

## Constructing Integral Lattices With Prescribed Minimum. I

By W. Plesken and M. Pohst

**Abstract.** Methods for computing integral laminated lattices with prescribed minimum are developed. Laminating is a process of stacking layers of an  $(n - 1)$ -dimensional lattice as densely as possible to obtain an  $n$ -dimensional lattice. Our side conditions are: All scalar products of lattice vectors are rational integers, and all lattices are generated by vectors of prescribed minimum (square) length  $m$ . For  $m = 3$  all such lattices are determined.

**1. Introduction.** An integral lattice of dimension  $n$  is a free Abelian group  $\Lambda$  contained in the Euclidean space  $\mathbf{R}^n$  such that  $\Lambda$  is generated by  $n$  linearly independent vectors with integral scalar products. Important invariants of  $\Lambda$  are the natural numbers  $m, d$ :

$$(1.1) \quad m = m(\Lambda) := \min\{\langle \mathbf{x}, \mathbf{x} \rangle \mid \mathbf{x} \in \Lambda, \mathbf{x} \neq \mathbf{0}\},$$

the minimum (square-) length of  $\Lambda$ ; the discriminant  $d(\Lambda)$  is defined by

$$(1.2) \quad d = d(\Lambda) := \det(\langle \mathbf{e}_i, \mathbf{e}_j \rangle)_{1 \leq i, j \leq n}$$

for some ( $\mathbf{Z}$ -) basis  $\mathbf{e}_1, \dots, \mathbf{e}_n$  of  $\Lambda$ .

For fixed  $m \in \mathbf{N}$  we consider sequences  $(\Lambda_n)_{n \in \mathbf{N}}$ ,  $\Lambda_1 \subseteq \Lambda_2 \subseteq \dots$ , of  $n$ -dimensional integral lattices  $\Lambda_n = \Lambda_n(m)$  subject to the following conditions:

- (i)  $m(\Lambda_n) = m$  for all  $n \in \mathbf{N}$ ;
- (ii)  $\Lambda_n$  is generated by vectors  $\mathbf{x}$  of length  $m = \langle \mathbf{x}, \mathbf{x} \rangle = \|\mathbf{x}\|^2$ ;
- (iii) if  $\Lambda_{n-1}$  is given,  $\Lambda_n$  has minimal discriminant among all  $n$ -dimensional integral lattices  $\tilde{\Lambda}_n$  containing  $\Lambda_{n-1}$  and satisfying (i) and (ii).

For this lattice construction J. Thompson conjectured (in a private communication to the first author) that for each sequence  $(\Lambda_n)_{n \in \mathbf{N}}$  with the properties just described, there is a dimension  $n \in \mathbf{N}$  such that  $\Lambda_n$  is unimodular (i.e.,  $d(\Lambda_n) = 1$ ).

Conway and Sloane [2] suggest a similar construction of (not necessarily integral) lattices  $\Lambda_n$ , which they call laminated lattices. In their construction  $\Lambda_0$  is the trivial lattice, and for  $n \in \mathbf{N}$  they chose among all  $n$ -dimensional lattices with minimum length 4, which contain at least one sublattice  $\Lambda_{n-1}$ , those of minimal discriminant. Any such lattice is called a laminated lattice  $\Lambda_n$ . It turns out that all laminated lattices up to dimension  $n = 24$  are integral and generated by vectors of length 4. If one also imposes these two conditions—namely,  $\Lambda_n$  to be integral and generated by

---

Received April 6, 1983; revised June 25, 1984.

1980 *Mathematics Subject Classification.* Primary 10E25, 10E30, 10E45.

vectors of minimum length  $m$  ( $m \in \mathbf{N}$  rather than 4)—one could speak about an arithmetic laminating process, whereas the construction of Conway and Sloane is rather a geometric laminating process. The arithmetic laminating process is a slightly more restricted construction than the one given at the beginning of this introduction. Namely, it happens that some sequences of laminated lattices terminate (e.g., in dimensions  $n = 13$  for  $m = 4$  [2], and  $n = 14$  for  $m = 3$  (see Section 4 of this paper)). Therefore we call the lattices of the construction above, with properties (i)–(iii), weakly (arithmetic) laminated. In this paper the weakly laminated lattices of minimum length  $m = 3$  are classified.

In Section 2 the process of passing from  $\Lambda_n$  to  $\Lambda_{n+1}$  in a sequence of weakly laminated lattices is discussed. As a result of this analysis, three computational tasks must be solved for performing the necessary (computer) calculations: Find a vector of minimum length  $m(\mathbf{x} + \Lambda_n)$  in a coset  $\mathbf{x} + \Lambda_n$ ,  $\mathbf{x} \in \mathbf{R}^n \setminus \Lambda_n$ ; find automorphisms (or even the full automorphism group) of a lattice  $\Lambda_n$ ; and decide if two lattices are isometric. Solutions of these problems are given in Section 3. Finally, in Section 4, we list the results for minimum  $m = 3$ . Results for other minima ( $m = 4, 5$ ) and for lattices over maximal orders of number fields will appear in a subsequent paper.

We acknowledge with pleasure stimulating discussions with J. H. Conway and J. Thompson. In particular, we thank the referee for his careful reading of the manuscript.

The extensive electronic computations were carried out on the CDC Cyber 76 of the Rechenzentrum of the Universität zu Köln and on the CDC Cyber 175 of the Rechenzentrum of the RWTH Aachen.

**2. The Basic Construction.** The following two remarks a priori restrict the possibilities for sequences  $(\Lambda_n)_{n \in \mathbf{N}}$  of weakly laminated lattices with fixed minimum length  $m$ .

(2.1) *Remark.* If  $\Lambda_n$  is unimodular for some  $n \in \mathbf{N}$ , then  $\Lambda_{n+k} = \Lambda_n \perp \Gamma_k$  ( $k \in \mathbf{N}$ ,  $\perp$  means orthogonal direct sum), and  $(\Gamma_i)_{i \in \mathbf{N}}$  is again a sequence of weakly laminated lattices.

*Proof.* Since  $\Lambda_n$  is unimodular, it has an orthogonal complement  $\Gamma_k$  in  $\Lambda_{n+k}$  ( $k \in \mathbf{N}$ ) (Proposition 3.1 of Chapter 1 in [6]). The rest of the proof is straightforward, since a vector of minimum length in  $\Lambda_{n+k}$  is either in  $\Lambda_n$  or in  $\Gamma_k$ .  $\square$

(2.2) *Remark.* For all  $n \in \mathbf{N}$  the discriminants satisfy  $d(\Lambda_{n+1}) \leq d(\Lambda_n)m$ . In particular, there are only finitely many possibilities for  $\Lambda_{n+1}$ .

*Proof.*  $\Lambda_n \perp \mathbf{Z}\mathbf{e}$  with  $\langle \mathbf{e}, \mathbf{e} \rangle = m$  satisfies conditions (i) and (ii); hence,  $d(\Lambda_{n+1}) \leq d(\Lambda_n \perp \mathbf{Z}\mathbf{e}) = d(\Lambda_n)m$ . Now the second statement follows by reduction theory.  $\square$

For instance, all integral lattices generated by vectors of length 2 are well-known. They are the so-called Witt lattices, i.e., orthogonal direct sums of root lattices of type  $A_n$  ( $n \geq 1$ ),  $D_n$  ( $n \geq 4$ ),  $E_6, E_7, E_8$  with discriminants  $d(A_n) = n + 1$ ,  $d(D_n) = 4$ ,  $d(E_6) = 3$ ,  $d(E_7) = 2$ ,  $d(E_8) = 1$ , respectively. With this information one easily verifies that, in case  $m = 2$ , there is—up to isometry—exactly one sequence of weakly laminated lattices, namely:  $A_1, A_2, A_3, D_4, D_5, E_6, E_7, E_8, E_8 \perp A_1, \dots$

For  $m \geq 3$  the situation is much more complicated. Therefore we need to analyze the transition from  $\Lambda_n$  to  $\Lambda_{n+1}$  in some detail. The orthogonal projection  $\mathbf{x}_p$  of a

vector  $\mathbf{x} \in \Lambda_{n+1}$  into  $\mathbf{R}\Lambda_n = \mathbf{R}^n$  satisfies  $\langle \mathbf{x}_p, \Lambda_n \rangle \subseteq \mathbf{Z}$ . This leads to the dual lattice  $\Lambda_n^\#$  of  $\Lambda_n$ .

For an  $n$ -dimensional integral lattice  $\Gamma$ , the dual lattice is given by  $\Gamma^\# := \{\mathbf{x} \in \mathbf{R}^n \mid \langle \mathbf{x}, \Gamma \rangle \subseteq \mathbf{Z}\}$ . If  $\mathbf{e}_1, \dots, \mathbf{e}_n$  is a basis of  $\Gamma$ , the dual basis  $\mathbf{e}_1^\#, \dots, \mathbf{e}_n^\#$ , defined by  $\langle \mathbf{e}_i, \mathbf{e}_j^\# \rangle = \delta_{ij}$  ( $1 \leq i, j \leq n$ ), is a  $\mathbf{Z}$ -basis of  $\Gamma^\#$ . In particular,  $d(\Gamma) = (\Gamma^\# : \Gamma)$ . More precisely, the isomorphism type of the finite Abelian group  $\Gamma^\#/\Gamma$  is described by the elementary divisors of the Gram matrix  $(\langle \mathbf{e}_i, \mathbf{e}_j \rangle)_{1 \leq i, j \leq n}$ . These elementary divisors are a considerable refinement of the discriminant and turn out to be useful invariants of  $\Gamma$ .

The candidates in  $\Lambda_n^\#$  for the orthogonal projections of vectors  $\mathbf{x}$  of  $\Lambda_{n+1}$  of minimum length  $m$  can easily be characterized.

(2.3) LEMMA. *Let  $\mathbf{x} \in \Lambda_{n+1}$  be of minimum length  $m$ . Then its orthogonal projection  $\mathbf{x}_p$  into  $\mathbf{R}\Lambda_n$  is in  $\Lambda_n^\#$  and of shortest length  $m(\mathbf{x}_p + \Lambda_n)$  in the residue class  $\mathbf{x}_p + \Lambda_n$ .*

*Proof.* Assume that there is  $\mathbf{y} \in \Lambda_n$  such that  $\mathbf{x}_p + \mathbf{y}$  is of shorter length than  $\mathbf{x}_p$ . Then  $\mathbf{x} + \mathbf{y}$  is of shorter length than  $\mathbf{x}$  in  $\Lambda_{n+1}$ , which is a contradiction.  $\square$

As a consequence of this elementary lemma, the number of candidates for  $\Lambda_{n+1}$  contained in  $\mathbf{R}^{n+1}$  is bounded by the crude estimate  $2^{d(\Lambda_n)}$ . Though this bound can easily be improved, it is unrealistic to take it as a starting point for the computations. It is much more effective to proceed as follows.

We adjoin just one additional basis vector  $\mathbf{x} \in \mathbf{R}^{n+1} \setminus \mathbf{R}\Lambda_n$  of minimum length  $m$  to  $\Lambda_n$  subject to the conditions (i), (ii). Among the obtained lattices, we select one of minimal discriminant. This is done by choosing  $\mathbf{x}$  such that  $m(\mathbf{x}_p + \Lambda_n)$  is maximal among the shortest lengths of all residue classes  $\neq \Lambda_n$  of  $\Lambda_n^\#/\Lambda_n$ . Namely, Pythagoras' theorem yields

(2.4) LEMMA. *Let  $\mathbf{x} \in \mathbf{R}^{n+1} \setminus \mathbf{R}\Lambda_n$ . Then*

$$d(\Lambda_n \oplus \mathbf{Z}\mathbf{x}) = d(\Lambda_n)(\|\mathbf{x}\| - \|\mathbf{x}_p\|).$$

(2.5) PROPOSITION. *Let  $\Lambda_n$  be an  $n$ -dimensional integral lattice, with  $d(\Lambda_n) \neq 1$ , satisfying (i) and (ii), and let  $\bar{m} := \max\{m(\mathbf{x} + \Lambda_n) \mid \mathbf{x} \in \Lambda_n^\# \setminus \Lambda_n\} < m$ . For each residue class  $X = \mathbf{x} + \Lambda_n$  of  $\Lambda_n^\#/\Lambda_n$ , with  $\|\mathbf{x}\| = m(X) = \bar{m}$ , let  $\Lambda_n(X)$  be the  $(n + 1)$ -dimensional lattice generated by  $\Lambda_n$  and a vector  $\tilde{\mathbf{x}} \in \mathbf{R}^{n+1} \setminus \mathbf{R}\Lambda_n$  with orthogonal projection  $\tilde{\mathbf{x}}_p = \mathbf{x}$  and  $\|\tilde{\mathbf{x}}\| = m$ . (Note that  $\Lambda_n(X)$  is uniquely defined up to an orthogonal reflection.)*

*Then  $\Lambda_{n+1}$  is among the lattices  $\Lambda_n(X)$ , and, conversely, each  $\Lambda_n(X)$  can be chosen as  $\Lambda_{n+1}$ . The discriminant of  $\Lambda_{n+1}$  is given by  $d(\Lambda_{n+1}) = d(\Lambda_n)(m - \bar{m})$ .*

*Proof.* It suffices to prove that each  $\Lambda_{n+1}$  is obtained by adjoining one vector  $\mathbf{y} \in \mathbf{R}^{n+1} \setminus \mathbf{R}\Lambda_n$  of minimum length  $m$  to  $\Lambda_n$ . Namely, in this case Lemma (2.4) implies Proposition (2.5).

We first show that we can always obtain  $\Lambda_{n+1}$  by adjoining one vector  $\mathbf{y} \in \mathbf{R}^{n+1} \setminus \mathbf{R}\Lambda_n$  of length  $\|\mathbf{y}\| = s \geq m$ . This is tantamount to  $\mathbf{R}\Lambda_n \cap \Lambda_{n+1} = \Lambda_n$ . But  $\mathbf{R}\Lambda_n \cap \Lambda_{n+1}$  is contained in  $\Lambda_n^\#$ , and our hypothesis on  $\Lambda_n^\#/\Lambda_n$  implies  $\mathbf{R}\Lambda_n \cap \Lambda_{n+1} = \Lambda_n$  because of  $m(\Lambda_{n+1}) = m$ .

Clearly, we can choose this vector  $\mathbf{y}$  such that  $m(\mathbf{y}_p + \Lambda_n) = \|\mathbf{y}_p\|$ . Since  $\Lambda_{n+1}$  satisfies condition (iii), we have

$$d(\Lambda_{n+1}) = d(\Lambda_n)(s - \|\mathbf{y}_p\|) \leq d(\Lambda_n(X)) = d(\Lambda_n)(m - \bar{m})$$

for  $X \in \Lambda_n^\#/\Lambda_n$  with  $m(X) = \bar{m}$ . Hence,

$$s = d(\Lambda_{n+1})/d(\Lambda_n) + \|\mathbf{y}_p\| \leq m - \bar{m} + \|\mathbf{y}_p\| \leq m,$$

and therefore the additional generator  $\mathbf{y}$  is of length  $m$  and has a projection of length  $\bar{m}$ .  $\square$

In the above construction of  $\Lambda_{n+1}$  from  $\Lambda_n$ , the elementary divisors of the corresponding Gram matrices cannot change drastically.

(2.6) *Remark.* Under the hypothesis of (2.5) there is a finite Abelian group  $U$  with embeddings  $\sigma_i: U \rightarrow \Lambda_i^\#/\Lambda_i$  ( $i = n, n + 1$ ) such that  $(\Lambda_i^\#/\Lambda_i)/\sigma_i(U)$  is cyclic for  $i = n, n + 1$ .

*Proof.* Let  $\Lambda_{n+1} = \Lambda_n \oplus \mathbf{Z}\tilde{\mathbf{x}}$  and denote the orthogonal projection  $\tilde{\mathbf{x}}_p$  of  $\tilde{\mathbf{x}}$  into  $\Lambda_n^\#$  by  $\mathbf{x}$ . The sublattice  $\Gamma := \Lambda_n + \mathbf{Z}\mathbf{x}$  of  $\Lambda_n^\#$  contains  $\Lambda_n$  such that  $\Gamma/\Lambda_n$  is cyclic. Its dual lattice

$$\Gamma^\# := \{\mathbf{y} \in \mathbf{R}^n \mid \langle \mathbf{y}, \Gamma \rangle \subseteq \mathbf{Z}\}$$

has the property

$$(*) \quad \mathbf{R}\Lambda_n \cap \Lambda_{n+1}^\# = \Gamma^\#.$$

Let  $U := \Gamma^\#/\Lambda_n$ ,  $\sigma_n$  be the natural embedding of  $U$  into  $\Lambda_n^\#/\Lambda_n$  and  $\sigma_{n+1}: U \rightarrow \Lambda_{n+1}^\#/\Lambda_{n+1}: \mathbf{z} + \Lambda_n \rightarrow \mathbf{z} + \Lambda_{n+1}$ , which is an embedding by the isomorphism theorem. We conclude that  $\Lambda_n^\#/\sigma_n(U) = \Lambda_n^\#/\Gamma^\#$  is isomorphic to the cyclic group  $\Gamma/\Lambda_n$  (by duality), and  $\Lambda_{n+1}^\#/\sigma_{n+1}(U)$  is cyclic, since  $\Lambda_{n+1}^\#/\Gamma^\#$  is cyclic by (\*).  $\square$

In order to reduce the number of residue classes of  $\Lambda_n^\#/\Lambda_n$  to be investigated according to (2.5), it is a great advantage to know a big subgroup of the automorphism group  $\text{Aut}(\Lambda_n)$ , defined as the group of all orthogonal transformations of  $\mathbf{R}^n$  mapping  $\Lambda_n$  onto itself. Obviously,  $m(\mathbf{x} + \Lambda_n) = m(\alpha(\mathbf{x}) + \Lambda_n)$  for all  $\mathbf{x} \in \Lambda_n^\#$  and  $\alpha \in \text{Aut}(\Lambda_n)$ . Moreover, one easily verifies the following remark.

(2.7) *Remark.* Under the assumption and in the notation of (2.5),  $\Lambda_n(X)$  is isometric to  $\Lambda_n(X')$  for two residue classes  $X, X'$  of  $\Lambda_n^\#/\Lambda_n$  if  $X, X'$  are in the same orbit of  $\Lambda_n^\#/\Lambda_n$  under  $\text{Aut}(\Lambda_n)$ .

However, we note that  $\Lambda_n(X)$  and  $\Lambda_n(X')$  may still be isometric without  $X, X'$  lying in the same orbit of  $\Lambda_n^\#/\Lambda_n$  under  $\text{Aut}(\Lambda_n)$ . To understand this phenomenon, the following definition is helpful.

(2.8) *Definition.* Let  $\Lambda$  and  $\Gamma$  be lattices. Two (isometric) embeddings  $\sigma_i: \Gamma \rightarrow \Lambda$  ( $i = 1, 2$ ) are said to be of the same *type* if there are  $\alpha \in \text{Aut}(\Lambda)$  and  $\beta \in \text{Aut}(\Gamma)$  such that  $\sigma_1\beta = \alpha\sigma_2$ . The number of different types of embeddings is called the *embedding number*  $\eta(\Gamma, \Lambda)$ .

For example, if  $\Gamma$  is a one-dimensional lattice generated by a vector of length  $l$ , then  $\eta(\Gamma, \Lambda)$  is equal to the number of orbits of  $\text{Aut}(\Lambda)$  on the vectors of length  $l$  in  $\Lambda$ . We use Definition (2.8) in the situation of (2.5).

(2.9) **PROPOSITION.** *Under the hypothesis of (2.5) let  $X \in \Lambda_n^\#/\Lambda_n$  with  $m(X) = \bar{m}$ , and set  $L(X) := \{Y \in \Lambda_n^\#/\Lambda_n \mid m(Y) = \bar{m} \text{ and } \Lambda_n(Y) \text{ isometric to } \Lambda_n(X)\}$ . Then the number of orbits of  $\text{Aut}(\Lambda_n)$  on  $L(X)$  is equal to the embedding number  $\eta(\Lambda_n, \Lambda_n(X))$ .*

*Proof.* We abbreviate  $\Lambda_n(X)$  by  $\Lambda_{n+1}$ . Clearly,  $\eta(\Lambda_n, \Lambda_{n+1})$  is equal to the number of orbits of  $\text{Aut}(\Lambda_{n+1})$  on the set  $\mathfrak{S}$  of all sublattices of  $\Lambda_{n+1}$  which are isometric to  $\Lambda_n$ . We define a mapping  $\Psi$  from  $L(X)$  into  $\mathfrak{S}$  in the following way. For  $Y \in L(X)$  let  $\sigma_Y$  be a fixed isometry,  $\sigma_Y: \Lambda_n(Y) \rightarrow \Lambda_{n+1}$ , and set  $\Psi(Y) = \Gamma_Y := \sigma_Y(\Lambda_n)$ . ( $\Lambda_n$  is viewed as a sublattice of  $\Lambda_n(Y)$ .) We claim that  $\Psi$  induces a bijection  $\tilde{\Psi}$  between the set  $\tilde{L}(X)$  of orbits of  $L(X)$  under  $\text{Aut}(\Lambda_n)$  and the set  $\tilde{\mathfrak{S}}$  of orbits of  $\mathfrak{S}$  under  $\text{Aut}(\Lambda_{n+1})$ . Note that  $\tilde{\Psi}$  does not depend on the choice of  $\sigma_Y$ , although  $\Psi$  itself does.

Next we show that  $\tilde{\Psi}$  is well-defined. Let  $Y, Z \in L(X)$  and  $\tau \in \text{Aut}(\Lambda_n)$  such that  $Y = \tau Z$ . We extend  $\tau$  to an isometry  $\bar{\tau}$  between  $\Lambda_n(Y)$  and  $\Lambda_n(Z)$  in the obvious way. Then  $\sigma_Y \bar{\tau} \sigma_Z^{-1}$  is an automorphism of  $\Lambda_{n+1}$  which maps  $\Gamma_Z$  onto  $\Gamma_Y$ . Hence,  $\tilde{\Psi}$  is well-defined.

To prove the injectivity of  $\tilde{\Psi}$ , let  $\Gamma_Y, \Gamma_Z \in \mathfrak{S}$ , and let  $\alpha$  be an automorphism of  $\Lambda_{n+1}$  mapping  $\Gamma_Z$  onto  $\Gamma_Y$ .  $\bar{\tau} := \sigma_Y^{-1} \alpha \sigma_Z$  is an isometry of  $\Lambda_n(Z)$  onto  $\Lambda_n(Y)$  which maps the sublattice  $\Lambda_n = \sigma_Z^{-1}(\Gamma_Z)$  of  $\Lambda_n(Z)$  onto the sublattice  $\Lambda_n = \sigma_Y^{-1}(\Gamma_Y)$  of  $\Lambda_n(Y)$ . Hence,  $\bar{\tau}$  induces an automorphism  $\tau$  of  $\Lambda_n$  mapping  $Z$  onto  $Y$ .

To prove the surjectivity of  $\tilde{\Psi}$ , let  $\Gamma \in \mathfrak{S}$ . Analogous to the proof of (2.5), one sees  $\Lambda_{n+1} = \Gamma \oplus \mathbf{Z}\tilde{\mathbf{y}}$  for some  $\tilde{\mathbf{y}} \in \Lambda_{n+1}$  of length  $m$ . Let  $\mathbf{y}' \in \Gamma^\#$  be the orthogonal projection of  $\tilde{\mathbf{y}}$  into  $\mathbf{R}\Gamma$ . We choose  $\mathbf{y} \in \Lambda_n^\#$ , which corresponds to  $\mathbf{y}'$  by some isometry between  $\Gamma$  and  $\Lambda_n$ . Then  $\Gamma$  is in the orbit of  $\Gamma_Y$ , with  $Y = \mathbf{y} + \Lambda_n$ , under the action of  $\text{Aut}(\Lambda_n)$ .  $\square$

**3. Computational Methods.** As a consequence of Section 2, there are three main computational tasks to solve:

- (a) determine a vector of minimum length in a residue class of  $\Lambda_n^\#/\Lambda_n$ ;
- (b) determine the automorphism group of  $\Lambda_n$  (and its orbits on  $\Lambda_n^\#/\Lambda_n$ );
- (c) decide whether two lattices  $\Lambda_n, \tilde{\Lambda}_n$  are isometric and, in case they are, find an isometry.

Ad(a). We apply the methods of [7], which are based on quadratic supplementing of positive-definite quadratic forms. The amount of necessary computation time and storage is negligible compared to (b) and (c).

Ad(b). All lattices  $\Lambda$  under consideration are generated by the set  $M$  of vectors of minimum length (property (ii)). Therefore,  $\text{Aut}(\Lambda)$  can be identified with those permutations  $\alpha$  of  $M$  which satisfy  $\langle \alpha(\mathbf{x}), \alpha(\mathbf{y}) \rangle = \langle \mathbf{x}, \mathbf{y} \rangle$  for all  $\mathbf{x}, \mathbf{y} \in M$  (and, hence, also  $\alpha(-\mathbf{x}) = -\alpha(\mathbf{x})$ ). An automorphism  $\sigma$  of  $\Lambda$  is determined by the image  $(\sigma(\mathbf{e}_1), \dots, \sigma(\mathbf{e}_n))$  of some basis  $B = (\mathbf{e}_1, \dots, \mathbf{e}_n)$  of  $\Lambda$ . Our computations have shown that we can always choose a suitable basis  $B$  as a subset of  $M$  (for minimum length  $m = 3$ ). This assumption is used in our computations, though it is not essential.

The first problem is to restrict the number of candidates for  $\sigma(\mathbf{e}_i)$  in  $M$  ( $1 \leq i \leq n$ ). Therefore, we define the *type*  $t(\mathbf{x})$  of  $\mathbf{x} \in M$  by

$$(3.1) \quad t(\mathbf{x}) := (t(\mathbf{x}, 0), \dots, t(\mathbf{x}, \lfloor m/2 \rfloor)),$$

where  $t(\mathbf{x}, i) := |\{\mathbf{y} \in M \mid |\langle \mathbf{x}, \mathbf{y} \rangle| = i\}|$  ( $0 \leq i \leq m/2$ ) and  $\lfloor \cdot \rfloor$  denotes the floor function. Note,  $t(\mathbf{x}, i) = 0$  for  $m/2 < i < m$ . All vectors  $\mathbf{x} \in M$  which are of the same type as  $\mathbf{a} \in M$  belong to the equivalence class

$$(3.2) \quad T(\mathbf{a}) := \{\mathbf{x} \in M \mid t(\mathbf{x}) = t(\mathbf{a})\}.$$

We note that  $T(\mathbf{a})$  is a union of orbits of  $M$  under the action of  $\text{Aut}(\Lambda)$ .

To find an automorphism  $\sigma$  of  $\Lambda$  we compute  $\mathbf{a}_i \in M$  ( $1 \leq i \leq n$ ) subject to the condition  $\langle \mathbf{a}_i, \mathbf{a}_j \rangle = \langle \mathbf{e}_i, \mathbf{e}_j \rangle$  ( $1 \leq j \leq i$ ); then  $\sigma$  is given by  $\sigma: \mathbf{e}_i \rightarrow \mathbf{a}_i$  ( $1 \leq i \leq n$ ). Unfortunately, not every  $r$ -tuple  $\mathbf{a}_1, \dots, \mathbf{a}_r$  ( $1 \leq r < n$ ) of vectors of  $M$  satisfying  $\langle \mathbf{a}_i, \mathbf{a}_j \rangle = \langle \mathbf{e}_i, \mathbf{e}_j \rangle$  ( $1 \leq i \leq j \leq r$ ) can be extended to an  $n$ -tuple  $\mathbf{a}_1, \dots, \mathbf{a}_n$  corresponding to an automorphism of  $\Lambda$ . The necessary backtrack search can be improved in two ways. Firstly, we choose a more suitable order of succession  $\mathbf{e}_i, \dots, \mathbf{e}_n$  of the basis vectors which makes the number of candidates for  $\mathbf{a}_{i_{r+1}}$  for given  $\mathbf{a}_1, \dots, \mathbf{a}_r$  ( $1 \leq r < n$ ) as small as possible. Secondly, we give another necessary condition for  $\mathbf{a}_r$  which at least guarantees the existence of  $\mathbf{a}_{i_{r+1}}$  ( $1 \leq r < n$ ). The device for this improvement is called the fingerprint of  $\Lambda$  with respect to the basis  $\mathbf{e}_1, \dots, \mathbf{e}_n$ . It is defined as an  $(n-1) \times n$  integral matrix  $C$ , the rows of which can be computed inductively.

(3.3) *Definition.* Let  $\Lambda$  be a lattice with basis  $\mathbf{e}_1, \dots, \mathbf{e}_n$  of vectors of minimum length. We define a sequence  $(i_1, \dots, i_n)$  (new order of basis vectors) and set  $C(i_j, k)$  ( $1 \leq k \leq n$ ,  $1 \leq j \leq n-1$ ) inductively by:

Let  $i_1$  be the smallest index such that  $|T(\mathbf{e}_{i_1})| \leq |T(\mathbf{e}_k)|$  ( $1 \leq k \leq n$ ).

If  $i_1, \dots, i_j$  are determined ( $1 \leq j \leq n-1$ ), let

$$C(i_j, k) := \begin{cases} \emptyset & \text{for } k \in \{i_1, \dots, i_j\}, \\ \{\mathbf{x} \in T(\mathbf{e}_k) \mid \langle \mathbf{e}_{i_\nu}, \mathbf{e}_k \rangle = \langle \mathbf{e}_{i_\nu}, \mathbf{x} \rangle \text{ for } \nu = 1, \dots, j\} & \text{otherwise.} \end{cases}$$

In case  $j < n-1$  let  $i_{j+1}$  be the smallest index such that  $|C(i_j, i_{j+1})|$  is minimal among all  $|C(i_j, k)| > 0$ . For  $j = n-1$  let  $i_n$  be the remaining element of  $\{1, \dots, n\} \setminus \{i_1, \dots, i_{n-1}\}$ . Then the fingerprint is the matrix  $C = (c_{jk}) \in \mathbf{Z}^{(n-1) \times n}$  with  $c_{jk} = |C(i_j, k)|$  ( $1 \leq k \leq n$ ,  $1 \leq j \leq n-1$ ).

With the fingerprint given, our procedure for computing an automorphism of  $\Lambda$  is as follows. Let  $0 \leq r < n$  and  $\mathbf{a}_{i_1}, \dots, \mathbf{a}_{i_r} \in M$  satisfying  $\langle \mathbf{a}_{i_\mu}, \mathbf{a}_{i_\nu} \rangle = \langle \mathbf{e}_{i_\mu}, \mathbf{e}_{i_\nu} \rangle$  ( $1 \leq \mu < \nu \leq r$ ). The procedure decides whether there is an automorphism  $\sigma$  in  $\text{Aut}(\Lambda)$  such that  $\sigma(\mathbf{e}_j) = \mathbf{a}_j$  ( $1 \leq j \leq r$ ), and, in case  $\sigma$  exists, it computes  $\sigma(\mathbf{e}_j)$  for  $j = r+1, \dots, n$ .

(3.4) *Procedure for finding an automorphism  $\sigma$ .*

*Input.* The fingerprint  $(c_{ij}) \in \mathbf{Z}^{(n-1) \times n}$ , the new ordering  $(i_1, \dots, i_n)$  obtained from it, and the sets  $T(\mathbf{e}_j)$  ( $1 \leq j \leq n$ ). As an option we can prescribe the images of the first  $r$  basis vectors ( $0 \leq r < n$ ), which means adding  $\mathbf{a}_{i_1}, \dots, \mathbf{a}_{i_r}$  satisfying  $\langle \mathbf{a}_{i_\mu}, \mathbf{a}_{i_\nu} \rangle = \langle \mathbf{e}_{i_\mu}, \mathbf{e}_{i_\nu} \rangle$  ( $1 \leq \mu \leq \nu \leq r$ ), to the input.

*Output.* Either vectors  $\mathbf{a}_i$  ( $1 \leq i \leq n$ ) are printed such that  $\sigma: \mathbf{e}_i \mapsto \mathbf{a}_i$  yields an automorphism, or "No solution" is printed in case there is no automorphism satisfying  $\sigma(\mathbf{e}_j) = \mathbf{a}_j$  ( $1 \leq j \leq r$ ). (The latter cannot occur in case  $r = 0$ .)

*Step 1 (Initialization).* Set  $k \leftarrow r$ .

*Step 2 (Computation of candidates for  $\mathbf{a}_{i_{k+1}}$ ).* Let

$$\tilde{C}(i_k, i_j) := \{\mathbf{x} \in T(\mathbf{e}_{i_j}) \mid \langle \mathbf{a}_{i_\nu}, \mathbf{x} \rangle = \langle \mathbf{e}_{i_\nu}, \mathbf{e}_{i_j} \rangle \text{ (} 1 \leq \nu \leq k \text{)}\}$$

( $k < j \leq n$ ). For  $k+1 \leq j \leq n$ , test whether each number  $|\tilde{C}(i_k, i_j)|$  coincides with  $c_{ki_j}$ . If this is the case, compute  $\tilde{C}(i_k, i_{k+1})$  and go to Step 4.

*Step 3 (Decrease  $k$ ).* Decrease  $k$  by 1 until either  $k < r$ —in which case “No solution” is printed and the procedure stops—or  $\tilde{C}(i_k, i_{k+1}) \neq \emptyset$ .

*Step 4 (Increase  $k$ ).* Choose  $\mathbf{a}_{i_{k+1}} \in \tilde{C}(i_k, i_{k+1})$  and replace  $\tilde{C}(i_k, i_{k+1})$  by  $\tilde{C}(i_k, i_{k+1}) \setminus \{\mathbf{a}_{i_{k+1}}\}$ . For  $k + 1 = n$ , print  $\mathbf{a}_j$  ( $1 \leq j \leq n$ ) and terminate. Otherwise set  $k \leftarrow k + 1$  and return to Step 2.

*Remarks concerning the implementation.* (1) For the fingerprint and the computation of an automorphism, a list  $M$  of the shortest vectors in  $\Lambda$  is needed.  $M$  is computed by the methods of [7]. One vector  $\mathbf{x}$  for each pair  $\pm \mathbf{x} \in M$  is stored in a very compact way by using the scalar products of  $\mathbf{x}$  with the basis vectors  $\mathbf{e}_1, \dots, \mathbf{e}_n$  which belong to the set  $\{0, \pm 1, \pm 2, \dots, \pm \lfloor m/2 \rfloor, m\}$ . (In case  $m \leq 7$  we need only one computer word (consisting of 60 bits on the CDC-machines used) for one vector in dimensions  $\leq 20$ .) Also the inner products of  $\mathbf{x}$  with all vectors of  $M$  (to determine  $T(\mathbf{x})$ ) are available rather quickly, using the inverse of the Gram matrix of  $\mathbf{e}_1, \dots, \mathbf{e}_n$ . We note that this matrix is needed anyway for the investigation of the residue classes of  $\Lambda^\#/\Lambda$ .

(2) If the number of vectors is large, we rearrange  $M$  according to the types of the vectors in  $M$ .

(3) It is obvious that the procedure is flexible enough so that not only the identity is generated (for example, by a suitable choice of  $\mathbf{a}_{i_{k+1}}$  in Step 4).

The procedure of computing automorphisms is designed such that we can find generators for the full automorphism group of the lattice  $\Lambda_n$  by using permutation group routines which perform the following three tasks:

- (a) Determine the order of a permutation group given by generators.
- (b) Find generators for stabilizers of points.
- (c) Compute orbits of permutation groups given by generators.

For our computations we made use of CAYLEY [1].

The fingerprint  $C$  already yields an upper bound for the order of  $\text{Aut}(\Lambda_n)$ , namely,

$$(3.5) \quad |\text{Aut}(\Lambda_n)| \leq \prod_{j=0}^{n-1} c_{ji_{j+1}} =: b,$$

since  $c_{ji_{j+1}}$  is an upper bound for the orbit containing  $\mathbf{e}_{i_{j+1}}$  under the stabilizer of  $(\mathbf{e}_{i_1}, \dots, \mathbf{e}_{i_j})$  in  $\text{Aut}(\Lambda_n)$ .

We determine  $|\text{Aut}(\Lambda_n)|$  and generators for  $\text{Aut}(\Lambda_n)$  in several steps. First we randomly compute two or more automorphisms and check whether they generate a group of order  $b$ . If this is not the case, let  $U = U_0$  be the group they generate, and let  $U_j$  be the stabilizer of  $(\mathbf{e}_{i_1}, \dots, \mathbf{e}_{i_j})$  in  $U$ . Set  $f = -1$ . We determine the smallest index  $j > f$  with orbit length  $|U_j(\mathbf{e}_{i_{j+1}})| < c_{ji_{j+1}}$ . We check with our procedure to see if there is an automorphism stabilizing  $\mathbf{e}_{i_1}, \dots, \mathbf{e}_{i_j}$  and mapping  $\mathbf{e}_{i_{j+1}}$  onto the first element of  $C(i_j, i_{j+1})$  which is not in the orbit  $U_j(\mathbf{e}_{i_{j+1}})$ . If there is such an automorphism  $\sigma$ , then replace  $U$  by  $\langle U, \sigma \rangle$  and start over again. If not, replace  $f$  by  $j$ . Repeating this process until no  $j$ , with  $f < j \leq n$ , exists such that  $|U_j(\mathbf{e}_{i_{j+1}})| < c_{ji_{j+1}}$ , we obtain the full automorphism group of  $\Lambda_n$ .

We note that similar methods of building up generating sets of automorphism groups, for instance of finite groups and special combinatorial structures, were also developed in [5] (also used in CAYLEY [1]) and [8].

(3.6) *Example.* Let the minimum length be  $m = 3$  and the dimension  $n = 8$ . A typical Gram matrix obtained by our computations is

$$\begin{pmatrix} 3 & 1 & -1 & 1 & 1 & 1 & -1 & 1 \\ 1 & 3 & 1 & 1 & 1 & 1 & -1 & 0 \\ -1 & 1 & 3 & 1 & -1 & 1 & 1 & -1 \\ 1 & 1 & 1 & 3 & 1 & 1 & 0 & 1 \\ 1 & 1 & -1 & 1 & 3 & 0 & -1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 3 & 1 & 1 \\ -1 & -1 & 1 & 0 & -1 & 1 & 3 & 0 \\ 1 & 0 & -1 & 1 & 1 & 1 & 0 & 3 \end{pmatrix}.$$

There are—up to sign—20 shortest vectors in the corresponding lattice listed in the standard coordinates:

$i$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$x_i$	1	0	1	0	-1	0	1	0	0	0	-1	0	1	0	0	0	1	0	0	0
	0	1	-1	0	0	0	-1	0	0	-1	0	0	0	1	1	0	0	0	0	0
	0	0	1	1	-1	0	1	1	0	1	-1	0	0	0	-1	0	1	1	1	0
	0	0	0	0	1	1	-1	-1	0	0	0	0	0	0	0	0	-1	0	-1	0
	0	0	0	0	0	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	1	1	-1	-1	0	0	-1	-1	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1

These vectors belong to three equivalence classes of different types:

$$\begin{aligned} T(x_1) &= \{\pm x_1, \pm x_4\}, & t(x_1) &= (0, 38); \\ T(x_2) &= \{\pm x_2, \pm x_3, \pm x_5, \pm x_6, \pm x_{11}, \pm x_{12}\}, & t(x_2) &= (8, 30); \\ T(x_9) &= \{\pm x_i \mid 1 \leq i \leq 20, x_i \notin T(x_1) \cup T(x_2)\}, & t(x_9) &= (12, 26). \end{aligned}$$

The corresponding fingerprint matrix is

$$\begin{pmatrix} 0 & 6 & 1 & 6 & 12 & 6 & 12 & 12 \\ 0 & 6 & 0 & 6 & 12 & 6 & 12 & 12 \\ 0 & 0 & 0 & 4 & 4 & 4 & 4 & 4 \\ 0 & 0 & 0 & 0 & 1 & 2 & 2 & 2 \\ 0 & 0 & 0 & 0 & 0 & 2 & 2 & 2 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

and therefore the new order of succession  $(i_1, \dots, i_8) = (1, 3, 2, 4, 5, 6, 7, 8)$ .

Our computer program easily produces the following matrices:

$$\begin{aligned} \sigma_1 &= (x_4, x_3, x_1, -x_5, -x_9, -x_{11}, -x_{16}, -x_{20}), \\ \sigma_2 &= (x_1, -x_{11}, x_4, x_3, x_{13}, -x_5, x_{19}, x_7), \\ \sigma_3 &= (x_1, x_2, x_4, x_{12}, x_{15}, -x_5, -x_9, -x_{18}), \\ \sigma_4 &= -I_\infty. \end{aligned}$$

$\sigma_1, \sigma_2, \sigma_3, \sigma_4$  generate the full automorphism group of the lattice of order  $192 = 4 \cdot 1 \cdot 6 \cdot 4 \cdot 1 \cdot 2 \cdot 1 \cdot 1$  (see fingerprint).  $\square$

Determining the orbits of  $\Lambda_n^\# / \Lambda_n$  under  $\text{Aut}(\Lambda_n)$  is straightforward. It hinges on finding compatible bases for  $\Lambda_n, \Lambda_n^\#$  which can be obtained by diagonalizing the inverse of the Gram matrix. Since the computation of  $\text{Aut}(\Lambda_n)$  is time consuming



and done interactively, we usually work with a subgroup of  $\text{Aut}(\Lambda_n)$  which is constructed by machine alone.

For this reason, and because the embedding numbers of  $\Lambda_{n-1}$  into  $\Lambda_n$  can be greater than one, we also need a program which decides whether two  $n$ -dimensional lattices are isometric.

Ad(c). Let  $\Lambda_n$  and  $\tilde{\Lambda}_n$  be  $n$ -dimensional lattices with the usual properties (i) and (ii) of the introduction. We first compare the following invariants:

- (i) elementary divisors of the Gram matrices,
- (ii) number of vectors of minimum length,
- (iii) types (and type frequencies) of the vectors of minimum length.

We note that (i) and (ii) (but not the discriminant and (iii)) suffice to distinguish the lattices for  $m = 3$  discussed in this paper.

If all three invariants coincide, we try to construct an isometry by a slight modification of Procedure (3.4) for finding an automorphism.

- (i) Compute the fingerprint  $C$  of  $\Lambda_n$  with respect to a given bases  $\mathbf{e}_1, \dots, \mathbf{e}_n$ .
- (ii) Compute the list  $\tilde{M}$  of shortest vectors of  $\tilde{\Lambda}_n$  (the shortest vectors of  $\Lambda_n$  can be deleted).
- (iii) Using the fingerprint  $C$ , construct an  $n$ -tuple  $(\tilde{\mathbf{a}}_1, \dots, \tilde{\mathbf{a}}_n)$  of vectors of  $\tilde{M}$  with the same Gram matrix as  $\mathbf{e}_1, \dots, \mathbf{e}_n$  by Procedure (3.4). (A slightly more complicated version of the procedure also states if there is no isometry.)

Examples of isometries can be found in the next section.

**4. Results for  $m = 3$ .**

(4.1) THEOREM. (i) *Each sequence of weakly laminated (integral) lattices for minimum  $m = 3$  contains the unimodular lattice  $\Lambda_{23} = \Lambda_{23}(3)$  with Gram matrix  $Q_{23}$  (on page S5 of the supplements section). The possible sequences  $\Lambda_1, \Lambda_2, \dots, \Lambda_{23}$  can be read off from Figure 1, in which the possible successors  $\Lambda_{n+1}$  of  $\Lambda_n$  are those connected to  $\Lambda_n$  by a line.*

(ii) *A sequence of weakly laminated (integral) lattices  $(\Lambda_i)_{i \in \mathbf{N}}$  for minimum  $m = 3$  is also a sequence of laminated lattices if it does not contain a lattice with  $\Lambda_{14}^d$  or  $\Lambda_{14}^e$  as orthogonal component. If it does contain a lattice with  $\Lambda_{14}^d$  or  $\Lambda_{14}^e$  as orthogonal component, it yields only a finite sequence of laminated lattices stopping in the smallest dimension  $k \cdot 23 + 14$  ( $k \in \mathbf{Z}^{\geq 0}$ ) for which  $\Lambda_{k \cdot 23 + 14}$  contains  $\Lambda_{14}^d$  or  $\Lambda_{14}^e$  as orthogonal component. This exhausts all possibilities for sequences of laminated lattices.*

We remark that the embedding number of  $\Lambda_n$  in  $\Lambda_{n+1}$  might be greater than one. The automorphism group of  $\Lambda_{23}$  is the direct product of  $\langle -\text{Id} \rangle$  with the second Conway group  $\cdot 2$ ; its order is  $2^{19} 3^6 5^3 7 \cdot 11 \cdot 23$ .

Gram matrices of all lattices occurring in Figure 1 can be obtained from the Gram matrices  $Q_{23}$ ,  $Q'_{19}$ , and  $Q''_{23}$  on pages S5 and S6 of the supplements section (described on pages S6 to S7).

For each lattice  $\Lambda_i$  in Figure 1, additional information is given in Table 1 (pages S10 to S11 of the supplements section). In particular, we list

- (i) the discriminant  $d(\Lambda)$  factored into elementary divisors of a Gram matrix of  $\Lambda$ —i.e., the isomorphism type of  $\Lambda^\#/\Lambda$ ;

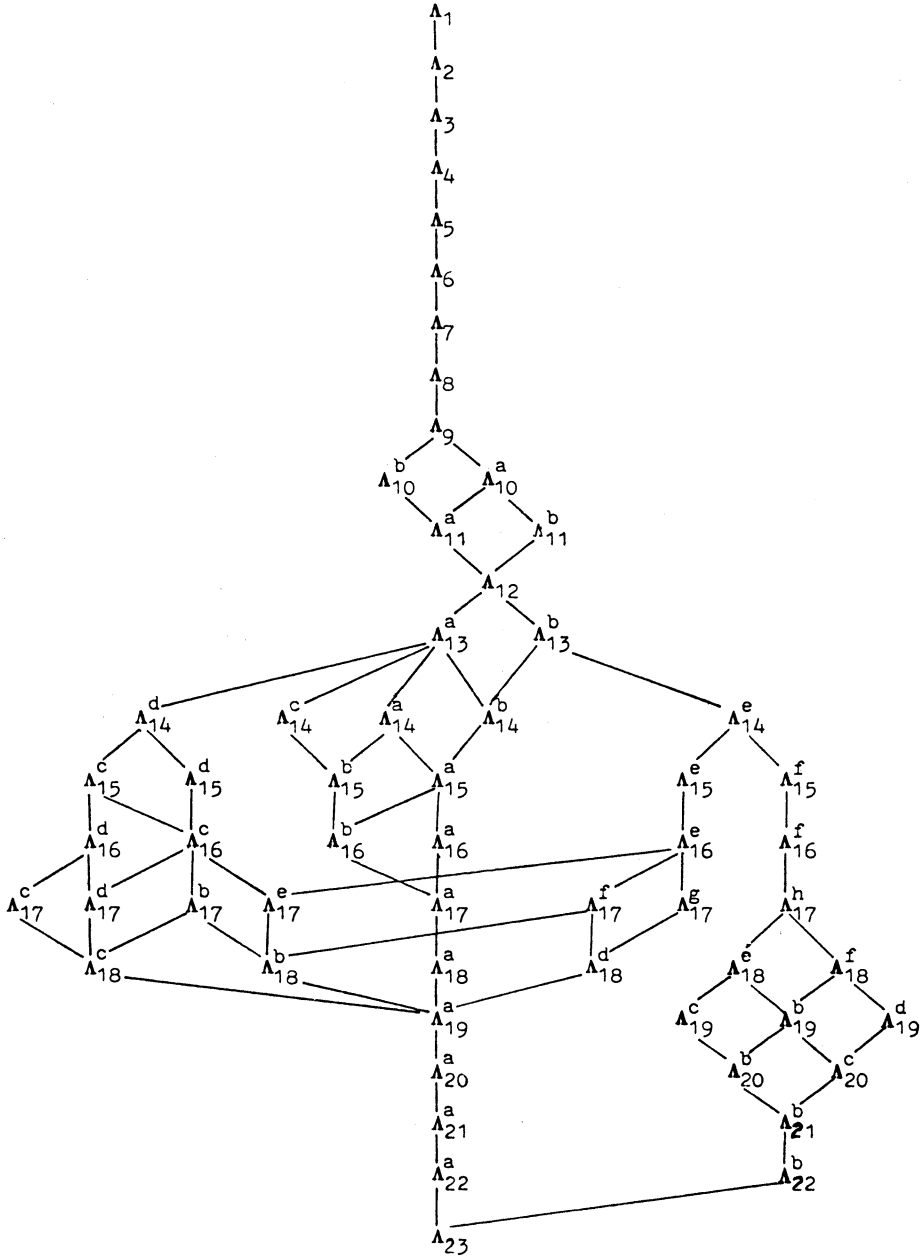


FIGURE 1

(ii) the lengths of the equivalence classes  $T(\mathbf{a})$  defined in (3.2) of vectors of minimum length in  $\Lambda$ .

We computed the automorphism groups of the lattices  $\Lambda_i$  using Procedure (3.4) and CAYLEY [1] interactively up to dimension  $i = 18$ .

Table 2 (pages S12 and S13 of the supplements section) lists the orders of the automorphism groups and the lengths of the orbits on  $M$  (compatible with Table 1). If the automorphism group is not solvable, the nonabelian composition factors are also given.

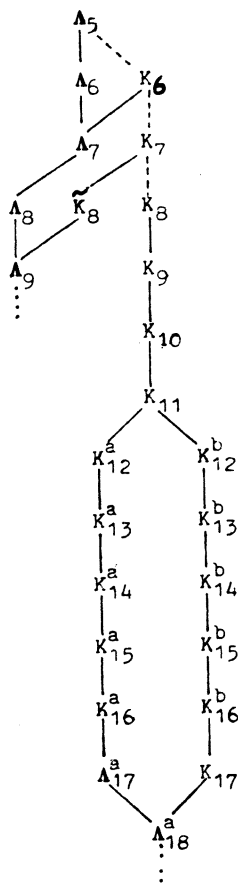


FIGURE 2

The lattice  $\Lambda_{23}$  is closely related to the Leech lattice  $L_{24}$ . It can be derived from  $L_{24}$  as follows. Choose a vector  $x_0$  of minimum length in  $L_{24}$ . Let  $L'_{24} = \{y \in L_{24} | \langle x_0, y \rangle \equiv 0 \pmod{2}\}$ , and let  $\pi$  be the orthogonal projection of  $\mathbf{R}^{24} = \mathbf{R}L_{24}$  onto  $\langle x_0 \rangle^\perp$ . Then  $\Lambda_{23} \approx \pi(L'_{24})$ . Therefore, this paper can be viewed as part of the internal study of the Leech lattice, although this was not clear in the beginning. Hence, it seems natural to investigate the connections between the lattices of this paper and those determined by Conway and Sloane [2].

After rescaling their lattice  $\Lambda_{13}^{\max}$  such that the minimum length becomes 4 (we denote this lattice by  $\tilde{\Lambda}_{13}^{\max}$ ), it contains a vector  $x_0$  of length 4 having even scalar products with all other vectors of  $\tilde{\Lambda}_{13}^{\max}$ . Projecting  $\tilde{\Lambda}_{13}^{\max}$  and the sublattices of dimensions 1–12 given in [2] onto  $\langle x_0 \rangle^\perp$ , exactly yields our lattices up to dimension 12. (The lattices in dimensions  $n > 13$  do not contain such a vector  $x_0$  (see also [3]).)

Conway and Sloane [2] also discuss a second important sequence of sections of lattices ( $\kappa$ -sequence). The 11-dimensional lattice in this sequence (rescaled as above) also contains a vector  $x_0$  of length 4 having even scalar products with all other

vectors in the lattice. By orthogonal projections as above, we obtain lattices  $K_i$  generated by vectors of minimum length 3 ( $1 \leq i \leq 10$ ) and  $K_i \simeq \Lambda_i$  ( $1 \leq i \leq 5$ ). As Conway pointed out, the discriminant of  $K_{10}$  is smaller than 256, the discriminant of  $\Lambda_{10}^a$  and  $\Lambda_{10}^b$ . This suggested the application of the arithmetic laminating process to  $K_i$  ( $6 \leq i \leq 10$ ).

The results are contained in Figure 2 and Tables 3, 4 (supplements section, pages S15 to S16). In Figure 2, the dotted lines mean inclusion without property (iii) of the introduction. For instance,  $K_6$  is contained in  $K_7$ , but the laminating process leads to  $\Lambda_7$  instead. Both sequences, obtained by starting from  $K_8$ , join with the main branch of Figure 1 in dimensions 17, 18, respectively.

Gram matrices of the lattices occurring in Figure 2 can be obtained from the matrices  $\tilde{Q}_{17}$  and  $\tilde{Q}_{18}$  (cf. pages S13 to S14 in the supplements section).

We note that the lattices  $K_{10}$ ,  $K_{14}^a$ ,  $K_{15}^a$ ,  $K_{16}^a$  have smaller discriminants than the lattices  $\Lambda_i$  in the corresponding dimensions and, therefore, yield denser sphere packings. The  $a$ -branch of the  $\kappa$ -sequence also deserves attention for another reason. The elementary divisors of the Gram matrices of  $\Lambda_i$  and  $\Lambda_{23-i}^a$  coincide for  $i = 1, 2, \dots, 6$ . This is a strong indication that the vectors of  $\Lambda_{23}$  which are orthogonal to  $\Lambda_i$  (with respect to some embedding) form a lattice isometric to  $\Lambda_{23-i}^a$  ( $1 \leq i \leq 6$ ) (cf. [2, Theorem 4]). Among the various lattices  $\Lambda_{23-i}$  ( $i = 7, 8, 9$ ) there is none with  $\Lambda_{23-i}^\# / \Lambda_{23-i} \simeq \Lambda_i^\# / \Lambda_i$ . However,  $K_{23-i}^{a\#} / K_{23-i}^a \simeq \Lambda_i^\# / \Lambda_i$  for  $i = 7, 8, 9$ . Also the elementary divisors of the Gram matrices of the lattices  $\Lambda_{23-i}$  which contain  $\Lambda_{15}^f$  are equal to those of  $\Lambda_i(4)$  for  $i = 1, 2, \dots, 8$ . The same interpretation as above is forced upon one's mind. However, we do not have an explanation for the isomorphism of  $\Lambda_{12-i}^\# / \Lambda_{12-i}$  with  $\Lambda_{12+i}^\# / \Lambda_{12+i}$  for certain of the lattices  $\Lambda_{12+i}$ ,  $i = 0, 1, 2, 3, 4$  (see [3] for proofs of some of these and related statements). The lattices  $\Lambda_7$  and  $\Lambda_{15}^f$  are closely related to the Hamming codes of lengths 7, 15, respectively: They can be embedded into the orthogonal lattices  $\mathbf{Z}^7$ ,  $\mathbf{Z}^{15}$  with standard scalar product such that they contain  $2\mathbf{Z}^7$ ,  $2\mathbf{Z}^{15}$ , and correspond to the dual of the Hamming code in  $\mathbf{Z}^7/2\mathbf{Z}^7$ ,  $\mathbf{Z}^{15}/2\mathbf{Z}^{15}$ , respectively (see also [4]). Whereas  $\Lambda_7$  is contained in several orthogonal lattices which are permuted by  $\text{Aut}(\Lambda_7)$ , there is only one orthogonal superlattice for  $\Lambda_{15}^f$  in  $\mathbf{R}\Lambda_{15}^f$ , from which it is immediate that  $\text{Aut}(\Lambda_{15}^f)$  is an extension of  $C_2^{15}$  by  $\text{GL}(4, 2)$ . The lattices  $\Lambda_i$  not contained in  $\Lambda_{15}^f$  cannot be embedded into orthogonal lattices.

Finally, we remark that the automorphism group of  $K_{10}$  is isomorphic to  $C_2 \times W(E_6)'$ . It is the first example known to us of an irreducible maximal finite subgroup of  $\text{GL}(n, \mathbf{Z})$  that is not absolutely irreducible, which answers a question of H. Zassenhaus.

Queen Mary College  
School of Mathematical Sciences  
Mile End Road  
London E1 4NS, England

Mathematisches Institut  
Universität Düsseldorf  
Universitätsstr. 1  
4000 Düsseldorf, West Germany

1. J. CANNON, *A General Purpose Group Theory Program*, Proc. Second Internat. Conf. Theory of Groups, Canberra 1973, Lecture Notes in Math., vol. 372, Springer-Verlag, Berlin and New York, 1974, pp. 204–217.
2. J. H. CONWAY & N. J. A. SLOANE, “Laminated lattices,” *Ann. of Math.*, v. 116, 1982, pp. 593–620.
3. J. H. CONWAY & N. J. A. SLOANE, “Complex and integral laminated lattices,” *Trans. Amer. Math. Soc.*, v. 280, 1983, pp. 463–490.
4. J. LEECH & N. J. A. SLOANE, “Sphere packings and error-correcting codes,” *Canad. J. Math.*, v. 23, 1971, pp. 718–745.
5. J. S. LEON, “Computing automorphism groups of combinatorial objects,” in *Computational Group Theory* (M. D. Atkinson, ed.), Academic Press, London, New York, 1984, pp. 321–336.
6. J. MILNOR & D. HUSEMOLLER, *Symmetric Bilinear Forms*, Ergebnisse Math. Grenzgeb., Band 73, Springer-Verlag, Berlin and New York, 1973.
7. M. POHST, “On the computation of lattice vectors of minimal length, successive minima, and reduced bases with applications,” *ACM Sigsam Bull.*, v. 15, 1981, pp. 37–44.
8. H. ROBERTZ, *Eine Methode zur Berechnung der Automorphismengruppe einer endlichen Gruppe*, Diplomarbeit, Aachen, 1976.