ON SEMISTABILITY OF ROOT LATTICES AND PERFECT LATTICES

YOUNGSOO KIM

Abstract. We prove that all irreducible root lattices and all perfect lattices of dimension at most 7 are semistable. An algorithm to compute the canonical filtration of a lattice is presented, and it is used to prove or disprove semistability of all presently known perfect lattices. All 8 dimensional perfect lattices are semistable except one. The Coxeter-Barnes lattice $\mathbb{A}_8^2$ is the unique 8-dimensional perfect lattice that is not semistable.

1. Introduction

The classical reduction theory developed by Minkowski [12] and others is concerned with the upper bound on lengths of shortest vectors. Another, more recent reduction theory using the notion of semistability [8] is related to the lower bounds on lengths of vectors. The notion of semistability of lattices in Euclidean spaces was first introduced by Stuhler [18]. He defined the canonical filtration of a lattice in analogy with a similar filtration for vector bundles over algebraic curves. Then he defined a lattice to be semistable if its canonical filtration is trivial. Grayson [8] developed the idea further and produced an alternative method of proving the results of Borel and Serre [3] on arithmetic groups. He did it by studying the manifold of semistable lattices.

In this paper, we study the semistability of perfect lattices. A lattice is said to be *perfect* if it can be determined (up to isometry) by the length of shortest vectors and the components of those vectors on some (unknown) basis [19],[11]. There are finitely many perfect lattices in each dimension (up to similarity). All perfect lattices of dimension up to 8 has been found [17], and the computation for dimension 9 is still in progress [16]. They play an interesting role in the theory of lattices. In particular, extreme lattices, the lattices whose density is a local maximum, are among perfect lattices (Theorem 3.4.6 [11]). A lattice is called a *root lattice* if it is spanned by a root system in a Euclidean space. Such a lattice is characterized by the property that it is similar to an integral lattices generated by vectors of norm 1 or 2 (Theorem 4.10.6 [11]). A lattice is said to be *irreducible* if it is nonzero and is not an orthogonal sum of nonzero sublattices. The irreducible root lattices form a subclass of perfect lattices. The main result of this paper is that all irreducible root lattices are semistable, but not all perfect lattices are so.

In section 2, we review the definition and some properties of canonical filtrations of lattices. In section 3, we prove that all root lattices are semistable. It is proved by computing the norm of (nonzero) smallest vectors of their exterior powers. In section 4, we develop an algorithm to compute the canonical filtration of a lattice, then in section 5, we present the computational result that shows there is exactly one perfect lattice in dimension 8 that is not semistable.

This work is a result of an attempt to find a CW-structure of the manifold constructed by Grayson. For example, in dimension 2, the set of semistable lattices modulo isometries (minus the boundary) is a CW-complex. (See the picture of 1.25 [8].) The 0-cell is the perfect lattice of dimension 2, which has three pairs of shortest vectors. The 1-cells are the lattices with 2 pairs of shortest vectors, and the rest of the lattices constitute 2-cells. The guess that perfect lattices might constitute the 0-cells because of the abundance of shortest vectors was proved wrong by the discovery of the unstable perfect lattice in dimension 8. I owe the referee for the identification of that lattice as the Coxeter-Barnes lattice $\mathbb{A}_8^2$, and thank Daniel R. Grayson for helpful discussions and ideas.

2. Canonical Filtration

We review the definition and some properties of canonical filtration of a lattice from [18] and [8]. Let L be a lattice in a Euclidean space E. We denote the inner product of $x, y \in E$ by $x \cdot y$. A subgroup M of L is called a *sublattice* if the quotient group L/M has no torsion. A sublattice is again a lattice with the inner product inherited from that on L. For each sublattice M of L, we define the volume $\operatorname{vol} M$ to be the (nonzero) covolume of the fundamental domain of M in the real span of the generators of M. Then $(\operatorname{vol} M)^2$ is the determinant of the Gram matrix $(v_i \cdot v_j)_{1 \le i,j \le k}$.

Suppose M is a sublattice. The quotient group L/M can be given the structure of a lattice if it is identified with the projection of L onto the orthogonal complement of the subspace of E generated by M. Then $\operatorname{vol} L = \operatorname{vol} M \operatorname{vol}(L/M)$. If L_1 and L_2 are sublattices, then so are $L_1 \cap L_2$ and $L_1 + L_2$. The following theorem compares their volumes.

Theorem 1 (Theorem 1.12 [8], Proposition 2 [18]). *Suppose L_1 and L_2 are sublattices of L. Then*

$$\begin{aligned} \dim(L_1 \cap L_2) + \dim(L_1 + L_2) &= \dim(L_1) + \dim(L_2), \\ \operatorname{vol}(L_1 \cap L_2)\operatorname{vol}(L_1 + L_2) &\le \operatorname{vol}(L_1)\operatorname{vol}(L_2). \end{aligned}$$

Suppose we plot the points $(\dim M, \log \operatorname{vol} M)$ in the (x, y)-plane for all sublattices M of L. (The log is added to turn multiplicative relations to additive relations.) The plot is called the *canonical plot* of L. The above theorem tells us the relative positions of the points corresponding to L_1, L_2,$L_1 \cap L_2$, and $L_1 + L_2$. If three of them are given, they determine a parallelogram. If the fourth point comes from L_1 or L_2, then it lies at or above the fourth vertex of that parallelogram. On the other hand, if the fourth point comes from $L_1 \cap L_2$ or $L_1 + L_2$, then it lies at or below the fourth vertex of that parallelogram. This is called *the parallelogram constraint.*

The canonical plot of L is bounded below since there are only finitely many sublattices if we restrict the volume by an upper bound (Corollary 14). Thus its convex hull is bounded below by a convex polygon. It is called the *canonical polygon* of L. Suppose L_1 and L_2 are sublattices of L whose points lie on adjacent vertices of the polygon, and consider the line joining them. Assume $\dim L_1 < \dim L_2$. If $\dim(L_1 + L_2)$ is strictly bigger than $\dim L_2$, then the point corresponding to $L_1 + L_2$ has to lie above the line, and by the parallelogram constraint, the point corresponding to $L_1 \cap L_2$ has to lie below the line. This is a contradiction to the convexity. Therefore, $\dim(L_1 + L_2) = \dim L_2$ and it follows that $L_1 + L_2 = L_2$.

Otherwise, $L_1 + L_2$ would have a smaller volume, which is a contradiction. Thus, $L_1 \subset L_2$. Applying a similar argument to the lattices whose points lie on the same vertex of the polygon, it can be proved that they are equal. Therefore, the vertices of the polygon are represented by unique sublattices of L, and they form a chain $0 = L_0 \subset L_1 \subset \cdots \subset L_r = L$. This is called the *canonical filtration* of L.

Definition 2. A lattice L is said to be *semistable* if its canonical filtration consists of only 0 and L. It is said to be *unstable* otherwise.

For each $1 \le k \le n$, define the *minimum average length* of k-dimensional sublattices of L as follows.

$$\gamma_k(L) = \min \left\{ (\operatorname{vol} M)^{1/k} \;\middle|\; M \text{ is a } k\text{-dimensional sublattice of } L. \right\}.$$

If $k = 1$, then $\gamma_1(L)$ is simply the length of smallest nonzero vectors of L. For any lattice L of dimension n, define $\operatorname{slope}(L) = \log(\operatorname{vol} L^{1/n})$. Then, for each pair $L_1 \subsetneq L_2$ of sublattices, $\operatorname{slope}(L_2/L_1) = (\log \operatorname{vol} L_2 - \log \operatorname{vol} L_1)/(\dim L_2 - \dim L_1)$. This is the slope of the line joining the points corresponding to L_1 and L_2. If $0 = L_0 \subset L_1 \subset \cdots \subset L_r = L$ is the canonical filtration of L, then $\operatorname{slope}(L_{i+1}/L_i)$ is strictly increasing since it is the slope of the line segment comprising the canonical polygon of L. A lattice L is semistable if and only if $\operatorname{slope} M \ge \operatorname{slope} L$ for every sublattice M of L, or equivalently, $\gamma_k(L) \ge \gamma_n(L)$ for every $1 \le k \le n$. Therefore, proving the semistability of a lattice amounts to proving that the volume of every k-dimensional sublattice is bounded below by $(\operatorname{vol} L)^{k/n}$.

We will use the following theorem for the recursive algorithm in section 4 to compute the canonical filtration of a lattice. For a lattice L, let $\min L$ denote the smallest slope of the canonical polygon of L, and let $\max L$ denote the largest. If $0 = L_0 \subset L_1 \subset \cdots \subset L_r = L$ is the canonical filtration of L, then $\min L = \operatorname{slope} L_1$ and $\max L = \operatorname{slope}(L/L_{r-1})$.

Theorem 3 (Corollary 1.29 [8])**.** *Suppose L has a filtration $0 = L_0 \subsetneq L_1 \subsetneq \cdots \subsetneq L_r = L$ by sublattices such that $\max L_i/L_{i-1} \le \min L_{i+1}/L_i$. Then*

1. *The canonical polygon of L is formed by laying the canonical polygons of the subquotients L_i/L_{i-1} end to end.*
2. *Each L_i lies on the canonical polygon of L.*
3. *If $\max L_i/L_{i-1} < \min L_{i+1}/L_i$, then L_i is in the canonical filtration of L.*
4. *If $L_i \subset L' \subset L_{i+1}$ and L' is in the canonical filtration of L_{i+1}/L_i, then L' is in the canonical filtration of L.*
5. *The canonical filtration of L consists solely of sublattices arising as in (3) and (4).*

Corollary 4. *The orthogonal sum $L_1 \perp L_2$ of two lattices is semistable if and only if both are semistable and* $\operatorname{slope}(L_1) = \operatorname{slope}(L_2)$.

3. Root Lattices

The aim of this section is to prove the following theorem.

Theorem 5. *All irreducible root lattices are semistable.*

Irreducible root lattices consist of $\mathbb{Z}$, two infinite families $\mathbb{A}_n$ and $\mathbb{D}_n$, and three exceptional lattices $\mathbb{E}_6$, $\mathbb{E}_7$, and $\mathbb{E}_8$. (See Chapter 4 of [11] for detailed properties of those lattices.) It is easy to see that $\mathbb{Z}$ is semistable since its dimension is 1. Three exceptional lattices are treated individually using the algorithm of section 4, and they turn out to be semistable. (See Theorem 15.) So we need to treat $\mathbb{A}_n$ and $\mathbb{D}_n$.

Let's consider $\mathbb{A}_n$ first. We use the following vectors for its basis: $e_i = \varepsilon_0 - \varepsilon_i$, $1 \le i \le n$ where $\varepsilon_0, \dots, \varepsilon_n$ is the standard orthonormal basis of $\mathbb{R}^{n+1}$. The Gram matrix of $\mathbb{A}_n$ with respect to this basis is

$$A_n = \begin{pmatrix} 2 & 1 & \cdots & 1 \\ 1 & 2 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 2 \end{pmatrix}. \tag{1}$$

Lemma 6. *Let B_n be the matrix obtained by replacing $(1,1)$-entry of A_n by 1. Then $\det A_n = n+1$, and $\det B_n = 1$.*

Proof. Let $a_n = \det A_n$, and $b_n = \det B_n$. We get the following recursive formulas by row expansion of determinant.

$$a_1 = 2, \quad b_1 = 1, \quad a_n = 2a_{n-1} - (n-1)b_{n-1}, \quad b_n = a_{n-1} - (n-1)b_{n-1}.$$

They are satisfied by $a_n = n+1$ and $b_n = 1$. □

To show that $\mathbb{A}_n$ is semistable, we need to show $\gamma_k(\mathbb{A}_n) \ge \gamma_n(\mathbb{A}_n)$ for all $k = 1, 2, \dots, n$. Since $\mathbb{A}_n$ contains $\mathbb{A}_k$ as a sublattice,

$$\gamma_k(\mathbb{A}_n) \le \operatorname{vol}(\mathbb{A}_k)^{1/k} = (\sqrt{1+k})^{1/k}. \tag{2}$$

We will show that any k-dimensional sublattice of $\mathbb{A}_n$ actually has volume $\ge \sqrt{k+1}$. We do this by considering the k-th exterior power of $\mathbb{A}_n$.

If L is a lattice with basis $e_1, \dots, e_n$, then its k-th exterior power $\bigwedge^k L$ is the lattice with basis $e_I = e_{i_1} \wedge \cdots \wedge e_{i_k}$ for all $I = (i_1, \dots, i_k)$, $1 \le i_1 < \cdots < i_k \le n$. The inner product is given by

$$e_I \cdot e_J = \det(e_{i_s} \cdot e_{j_t})_{1 \le s \le k, 1 \le t \le k}.$$

Each k-dimensional sublattice M of L corresponds to the vector $v_1 \wedge \cdots \wedge v_k$ in $\bigwedge^k L$ if $v_1, \dots, v_k$ is a basis of M, and the volume of M is the length of the vector. Hence, the least volume of k-dimensional sublattices of L is the same as the least length of nonzero decomposable vectors of $\bigwedge^k L$. Therefore,

$$\gamma_k(L) \ge \gamma_1(\textstyle\bigwedge^k L)^{1/k}. \tag{3}$$

The equality does not hold in general, although in some special cases it does. For example, Coulangeon considered the case when $k = 2$ in detail in [6]. We prove that the equality holds for $\mathbb{A}_n$.

Theorem 7. *For the root lattice $\mathbb{A}_n$, we have*

$$\gamma_k(\mathbb{A}_n) = (\sqrt{k+1})^{1/k}.$$

Proof. By inequalities (2) and (3), it is enough to prove that $\gamma_1(\bigwedge^k \mathbb{A}_n) = \sqrt{k+1}$. We will find the Gram matrix of $\bigwedge^k \mathbb{A}_n$ and show that the minimum of the corresponding quadratic form is $k+1$.

First, we compute $e_I \cdot e_J = \det(E_{IJ})$ where E_{IJ} is the matrix

$$E_{IJ} = (e_{i_s} \cdot e_{j_t})_{1 \le s \le k, 1 \le t \le k}$$

where $I = (i_1, \dots, i_k)$, and $J = (j_1, \dots, j_k)$. Let $H = I \cap J$. There are three cases to consider: $|H| = k$, $|H| = k-1$, and $|H| < k-1$. If $|H| = k$, then $I = J$ and

$E_{IJ} = A_k$ so that $e_I \cdot e_J = k+1$. If $|H| < k-1$, then the matrix E_{IJ} has at least two common rows of the form $(1\ 1 \cdots 1)$, so $e_I \cdot e_J = 0$. Now suppose $|H| = k-1$ and let p be the index that is in I only, and q be the index in J only. We introduce a notation to keep track of the sign:

$$\mathrm{sgn}_I(i_s) = (-1)^{s-1} \quad \text{if} \quad I = (i_1, \dots, i_s, \dots, i_k).$$

Then $e_I \cdot e_J = \mathrm{sgn}_I(p)\mathrm{sgn}_J(q)$ because if

$$H = (h_1, \dots, h_{k-1}) = (i_1, \dots, \hat{p}, \dots, i_k) = (j_1, \dots, \hat{q}, \dots, j_k),$$

then by moving the p-th row to the top and the q-th column to the left,

$$\det(E_{IJ}) = \det \begin{pmatrix} e_{i_1} \cdot e_{j_1} & \cdots & e_{i_1} \cdot e_q & \cdots & e_{i_1} \cdot e_{j_k} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ e_p \cdot e_{j_1} & \cdots & e_p \cdot e_q & \cdots & e_p \cdot e_{j_k} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ e_{i_k} \cdot e_{j_1} & \cdots & e_{i_k} \cdot e_q & \cdots & e_{i_k} \cdot e_{j_k} \end{pmatrix}$$

is equal to

$$\mathrm{sgn}_I(p)\mathrm{sgn}_J(q) \det \begin{pmatrix} e_p \cdot e_q & e_p \cdot e_{h_1} & \cdots & e_p \cdot e_{h_{k-1}} \\ e_{h_1} \cdot e_q & e_{h_1} \cdot e_{h_1} & \cdots & e_{h_1} \cdot e_{h_{k-1}} \\ \vdots & \vdots & \ddots & \vdots \\ e_{h_{k-1}} \cdot e_q & e_{h_{k-1}} \cdot e_{h_1} & \cdots & e_{h_{k-1}} \cdot e_{h_{k-1}} \end{pmatrix}.$$

This matrix is B_k. Thus, $\det(E_{IJ}) = \mathrm{sgn}_I(p)\mathrm{sgn}_J(q) \det(B_k) = \mathrm{sgn}_I(p)\mathrm{sgn}_J(q)$ by Lemma 6.

Next, we compute the quadratic form associated to $\bigwedge^k \mathbb{A}_n$. Let $v = \sum_I x_I e_I$ be a nonzero vector in $\bigwedge^k \mathbb{A}_n$. Then,

$$\begin{aligned} |v|^2 &= \sum_{I,J} x_I x_J e_I \cdot e_J \\ &= \sum_I (k+1) x_I^2 + \sum_{\substack{I,J \\ |I \cap J| = k-1}} \pm x_I x_J \end{aligned}$$

where the sign of $\pm x_I x_J$ is $\mathrm{sgn}_I(p)\mathrm{sgn}_J(q)$ if $I - J = \{p\}$ and $J - I = \{q\}$. In order to write the sign uniformly, we introduce another notation. Suppose $I' = (i_1, \cdots, i_r)$ is an r-tuple of indices, not necessarily in an increasing order. Define $x_{I'} = 0$ if there are duplicate indices in I', or $x_{I'} = \mathrm{sgn}(\sigma) x_I$ where σ is the permutation reordering I' in ascending order, and $I = \sigma I'$. Also if $I = (i_1, \dots, i_r)$ and $J = (j_1, \dots, j_s)$ are two sequences of indices, then define their join by $IJ = (i_1, \dots, i_r, j_1, \dots, j_s)$. If I consists of a single index i, then we simply write iJ for IJ. With this notation, the second summation of $|v|^2$ is

$$\sum_{\substack{I,J \\ |I \cap J| = k-1}} \pm x_I x_J = \sum_{\substack{|H| = k-1 \\ 1 \le p \ne q \le n}} x_{pH} x_{qH}.$$

Therefore,

$$\begin{aligned}|v|^2 &= \sum_I (k+1)x_I^2 + \sum_{\substack{|H|=k-1\\1\le p\ne q\le n}} x_{pH}x_{qH}\\ &= \sum_I x_I^2 + \sum_{\substack{|H|=k-1\\1\le p,q\le n}} x_{pH}x_{qH}\\ &= \sum_I x_I^2 + \sum_{|H|=k-1}\left(\sum_{p=1}^n x_{pH}\right)^2\end{aligned}$$

Let $P = \sum_I x_I^2$, and $Q = \sum_{|H|=k-1} L_H^2$ where L_H is the linear form $\sum_{p=1}^n x_{pH}$. We want to show that $|v|^2 = P+Q$ is at least $k+1$. Suppose that x_I is nonzero only for l index sets $I = I_1, \dots, I_l$. If $l \ge k+1$, then P has enough nonzero terms, and $|v|^2 \ge P \ge k+1$. So suppose $1 \le l \le k$. Then $P \ge l$ and we need to show that $Q \ge k-l+1$. We count the number of index sets H of size $k-1$ such that $L_H \ne 0$ and show that the count is at least $k-l+1$. Note that x_{I_i} appears in L_H if and only if H is a subset of I_i. Therefore, x_{I_1} and x_{I_i} appear in L_H for the same H if and only if I_1 and I_i differ only by one index. Since we are considering only $l-1$ index sets different from I_1, there are at least $k-l+1$ possibilities that x_{I_1} appears alone in L_H, that is, $L_H = x_{I_1}$. Therefore, $Q \ge k-l+1$. This completes the proof. □

Corollary 8. *The root lattice $\mathbb{A}_n$ is semistable for $n \ge 1$.*

Proof. Consider the canonical plot of $\mathbb{A}_n$. In each dimension k, the lowest point is $\left(k, \frac{\log(k+1)}{2}\right)$ by Theorem 7. Since the graph of log function is concave downward, the convex hull of the canonical plot is bounded below by the line connecting the origin and the point corresponding to the whole lattice $\mathbb{A}_n$. Therefore, $\mathbb{A}_n$ is semistable. □

Now consider the root lattice $\mathbb{D}_n$. We use the basis $f_1, \dots, f_n$ where $f_1 = \varepsilon_0 + \varepsilon_2$, and $f_i = \varepsilon_0 - \varepsilon_i$ for $2 \le i \le n$. The Gram matrix with respect to this basis is

$$D_n = \begin{pmatrix} 2 & 0 & 1 & \cdots & 1\\ 0 & 2 & 1 & \cdots & 1\\ 1 & 1 & 2 & \cdots & 1\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ 1 & 1 & 1 & \cdots & 2\end{pmatrix}.$$

When $n = 2$ or 3, $\mathbb{D}_2$ is similar to $\mathbb{Z}^2$, and $\mathbb{D}_3$ is isometric to $\mathbb{A}_3$. Hence we assume $n \ge 4$. Since $f_1 = e_1 + \varepsilon_1 + \varepsilon_2$ and $f_i = e_i$ for $2 \le i \le n$ where $e_1, \dots, e_n$ is the basis of $\mathbb{A}_n$, we can use the results for $\mathbb{A}_n$ to derive the properties for $\mathbb{D}_n$.

Lemma 9. *The determinant of D_n is 4 for $n \ge 2$.*

Proof. Among many proofs, we show the one using the linearity of determinant and lemma 6. This method will be used again in the proof of Theorem 10. The first row of D_n is $(2,1,1,\dots,1)-(0,1,0,\dots,0)$. Hence

$$\det D_n = \begin{vmatrix} 2 & 1 & 1 & \cdots & 1 \\ 0 & 2 & 1 & \cdots & 1 \\ 1 & 1 & 2 & \cdots & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & \cdots & 2 \end{vmatrix} - \begin{vmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 2 & 1 & \cdots & 1 \\ 1 & 1 & 2 & \cdots & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & \cdots & 2 \end{vmatrix}$$

Similarly, the first column of the left matrix is $(2,1,1,\dots,1)^t-(0,1,0,\dots,0)^t$.

$$\det D_n = \det A_n - \begin{vmatrix} 0 & 1 & 1 & \cdots & 1 \\ 1 & 2 & 1 & \cdots & 1 \\ 0 & 1 & 2 & \cdots & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 1 & 1 & \cdots & 2 \end{vmatrix} - \begin{vmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 2 & 1 & \cdots & 1 \\ 1 & 1 & 2 & \cdots & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & \cdots & 2 \end{vmatrix}$$

By column and row expansions,

$$\det D_n = \det A_n + \det B_{n-1} + \begin{vmatrix} 0 & 1 & \cdots & 1 \\ 1 & 2 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 2 \end{vmatrix}$$

Expanding the last matrix similarly, we obtain

$$\det D_n = \det A_n + \det B_{n-1} + \det B_{n-1} - \det A_{n-2} = 4$$

□

The lattice $\mathbb{D}_n$ contains $\mathbb{D}_k$ and $\mathbb{A}_k$ for all $k \in \{1,2,\dots,n-1\}$. Therefore, $\gamma_1(\mathbb{D}_n) \le \sqrt{2}$, $\gamma_2(\mathbb{D}_n) \le \sqrt{3}^{1/2}$, and $\gamma_k(\mathbb{D}_n) \le \sqrt{4}^{1/k}$ for $3 \le k \le n$. We show that these are actually equalities.

Theorem 10. *For the root lattice $\mathbb{D}_n$, we have $\gamma_1(\mathbb{D}_n) = \sqrt{2}$, $\gamma_2(\mathbb{D}_n) = \sqrt{3}^{1/2}$, and $\gamma_k(\mathbb{D}_n) = \sqrt{4}^{1/k}$ for $3 \le k \le n$.*

Proof. We prove this by computing the lower bound on the length of nonzero vectors of $\bigwedge^k \mathbb{D}_n$ as in Theorem 7. The first step is to compute the quadratic form of $\bigwedge^k \mathbb{D}_n$ with respect to the basis $f_I = f_{i_1} \wedge \cdots \wedge f_{i_k}$ where $I = (i_1,\dots,i_k)$ and $1 \le i_1 < \cdots < i_k \le n$. Note that $f_i \cdot f_j = e_i \cdot e_j$ for all (i,j) except when $(i,j) = (1,2)$ or $(2,1)$. Therefore, $f_I \cdot f_J = e_I \cdot e_J$ in two cases: (1) I and J don't have 1, or (2) I has 1, but J doesn't have 2, or vice versa. In other cases, using the linearity of determinant as in Lemma 9, we get the following list where I and J are index sets not containing 1 nor 2.

$$\begin{aligned} f_{12I} \cdot f_{12J} &= e_{12I} \cdot e_{12J} + e_{2I} \cdot e_{1J} + e_{1I} \cdot e_{2J} - e_I \cdot e_J, \\ f_{12I} \cdot f_{1J} &= e_{12I} \cdot e_{1J} + e_{1I} \cdot e_J, \\ f_{12I} \cdot f_{2J} &= e_{12I} \cdot e_{2J} - e_{2I} \cdot e_J, \\ f_{1I} \cdot f_{2J} &= e_{1I} \cdot e_{2J} - e_I \cdot e_J. \end{aligned}$$

Let $v = \sum_I x_I f_I$ be a nonzero vector of $\bigwedge^k \mathbb{D}_n$. Then $|v|^2 = \sum_{I,J} x_I x_J f_I \cdot f_J$. Using the formulas above, we can turn $f_I \cdot f_J$ into $e_I \cdot e_J$ with a few additional terms.

$$\begin{aligned}
|v|^2 &= \sum_{I,J} x_I x_J e_I \cdot e_J + \sum_{\substack{1,2\notin I,J\\|I|=k-2\\|J|=k-2}} x_{12I}x_{12J}(e_{2I}\cdot e_{1J} + e_{1I}\cdot e_{2J}) \\
&+ \sum_{\substack{1,2\notin I,J\\|I|=k-2\\|J|=k-2}} -x_{12I}x_{12J}e_I\cdot e_J + \sum_{\substack{1,2\notin I,J\\|I|=k-2\\|J|=k-1}} 2x_{12I}x_{1J}e_{1I}\cdot e_J \\
&+ \sum_{\substack{1,2\notin I,J\\|I|=k-2\\|J|=k-1}} -2x_{12I}x_{2J}e_{2I}\cdot e_J + \sum_{\substack{1,2\notin I,J\\|I|=k-1\\|J|=k-1}} -2x_{1I}x_{2J}e_I\cdot e_J
\end{aligned}$$

We call these summations $S_1, S_2, \ldots, S_6$. As proved in Theorem 7, the first summation is

$$S_1 = \sum_{|I|=k} x_I^2 + \sum_{|I|=k-1} L_I^2.$$

For S_2, note that $e_{2I}\cdot e_{1J} = e_{1I}\cdot e_{2J} = 1$ if $I = J$, and it is 0 if $I \neq J$. Hence,

$$S_2 = 2\sum_{\substack{1,2\notin I\\|I|=k-2}} x_{12I}^2.$$

Next, S_3 is similar to S_1 except that $(1,2)$ is joined to the indices for x.

$$S_3 = -\sum_{\substack{1,2\notin I\\|I|=k-2}} x_{12I}^2 - \sum_{\substack{1,2\notin I\\|I|=k-3}} L_{12I}^2.$$

For S_4, note that $e_{1I}\cdot e_J = \operatorname{sgn}_J(p)$ if J contains I and p, and 0 otherwise. Therefore,

$$\begin{aligned}
S_4 &= 2\sum_{\substack{1,2\notin I\\|I|=k-2}} x_{12I}\left(\sum_{\substack{1,2\notin J\\|J|=k-1}} x_{1J}e_{1I}\cdot e_J\right) \\
&= 2\sum_{\substack{1,2\notin I\\|I|=k-2}} x_{12I}\left(\sum_{p\geq 3} x_{1pI}\right) \\
&= 2\sum_{\substack{1,2\notin I\\|I|=k-2}} x_{12I}\left(-x_{12I} - L_{1I}\right) \\
&= -2\sum_{\substack{1,2\notin I\\|I|=k-2}} x_{12I}^2 - 2\sum_{\substack{1,2\notin I\\|I|=k-2}} x_{12I}L_{1I}
\end{aligned}$$

Similarly,

$$S_5 = -2\sum_{\substack{1,2\notin I\\|I|=k-2}} x_{12I}^2 + 2\sum_{\substack{1,2\notin I\\|I|=k-2}} x_{12I}L_{2I}$$

Finally, S_6 is similar to S_1 and S_3. The difference is that we are considering a bilinear form instead of a quadratic form.

$$\begin{aligned} S_6 &= -\sum_{\substack{1,2\notin I\\|I|=k-1}} 2x_{1I}x_{2I} - \sum_{\substack{1,2\notin I\\|I|=k-2}} 2(L_{1I}+x_{12I})(L_{2I}-x_{12I}) \\ &= -\sum_{\substack{1,2\notin I\\|I|=k-1}} 2x_{1I}x_{2I} - \sum_{\substack{1,2\notin I\\|I|=k-2}} 2L_{1I}L_{2I} + \sum_{\substack{1,2\notin I\\|I|=k-2}} 2x_{12I}(L_{1I}-L_{2I}) + \sum_{\substack{1,2\notin I\\|I|=k-2}} 2x_{12I}^2 \end{aligned}$$

Combining $S_2, S_3, \dots, S_6$ together, we get

$$S_2+S_3+\cdots+S_6 = -\sum_{\substack{1,2\notin I\\|I|=k-2}} x_{12I}^2 - \sum_{\substack{1,2\notin I\\|I|=k-3}} L_{12I}^2 - 2\sum_{\substack{1,2\notin I\\|I|=k-1}} x_{1I}x_{2I} - 2\sum_{\substack{1,2\notin I\\|I|=k-2}} L_{1I}L_{2I}.$$

Now S_1 can be written as

$$\begin{aligned} S_1 &= \sum_{\substack{1,2\notin I\\|I|=k-2}} x_{12I}^2 + \sum_{\substack{1,2\notin I\\|I|=k-1}} x_{1I}^2 + \sum_{\substack{1,2\notin I\\|I|=k-1}} x_{2I}^2 + \sum_{\substack{1,2\notin I\\|I|=k}} x_I^2 \\ &+ \sum_{\substack{1,2\notin I\\|I|=k-3}} L_{12I}^2 + \sum_{\substack{1,2\notin I\\|I|=k-2}} L_{1I}^2 + \sum_{\substack{1,2\notin I\\|I|=k-2}} L_{2I}^2 + \sum_{\substack{1,2\notin I\\|I|=k-1}} L_I^2. \end{aligned}$$

Therefore,

$$|v|^2 = \sum_{\substack{1,2\notin I\\|I|=k-1}} (x_{1I}-x_{2I})^2 + \sum_{\substack{1,2\notin I\\|I|=k-2}} (L_{1I}-L_{2I})^2 + \sum_{\substack{1,2\notin I\\|I|=k}} x_I^2 + \sum_{\substack{1,2\notin I\\|I|=k-1}} L_I^2$$

We analyze this form case by case now. Suppose $k=1$. It is simple to show that

$$|v|^2 = (x_1-x_2)^2 + x_3^2 + \cdots + x_n^2 + (x_1+x_2+\cdots+x_n)^2 \geq 2.$$

Suppose $k=2$. Then,

$$|v|^2 = \sum_{i\geq 3}(x_{1i}-x_{2i})^2 + \left(\sum_{i\geq 3}(x_{1i}-x_{2i})\right)^2 + \sum_{3\leq i<j\leq n} x_{ij}^2 + \sum_{i\geq 3} L_i^2.$$

Consider several cases as follows.

(1) $x_{1i}-x_{2i}=0$ for all $i\geq 3$.
In this case $L_i = 2x_{1i} + \sum_{j\geq 3} x_{ji}$, and

$$|v|^2 = \sum_{3\leq i<j\leq n} x_{ij}^2 + \sum_{i\geq 3}\left(2x_{1i} + \sum_{j\geq 3} x_{ji}\right)^2.$$

If the first summation is zero, then $|v|^2$ is a multiple of 4. If it is 1, then all x_{ij}^2 is zero except one. Assume $x_{34}^2=1$ without loss of generality. Then

$$|v|^2 = 1 + (2x_{13}\pm 1)^2 + (2x_{14}\mp 1)^2 + 4\sum_{i\geq 5} x_{1i}^2 \geq 3.$$

Suppose $\sum_{3\le i<j\le n} x_{ij}^2 = 2$. We may assume $x_{34}^2 = 1$ and $x_{35}^2 = 1$, or $x_{34}^2 = 1$ and $x_{56}^2 = 1$. In each case,

$$\begin{aligned}|v|^2 &= 2 + (2x_{13} - x_{34} - x_{35})^2 \\ &\quad + (2x_{14} + x_{34})^2 + (2x_{15} + x_{35})^2 + 4\sum_{i\ge 6} x_{1i}^2 \ge 4, \\ |v|^2 &= 2 + (2x_{13} - x_{34})^2 \\ &\quad + (2x_{14} + x_{34})^2 + (2x_{15} - x_{56})^2 + (2x_{16} + x_{56})^2 + 4\sum_{i\ge 6} x_{1i}^2 \ge 6.\end{aligned}$$

In other cases, the first summation is at least 3.

(2) $x_{ij} = 0$ for all $i, j \ge 3$.
In this case $L_i = x_{1i} + x_{2i}$, and

$$|v|^2 = \sum_{i\ge 3}(2x_{1i}^2 + 2x_{2i}^2) + \left(\sum_{i\ge 3}(x_{1i} - x_{2i})\right)^2.$$

If $x_{1i} = 0$ for all i, then $|v|^2 = 3\sum x_{2i}^2 \ge 3$. Similarly $|v|^2 \ge 3$ if $x_{2i} = 0$ for all i. Otherwise, $|v|^2 \ge 2 + 2 = 4$.

(3) $x_{1i} - x_{2i} \ne 0$ for some $i \ge 3$ and $x_{jk} \ne 0$ for some $j, k \ge 3$.
In this case, if $|x_{1i} - x_{2i}|$ is greater than 1, then $|v|^2 \ge 4$. If $|x_{1i} - x_{2i}|$ is nonzero for more than one i, then $|v|^2$ has at least three nonzero terms, thus $|v|^2 \ge 3$. Otherwise, $|v|^2 = (x_{1i} - x_{2i})^2 + (x_{1i} - x_{2i})^2 + x_{jk}^2 + \cdots \ge 3$.

Finally, suppose $k \ge 3$. We will show that $|v|^2 \ge 4$.

(1) $x_I = 0$ for any I such that $1, 2 \notin I$.
In this case,

$$|v|^2 = \sum_{\substack{1,2\notin I \\ |I|=k-1}} (2x_{1I}^2 + 2x_{2I}^2) + \sum_{\substack{1,2\notin J \\ |J|=k-2}} (L_{1J} - L_{2J})^2.$$

If there are at least two nonzero terms for x_{1I} and x_{2I}, then $|v|^2 \ge 4$. So assume that $x_{1I} = 0$ for all I, and $x_{2I} \ne 0$ for exactly one index set. We denote that index set simply by I. Since

$$(L_{1J} - L_{2J})^2 = \left(\sum_{p\ge 3}(x_{p1J} - x_{p\,2J})\right)^2 = \left(\sum_{p\ge 3} x_{2pJ}\right)^2,$$

there are $k - 1$ index sets J such that $x_{2pJ} = \pm x_{2I}$ for some $p \ge 3$, and $(L_{1J} - L_{2J})^2 = x_{2I}^2$ for such J, and 0 for other J's. Hence, $|v|^2 = 2x_{2I}^2 + (k-1)x_{2I}^2 \ge k + 1 \ge 4$.

(2) $x_{1I} - x_{2I} = 0$ for all I such that $1, 2 \notin I$.
In this case,

$$|v|^2 = \sum_{\substack{1,2\notin I \\ |I|=k}} x_I^2 + \sum_{\substack{1,2\notin J \\ |J|=k-1}} \left(2x_{1J} + \sum_{i\ge 3} x_{iJ}\right)^2.$$

If the first term is zero, then $|v|^2 = \sum(2x_{1I})^2 \ge 4$. If $|x_I| \ge 2$ for some I, then $|v|^2 \ge 4$. So assume that $x_I^2 = 1$ for at least one and at most three index sets I. Suppose $x_I^2 = 1$ for one index set $I = (i_1, i_2, i_3, \ldots, i_k)$. Let $J_l = (i_1, \ldots, \widehat{i_l}, \ldots, i_k)$. Then

$$\begin{aligned} |v|^2 &= x_I^2 + \sum_{l=1}^{k} (2x_{1J_l} \pm x_I)^2 + \sum_{\substack{1,2 \notin J \\ |J|=k-1 \\ J \not\subset I}} (2x_{1J})^2 \\ &\geq 1 + \sum_{l=1}^{k} (2x_{1J_l} \pm 1)^2 \geq 1 + k \geq 4. \end{aligned}$$

Next, suppose $x_I^2 = x_{I'}^2 = 1$ for two index sets I and I'. Pick two elements $p \in I - I'$ and $p' \in I' - I$. Let $H = I \cap I'$. If H is empty, then let $J = I - \{p\}$ and $J' = I' - \{p'\}$. Then $|v|^2$ has 4 nonzero terms x_I^2, $x_I'^2$, $(2x_{1J} + x_{pJ})^2$, and $(2x_{1J'} + x_{p'J'})^2$. If H is nonempty, pick an element $h \in H$, and let $J = I - \{h\}$, and $J' = I' - \{h\}$. Then $|v|^2$ has 4 nonzero terms x_I^2, $x_I'^2$, $(2x_{1J} + x_{hJ})^2$, and $(2x_{1J'} + x_{hJ'})^2$. Now suppose $x_I^2 = x_{I'}^2 = x_{I''}^2 = 1$ for three index sets. It is enough to prove that $|v|^2$ has one more nonzero term. Let $H = I \cap I' \cap I''$. If H is nonempty, choose $h \in H$, and let $J = I - \{h\}$. Then $|v|^2$ has the nonzero term $(2x_{1J} + x_{hJ})^2$. Now assume H is empty. If $I' \cap I''$ is empty, then $|I| \geq |I \cap I'| + |I \cap I''|$. Thus either $|I \cap I'| \leq k/2$ or $|I \cap I''| \leq k/2$. Suppose $|I \cap I'| \leq k/2$ without loss of generality. Then $|I' - I| \geq k/2 \geq 3/2$, and there exist two elements p, q that belongs to I' only. Then letting $J = I' - \{p\}$, we see that $|v|^2$ has the nonzero term $(2x_{1J} + x_{pJ})^2$. The same argument works if $I \cap I''$ or $I \cap I'$ is empty. Suppose that $I \cap I' \cap I''$ is empty, but $I \cap I'$, $I' \cap I''$, and $I \cap I''$ are not empty. If there exists an element p that belongs to I only, then let $J = I - \{p\}$. Since J intersects with both I' and I'', we see that iJ cannot be I'' or I' for any i. Hence $|v|^2$ has the nonzero term $(2x_{1J} + x_{pJ})^2$. The same argument works if there exists an element that belongs to I' only, or I'' only. The remaining case is that $I \cap I' \cap I'' = \emptyset$, $I = (I \cap I') \cup (I \cap I'')$, $I' = (I' \cap I) \cup (I' \cap I'')$, and $I'' = (I'' \cap I) \cup (I'' \cap I')$. Since each of I, I', and I'' has at least three elements, one of $I \cap I'$, $I \cap I''$, and $I' \cap I''$ has at least 2 elements. Suppose $I \cap I'$ has at least 2 elements, say p and q, without loss of generality. Then let $J = I - \{p\}$. Since J contains an element of $I \cap I''$, which does not belong to I', the set iJ cannot be I' for any i. It cannot be I'' either since q belongs to J, but not to I''. Therefore, $|v|^2$ contains the nonzero term $(2x_{1J} + x_{pJ})^2$.

(3) $x_{1I} - x_{2I} = 0$ for all but one I such that $1, 2 \notin I$.
We denote such index set simply by I. Then

$$|v|^2 = (x_{1I} - x_{2I})^2 + \sum_{\substack{1,2 \notin J \\ |J|=k-2}} (L_{1J} - L_{2J})^2 + \sum_{\substack{1,2 \notin K \\ |K|=k}} x_K^2 + \sum_{\substack{1,2 \notin H \\ |H|=k-1}} L_H^2.$$

Note that $(L_{1J} - L_{2J})^2 = \left(\sum_{p \geq 3} x_{1pJ} - x_{2pJ}\right)^2$ is zero if $pJ \neq I$ for any $p \geq 3$. It is nonzero only for $J = I - \{i\}$, $i \in I$, and for those J's,

$(L_{1J}-L_{2J})^2=(x_{1I}-x_{2I})^2$. Therefore,

$$|v|^2 \geq (x_{1I}-x_{2I})^2+(k-1)(x_{1I}-x_{2I})^2+\sum_{\substack{1,2\notin K\\|K|=k}} x_K^2+\sum_{\substack{1,2\notin H\\|H|=k-1}} L_H^2.$$

We have already considered the case where $x_K=0$ for all K, thus we may assume that x_K is nonzero for some K. Then $|v|^2\geq 1+(k-1)+1\geq 4$.

(4) $x_{1I}-x_{2I}=0$ for all but two I's such that $1,2\notin I$.
We denote those index sets by I and I'. If they differ by more than one element, then $(L_{1J}-L_{2J})^2=(x_{1I}-x_{2I})^2$ for those J's obtained by removing an element from I. and $(L_{1J}-L_{2J})^2=(x_{1I'}-x_{2I'})^2$ for those J's obtained by removing an element from I'. So $|v|^2$ has at least four nonzero terms. If I and I' differ by only one element, say p, then $(L_{1J}-L_{2J})^2=(x_{1I}-x_{2I})^2$ for those J's obtained by removing an element other than p from I. This is possible because $|I|=k-1\geq 2$. The same holds for I'. Therefore $|v|^2\geq 4$.

(5) $x_{1I}-x_{2I}=0$ for at least three I's such that $1,2\notin I$.
In this case, we may assume at least one x_J is nonzero for some J such that $1,2\notin J$ and $|J|=k$ since we have considered the contrary case already. Then $|v|^2$ has at least four nonzero terms.

□

Corollary 11. *The root lattice $\mathbb{D}_n$ is semistable for $n\geq 4$.*

Proof. Consider the canonical plot $\mathbb{D}_n$. By Theorem 10, the lowest point in dimension 1 is $\left(1,\frac{\log 2}{2}\right)$. In dimension 2, the lowest point is $\left(2,\frac{\log 3}{2}\right)$. In dimension $k\geq 3$, the lowest point is $\left(k,\frac{\log 4}{2}\right)$. Therefore, the canonical polygon of $\mathbb{D}_n$ consists of the single line connecting the origin and $\left(n,\frac{\log 4}{2}\right)$. □

4. Computing the canonical filtration of a lattice

We describe a recursive algorithm to compute the canonical filtration of a lattice in this section. Suppose L is a lattice of dimension n, and M is its sublattice of dimension k for $1\leq k\leq n-1$. If $\max M\leq \min L/M$, then by Theorem 3, M lies on the canonical polygon of L, and the canonical filtration of L is obtained by combining the canonical filtration of M and the canonical filtration of L/M. Such a sublattice M should satisfy the following conditions: $\operatorname{vol} M$ is minimal among k-dimensional sublattices, and $\operatorname{vol} M^{1/k}\leq \operatorname{vol} L^{1/n}$. The algorithm first tries to find such a lattice M, and if it succeeds, then it recursively finds the canonical filtrations of M and L/M, and they are combined together.

Finding a k-dimensional sublattice of L of smallest volume is roughly equivalent to finding a smallest nonzero vector in $\bigwedge^k L$, which is a lattice of dimension $\binom{n}{k}$. So it is most time-consuming when k is close to $n/2$, and is fast when k is close to 0 or n.

When the dimension of M is larger than $n/2$, we use the dual lattice L^* of L. The relationship between the canonical plot of L and the canonical plot of L^* is explained in [8, section 7]. The transformation

$$(x,y)\mapsto (n-x,\,y-\log\operatorname{vol} L) \tag{4}$$

of the plane transforms the canonical plot of L to the canonical plot of L^*.

The dual lattice L^* is defined to be $\mathrm{Hom}_{\mathbb{Z}}(L,\mathbb{Z})$ considered as a subgroup of $E^* = \mathrm{Hom}_{\mathbb{R}}(E,\mathbb{R})$ where E is the Euclidean space in which L is embedded. The isomorphism $E \to E^*$ defined by $v \mapsto (w \mapsto v \cdot w)$ transports the inner product on E to the inner product on E^*. The dual basis of the orthonormal basis becomes an orthonormal basis, and E^{**} is isometric to E via the canonical isomorphism $E \to E^{**}$. If A is the Gram matrix of L with respect to the basis $\mathcal{E} = \{e_1, \dots, e_n\}$, then the matrix of the map $E \to E^*$ with respect to $\mathcal{E}$ and the dual basis $\mathcal{E}^*$ is the same as A. Therefore, the Gram matrix of L^* with respect to $\mathcal{E}^*$ is $(A^{-1})^t A (A^{-1}) = (A^{-1})^t = A^{-1}$. This implies that $\mathrm{vol}\, L^* = (\mathrm{vol}\, L)^{-1}$.

Suppose M is a sublattice of L and $\{b_1, \dots, b_k\}$ is a basis of M. The basis can be extended to a basis $\{b_1, \dots, b_k, b_{k+1}, \dots, b_n\}$ of L. The additional vectors can be computed explicitly by reversing the row and column operations for the smith normal form of the inclusion map $M \to L$. (Every diagonal entry of the smith normal form is 1 since L/M is torsion-free.) Dualizing the exact sequence $0 \to M \to L \to L/M \to 0$, we get an exact sequence $0 \to (L/M)^* \to L^* \to M^* \to 0$. The image of $(L/M)^*$ in L^* is denoted by $M^{\#}$. The lattice $(L/M)^*$ is generated by the dual basis of $\{\overline{b_{k+1}}, \dots, \overline{b_n}\}$, and the image of $\overline{b_i}^*$ in L^* is b_i^*. Therefore, $M^{\#}$ is generated by $\{b_{k+1}^*, \dots, b_n^*\}$. The assignment $M \mapsto M^{\#}$ defines a one-to-one correspondence between the sublattices of L and the sublattices of L^* since $M^{\#\#}$ is identified with M via the identification of L^{**} with L.

Let `CanonicalFiltration`(L) denote the program returning the canonical filtration of L, and let `SmallestSublattice`(L,k,V) be the program that returns `fail` if there is no sublattice of L of volume $\leq V$ and returns a sublattice of the smallest volume in dimension k otherwise. Table 1 describes the algorithm for `CanonicalFiltration`.

The function `SmallestSublattice` requires more explanation. In dimension 1, the problem of finding the smallest sublattice is known as the shortest vector problem. In higher dimensions, it is to find a basis of the sublattice consisting of short vectors. We use a backtracking algorithm to solve the problem in dimensions > 1.

Assuming that the basis of a sublattice is reduced, it is possible to bound the length of each basis vector by an expression involving the volume of the sublattice (or an upper bound on the volume). We first construct a database of short vectors with this bound (which is a finite set), and then search for a sublattice of smallest volume among those generated by the vectors in the database.

We will use LLL-reduced basis [10], [4], which gives an explicit upper bound on the length of the largest basis vector. Suppose that $= \{b_1, b_2, \dots, b_k\}$ is a basis of a lattice M and that $\widetilde{B} = \{\widetilde{b_1}, \widetilde{b_2}, \dots, \widetilde{b_k}\}$ is its Gram-Schmidt orthogonal basis where $\widetilde{b_i} = b_i - \sum_{j=1}^{i-1} \mu_{ij} \widetilde{b_j}$ and $\mu_{ij} = (b_i, \widetilde{b_j})/(\widetilde{b_j}, \widetilde{b_j})$.

Definition 12. [10] Suppose $B = \{b_1, \dots, b_k\}$ is a basis of a lattice M, and $\widetilde{B}$ and μ are defined as above. Then B is called LLL-reduced if the following two conditions are satisfied.

1. $|\mu_{ij}| \leq 1/2$ for $1 \leq j < i \leq k$,
2. $|\widetilde{b_i} + \mu_{ii-1}\widetilde{b_{i-1}}|^2 \geq y|\widetilde{b_{i-1}}|^2$ for $1 < i \leq k$, where y is an adjustable parameter in the interval $(1/4, 1)$.

There is an algorithm called LLL-reduction that computes an LLL-reduced basis from an arbitrary basis of a lattice. As the parameter y gets closer to 1, the

	`CanonicalFiltration`(L)
(1)	If $\dim L$=1, then return the trivial filtration $0 \subset L$.
(2)	Set $k \leftarrow 1$.
(3)	[Finding a sublattice]
	If $k > n/2$, then return the trivial filtration $0 \subset L$.
	Perform $M \leftarrow$`SmallestSublattice`$(L,k,\mathrm{vol}\, L^{k/n})$.
	If M=`fail`, then go to step (4).
	Check the slope condition: $\max M \leq \min L/M$.
	If the condition is not satisfied, then go to step (4).
	Otherwise, go to step (6).
(4)	[Finding a dual sublattice]
	If $k \geq n/2$, then return the trivial filtration $0 \subset L$.
	Perform $N \leftarrow$`SmallestSublattice`$(L^*,n-k,\mathrm{vol}\, L^{-k/n})$,
	If N=`fail`, then go to step (5).
	Check the slope condition: $\max N \leq \min L^*/N$.
	If the condition is not satisfied, then go to step (5).
	Otherwise, set $M \leftarrow N^{\#}$, then go to step (6).
(5)	[Loop]
	$k \leftarrow k+1$ and go to step (3),
(6)	[Recursive step]
	Perform `CanonicalFiltration`(M) and `CanonicalFiltration`(L/M).
	Combine two filtrations together to obtain
	the canonical filtration of L and return it.
	M is a part of the filtration if and only if $\max M \lneqq \min L/M$.

Table 1. Canonical Filtration

algorithm produces shorter basis of the lattice but takes longer time. Theoretically, we just may assume $y = 1$, that is, there exists a basis B satisfying two conditions of the definition with the parameter $y = 1$.

One of the properties derived from the definition is the following inequality [10, Proposition 1.6].

$$|b_j|^2 \leq (4/3)^{i-1}|\widetilde{b_i}|^2 \quad \text{for} \quad 1 \leq j \leq i \leq k. \tag{5}$$

The volume of L is $\gamma_k(L) = \prod_{i=1}^{k} |\widetilde{b_i}|$. Multiplying these inequalities for $j \leq i \leq k$, we get a bound of b_j,

$$|b_j| \leq (4/3)^{(k+j-2)/4} \left(\frac{\gamma_k(M)}{\prod_{i=1}^{j-1} |b_i^*|} \right)^{\frac{1}{k-j+1}}.$$

Using inequalities (5) again to replace $|b_i^*|$ by $|b_i|$, we obtain

$$|b_j| \leq (4/3)^{(k+j^2-2j)/4} \left(\frac{\gamma_k(M)}{\prod_{i=1}^{j-1} |b_i|} \right)^{\frac{1}{k-j+1}}.$$

The greatest upper bound occurs when b_i's are smallest vectors for $1 \leq i \leq j-1$. Therefore, we have

$$|b_j| \leq (4/3)^{(k+j^2-2j)/4} \left(\frac{\gamma_k(M)}{\gamma_1(M)^{j-1}} \right)^{\frac{1}{k-j+1}} \quad \text{for } 1 \leq j \leq k.$$

We have proved the following proposition.

Proposition 13. *Let M be a lattice of dimension k such that* $\operatorname{vol} M \leq V$. *Then there exists a basis $B = (b_1, \dots, b_k)$ of M such that*

$$|b_j| \leq (4/3)^{(k+j-2)/4} \left(\frac{V}{\operatorname{vol} M_{j-1}} \right)^{\frac{1}{k-j+1}} . \tag{6}$$

for each $1 \leq j \leq n$, where M_j is the sublattice of M generated by $b_1, \dots, b_j$. Moreover, the lengths of all vectors of B are bounded above by the constant

$$\max_{1 \leq j \leq k} (4/3)^{(k+j^2-2j)/4} \left(\frac{V}{\gamma_1(M)^{j-1}} \right)^{\frac{1}{k-j+1}} . \tag{7}$$

Now consider the problem of finding a k-dimensional sublattice M of L whose volume is $\leq V$ and is smallest among all k-dimensional sublattices. Such a sublattice can be described by its basis. A sequence $(b_1, \dots, b_k)$ of k vectors will be called a *solution* if they generated such a sublattice.

Consider the set of all j-tuples of vectors of L whose length is bounded above by the constant (7) where j varies from 0 to k. The set can be described as the set of all vertices of the rooted tree defined as follows. The root is the empty tuple, and there is a edge from $B = (b_1, \dots, b_j)$ to $B' = (b'_1, \dots, b'_{j'})$ if and only if $j' = j + 1$ and $b'_i = b_i$ for $i = 1, \dots, j$. By the previous proposition, all solutions (if there are any) are leaves of this tree. The tree is finite. In particular, we have the following corollary.

Corollary 14. *Suppose L is an n-dimensional lattice. For each $0 < k < n$ and $V > 0$, there are only finitely many k-dimensional lattices with volume $\leq V$.*

We traverse the tree starting from the root to search for a solution. A vertex will be called a *partial solution* if it leads to a leaf that is a solution. Two vertices are said to be *equivalent* if both are partial solutions, or if both are not partial solutions. As soon as we find that a vertex is not a partial solution, we prune out that vertex (including the subtree starting from it) as well as equivalent vertices, and then we continue searching other parts of the tree. Since we want to find a sublattice with the smallest volume, we need to search the whole tree after finding a sublattice of volume $\leq V$ to see if there are sublattices of smaller volume. The search can be completed faster if it can be proven in an early stage that a vertex is not a partial solution, and if as many equivalent vertices can be detected and removed for each visited vertex as possible without too much computation.

Suppose $B_j = (b_1, \dots, b_j)$ is the vertex we're currently visiting, and let M_j be the subgroup of L generated by B_j. We discuss several criteria to test if B_j is possibly a partial solution and some simple methods to find some of the equivalent vertices to B_j.

First, by Proposition 13, B_j is not a partial solution if the length of b_j is greater than the bound (6).

Second, if B'_j is another vertex with the same set of vectors as that of B_j (listed in a different order), then the subgroup generated by B'_j is the same as M_j. So we may prune out all vertices obtained by reordering the vectors of B_j. In other words, we may give an order to the set of all vectors of L from the beginning and consider only increasing tuples of vectors.

	`SmallestSublattice`(L, k, V)
(1)	Set $M \leftarrow$ `fail`, $j \leftarrow 1$, and $X_1 \leftarrow \{v \in L \,\vert\, 0 < \vert v\vert \leq \texttt{bound}(0)\}$
(2)	If $j = 0$ then return M.
(3)	$b_j \leftarrow \texttt{next}(X_j)$
(4)	If b_j=`fail`, then set $j \leftarrow j - 1$, and go to step (2)
(5)	If $j < k$, then set $X_{j+1} \leftarrow \{v \in L \,\vert\, 0 < \vert v\vert \leq \texttt{bound}(B_j)\}$, $j \leftarrow j + 1$, and go to step (3)
(6)	Compare the volume of M_k with V. If $\operatorname{vol} M_k \leq V$, then set $M \leftarrow M_k$, $V \leftarrow \operatorname{vol} M_k$, and update the sets $X_1, \ldots, X_k$ with the new bounds.
(7)	Go to step (3).

Table 2. Sublattice of Smallest Volume

Third, every sublattice of a sublattice is a sublattice, that is, if L/M_j has torsion, then B_j cannot be a partial solution, because for any subgroup containing M_j, there will be a sublattice with strictly smaller volume. We test this by computing the smith normal form of the inclusion map $M_j \to L$, then by checking whether all diagonal entries are 1's. The test will also ensure that M_j is of dimension j, that is, the vectors of B_j form an independent set of vectors.

Fourth, we use the automorphism group of L if it is nontrivial. Note that if g is an automorphism of L, then M and gM have the same volume for any sublattice M of L. Suppose g fixes $b_1, \ldots, b_j$, that is g is an element of the (pointwise) stabilizer G of M_j. Then the vertex $(b_1, \ldots, b_j, b)$ is equivalent to $(b_1, \ldots, b_j, gb)$. Let X be the set of all children of the vertex B_j. Then the stabilizer group G acts on X. Let $\overline{X}$ be the orbit space. We may visit only one representative of each orbit. Computing the whole stabilizer group can be time consuming since the number of such groups we have to compute increases exponentially with k. Therefore, we only compute a few random elements of the group and build the orbit space $\overline{X}$ using them. We construct $\overline{X}$ inductively using a probabilistic method. Suppose $g_1, \ldots, g_r$ are randomly chosen elements of G, and G_r is the subgroup of G generated by them. Then G_r acts on X. We denote the orbit of $x \in X$ by $G_r \cdot x$, and denote the orbit space under G_r by X_r. Let

$$H_r = \{g \in G \,|\, gx \in G_r \cdot x \quad \text{for all } x \in X\}\,.$$

It is a subgroup of G since G is a finite group, and $H_r = G$ if and only if $X_r = \overline{X}$. Let g_{r+1} be another random element of G. Then the orbit space of X under G_r and the one under G_{r+1} are equal if and only if g_{r+1} is an element of H_r. Therefore, the probability that $X_r = X_{r+1}$ is $|H_r|/|G|$. It implies the probability that $X_r = X_{r+1} = \cdots = X_{r+m}$ when $X_r \neq \overline{X}$ is as small as $(|H_r|/|G|)^m \leq (1/2)^m$. Thus we may assume with high probability that $X_r = \overline{X}$ if $X_r = X_{r+1} = \cdots X_{r+m}$ for sufficiently large m. A random element of the stabilizer group can be computed using the method of [14] by Plesken and Souvignier.

The algorithm of `SmallestSublattice` is described in Table 2. In this algorithm, X_j denotes the set of vectors corresponding to the edges from B_j to its children. The function $\texttt{next}(X_j)$ tests the criteria explained so far, and returns a vector b that has not been tested yet, and removes all vertices equivalent to b from X_j (including b itself). If X_j is empty, it returns `fail`.

5. Computational result

The classification of all perfect lattices of dimension 8 has been completed recently. Laïhem[9], Baril[1], Napias[13], and Batut and Martinet[2] found 10916 perfect lattices of dimension 8, and Mathieu Dutour Sikirić, Achill Schürmann, and Frank Vallentin proved that there are no more [17]. These lattices can be viewed in Jacques Martinet's homepage `http://www.math.u-bordeaux1.fr/~martinet/` or the web-page `http://www.math.uni-magdeburg.de/lattice_geometry/` maintained by Achill Schürmann and Frank Vallentin. The algorithm in the previous section implemented in GAP computer algebra system [7] on these data revealed that all perfect lattices of dimension 2–7 are semistable and that there exists exactly one perfect lattice of dimension 8 that is unstable. It is listed as 'Form Nr. 68' in the file [15]. The following is the Gram matrix of the lattice.

$$P_8^{68} = \begin{pmatrix} 4 & 2 & 2 & 0 & 0 & 0 & 0 & 2 \\ 2 & 4 & 2 & 0 & 1 & -1 & 1 & 1 \\ 2 & 2 & 4 & 2 & 1 & -1 & 1 & 1 \\ 0 & 0 & 2 & 4 & 0 & 0 & 2 & 0 \\ 0 & 1 & 1 & 0 & 4 & 2 & 2 & 2 \\ 0 & -1 & -1 & 0 & 2 & 4 & 2 & 2 \\ 0 & 1 & 1 & 2 & 2 & 2 & 4 & 2 \\ 2 & 1 & 1 & 0 & 2 & 2 & 2 & 4 \end{pmatrix}$$

This lattice is extreme as well as perfect. Its determinant is 576. It has 71 pairs of shortest vectors of norm 4. On the other hand, the inverse of P_8^{68} has a unique pair of shortest vectors $\pm(0,0,0,0,1,1,1,1)$ of norm 4/9, which implies that it has a unique sublattice of codimension 1 of determinant 256. Since $2.208 \approx 256^{1/7} < 576^{1/8} \approx 2.213$, this lattice is unstable. The lattice is called the Coxeter-Barnes lattice $\mathbb{A}_8^2$. The usual basis for the lattice is

$$\mathcal{B} = (e_1, e_2, e_3, e_4, e_5, e_6, e_7, f)$$

where $e_i = \varepsilon_i - \varepsilon_0$ and $f = \frac{1}{2}(e_1 + \cdots + e_8)$ (See [11, section 5.1]). The Gram matrix corresponding to the basis $\sqrt{2}\mathcal{B}$ (rescaled to make the matrix integral) is

$$A_8^2 = \begin{pmatrix} 4 & 2 & 2 & 2 & 2 & 2 & 2 & 9 \\ 2 & 4 & 2 & 2 & 2 & 2 & 2 & 9 \\ 2 & 2 & 4 & 2 & 2 & 2 & 2 & 9 \\ 2 & 2 & 2 & 4 & 2 & 2 & 2 & 9 \\ 2 & 2 & 2 & 2 & 4 & 2 & 2 & 9 \\ 2 & 2 & 2 & 2 & 2 & 4 & 2 & 9 \\ 2 & 2 & 2 & 2 & 2 & 2 & 4 & 9 \\ 9 & 9 & 9 & 9 & 9 & 9 & 9 & 36 \end{pmatrix}$$

A transition matrix from A_8^2 to P_8^{69} is, for example,

$$T = \begin{pmatrix} -1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ -1 & -1 & -1 & -1 & 0 & 0 & 0 & 1 \\ -1 & -1 & -1 & 0 & -1 & 0 & 0 & 1 \\ -1 & -1 & -1 & -1 & -2 & -1 & -1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix},$$

that is, $TA_8^2T^t = P_8^{68}$. The unique pair of shortest vectors in $(\mathbb{A}_8^2)^*$ is

$$\pm(e_1^* + e_2^* + e_3^* + e_4^* + e_5^* + e_6^* + e_7^* + 4f^*)$$

and the corresponding sublattice of $\mathbb{A}_8^2$ of dimension 7 is spanned by

$$(e_1 - e_2, e_2 - e_3, e_3 - e_4, e_4 - e_5, e_5 - e_6, e_6 - e_7, f - e_1 - e_2 - e_3 - e_4)$$

and is the exceptional lattice $\mathbb{E}_7 \subset \mathbb{A}_8^2$.

Theorem 15. (1) *All perfect lattices in dimension 2–7 are semistable.*
(2) *Among 10916 perfect lattices of dimension 8, the Coxeter-Barnes lattice $\mathbb{A}_8^2$ is the unique unstable lattice, and $0 \subset \mathbb{E}_7 \subset \mathbb{A}_8^2$ is its canonical filtration. All other 8-dimensional perfect lattices are semistable.*

The classification of perfect forms in dimension 9 is still in progress. There are more than 500000 perfect lattices currently known [16]. Unstable lattices among dimension 9 are scarcer. All known 9-dimensional lattices are semistable except the one with the following Gram matrix listed as 'Form Nr. 8' in the file [16].

$$P_9^8 = \begin{pmatrix} 6 & 3 & 2 & 3 & 3 & 3 & 3 & 0 & 3 \\ 3 & 6 & 2 & 3 & 3 & 3 & 3 & 0 & 3 \\ 2 & 2 & 6 & 2 & 2 & 2 & 3 & 0 & 0 \\ 3 & 3 & 2 & 6 & 3 & 3 & 3 & 0 & 3 \\ 3 & 3 & 2 & 3 & 6 & 3 & 3 & 0 & 3 \\ 3 & 3 & 2 & 3 & 3 & 6 & 3 & 3 & 3 \\ 3 & 3 & 3 & 3 & 3 & 3 & 6 & 3 & 3 \\ 0 & 0 & 0 & 0 & 0 & 3 & 3 & 6 & 3 \\ 3 & 3 & 0 & 3 & 3 & 3 & 3 & 3 & 6 \end{pmatrix}$$

If $b_1, \ldots, b_9$ are the basis vectors of the lattice L giving the above Gram matrix, then the canonical filtration of L is $0 \subset M \subset L$ where M is the 8-dimensional sublattice of L generated by $b_1, b_2, b_4, b_5, b_6, b_7, b_8$, and b_9. The lattice $M/\sqrt{3}$ is even, unimodular, and integral, thus is the exceptional lattice $\mathbb{E}_8$. (See [5, 4.8.1].) Therefore, $M = \sqrt{3}\mathbb{E}_8$. The determinant of M and the determinant of L are 6561 and 21870, respectively. The lattice L is unstable as we can see from the inequality $3 = 6561^{1/8} < 21870^{1/9} \approx 3.035$.

References

[1] J-L. Baril, 'Autour de l'algorithme de Voronoi: Construction de réseaux Euclidiens.' Ph.D. thesis, Bordeaux, (1996).

[2] C. Batut and J. Martinet, 'A catalogue of perfect lattices.' http://www.math.u-bordeaux.fr/~martinet/.

[3] A. Borel and J.-P. Serre, 'Corners and arithmetic groups.' *Comment. Math. Helv.* 48 (1973) 436–491. Avec un appendice: Arrondissement des variétés à coins, par A. Douady et L. Hérault.

[4] Henri Cohen, *A course in computational algebraic number theory*, vol. 138 of *Graduate Texts in Mathematics* (Springer-Verlag, Berlin, 1993). ISBN 3-540-55640-0.

[5] J. H. Conway and N. J. A. Sloane, *Sphere packings, lattices and groups*, vol. 290 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]* (Springer-Verlag, New York, 1999), 3rd edn. ISBN 0-387-98585-9. With additional contributions by E. Bannai, R. E. Borcherds, J. Leech, S. P. Norton, A. M. Odlyzko, R. A. Parker, L. Queen and B. B. Venkov.

[6] Renaud Coulangeon, 'Minimal vectors in the second exterior power of a lattice.' *J. Algebra* 194 (1997) 467–476.

[7] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.4.12*, (2008). http://www.gap-system.org

[8] Daniel R. Grayson, 'Reduction theory using semistability.' *Comment. Math. Helv.* 59 (1984) 600–634.

[9] M. Laïhem, 'Construction algorithmique des réseaux parfaits.' Ph.D. thesis, Bordeaux, (1992).

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

[11] Jacques Martinet, *Perfect lattices in Euclidean spaces*, vol. 327 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]* (Springer-Verlag, Berlin, 2003). ISBN 3-540-44236-7.

[12] Hermann Minkowski, *Geometrie der Zahlen.* Bibliotheca Mathematica Teubneriana, Band 40 (Johnson Reprint Corp., New York, 1968).

[13] H. Napias, 'Étude expérimentale et algorithmique des réseaux Euclidiens.' Ph.D. thesis, Bordeaux, (1996).

[14] W. Plesken and B. Souvignier, 'Computing isometries of lattices.' *J. Symbolic Comput.* 24 (1997) 327–334. Computational algebra and number theory (London, 1993).

[15] Achill Schürmann and Frank Vallentin, 'perfect-forms-dim8.txt.' http://www.math.uni-magdeburg.de/lattice_geometry/.

[16] Achill Schürmann and Frank Vallentin, 'perfect-forms-dim9.txt.' http://www.math.uni-magdeburg.de/lattice_geometry/.

[17] Mathieu Dutour Sikirić, Achill Schürmann and Frank Vallentin, 'Classification of eight-dimensional perfect forms.' *Electron. Res. Announc. Amer. Math. Soc.* 13 (2007) 21–32 (electronic).

[18] Ulrich Stuhler, 'Eine Bemerkung zur Reduktionstheorie quadratischer Formen.' *Arch. Math. (Basel)* 27 (1976) 604–610.

[19] G. Voronoï, 'Nouvelles applications des paramètres continus à la théorie des formes quadratiques: 1 sur quelques propriétés des formes quadratiques positive parfaites.' *J. reine angew. Math* 133 (1908) 97–178.