $r \in \mathrm{Rats}(X)$ if and only if

$$\mathrm{Roots}(\,[a'_r]^\perp) = \{r, -r\} \quad \textit{and} \quad \mathrm{Sep}(a'_r, \boldsymbol{a}) = \emptyset. \tag{5.2}$$

Proof. First note that $\langle a'_r, r\rangle = 0$ and $\langle a'_r, a'_r\rangle > 0$. Hence $a'_r \in (r)^\perp$ is the image of $\boldsymbol{a}$ by the orthogonal projection to the hyperplane $(r)^\perp$. In particular, we have $\{r, -r\} \subset \mathrm{Roots}(\,[a'_r]^\perp)$.

If (5.2) holds, then $a'_r \in N_X$ and a small neighborhood of a'_r in $(r)^\perp$ is contained in N_X. In particular, r is a defining vector of a wall of N_X satisfying $\langle r, \boldsymbol{a}\rangle > 0$ and hence $r \in \mathrm{Rats}(X)$.

Conversely, suppose that $r \in \mathrm{Rats}(X)$. Then for any $r' \in \mathrm{Rats}(X)$, if $r' \neq r$, then $\langle r, r'\rangle \geq 0$ and $\langle \boldsymbol{a}, r'\rangle > 0$, and hence

$$\langle a'_r, r'\rangle = \langle \boldsymbol{a}, r'\rangle + \frac{\langle \boldsymbol{a}, r\rangle\langle r, r'\rangle}{2} \quad > \quad 0.$$

Therefore (5.2) holds. □

5.5. **Is a vector with norm 0 nef?** We have the following:

Proposition 5.9. *Let f be a non-zero vector in $S_X \cap \overline{\mathcal{P}}_X$ with $\langle f, f\rangle = 0$. Then $f \in \overline{N}_X$ if and only if $\mathrm{Sep}(a', \boldsymbol{a}) = \emptyset$, where $a' := \boldsymbol{a} + \langle \boldsymbol{a}, f\rangle f$.*

Proof. First note that, since $f \in \overline{\mathcal{P}}_X$ and $f \neq 0$, we have $\langle f, \boldsymbol{a}\rangle > 0$ and hence $\langle a', \boldsymbol{a}\rangle > 0$ and $\langle a', a'\rangle > 0$. Therefore we can calculate $\mathrm{Sep}(a', \boldsymbol{a})$.

Suppose that $f \in \overline{N}_X$. Since $\boldsymbol{a} \in N_X^\circ$, we have $a' \in N_X^\circ$ and hence $\mathrm{Sep}(a', \boldsymbol{a}) = \emptyset$. Suppose that $f \notin \overline{N}_X$. Then there exists a smooth rational curve C such that $\langle f, [C]\rangle < 0$. We put $r := [C]$. Then we have $\langle f, r\rangle \leq -1$. Since $\langle f, f\rangle = 0$ and $\langle f, \boldsymbol{a}\rangle > 0$, there exists an effective divisor F on X such that $f = [F]$. Then C is an irreducible component of F such that $C \neq F$, and hence $\langle r, \boldsymbol{a}\rangle < \langle f, \boldsymbol{a}\rangle$. The intersection point of $(r)^\perp$ and

$$[\boldsymbol{a}, f[:= \{\, p(t) = \boldsymbol{a} + tf \mid t \in \mathbb{R}_{\geq 0}\,\}$$

is equal to $p(t_0)$, where

$$t_0 := -\frac{\langle \boldsymbol{a}, r\rangle}{\langle f, r\rangle} \leq \langle \boldsymbol{a}, r\rangle < \langle \boldsymbol{a}, f\rangle.$$

Since $a' = p(\langle \boldsymbol{a}, f\rangle)$, the point $p(t_0)$ is on the open line segment $]\boldsymbol{a}, a'[$. Therefore r is a (-2)-vector separating a' and $\boldsymbol{a}$. □

5.6. **Calculating the singularities of a normal surface birational to X.** Let h be a vector in $S_X \cap N_X$, and let $\mathcal{L}$ be the line bundle whose class is h. Then, for some large positive integer m, the complete linear system $|\mathcal{L}^{\otimes m}|$ gives a birational morphism $X \to \overline{X}$ to a normal surface $\overline{X}$. The surface $\overline{X}$ is smooth if and only if $h \in N_X^\circ$. Suppose that $h \notin N_X^\circ$. Then the singularities of $\overline{X}$ consists of rational double points, and the set of classes of smooth rational curves contracted by $X \to \overline{X}$ is equal to

$$\{\, r \in \mathrm{Rats}(X) \mid \langle r, h\rangle = 0\,\} \quad = \quad \mathrm{Rats}(X) \cap \mathrm{Roots}([h]^\perp).$$

Hence we can calculate this set effectively.

5.7. **Finding automorphisms from nef-vectors of norm 2.** Let h be a vector in $S_X \cap N_X$ with $\langle h, h\rangle = 2$, and let $\mathcal{L}$ be the line bundle whose class is h. Then either one of the following holds. (See Saint-Donat [9] or Nikulin [7].)

- The complete linear system $|\mathcal{L}|$ is base-point free, and defines a double covering $X \to \mathbb{P}^2$, or

- $|\mathcal{L}|$ has a fixed component Z, which is a smooth rational curve, and every member of $|\mathcal{L}|$ is of the form $Z+E_1+E_2$, where E_1 and E_2 are members of a pencil $|E|$ of elliptic curves such that $\langle [E],[Z]\rangle = 1$. The pencil $|E|$ gives rise a Jacobian fibration $\phi\colon X \to \mathbb{P}^1$ with the zero section Z.

These two cases can be distinguished by the following method. We put

$$\mathcal{E} := \{\, e \in S_X \mid \langle e,e\rangle = 0, \langle e,h\rangle = 1 \,\}.$$

Since the intersection form $\langle\ ,\ \rangle$ restricted to the affine hyperplane defined by $\langle x,h\rangle = 1$ is negative-definite, the set $\mathcal{E}$ is finite and can be calculated by Fincke-Pohst algorithm with LLL-preprocessing.

- If $\mathcal{E} = \emptyset$, then $|\mathcal{L}|$ is base-point free. Let $i(h) \in \mathrm{Aut}(X)$ be the involution associated with the double covering $X \to \mathbb{P}^2$ given by $|\mathcal{L}|$. We can calculate the set
$$\{\, r \in \mathrm{Rats}(X) \mid \langle r,h\rangle = 0 \,\}$$
of classes of smooth rational curves contracted by $X \to \mathbb{P}^2$. Hence we can calculate the invariant part
$$\{\, v \in S_X \mid v^{i(h)} = v \,\}$$
of the action of $i(h)$ on S_X. From this sublattice, we can calculate the action of the involution $i(h)$ on S_X.
- Suppose that $\mathcal{E} \neq \emptyset$. Then we have a unique element $f \in \mathcal{E}$ such that
$$f \in \overline{N}_X \quad \text{and} \quad z := h - 2f \in \mathrm{Rats}(X).$$
Then f is the class of a fiber of a Jacobian fibration $\phi\colon X \to \mathbb{P}^1$ with z being the class of the zero section $s\colon \mathbb{P}^1 \to X$. The classes of irreducible components of reducible fibers of ϕ that is disjoint from s is equal to
$$\{\, r \in \mathrm{Rats}(X) \mid \langle r,f\rangle = \langle r,z\rangle = 0 \,\},$$
which can be calculated effectively. Therefore we can calculate the ADE-types of reducible fibers of ϕ. From this data, we can calculate the Mordell-Weil group $\mathrm{MW}(\phi,s)$ and its action on S_X.

Remark 5.10. Let $B \subset \mathbb{P}^2$ be the branch curve of a double covering $X \to \mathbb{P}^2$. Suppose that $\bar{p}$ is a singular point of B that is not of type A_1. Then, considering the pull-back of the pencil of lines $\ell \subset \mathbb{P}^2$ passing through $\bar{p}$, we obtain a Jacobian fibration $\phi\colon X \to \mathbb{P}^1$ with a zero section $s\colon \mathbb{P}^1 \to X$ being one of the exceptional curves of $X \to \mathbb{P}^2$ contracted to $\bar{p}$. Thus we obtain automorphisms of X coming from $\mathrm{MW}(\phi,s)$.

Example 5.11. Let X be $X_{f,g}$ with f and g being general, and let $\boldsymbol{h}, \boldsymbol{e}_i^{(\pm)}$ be the elements of S_X defined above. Let M be the group of isometries of S_X that preserve $\boldsymbol{h}$ and the set $\{\boldsymbol{e}_i^{(\pm)}\}$. Then M is isomorphic to the group $\mathbb{Z}/2\mathbb{Z} \times S_6$ of order 1440. We have $M \cap \mathrm{aut}(X) = \{1, i(\boldsymbol{h})\}$. The action of M on $\mathcal{P}_X$ preserves $N_X \subset \mathcal{P}_X$. We have calculated vectors $h \in S_X \cap N_X$ with $\langle h,h\rangle = 2$ and $\langle h,\boldsymbol{h}\rangle \leq 16$ modulo the action of M. In Table 5.1, we give the list of these vectors $h \in N_X$ with $\langle h,\boldsymbol{h}\rangle \leq 12$. In this table, the column "size" indicates the size of the orbit h^M of h under the action of M.

No.	$\langle h, \boldsymbol{h} \rangle$	size	bp free	root type
1	2	1	yes	$6A_2$
2	4	12	no	$5A_2$
3	4	12	yes	$A_2 + 5A_1$
4	4	20	yes	$3A_2 + 3A_1$
5	6	60	yes	$A_4 + 4A_1$
6	6	12	no	$5A_2$
7	6	120	yes	$D_4 + 2A_2$
8	6	180	yes	$A_3 + 2A_2$
9	6	180	yes	$A_5 + A_3$
10	6	30	yes	$A_4 + 4A_1$
11	6	180	yes	$2A_3 + A_1$
12	8	120	yes	$D_4 + 2A_2$
13	8	120	yes	$3A_2 + 3A_1$
14	8	360	yes	$2A_3 + A_1$
15	8	360	yes	$A_3 + 2A_2$
16	8	720	yes	$A_5 + A_2$
17	8	120	yes	$A_3 + 5A_1$
18	8	120	no	$D_4 + A_3$
19	8	720	yes	$A_4 + A_3$
20	8	120	no	$A_5 + 3A_1$
21	8	360	yes	$A_6 + A_1$
22	8	120	yes	$D_5 + 3A_1$
23	10	12	no	$5A_2$
24	10	60	yes	$A_4 + 4A_1$
25	10	12	yes	$A_2 + 5A_1$
26	10	360	yes	$2A_3 + A_1$
27	10	12	yes	$6A_2$
28	10	60	yes	$A_2 + 5A_1$
29	10	120	yes	$D_4 + A_5$
30	10	60	yes	$A_2 + 5A_1$
31	10	720	yes	$A_4 + A_3$
32	10	60	yes	$A_4 + 4A_1$
33	10	240	yes	$A_3 + 5A_1$
34	10	360	yes	$D_5 + 3A_1$
35	10	360	yes	$2A_3 + A_1$
36	10	360	yes	$A_5 + A_3$
37	10	120	yes	$A_3 + 5A_1$
38	10	240	no	$D_4 + A_3$
39	10	120	yes	$D_4 + A_5$
40	10	360	yes	$D_4 + A_3 + A_2$
41	10	360	yes	$D_4 + A_3 + A_1$
42	10	360	yes	$A_2 + 5A_1$
43	10	360	yes	$D_5 + 3A_1$
44	10	360	yes	$A_5 + A_2 + 3A_1$
45	10	360	yes	$3A_2 + 3A_1$
46	10	120	yes	$E_6 + 3A_1$
47	10	1440	yes	$A_4 + A_3$
48	10	360	yes	$D_6 + A_1$
49	10	720	yes	$A_6 + A_1$
50	10	120	yes	$D_4 + A_5$
51	10	360	yes	$D_4 + A_3 + A_1$
52	12	12	yes	$A_2 + 5A_1$
53	12	120	yes	$3A_2 + 3A_1$
54	12	360	yes	$A_5 + A_3$
55	12	720	yes	$A_5 + A_2$
56	12	360	yes	$A_5 + A_3$
57	12	360	yes	$A_5 + A_3$
58	12	360	no	$A_5 + 3A_1$
59	12	1440	yes	$A_6 + A_1$
60	12	240	yes	$A_4 + 4A_1$
61	12	360	yes	$A_5 + A_2 + 3A_1$
62	12	720	yes	$A_4 + 4A_1$
63	12	1440	yes	$A_6 + A_1$
64	12	720	yes	$A_5 + A_2$
65	12	240	yes	$D_4 + 2A_2$
66	12	240	yes	$D_5 + 3A_1$
67	12	720	yes	$D_6 + A_1$
68	12	720	yes	$D_4 + 2A_2$
69	12	360	yes	$A_3 + 2A_2$
70	12	720	yes	$A_5 + A_3$
71	12	720	yes	$A_6 + A_1$
72	12	720	yes	$D_4 + 2A_2$
73	12	360	yes	$A_5 + A_2$
74	12	1440	yes	$A_6 + A_2$
75	12	720	yes	$A_5 + A_3$
76	12	1440	yes	$A_3 + 2A_2$
77	12	720	yes	$A_4 + 4A_1$
78	12	720	no	A_6
79	12	1440	yes	A_7
80	12	360	yes	$D_4 + 2A_2$
81	12	720	yes	$2A_3 + A_1$
82	12	720	yes	A_7
83	12	720	yes	$2A_3 + A_1$
84	12	1440	yes	$2A_3 + A_1$
85	12	720	yes	$2A_3 + A_1$

TABLE 5.1. Nef vectors of degree 2

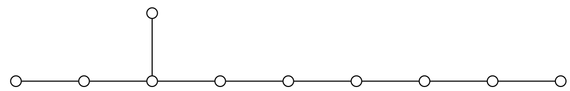

FIGURE 6.1. Coxeter graph of $W(L_{10})$

6. Borcherds' method

The following is well known. See, for example, Serre's book [10].

Theorem 6.1. *There exists an even unimodular hyperbolic lattice of rank n if and only if $n \equiv 2 \bmod 8$. Suppose that $n \equiv 2 \bmod 8$. Then an even unimodular hyperbolic lattice L_n of rank n is unique up to isomorphism.*

The lattice L_2 is the hyperbolic plane U, which has a basis u_1, u_2 with respect to which the Gram matrix is

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

If $n = 2 + 8k$, then L_n is isomorphic to

$$U \oplus R(kE_8) = U \oplus R(E_8)^{\oplus k},$$

where $R(\tau)$ is the *negative-definite* root lattice of ADE-type τ. (Previously, we denote by $R(\tau)$ the *positive-definite* root lattice of ADE-type τ.)

We choose a positive cone $\mathcal{P}_n \subset L_n \otimes \mathbb{R}$. The shape of a standard fundamental domain of $W(L_n)$ was determined by Vinberg for $n = 10, 18$ in [11], and by Conway for $n = 26$ in [3].

Theorem 6.2 (Vinberg)**.** *A standard fundamental domain N_{10} of $W(L_{10})$ has exactly* 10 *walls, and they are defined by* (-2)*-vectors that form the dual graph given in Figure 6.1. Since this graph has no non-trivial symmetries, we have* $\mathrm{O}(L_{10}, N_{10}) = \{1\}$ *and* $\mathrm{O}(L_{10}, \mathcal{P}_{10}) = W(L_{10})$.

Vinberg also calculated the walls of a standard fundamental domain N_{18} of $W(L_{18})$. It has 19 walls, and $\mathrm{O}(L_{18}, N_{18})$ is of order 2.

We investigate the case where $n = 26$. The lattice L_{26} is isomorphic to $U \oplus N$, where N is any one of the 24 *negative-definite* Niemeier lattices. In particular, we have

$$L_{26} \cong U \oplus \Lambda,$$

where Λ is the *negative-definite* Leech lattice, that is, the even unimodular negative-definite lattice with no roots. A standard fundamental domain N_{26} of $W(L_{26})$ has infinitely many walls. We write elements of $L_{26} = U \oplus \Lambda$ as

$$(a, b, \lambda) = au_1 + bu_2 + \lambda,$$

where u_1, u_2 are the basis of U. We choose the positive cone $\mathcal{P}_{26}$ in such a way that the vector

$$\mathbf{w}_0 := (1, 0, 0)$$

of norm 0 is contained in $\overline{\mathcal{P}}_{26}$.

Definition 6.3. A vector $\mathbf{w} \in L_{26}$ is called a *Weyl vector* if $\mathbf{w}$ is a non-zero primitive vector of L_{26} contained in $\partial\overline{\mathcal{P}}_{26}$ (in particular, we have $\langle \mathbf{w}, \mathbf{w} \rangle = 0$ and hence $\mathbb{Z}\mathbf{w} \subset (\mathbb{Z}\mathbf{w})^{\perp}$) such that $(\mathbb{Z}\mathbf{w})^{\perp}/\mathbb{Z}\mathbf{w}$ is isomorphic to the negative-definite Leech lattice Λ.

Definition 6.4. Let $\mathbf{w}$ be a Weyl vector. A (-2)-vector $r \in L_{26}$ is said to be a *Leech root* with respect to $\mathbf{w}$ if $\langle \mathbf{w}, r \rangle = 1$. We then put

$$N_{26}(\mathbf{w}) := \{\, x \in \mathcal{P}_{26} \mid \langle x, r \rangle \geq 0 \ \text{ for all Leech roots } r \text{ with respect to } \mathbf{w} \,\}.$$

Example 6.5. The vector $\mathbf{w}_0 = (1, 0, 0)$ is a Weyl vector. The set of Leech roots with respect to the Weyl vector $\mathbf{w}_0$ is

$$\left\{ \ \left(\frac{-2 - \lambda^2}{2}, 1, \lambda \right) \ \middle| \ \ \lambda \in \Lambda \right\},$$

where $\lambda^2 := \langle \lambda, \lambda \rangle$, which is a non-positive integer.

Conway proved the following by means of a generalization of Vinberg algorithm.

Theorem 6.6 (Conway)**.** *The mapping* $\mathbf{w} \mapsto N_{26}(\mathbf{w})$ *gives a bijection from the set of Weyl vectors to the set of standard fundamental domains of* $W(L_{26})$*.*

Definition 6.7. A standard fundamental domain of $W(L_{26})$ is called a *Conway chamber*. From now on, we write $C(\mathbf{w})$ for $N_{26}(\mathbf{w})$.

Theorem 6.8 (Conway)**.** *The mapping* $r \mapsto C(\mathbf{w}) \cap (r)^{\perp}$ *gives a bijection from the set of Leech roots with respect to the Weyl vector* $\mathbf{w}$ *to the set of walls of the Conway chamber* $C(\mathbf{w})$*.*

Corollary 6.9 (Conway)**.** *The group* $\mathrm{O}(L_{26}, N_{26}) = \{\, g \in \mathrm{O}(L_{26}) \mid N_{26}^{g} = N_{26} \,\}$ *is the group* Co_{∞} *of* affine *isometries of* Λ*, that is, the group generated by* $\mathrm{Co}_0 = \mathrm{O}(\Lambda)$ *and the affine translations of* Λ*, that is, we have* $\mathrm{Co}_{\infty} = \Lambda \rtimes \mathrm{Co}_0$*.*

Let X be a $K3$ surface. Suppose that we have a primitive embedding

$$S_X \hookrightarrow L_{26}.$$

By this embedding, we regard the positive cone $\mathcal{P}_X$ of S_X as a subspace of a positive cone $\mathcal{P}_{26}$ of L_{26}:

$$\mathcal{P}_X \quad = \quad (S_X \otimes \mathbb{R}) \cap \mathcal{P}_{26}.$$

Recall that the positive cone $\mathcal{P}_{26}$ is tessellated by Conway chambers $C(\mathbf{w})$.

Definition 6.10. An L_{26}/S_X*-chamber* is a chamber D of $\mathcal{P}_X$ that is obtained as the intersection $\mathcal{P}_X \cap C(\mathbf{w})$ of $\mathcal{P}_X$ with a Conway chamber $C(\mathbf{w})$.

The tessellation of $\mathcal{P}_{26}$ by Conway chambers induces a tessellation of $\mathcal{P}_X$ by L_{26}/S_X-chambers. By definition, the nef-and-big cone N_X, which is a standard fundamental domain of $W(S_X)$, is tessellated by L_{26}/S_X-chambers. In other words, the tessellation of $\mathcal{P}_X$ by L_{26}/S_X-chambers is a refinement of the tessellation by standard fundamental domains of $W(S_X)$.

Definition 6.11. We define the graph (V, E) by the following.

- The set V of vertices is the set of L_{26}/S_X-chambers contained in N_X.
- The set E of edges is the set of pairs of adjacent L_{26}/S_X-chambers.

Here, two distinct chambers are said to be *adjacent* if they share a common wall.

Let

$$D = \mathcal{P}_X \cap C(\mathbf{w}),$$

be an L_{26}/S_X-chamber, where $C(\mathbf{w})$ is the Conway chamber associated with a Weyl vector $\mathbf{w} \in L_{26}$. For each wall w of D, there exists a unique defining vector v of w in the dual lattice $S_X^\vee$ that is primitive in $S_X^\vee$. From now on, we call this vector $v \in S_X^\vee$ the *defining vector* of the wall w.

Proposition 6.12. *Suppose that the orthogonal complement of S_X in L_{26} contains at least one (-2)-vector. Then each L_{26}/S_X-chamber has only a finite number of walls. If $D = \mathcal{P}_X \cap C(\mathbf{w})$ is an L_{26}/S_X-chamber obtained by the Conway chamber $C(\mathbf{w})$ associated with a Weyl vector $\mathbf{w}$, then we can calculate the defining vectors of walls of D from $\mathbf{w}$.* □

Remark 6.13. For the calculation of walls of D, we have to use the classical "linear programming" algorithm.

Proposition 6.14. *Suppose that the period condition on isometries g of S_X is equivalent to the condition that the action of g on the discriminant group of S_X be ± 1. Then an isometry of S_X satisfying the period condition extends to an isometry of L_{26}. In particular, the action of* $\mathrm{aut}(X)$ *on N_X preserves the tessellation of N_X by L_{26}/S_X-chambers, and hence* $\mathrm{aut}(X)$ *acts on the graph (V, E).* □

Remark 6.15. Recall that the assumption in the proposition holds, for example, when $X = X_{f,g}$, where f and g are general.

Thus, in this situation, we can apply the abstract Borcherds' algorithm to the action of $G = \mathrm{aut}(X)$ on (V, E). If it terminates, then we obtain a finite set of generators of $\mathrm{aut}(X)$ and a fundamental domain of the action of $\mathrm{aut}(X)$ on N_X.

Example 6.16. We consider the case where $X = X_{f,g}$ with f and g being general. Then, up to the action of $\mathrm{O}(S_X)$ and $\mathrm{O}(L_{26})$, there exist 26 primitive embeddings $S_X \hookrightarrow L_{26}$. Table 6.1 indicates the data of the orthogonal complements $R = (S_X \hookrightarrow L_{26})^\perp$ of these primitive embeddings. The numbers m_k are half of the size of the set of vectors $v \in R$ with $\langle v, v\rangle = k$. This table was obtained by means of the Siegel-Minkowski mass formula.

We use the embedding whose orthogonal complement is No. 17 of Table 6.1. Then the ample class $\boldsymbol{a}$ given in Example 5.2 is contained in the interior of an L_{26}/S_X-chamber D_0. We start from this L_{26}/S_X-chamber D_0, and execute Borcherds' algorithm to the graph (V, E). It terminates, and produces the set $V_0 \cong V/G$ of representatives and a finite generating set $\mathcal{G}$ of $G = \mathrm{aut}(X) = \mathrm{Aut}(X)$. It turns out that V_0 consists of seven L_{26}/S_X-chambers:

$$D_0,\ \ D_1^{(1)},\ D_1^{(2)},\ D_1^{(3)},\ D_1^{(4)},\ D_1^{(5)},\ D_1^{(6)}.$$

The L_{26}/S_X-chamber $D_0 = C(\mathbf{w}) \cap \mathcal{P}_X$ has 110 walls. The stabilizer subgroup of D_0 in G is equal to $\{1, i(\boldsymbol{h})\}$. Recall that $M \cong \mathbb{Z}/2\mathbb{Z} \times S_6$ is the group of isometries of S_X that preserve $\boldsymbol{h}$ and the set $\{\boldsymbol{e}_i^{(\pm)}\}$. Then D_0 is invariant under the action of M, and the action of M decomposes the 110 walls into 4 orbits of size $2, 12, 6, 90$. Table 6.2 indicates properties of walls of D_0, where

$$n := \langle v, v\rangle, \quad a := \langle v, \mathbf{w}\rangle, \quad h := \langle v, \boldsymbol{h}\rangle$$

for the defining vectors v of walls. The walls in the orbits o_1 and o_2 are defined by the classes of smooth rational curves, and hence the L_{26}/S_X-chambers adjacent to

No.	root type	$\lvert\mathrm{O}(R)\rvert$	m_2	m_4	m_6	m_8
1	$3A_3$	$2^{13}\cdot 3^4$	18	963	8901	42516
2	A_5+2A_2	$2^{11}\cdot 3^4\cdot 5$	21	951	8892	42582
3	A_4+5A_1	$2^{12}\cdot 3^2\cdot 5^2$	15	975	8910	42450
4	A_6+A_3	$2^{11}\cdot 3^3\cdot 5\cdot 7$	27	981	8712	42714
5	A_6+A_3	$2^{10}\cdot 3^4\cdot 5\cdot 7$	27	927	8874	42714
6	D_5+4A_1	$2^{16}\cdot 3^2\cdot 5$	24	939	8883	42648
7	D_4+3A_2	$2^{12}\cdot 3^6$	21	1005	8730	42582
8	$2A_5$	$2^{13}\cdot 3^4\cdot 5^2$	30	1023	8541	42780
9	D_6+A_3	$2^{17}\cdot 3^3\cdot 5$	36	999	8523	42912
10	$D_4+A_5+A_1$	$2^{16}\cdot 3^4\cdot 5$	28	999	8523	43264
11	$D_4+A_5+A_2$	$2^{16}\cdot 3^4\cdot 5$	30	915	8865	42780
12	E_6+A_2	$2^{12}\cdot 3^7\cdot 5$	39	933	8676	42978
13	A_8+A_2	$2^{11}\cdot 3^6\cdot 5\cdot 7$	39	933	8676	42978
14	D_6+A_3	$2^{17}\cdot 3^4\cdot 5$	36	891	8847	42912
15	A_9	$2^{11}\cdot 3^5\cdot 5^2\cdot 7$	45	1017	8334	43110
16	A_8+A_1	$2^{12}\cdot 3^6\cdot 5\cdot 7$	37	963	8496	43462
17	$6A_2+A_1$	$2^{12}\cdot 3^8\cdot 5$	19	1035	8550	43066
18	$D_7+A_2+A_1$	$2^{17}\cdot 3^4\cdot 5\cdot 7$	46	927	8469	43660
19	D_7+2A_2	$2^{17}\cdot 3^4\cdot 5\cdot 7$	48	951	8487	43176
20	A_9	$2^{12}\cdot 3^5\cdot 5^3\cdot 7$	45	855	8820	43110
21	E_6+D_4	$2^{18}\cdot 3^6\cdot 5$	48	1059	8163	43176
22	E_7+A_2	$2^{16}\cdot 3^6\cdot 5\cdot 7$	66	987	8109	43572
23	$E_6+3A_2+A_1$	$2^{16}\cdot 3^8\cdot 5$	46	927	8469	43660
24	E_7+A_1	$2^{16}\cdot 3^6\cdot 5^2\cdot 7$	64	855	8415	44056
25	D_9	$2^{20}\cdot 3^5\cdot 5\cdot 7$	72	1071	7767	43704
26	E_8	$2^{19}\cdot 3^7\cdot 5^3\cdot 7$	120	1095	6975	44760

TABLE 6.1. Orthogonal complements of primitive embeddings

D_0 across these walls are not in N_X, that is, these chambers do not belong to V. The L_{26}/S_X-chamber adjacent to D_0 across the walls in the orbits o_3 and o_4 are indicated in the last column of Table 6.2. The isomorphisms between D_0 and the adjacent chambers across the walls in o_4 gives 90 elements of $\mathrm{aut}(X)$, which are a part of $\mathcal{G}$. The adjacent chambers across the walls in o_3 give new representatives $D_1^{(1)}, \dots, D_1^{(6)}$ of V/G.

The stabilizer subgroup of $D_1^{(\alpha)}$ in G is $\{1, i(\boldsymbol{h})\}$. The group M acts on the set $\{D_1^{(1)}, \dots, D_1^{(6)}\}$ transitively. Let M_α be the stabilizer subgroup of $D_1^{(\alpha)}$ in M. Then M_α is isomorphic to $\mathbb{Z}/2\mathbb{Z}\times S_5$. The chamber $D_1^{(\alpha)}$ has 110 walls, and the action of M_α decomposes the walls of $D_1^{(\alpha)}$ into seven orbits $o'_1, \dots, o'_7$. The data of these orbits are given in Table 6.3. The wall in the singleton o'_1 is the wall between D_0 and $D_1^{(\alpha)}$. The walls in the orbits o'_2, o'_3, o'_4 are defined by the classes of smooth rational curves. Here $\tilde{\ell}_{\alpha\beta}$ is the pullback of the line on $\mathbb{P}^2$ passing though the two cusps $\bar{p}_\alpha$ and $\bar{p}_\beta$ of the branch curve. The adjacent chambers across the walls in

	size	n	a	h	
o_1	2	-2	1	2	$\boldsymbol{\gamma}^{(\pm)}$
o_2	12	-2	1	0	$\boldsymbol{e}_i^{(\pm)}$
o_3	6	$-3/2$	$3/2$	1	isom with$D_1^{(\alpha)}$
o_4	90	$-2/3$	3	2	isom with D_0

TABLE 6.2. Walls of C_0

	size	n	a	h	
o'_1	1	$-3/2$	$3/2$	-1	back to C_0
o'_2	2	-2	1	2	$\boldsymbol{\gamma}^{(\pm)}$
o'_3	5	-2	1	2	$\tilde{\ell}_{\alpha\beta}$ $(\beta \neq \alpha)$
o'_4	10	-2	1	0	$\boldsymbol{e}_\beta^{(\pm)}$ $(\beta \neq \alpha)$
o'_5	2	$-3/2$	$3/2$	1	isom with $D_1^{(\alpha)}$
o'_6	30	$-1/6$	$7/2$	3	isom with $D_1^{(\beta)}$ $(\beta \neq \alpha)$
o'_7	60	$-2/3$	3	2	isom with $D_1^{(\beta)}$ $(\beta \neq \alpha)$

TABLE 6.3. Walls of $D_1^{(\alpha)}$

the orbits o'_5, o'_6, o'_7 are isomorphic to $D_1^{(\alpha)}$ or $D_1^{(\beta)}$, and the isomorphisms give a part of the generating set $\mathcal{G}$ of $\mathrm{aut}(X)$.

7. VINBERG ALGORITHM

Vinberg algorithm [11] is a method to enumerate the walls of convex polyhedrons of certain kind in a hyperbolic space. In particular, this algorithm can be used to calculate the set $\mathrm{Rats}(X)$ of walls of the nef-and-big cone N_X of a $K3$ surface X.

Example 7.1. The numbers $\nu(m)$ of smooth rational curves C on $X = X_{f,g}$ with $\langle [C], \boldsymbol{h}\rangle = m$ are as follows: When m is odd, then $\nu(m) = 0$, where as for m even, we have

m	0	2	4	6	8	10	12	14
$\nu(m)$	12	17	0	492	720	492	8292	8730

Note that the smooth rational curves with $m = 0$ are $\boldsymbol{e}_i^{\pm}$, and those $m = 2$ are $\boldsymbol{\gamma}^{\pm}$ and $\tilde{\ell}_{\alpha\beta}$.

Let h be a vector in $\overline{N}_X \cap S_X$, which is called the *control vector*. For each $d \in \mathbb{Z}_{\geq 0}$, we set

$$\begin{aligned} \widetilde{R}_d &:= \{ r \in S_X \mid \langle r, r\rangle = -2, \langle r, h\rangle = d \}, \\ R_d &:= \widetilde{R}_d \cap \mathrm{Rats}(X). \end{aligned}$$

When $\langle h, h\rangle > 0$, the set $\widetilde{R}_d$ can be calculated by Fincke-Pohst algorithm with LLL-preprocessing. (When $\langle h, h\rangle = 0$, we need to use another idea.) We calculate the subset R_d of $\widetilde{R}_d$ by induction on d. As was explained in the previous section, the set R_0 can be calculated, for example, when we have an ample class $\boldsymbol{a} \in S_X$.

Suppose that $d > 0$, and let r be an element of $\widetilde{R}_d$. Then r is the class of an effective divisor D, and $r \in R_d$ if and only if D is irreducible. Suppose that D is not irreducible. Then D contains as an irreducible component a smooth rational curve C such that $\langle [C], [D] \rangle < 0$. The class $r' := [C]$ is an element of $R_{d'}$ with $d' := \langle r', h \rangle < d$. Conversely, if there exists an element $r' \in R_{d'}$ with $d' < d$ such that $\langle r', r \rangle < 0$, then the smooth rartional curve C with $[C] = r'$ is an irreducible component of D such that $C \neq D$.

Therefore the following criterion holds. Suppose that $r \in \widetilde{R}_d$. If there exists an element $r' \in R_{d'}$ with $d' < d$ such that $\langle r', r \rangle < 0$, then r is rejected. Otherwise, we have $r \in R_d$.

We calculate the walls of the Conway chamber $C(\mathbf{w}_0)$ by Vinberg algorithm, regarding L_{26} as a numerical Néron-Severi lattice of a *non-existing* $K3$ surface, and $C(\mathbf{w}_0)$ as its nef-and-big cone. Using $h := \mathbf{w}_0$ as a control vector and executing Vinberg algorithm, we prove Conway's result that $r \mapsto (r)^{\perp} \cap C(\mathbf{w}_0)$ gives a bijection from the set of Leech roots to the set of the walls of $C(\mathbf{w}_0)$. For readability, we denote by $\langle\ ,\ \rangle_L$ the intersection pairing on $L_{26} = U \oplus \Lambda$, and by $\langle\ ,\ \rangle_\Lambda$ the intersection pairing on the negative-definite Leech lattice Λ. Note that we have

$$\langle\, (a, b, y),\ (a', b', y')\, \rangle_L = ab' + a'b + \langle y, y' \rangle_\Lambda$$

for any $(a, b, y), (a', b', y') \in L_{26}$. In particular, since $\mathbf{w}_0 = (1, 0, 0)$, we have

$$\langle (a, b, y), \mathbf{w}_0 \rangle_L = b.$$

We see that

$$R_0 = \{\, (a, 0, y) \mid y \in \Lambda, \langle y, y \rangle_\Lambda = -2 \,\}$$

is empty, because Leech lattice Λ cotains no (-2)-vectors. The set R_1 is exactly the set of Leech roots. Hence all that remains to prove is that, if $d > 1$, every element of R_d is rejected.

We use the following observation due to Conway and Sloane. We put

$$\begin{aligned} A \quad &:= \quad \{\, x \in L_{26} \otimes \mathbb{R} \mid \langle x, \mathbf{w}_0 \rangle_L = 1 \,\}, \\ A' \quad &:= \quad \{\, x \in A \mid \langle x, x \rangle_L = -2 \,\}. \end{aligned}$$

Then the additive group $\mathbb{R}$ acts on A by $x \mapsto x + t\mathbf{w}_0$ ($t \in \mathbb{R}$), and each orbit $x + \mathbb{R}\mathbf{w}_0$ intersects A' at a single point

$$p(x) := x - \frac{\langle x, x \rangle_L + 2}{2} \mathbf{w}_0.$$

We have a bijection $\Lambda \otimes \mathbb{R} \xrightarrow{\sim} A'$ given by

$$\Lambda \otimes \mathbb{R} \ \ni\ y \ \ \mapsto\ \ \tilde{y} := \left(\frac{-2 - y^2}{2}, 1, y \right) \ \in\ A',$$

where $y^2 = \langle y, y \rangle_\Lambda$. Note that, if $\lambda \in \Lambda$, then $\tilde{\lambda}$ is a Leech root. Note also that, for $y_1, y_2 \in \Lambda \otimes \mathbb{R}$, we have

$$\text{(7.1)} \qquad \langle \tilde{y}_1, \tilde{y}_2 \rangle_L = \frac{-2 - y_1^2}{2} + \frac{-2 - y_2^2}{2} + \langle y_1, y_2 \rangle_\Lambda = -2 - \frac{\langle y_1 - y_2, y_1 - y_2 \rangle_\Lambda}{2}.$$

We denote by

$$P \colon A \to \Lambda \otimes \mathbb{R}$$

the composite of $p\colon A \to A'$ and $A' \xrightarrow{\sim} \Lambda \otimes \mathbb{R}$, that is, we have

$$\widetilde{P(x)} = \left(\frac{-2 - P(x)^2}{2}, 1, P(x) \right) = x - \frac{\langle x, x \rangle_L + 2}{2} \mathbf{w}_0. \tag{7.2}$$

Suppose that $d > 1$ and $r \in \widetilde{R}_d$, and consider the point $P(r/d)$ of $\Lambda \otimes \mathbb{R}$. It is known that the covering radius of Leech lattice is $\sqrt{2}$. Hence there exists a lattice point $\lambda \in \Lambda$ such that

$$|\langle P(r/d) - \lambda, P(r/d) - \lambda \rangle_\Lambda| \le 2.$$

We have $\langle P(r/d) - \lambda, P(r/d) - \lambda \rangle_\Lambda \ge -2$, and hence by (7.1), we have

$$\langle \widetilde{P(r/d)}, \tilde{\lambda} \rangle_L \le -1.$$

Combining this with $\langle \mathbf{w}_0, \tilde{\lambda} \rangle_L = 1$ and (7.2), we have

$$\langle r/d, \tilde{\lambda} \rangle_L = \langle \widetilde{P(r/d)}, \tilde{\lambda} \rangle_L + \frac{\langle r/d, r/d \rangle_L + 2}{2} \le -1 + \frac{\langle r/d, r/d \rangle_L + 2}{2} = -\frac{1}{d^2} < 0.$$

Therefore we obtain an element $\tilde{\lambda} \in R_1$ such that $\langle r, \tilde{\lambda} \rangle_L < 0$, and r is rejected.

References

[1] Murray R. Bremner. *Lattice basis reduction*, volume 300 of *Pure and Applied Mathematics (Boca Raton)*. CRC Press, Boca Raton, FL, 2012. An introduction to the LLL algorithm and its applications.

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

[3] J. H. Conway. The automorphism group of the 26-dimensional even unimodular Lorentzian lattice. *J. Algebra*, 80(1):159–163, 1983.

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

[5] Phong Q. Nguyen and Brigitte Vallée, editors. *The LLL algorithm*. Information Security and Cryptography. Springer-Verlag, Berlin, 2010. Survey and applications.

[6] 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).

[7] Viacheslav V. Nikulin. Weil linear systems on singular $K3$ surfaces. In *Algebraic geometry and analytic geometry (Tokyo, 1990)*, ICM-90 Satell. Conf. Proc., pages 138–164. Springer, Tokyo, 1991.

[8] I. I. Pjateckiĭ-Šapiro and I. R. Šafarevič. Torelli's theorem for algebraic surfaces of type K3. *Izv. Akad. Nauk SSSR Ser. Mat.*, 35:530–572, 1971.

[9] B. Saint-Donat. Projective models of $K-3$ surfaces. *Amer. J. Math.*, 96:602–639, 1974.

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

[11] È. B. Vinberg. Some arithmetical discrete groups in Lobačevskiĭ spaces. In *Discrete subgroups of Lie groups and applications to moduli (Internat. Colloq., Bombay, 1973)*, pages 323–348. 1975.

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

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