Classification of integral lattices with large class number

Rudolf Scharlau Boris Hemkemeier

Abstract

A detailed exposition of Kneser's neighbour method for quadratic lattices over totally real number fields, and of the sub-procedures needed for its implementation, is given. Using an actual computer program which automatically generates representatives for all isomorphism classes in one genus of rational lattices, various results about genera of ℓ-elementary lattices, for small prime level ℓ, are obtained. For instance, the class number of 12-dimensional 7-elementary even lattices of determinant 7^6 is 395; no extremal lattice in the sense of Quebbemann exists. The implementation incorporates as essential parts previous programs of W. Plesken and B. Souvignier.

1 Introduction

We deal with integral lattices L in euclidean spaces, i.e. $L = \mathbb{Z}v_1 + ... + \mathbb{Z}v_n$ consists of the integral linear combinations of a basis $v_1, ..., v_n$ of a real (or rational) vector space V, equipped with a positive definite symmetric bilinear form. Integral means that the form takes integral values on the lattice: $(x, y) \in \mathbb{Z}$ for all $x, y \in L$. Classification of course means classification up to isometry. We refer to [O'Me71], Chap. 19 and [CoSl88a], Chap. 15 for general results about integral lattices (or, equivalently, integral quadratic forms) and their classification, and to [Nie73, Ven80, Que93, SchVe94, Bac93] for more specialized investigations close to the subject of the present paper. We follow the notation used in [SchVe94].

The class number $h(n, d)$ of lattices in dimension n and determinant d tends to infinity rapidly with n and d. This even holds for forms in a specified genus [Pfe71]. Therefore known classifications have been restricted to small values of n or d, or have been subject to further restrictions within one genus of lattices. The aim of this paper is to present a computer program which, for class numbers up to several hundreds and dimensions up to about 16, automatically generates all lattices (in terms of Gram matrices) of a given genus, deletes forms equivalent to previous ones, and finally produces a list of representatives for all isometry classes. In particular, the class number of the genus is obtained. Although

[0] *Key words and phrases:* lattice, integral quadratic form, class number of genus, neighbour method, p-elementary lattice, extremal modular lattice

some of the papers quoted above are partially computer assisted in the sense that certain auxiliary calculations have been carried out with the aid of a computer, a general approach like the present one up to now has been made only in dimension at most 4 [SPi91].

The principal method used for our algorithm is well known: it is Kneser's method of neighbouring lattices, more precisely the theorem of [Kne57] saying that (under mild conditions) every lattice in a genus can be obtained from a given one via a finite sequence of consecutively neighbouring lattices. The implementation of this method in dimensions 3 and 4 given by Schulze–Pillot [SPi91] heavily relies on the existence of a very fast test for isometry, coming from the existence of an almost unique normal form for the Gram matrix with respect to a reduced basis. This no longer holds in higher dimensions. Our main tool then is the –mathematically straightforward– idea of calculating the neighbours of a lattice only up to the action of the orthogonal group of that lattice. Results like those of [SchVe94], or already known tables of quaternary forms indicate that even for large class number it often happens that every lattice in the genus in question has a large orthogonal group. However, actual theorems on the relation between the mass, the class number, the sizes of the orthogonal groups, and the diameter of the neighbour graph on isometry classes are hardly known.

The methods for fast generation of orthogonal groups and for an efficient test for isometry that we use are described in [PlPo85] and [PlSo93]. We use, as subroutines of our program, implementations of the ideas of [PlSo93] kindly provided to us by Bernd Souvignier.

In the third section of this paper, we report on explicit results obtained by our program. We treat certain genera (of determinant $\ell^{n/2}$) containing ℓ-modular lattices, for small prime numbers ℓ, and suitable dimensions n. Thereby we answer some questions about modularity of ℓ-elementary lattices and about the existence and uniqueness of extremal modular lattices which were posed (implicitly) in the work of Quebbemann [Que93]; cf. also [SchVe94], Section 4.

2 The method

In this section we want to explain in some detail how Kneser's method of neighbouring lattices is used in a practical and efficient way to produce, starting from one Gram matrix G (always assumed to be positive definite), Gram matrices $G = G_1, G_2, \ldots, G_h$ which are representatives for all isometry classes in the genus of L. A detailed account of the neighbour method, including a sketch of the underlying theory, has been given recently in [SPi91]. Nevertheless, we found it convenient to recall a few facts here, in particular, concerning the uniqueness of the neighbour defined by a certain congruence class of vectors. At the same time, we take the opportunity to formulate the main facts for the general case of lattices over (totally real) algebraic number fields. The neighbour method has indeed recently been applied to quaternary lattices over real quadratic fields, including cases where the class number of the field is not one, [Hab94]. For the calculation of a basis and thus a Gram matrix of a neighbouring lattice we use a method which for $p \neq 2$ differs from the method proposed in Step 3 of [SPi91]. The main reason why we introduced our method (the algorithm `N-basis` described below) is that it works in the general number field case. It appears to be more straightforward also in the case of rational integers.

We fix the following notation:

$\mathfrak{o}$ is the ring of integers in a totally real number field F,
L is an integral $\mathfrak{o}$-lattice in an F-vector space with a totally positive definite symmetric bilinear form,
$\mathfrak{d}L$ is the determinant- (or volume-)ideal of L,
$\mathfrak{p}$ is a prime ideal in $\mathfrak{o}$ not dividing $\mathfrak{d}L$.

Definition 2.1 *a) Two lattices L and L' are called $\mathfrak{p}$-neighbours if $L/(L \cap L') \cong \mathfrak{o}/\mathfrak{p} \cong L'/(L \cap L')$ (as $\mathfrak{o}$-modules).*

b) For given L and $v \in L \setminus \mathfrak{p}L$, the lattice

$$L(v) := L_v + \mathfrak{p}^{-1}v, \text{ where } L_v := \{x \in L \mid (x,v) \in \mathfrak{p}\}$$

is called the $\mathfrak{p}$-neighbour of L with respect to v.

In the situation of b), we have $L_v \neq L$ because of our general assumption $\mathfrak{p} \nmid \mathfrak{d}L$, and consequently $L \cap L(v) = L_v$ (since $L/L_v \cong \mathfrak{o}/\mathfrak{p}$ is a simple $\mathfrak{o}$-module), and L and $L(v)$ are indeed neighbours in the sense of a). Conversely, if L and L' are as in a), we can write $L' = L(v)$, where $v = \pi w$, and w is an arbitrary element in $L' \setminus L$, and $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$. (To check this, observe that $L \cap L' \subseteq L_v$, and equality must hold because of the assumption on $L/L \cap L'$.) We observe that the line $(\mathfrak{o}/\mathfrak{p})v + \mathfrak{p}L$ in the $\mathfrak{o}/\mathfrak{p}$-vector-space $\overline{L} = L/\mathfrak{p}L$ is uniquely determined by the neighbour $L(v)$, since it is equal to the orthogonal complement of the hyperplane $\overline{L \cap L'}$ with respect to the regular $\mathfrak{o}/\mathfrak{p}$-valued bilinear form induced on $\overline{L}$. Pushing these considerations on little further leads to the following proposition (cf. [SPi91], properties (iii), (vi), (vii)).

Proposition 2.2 *a) Assume that $\mathfrak{p}$ does not divide 2. For a given isotropic residue class $\overline{v} = v + \mathfrak{p}L \in \overline{L} := L/\mathfrak{p}L$, that is $(v,v) \in \mathfrak{p}$, there exists a vector $\tilde{v} \in v + \mathfrak{p}L$ with $(\tilde{v},\tilde{v}) \in \mathfrak{p}^2$ and thus an integral neighbour $L(\tilde{v})$. Moreover, this neighbour is uniquely determined by the line $(\mathfrak{o}/\mathfrak{p})\overline{v}$. Conversely, each integral neighbour of L is obtained in this way, for a unique isotropic line $(\mathfrak{o}/\mathfrak{p})\overline{v} \subset \overline{L}$.*

b) We assume that L is even and allow that $\mathfrak{p}$ divides 2. For a given residue class $\overline{v} \in \overline{L}$ with $(v,v) \in 2\mathfrak{p}$, there exists a vector $\tilde{v} \in \overline{v}$ with $(\tilde{v},\tilde{v}) \in 2\mathfrak{p}^2$ and thus an even integral neighbour $L(\tilde{v})$. Moreover, this neighbour is uniquely determined by the line $(\mathfrak{o}/\mathfrak{p})\overline{v}$. Conversely, each even integral neighbour of L is obtained in this way, for a unique isotropic line $(\mathfrak{o}/\mathfrak{p})\overline{v} \subset \overline{L}$.

We want to emphazise that the correspondence between isotropic (lines of) residue classes in L and neighbours of L is really canonical in the sense that, if a vector is mapped under an isometry onto a multiple of another vector $\bmod \mathfrak{p}$, then the first neighbour is mapped onto the second by this isometry. Thus, for listing all isometry classes of (even) neighbours of L, it is sufficient to list representatives for the orbits under $\mathrm{O}(L)$ of vectors

$\bmod \mathfrak{p}L$, and only up to multiplication by scalars $\bmod \mathfrak{p}$. Since for $\mathfrak{p}|2$ this statement cannot be found in the literature, and does not seem to be completely obvious even in the case $\mathfrak{o} = \mathbb{Z}$, we present a proof.

First, it is readily checked that

(1) $L(v) = L(\alpha v)$ for every $\alpha \in \mathfrak{o} \setminus \mathfrak{p}$.

We next show that

(2) $v \equiv v' \,(\bmod\, \mathfrak{p}L_v) \Longrightarrow L(v) = L(v')$.

To see this, first notice that already $v \equiv v' \,(\bmod \mathfrak{p}L)$ implies $L_v = L_{v'}$. Now write $v' = v + z$, $z \in \mathfrak{p}L_v$. Then

$$\begin{aligned} \mathfrak{p}^{-1}v' = \mathfrak{p}^{-1}(v+z) \ &\subseteq \mathfrak{p}^{-1}v + \mathfrak{p}^{-1}z \\ &\subseteq \mathfrak{p}^{-1}v + L_v = L(v)\,, \end{aligned}$$

and thus $L(v') = L_v + \mathfrak{p}^{-1}v' \subseteq L(v)$. For reasons of symmetry, we have equality. Now we start with an isotropic class $\overline{v} = v + \mathfrak{p}L$, and we first observe that the condition $(v, v) \in \mathfrak{p}$, respectively $2\mathfrak{p}$, really depends only on $\overline{v}$. From now fix a local prime element $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$. For $\widetilde{v} = v + \pi y$, we can indeed solve the following congruence for y

$$\begin{aligned} (\widetilde{v}, \widetilde{v}) \ &= (v, v) + 2\pi(v, y) + \pi^2(y, y) \\ &\equiv (v, v) + 2\pi(v, y) \\ &\equiv 0 \,(\bmod\, \mathfrak{p}^2, \text{ respectively } 2\mathfrak{p}^2), \end{aligned}$$

and (v, y) is unique $\bmod\, \mathfrak{p}$ and thus the vector y unique $\bmod\, L_v$. Suppose we had started from another vector v' with $v' \equiv \alpha v \,(\bmod\, \mathfrak{p}L)$ for some $\alpha \in \mathfrak{o} \setminus \mathfrak{p}$. We want to show that $L(\widetilde{v}) = L(\widetilde{v}')$, where $\widetilde{v}' = v' + \pi y'$ is such that $(\widetilde{v}', \widetilde{v}') \equiv 0 \,(\bmod\, \mathfrak{p}^2$, respectively $2\mathfrak{p}^2$). By (1), we have $L(\widetilde{v}) = L(\alpha\widetilde{v})$, and we may write $\alpha\widetilde{v} = v' + w$, for some $w \in \mathfrak{p}L$. Thus the desired equality reads

$$L(v' + w) = L(v' + \pi y')\,.$$

The fact that both vectors have norm divisible by $\mathfrak{p}^2$, respectively $2\mathfrak{p}^2$, implies that $w \equiv \pi y' \bmod\ \mathfrak{p}L_v$. Now property (2) applies.

We have observed previously that the converse statement of 2.2 holds.

We now come to the procedure `N-Basis` which, for given L and $v \in L \setminus \mathfrak{p}L$, produces a basis for the neighbour $L(v)$. We consider the case of a general ground ring $\mathfrak{o}$, but for simplicity we shall restrict ourselves to the case of free lattices. The general theory of finitely generated torsion free modules over Dedekind domains then shows that any neighbour, more generally any lattice L' such that $L/(L \cap L') \cong L'/(L \cap L')$ (as $\mathfrak{o}$-modules) is again free (the Steinitz-class remains unchanged). Thus our lattices are equal to $\mathfrak{o}^n$ as modules, and are specified by a Gram matrix $G \in \mathfrak{o}^{n \times n}$, giving rise to the scalar product $(v, w) = (v, w)_G := v^t G w$, where v and w are column vectors. We shall furthermore assume that the prime ideal $\mathfrak{p}$ is principal. The general case for quadratic fields has been treated recently in [Hab94]. As it was seen above, the case $\mathfrak{p}|2$ requires a special treatment. To unify the two cases as far as possible, we introduce the notation

$$\mathfrak{q} = \begin{cases} \mathfrak{p}, & \text{if} \quad \mathfrak{p} \nmid 2 \\ \mathfrak{p}^2, & \text{if} \quad \mathfrak{p}|2\,. \end{cases}$$

In addition to the trivial functions: operations in $\mathfrak{o}$, row vector times matrix, matrix times column vector (which in particular calculate scalar products), the algorithm uses the following functions (α and β are always arguments in $\mathfrak{o}$):

$\texttt{rep-mod-q}(\alpha)$:	representative of $\alpha \pmod{\mathfrak{q}}$ (in a fixed set of representatives $R_\mathfrak{q} \subset \mathfrak{o}$)
$\texttt{mult-mod-q}(\alpha, \beta) :=$	$\texttt{rep-mod-q}(\alpha \cdot \beta)$
$\texttt{inv-mod-q}(\alpha)$:	representative of $\alpha^{-1} (\bmod\, \mathfrak{q})$, where $\alpha \notin \mathfrak{p}$.

In the case $\mathfrak{p}|2$, the simpler functions `rep-mod-p`, `mult-mod-p` and `inv-mod-p`, defined with $\mathfrak{p}$ instead of $\mathfrak{q}$, will be used as well. In the following description of the procedure, we assume that the prime ideal $\mathfrak{p}$ and a generating element $\pi \in \mathfrak{p}$ have been specified in advance. In practice, one has at least two versions of the program, one specifically for $|\mathfrak{o}/\mathfrak{p}| = 2$, using a fast arithmetic $(\bmod\, \mathfrak{p})$, and avoiding the function `normalize` to be described in a moment, and another implementation for the general case, admitting $\mathfrak{p}$ as an additional input variable, or choosing it automatically as the prime ideal of smallest norm not dividing $\mathfrak{d}L$.

A vector $v = (x_1, \ldots, x_n) \in \mathfrak{o}^n$ is called *normalized* if all x_i are representatives $(\bmod\, \mathfrak{q})$, $x_i \in R_\mathfrak{q}$, and the first x_i which is not in $\mathfrak{p}$ equals 1. The following function replaces a given vector $v \in \mathfrak{o}^n \smallsetminus \mathfrak{p}^n$ by a normalized vector v^* such that $L(v) = L(v^*)$:

$$\begin{array}{ll} \texttt{normalize}(v): & k = k(v) := \min\{i \in \{1, \ldots, n\} \mid x_i \notin \mathfrak{p}\} \\ & \alpha := \texttt{inv-mod-q}(x_k) \\ & v \longleftarrow \alpha v \pmod{\mathfrak{q}} . \end{array}$$

If an arbitrary vector v representing an isotropic class is given, i.e. with $(v, v) \in \mathfrak{p}$, respectively$2\mathfrak{p}$, we will in a first preparatory step replace it by $v - \pi\alpha e$. Here the auxiliary vector e satisfies $(e, v) \notin \mathfrak{p}$, and $\alpha = \texttt{mult-mod-p}((v, v), \beta)$, where $\beta = \texttt{inv-mod-p}(2(e, v))$, in the case $\mathfrak{p} \nmid 2$, and $\alpha = \texttt{mult-mod-p}((v, v)/2, \beta)$, where $\beta = \texttt{inv-mod-p}((e, v))$, in the case $\mathfrak{p}|2$. The vector e may be chosen as one of the canonical basis vectors $e_1, \ldots, e_n$ of $\mathfrak{o}^n$. The new vector then satisfies $(v, v) \in \mathfrak{p}^2$, respectively $2\mathfrak{p}^2$. A basis for the neighbouring lattice $L(v)$, and thus a Gram matrix $X^t G X$, where the columns of X are the basis vectors, is now determined as follows:

Algorithm `N-basis`

input (G, v) // assuming $v^t G v \in \mathfrak{p}^2$, $2\mathfrak{p}^2$ //
$v \longleftarrow \texttt{normalize}(v)$
$k := k(v)$ // as given by `normalize` //
find $m \in \{1, \ldots, n\} \smallsetminus \{k\}$ with $e_m^t G v \notin \mathfrak{p}$
$e'_k := v/\pi$
$e'_m := \pi e_m$
for $(i = 1$ to n, $i \neq k$, $i \neq m)$
    $e'_i = e_i - (e_i^t G v / e_m^t G v) e_m \pmod{\mathfrak{p}}$ // this achieves $(e'_i, v) \in \mathfrak{p}$ //
return $(e'_1, e'_2, \ldots, e'_n)$.

To verify that this algorithm is correct, we first have to prove that an index m with $(e_m, v) \notin \mathfrak{p}$ and $m \neq k$ always exists. Assume the contrary, so that $(e_i, v) \in \mathfrak{p}$ for all $i \neq k$. This means that $\overline{v} \in \overline{M}^\perp$, where $\overline{M} \subset \overline{L}$ is the subspace generated by the $\overline{e_i}$, $i \neq k$. Taking orthogonal complements given $\overline{M} \subseteq \overline{v}^{\perp}$, and for dimension reasons we have equality. In particular, $\overline{v} \in \overline{M}$ (recall that $(v,v) \equiv 0 \,(\mathrm{mod}\, \mathfrak{p})$, i.e. $\overline{v} \in \overline{v}^{\perp}$). But the choice of k was such that $x_k \notin \mathfrak{p}$, i.e. $\overline{v} \notin M$, a contradiction.

Now it is readily checked that the e_i' do indeed from a basis of $L(v)$. They are all contained in $L(v)$, since e_m' and the e_i', $i \neq k, m$ are in L_v by definition. The matrix formed by the e_i' has determinant 1 (assume w. l. o. g. $k = 1,\ m = n$):

$$\begin{pmatrix} 1/\pi & 0 & 0 & . & . & . & 0 \\ * & 1 & 0 & . & . & . & 0 \\ . & 0 & 1 & . & . & . & . \\ . & . & 0 & 1 & . & . & . \\ . & . & . & . & . & . & . \\ . & . & . & . & . & 1 & 0 \\ * & * & * & . & . & * & \pi \end{pmatrix}.$$

So the sublattice of $L(v)$ generated by the e_i' must coincide with $L(v)$.

We finish this section with a few words about the main procedure of iterating the calculation of neighbours. The formal framework of this is the following.

For a genus $\mathcal{G}$ let C the set of all isometry classes $[L]$ of lattices in $\mathcal{G}$ and $E = \{([L_1],[L_2]) \in C \times C \mid L_1$ and L_2 are neighbours$\}$. The graph (C,E) is called the *neighbour graph of* $\mathcal{G}$.

The neighbour graph is finite and connected. All isometry classes of neighbours of a given class are generated using the above ideas. So the classification of all lattices in a genus $\mathcal{G}$ can be implemented as a walk through the neighbour graph of $\mathcal{G}$.

We start with a given lattice and mark it "unexplored". Now we enter the following loop: If there is an "unexplored" lattice, mark it "explored", compute all its neighbours up to the action of its orthogonal group, test isometry with all lattices found before, insert the new one into the graph with mark "unexplored". The loop terminates once all lattices are "explored". For the computation of the complete neighbour graph we have to visit all vertices and to compute all edges. But usually we are only interested in the set of vertices and not in set set of edges. This restriction allows some improvements. For example we can use the mass formula (see table 6 p. 12) as break condition for our loop. In view of the large number of triangles in a neighbour graph, we could organize the priority queue for choosing the next vertex to be explored in a more subtle way than *Breadth-First Search* (see [Len90]) is. Strategies like "choose an unexplored vertex with a minimal number of vertices with distance equals 1 (or 2) from it" are usually faster than *Breadth-First Search* or *Depth-First Search.*

An important subroutine in the computation of all classes of neighbours of one fixed lattice is the computation of orbits of vectors modulo $\mathfrak{p}$ under the operation of the ($\mathfrak{p}-$reduced) orthogonal group. This is done via graph traversing too. The same applies to orbits on short vectors. In these cases the algorithm above needs a slight modification, because in general orbit graphs are not connected.

One particular version of our program handles $2-$neighbours, i.e. lattices of odd determinant. This special case can be implemented in a very efficient way, because the construction of neighbours is done using bit arithmetic in $\mathbb{F}_2$.

3 Results

We briefly recall a few definitions from [Que93] and [SchVe94]. A lattice is called *ℓ-elementary,* for some (prime) number ℓ, if $\ell L^{\#} \subseteq L$. Its determinant then is of the form ℓ^m, $0 \leq m \leq n$. For fixed m and odd ℓ, all ℓ-elementary lattices (always assumed to be even) form one genus. The ℓ-scaled dual lattice ${}^{\ell}(L^{\#})$ is again ℓ-elementary, of determinant ℓ^{n-m}. A lattice is *ℓ-modular* if it is isometric to its ℓ-scaled dual. This can only happen if $n = 2m$. For $\ell \equiv 3 \pmod 4$, such lattices exist in all even dimensions. For instance, one can take the orthogonal sum of m copies of the binary lattice $\left(\begin{smallmatrix} 2 & 1 \\ 1 & (\ell+1)/2 \end{smallmatrix}\right)$.

For $\ell = 2, 3, 5, 7, 11, 23$ Quebbemann defines the notion of an extremal modular ℓ-elementary lattice. This roughly means that its minimum is as large as is allowed by the space of modular forms where the theta series lives in. We recall the following values of the minimum of an extremal lattice:

	n	4	6	8	10	12	14	16	18
$\ell = 3:$	min	2	2	2	2	4	4	4	4
$\ell = 5:$	min	2		4		4		6	
$\ell = 7:$	min	2	4	4	4	6	6	6	8
$\ell = 11:$	min	4	4	6	6	8	8		

.

For $\ell = 11$ and $n = 16$, the extremal modular form has a negative coefficient, and thus extremal lattices cannot exist.

In the following, we consider some of the ℓ-elementary genera containing modular lattices, for $\ell = 3, 5, 7, 11$.

For $\ell = 3$ and $n = 12$ (genus of the Coxeter-Todd lattice), the classification had been obtained previously in [SchVe94], using a different method (root systems, glue codes, the mass formula). The classification for $n \leq 10$ is a trivial consequence. We only recall that the class number for $n = 2, 4, 6, 8, 10, 12$ is $1, 1, 1, 2, 3, 10$, respectively; all lattices are modular, and all except for the Coxeter-Todd lattice are reflective, in particular, have minimum 2. Here, we add a result concerning the situation in dimension 14.

Proposition 3.1 *The class number of* 3*-elementary even lattices of dimension* 14 *and determinant* 3^7 *is* 29*. There is a unique lattice with minimum* 4*. This lattice is modular and thus extremal modular. Its automorphism group is* $G_2(3).2$ *of order* $2^7 \cdot 3^6 \cdot 7 \cdot 13$*, see [*$\mathbb{ATLAS}$*] p. 60. For all other lattices in this genus, the order of the automorphism group is not divisible by* 13.

For $\ell = 5$, the genera in question exist only in dimensions divisible by 4. The result in dimension $n = 8$ mentioned in [SchVe94] should be completed by giving the root systems of the reflective lattices: $4\mathsf{A}_1 4\,{}^5\mathsf{A}_1, 2\mathsf{A}_2 2\,{}^5\mathsf{A}_2, \mathsf{D}_4\,{}^5\mathsf{D}_4, \mathsf{A}_4\,{}^5\mathsf{A}_4$. In dimension 12, the structure of this genus is less pleasing.

Proposition 3.2 [1] *The class number of* 5*-elementary even lattices of dimension* 12 *and determinant* 5^6 *is* 48*. Among these lattices,* 40 *are modular,* 4 *are modular extremal, and* 43 *are indecomposable.*

[1] This result has been obtained independently by G. Nebe of the RWTH at Aachen.

We now come to the case of level $\ell = 7$ where we obtained the main result of this paper.

Theorem 3.3 *There exists no* 7*-elementary even lattice of dimension* 12*, determinant* 7^6*, and with minimum* 6*. In particular, there exists no extremal* 7*-modular lattice of dimension* 12.

We recall that "usually" extremal lattices for a specified value of (n, ℓ) do not exist, because the extremal modular form has a negative coefficient and thus cannot be a θ-series. The case $(12, 7)$ is the first case where the non-existence is known although the modular form gives no obstruction. The proof of the theorem is obtained by classifying the whole genus: the class number is 395, and the minimum 6 just never occurs.

For level $\ell = 7$ and dimensions less than 12, we present the classification in some detail.

Proposition 3.4 *a) For* $n = 4, 6, 8$*, the genus of* n*-dimensional* 7*-elementary, even lattices of determinant* $7^{n/2}$ *has class number* $1, 3, 8$ *respectively. All these lattices are modular. In each of these dimensions there exists a unique extremal lattice. The number of indecomposable lattices is* $1, 2, 5$ *respectively.*

b) The class number of 7*-elementary even lattices of dimension* 10 *and determinant* 7^5 *is* 30*. Among these lattices,* 28 *are modular,* 4 *are modular extremal, and* 22 *are indecomposable.*

We now come to 11-elementary lattices. The 8-dimensional case is similar in size to the $(10, 7^5)$-case treated above. The structure of this genus is however more satisfactory, as the following result shows:

Theorem 3.5 *For* $n = 4, 6, 8$*, the genus of* n*-dimensional* 11*-elementary, even lattices of determinant* $11^{n/2}$ *has class number* $3, 5, 31$ *respectively. All these lattices are modular. In each dimension there exists a unique extremal lattice. The number of indecomposable lattices is* $2, 2, 23$ *respectively.*

In dimension 10, the question of existence of extremal 11-modular lattices is still easy in view of the Craig lattice. The following theorem complements this observation of H.-G. Quebbemann.

Theorem 3.6 *The class number of* 10*-dimensional* 11*-elementary, even lattices of determinant* 11^5 *is* 297*. In addition to the Craig lattice, there exists exactly one further lattice with minimum* 6*. It is modular and thus extremal; its automorphism group has order* $2^5 \cdot 3^2 \cdot 5$.

In the following tables, we list the lattices of some of the above genera with their main invariants and further properties, namely the following:

$\mathsf{R}(L)$	the root system of L (cf. [SchVe94])
$\lvert\mathrm{O}(L)\rvert$	the order of the orthogonal group of L
$\lvert\mathrm{A}(L)\rvert$	the order of $\mathrm{O}(L)/\mathrm{W}(L)$, where $\mathrm{W}(L)$ is the Weyl group
r_2, r_4	number of vectors of norm 2 resp. 4
o_2, o_4	number of orbits of $\mathrm{O}(L)$ on vectors of norm 2 resp. 4
Properties	NM non-modular
	E extremal
	R reflective
	D decomposable

The ordering of the lattices within one table is as follows. The indecomposable ones are listed first; they are ordered by considering hierarchically the following criteria:

largest minimum
largest number of vectors of minimal norm
largest rank of the root system
largest order of the automorphism group
smallest number of orbits on minimal vectors

The decomposable lattices, say with r components of dimensions $n_1 \geq n_2 \geq \ldots \geq n_r$ are listed in lexicographic order with respect to the dimension vector $(n_1, \ldots, n_r)$ and for fixed dimension vector, with respect to the previous ordering of the lower dimensional components.

Table 1: $\ell = 7, n = 6$

number	$\mathsf{R}(L)$	$\lvert\mathrm{O}(L)\rvert$	$\lvert\mathrm{A}(L)\rvert$	r_2	r_4	o_2	o_4	Properties
1		$2^5 3^1 7^1$	$2^5 3^1 7^1$	0	42	0	1	E
2	$\mathsf{A}_3\,{}^7\mathsf{A}_3$	$2^7 3^2$	2^1	12	6	1	1	R
3	$3\mathsf{A}_1 3\,{}^7\mathsf{A}_1$	$2^7 3^1$	$2^1 3^1$	6	24	1	2	D,R

Table 2: $\ell = 7, n = 8$

number	$\mathsf{R}(L)$	$\lvert\mathrm{O}(L)\rvert$	$\lvert\mathrm{A}(L)\rvert$	r_2	r_4	o_2	o_4	Properties
1		$2^8 3^2$	$2^8 3^2$	0	48	0	1	E
2	$\mathsf{D}_4\,{}^7\mathsf{D}_4$	$2^{13} 3^3$	$2^1 3^1$	24	24	1	1	R
3	$2\mathsf{A}_2 2\,{}^7\mathsf{A}_2$	$2^7 3^4$	2^3	12	36	1	1	R
4	$\mathsf{A}_2\,{}^7\mathsf{A}_2$	$2^5 3^3$	$2^3 3^1$	6	42	1	2	
5	$2\mathsf{A}_1 2\,{}^7\mathsf{A}_1$	2^9	2^5	4	44	1	3	
6	$\mathsf{A}_1\,{}^7\mathsf{A}_1$	$2^7 3^1 7^1$	$2^5 3^1 7^1$	2	46	1	2	D
7	$\mathsf{A}_3\mathsf{A}_1\,{}^7\mathsf{A}_3\,{}^7\mathsf{A}_1$	$2^9 3^2$	2^1	14	34	2	3	D,R
8	$4\mathsf{A}_1 4\,{}^7\mathsf{A}_1$	$2^{11} 3^2$	$2^3 3^1$	8	40	1	2	D,R

Table 3: $\ell = 7$, $n = 10$

number	R(L)	$\lvert\mathrm{O}(L)\rvert$	$\lvert\mathrm{A}(L)\rvert$	r_2	r_4	o_2	o_4	Properties
1		$2^8 3^1 5^1$	$2^8 3^1 5^1$	0	50	0	2	E
2		$2^5 3^2 5^1$	$2^5 3^2 5^1$	0	50	0	2	E
3		2^{10}	2^{10}	0	50	0	3	E
4		$2^6 5^1$	$2^6 5^1$	0	50	0	2	E
5	$D_5\,{}^7D_5$	$2^{15} 3^2 5^2$	2^1	40	90	1	2	R
6	$A_4\,{}^7A_4$	$2^8 3^2 5^2$	2^2	20	70	1	3	
7	$A_3A_1\,{}^7A_3\,{}^7A_1$	$2^{10} 3^2$	2^2	14	64	2	4	
8	$2A_2 2\,{}^7A_2$	$2^{11} 3^2$	2^7	12	62	1	3	
9	$A_3\,{}^7A_3$	$2^{11} 3^2$	2^5	12	62	1	3	
10	$A_3\,{}^7A_3$	$2^{11} 3^2$	2^5	12	62	1	3	
11	$A_2 2A_1\,{}^7A_2 2\,{}^7A_1$	$2^9 3^2$	2^3	10	60	2	4	
12	$4A_1 4\,{}^7A_1$	$2^{12} 3^1$	$2^4 3^1$	8	58	1	3	
13	$A_2A_1\,{}^7A_2\,{}^7A_1$	$2^6 3^2$	2^2	8	58	2	5	
14	$A_2\,{}^7A_2$	$2^7 3^2$	2^5	6	56	1	2	
15	$3A_1\,{}^7A_2$	$2^7 3^2$	$2^3 3^1$	6	56	1	4	NM
16	$A_2 3\,{}^7A_1$	$2^7 3^2$	$2^3 3^1$	6	56	1	5	NM
17	$2A_1 2\,{}^7A_1$	$2^9 3^1$	$2^5 3^1$	4	54	1	4	
18	$2A_1 2\,{}^7A_1$	2^8	2^4	4	54	1	5	
19	$2A_1 2\,{}^7A_1$	2^8	2^4	4	54	1	7	
20	$A_1\,{}^7A_1$	2^8	2^6	2	52	1	3	
21	$A_1\,{}^7A_1$	$2^6 3^1$	$2^4 3^1$	2	52	1	4	
22	$A_1\,{}^7A_1$	$2^6 3^1$	$2^4 3^1$	2	52	1	5	
23	$A_1\,{}^7A_1$	$2^{10} 3^2$	$2^8 3^2$	2	52	1	2	D
24	$D_4A_1\,{}^7D_4\,{}^7A_1$	$2^{15} 3^3$	$2^1 3^1$	26	76	2	3	D,R
25	$2A_2A_1 2\,{}^7A_2\,{}^7A_1$	$2^9 3^4$	2^3	14	64	2	3	D,R
26	$A_2A_1\,{}^7A_2\,{}^7A_1$	$2^7 3^3$	$2^3 3^1$	8	58	2	4	D
27	$3A_1 3\,{}^7A_1$	2^{11}	2^5	6	56	2	5	D
28	$2A_1 2\,{}^7A_1$	$2^{10} 3^1 7^1$	$2^6 3^1 7^1$	4	54	1	3	D
29	$A_3 2A_1\,{}^7A_3 2\,{}^7A_1$	$2^{12} 3^2$	2^2	16	66	2	4	D,R
30	$5A_1 5\,{}^7A_1$	$2^{13} 3^1 5^1$	$2^3 3^1 5^1$	10	60	1	2	D,R

Table 4: $\ell = 11$, $n = 6$

number	R(L)	$\lvert\mathrm{O}(L)\rvert$	$\lvert\mathrm{A}(L)\rvert$	r_2	r_4	o_2	o_4	Properties
1		$2^3 3^1 5^1$	$2^3 3^1 5^1$	0	12	0	1	E
2	$A_2\,{}^{11}A_2$	$2^4 3^3$	$2^2 3^1$	6	12	1	1	
3	$A_1\,{}^{11}A_1$	$2^5 3^1$	$2^3 3^1$	2	12	1	1	D
4	$A_2A_1\,{}^{11}A_2\,{}^{11}A_1$	$2^5 3^2$	2^1	8	12	2	1	D,R
5	$3A_1 3\,{}^{11}A_1$	$2^7 3^1$	$2^1 3^1$	6	12	1	1	D,R

Table 5: $\ell = 11$, $n = 8$

number	$\mathsf{R}(L)$	$\lvert \mathrm{O}(L) \rvert$	$\lvert \mathrm{A}(L) \rvert$	r_2	r_4	o_2	o_4	Properties
1		$2^6 3^2 5^2$	$2^6 3^2 5^2$	0	0	0	0	E
2		$2^7 3^2$	$2^7 3^2$	0	24	0	1	
3		$2^7 3^2$	$2^7 3^2$	0	24	0	1	
4		$2^5 3^1$	$2^5 3^1$	0	20	0	3	
5		$2^4 3^2$	$2^4 3^2$	0	18	0	1	
6		2^6	2^6	0	16	0	1	
7		$2^5 3^2$	$2^5 3^2$	0	12	0	1	
8		$2^4 3^1 5^1$	$2^4 3^1 5^1$	0	10	0	1	
9		$2^7 3^1$	$2^7 3^1$	0	8	0	1	
10	$\mathsf{D}_4\, {}^{11}\mathsf{D}_4$	$2^{13} 3^3$	$2^1 3^1$	24	24	1	1	R
11	$\mathsf{A}_4\, {}^{11}\mathsf{A}_4$	$2^7 3^2 5^2$	2^1	20	30	1	1	R
12	$\mathsf{A}_3\, {}^{11}\mathsf{A}_3$	$2^8 3^2$	2^2	12	20	1	3	
13	$3\mathsf{A}_1 3\, {}^{11}\mathsf{A}_1$	$2^8 3^1$	$2^2 3^1$	6	28	1	2	
14	$\mathsf{A}_2\, {}^{11}\mathsf{A}_2$	$2^4 3^3$	$2^2 3^1$	6	18	1	1	
15	$\mathsf{A}_2\, {}^{11}\mathsf{A}_2$	$2^5 3^2$	2^3	6	16	1	2	
16	$2\mathsf{A}_1 2\, {}^{11}\mathsf{A}_1$	2^8	2^4	4	24	1	3	
17	$2\mathsf{A}_1 2\, {}^{11}\mathsf{A}_1$	2^7	2^3	4	22	1	4	
18	$2\mathsf{A}_1 2\, {}^{11}\mathsf{A}_1$	2^7	2^3	4	20	1	2	
19	$\mathsf{A}_1\, {}^{11}\mathsf{A}_1$	$2^5 3^1 5^1$	$2^3 3^1 5^1$	2	24	1	1	
20	$\mathsf{A}_1\, {}^{11}\mathsf{A}_1$	$2^5 3^1$	$2^3 3^1$	2	12	1	1	
21	$\mathsf{A}_1\, {}^{11}\mathsf{A}_1$	2^6	2^4	2	20	1	2	
22	$\mathsf{A}_1\, {}^{11}\mathsf{A}_1$	$2^4 3^1$	$2^2 3^1$	2	18	1	2	
23	$\mathsf{A}_1\, {}^{11}\mathsf{A}_1$	2^5	2^3	2	16	1	4	
24	$\mathsf{A}_1\, {}^{11}\mathsf{A}_1$	$2^5 3^1 5^1$	$2^3 3^1 5^1$	2	12	1	1	D
25	$\mathsf{A}_2\mathsf{A}_1\, {}^{11}\mathsf{A}_2\, {}^{11}\mathsf{A}_1$	$2^6 3^2$	2^2	8	24	2	2	D
26		$2^4 3^1 5^1$	$2^4 3^1 5^1$	0	20	0	1	D
27	$\mathsf{A}_2\, {}^{11}\mathsf{A}_2$	$2^6 3^3$	$2^4 3^1$	6	11	1	1	D
28	$2\mathsf{A}_2 2\, {}^{11}\mathsf{A}_2$	$2^7 3^4$	2^3	12	36	1	1	D,R
29	$2\mathsf{A}_1 2\, {}^{11}\mathsf{A}_1$	$2^8 3^1$	$2^4 3^1$	4	16	1	2	D
30	$\mathsf{A}_2 2\mathsf{A}_1\, {}^{11}\mathsf{A}_2 2\, {}^{11}\mathsf{A}_1$	$2^8 3^2$	2^2	10	28	2	2	D,R
31	$4\mathsf{A}_1 4\, {}^{11}\mathsf{A}_1$	$2^{11} 3^1$	$2^3 3^1$	8	24	1	1	D,R

Table 6: Table of masses and class numbers.

genus	mass				h
$(8,3^4)$	$\frac{13}{1990656}$	$=$	$\frac{13}{2^{13}\cdot 3^5}$	≈ 0.000006530510	2
$(10,3^5)$	$\frac{533}{597196800}$	$=$	$\frac{13\cdot 41}{2^{15}\cdot 3^6\cdot 5^2}$	≈ 0.0000008925031	3
$(12,3^6)$	$\frac{4649359}{4213820620800}$	$=$	$\frac{11\cdot 13^2\cdot 41\cdot 61}{2^19\cdot 3^8\cdot 5^2\cdot 7^2}$	≈ 0.000001103359	10
$(14,3^7)$	$\frac{1387737373}{93908002406400}$	$=$	$\frac{11\cdot 41\cdot 61\cdot 73\cdot 691}{2^{21}\cdot 3^9\cdot 7\cdot 13}$	≈ 0.00001477762	29
$(16,3^8)$	$\frac{34017205168248203}{12621235523420160000}$	$=$	$\frac{11\cdot 41^2\cdot 61^2\cdot 73\cdot 547\cdot 691\cdot 1093}{2^{29}\cdot 3^{10}\cdot 5^4\cdot 7^2\cdot 13}$	≈ 0.002695235	163
$(8,5^4)$	$\frac{5239}{16588800}$	$=$	$\frac{13\cdot 31}{2^{13}\cdot 3^4\cdot 5^2}$	≈ 0.0003158154	5
$(12,5^6)$	$\frac{11126633863}{1053455155200}$	$=$	$\frac{31^2\cdot 71\cdot 313\cdot 521}{2^{17}\cdot 3^8\cdot 5^2\cdot 7^2}$	≈ 0.010562038	48
$(16,5^8)$	$\frac{382741967819368836662539}{12621235523420160000}$	$=$	$\frac{29\cdot 71\cdot 313\cdot 449\cdot 521\cdot 601\cdot 691\cdot 19531}{2^{19}\cdot 3^{10}\cdot 5^4\cdot 7^2\cdot 13}$	≈ 30325.23	?
$(6,7^3)$	$\frac{5}{1008}$	$=$	$\frac{5}{2^4\cdot 3^2\cdot 7}$	≈ 0.004960317	3
$(8,7^4)$	$\frac{20425}{4644864}$	$=$	$\frac{5^2\cdot 19\cdot 43}{2^{13}\cdot 3^4\cdot 7}$	≈ 0.004397330	8
$(10,7^5)$	$\frac{981217}{29030400}$	$=$	$\frac{19\cdot 43\cdot 1201}{2^{11}\cdot 3^4\cdot 5^2\cdot 7}$	≈ 0.03379963	30
$(12,7^6)$	$\frac{231951232951}{52022476800}$	$=$	$\frac{19\cdot 191\cdot 1201\cdot 2801}{2^{19}\cdot 3^4\cdot 5^2\cdot 7^2}$	≈ 4.458673	395
$(14,7^7)$	$\frac{5866363445756953}{421382062080}$	$=$	$\frac{73\cdot 181\cdot 191\cdot 691\cdot 1201\cdot 2801}{2^{18}\cdot 3^8\cdot 5\cdot 7^2}$	≈ 13921.72	?
$(4,11^2)$	$\frac{25}{288}$	$=$	$\frac{5^2}{2^5\cdot 3^2}$	≈ 0.01736111	3
$(6,11^3)$	$\frac{61}{1920}$	$=$	$\frac{61}{2^7\cdot 3\cdot 5}$	≈ 0.03177083	5
$(8,11^4)$	$\frac{2615863}{16588800}$	$=$	$\frac{19\cdot 37\cdot 61^2}{2^{13}\cdot 3^4\cdot 5^2}$	≈ 0.1576885	31
$(10,11^5)$	$\frac{87493271}{9732096}$	$=$	$\frac{17\cdot 19\cdot 37\cdot 7321}{2^{15}\cdot 3^3\cdot 11}$	≈ 8.990177	297
$(12,11^6)$	$\frac{571246055535605}{37838389248}$	$=$	$\frac{5\cdot 19^2\cdot 3221\cdot 7321\cdot 13421}{2^{19}\cdot 3^8\cdot 11}$	≈ 15096.99	?

References

[ATLAS] J.H. Conway et al.: *Atlas of finite groups.* Oxford University Press, 1985.

[Bac93] C. Bachoc: Voisinage au sens de Kneser pur les réseaux quaterioniens. Preprint Université Bordeaux I, 1993.

[CoSl88a] J.H. Conway, N.J.A. Sloane: *Sphere packings, lattices and groups.* Springer-Verlag New York, 1988.

[CoSl88b] J.H. Conway, N.J.A. Sloane: Low dimensional lattices. IV. The mass formula. Proc. R. Soc. London A **419** (1988), 259–286.

[Hab94] B. Habdank: Unimodulare Gitter über reell-quadratischen Zahlkörpern. Dissertation, Bielefeld 1994.

[Kne57] M. Kneser: Klassenzahlen definiter quadratischer Formen. Arch. Math. **8** (1957), 241–250.

[Len90] T. Lengauer: *Combinatorial Algorithms for Integrated Circuit Layout,* Teubner/Wiley 1990.

[Nie73] H.-V. Niemeier: Definite quadratische Formen der Dimension 24 und Diskriminante 1. J. Number Theory **5** (1973), 142-178.

[O'Me71] O.T. O'Meara: *Introduction to quadratic forms*, Springer–Verlag Berlin 1971.

[Pfe71] H. Pfeuffer: Einklassige Geschlechter totalpositiver quadratischer Formen in totalreellen algebraischen Zahlkörpern. J. Number Theory **4** (1971), 371–411.

[PlPo85] W. Plesken, M. Pohst: Constructing integral lattices with prescribed minimum. I. Math. Comp. **45** (1985), 209–221.

[PlSo93] W. Plesken, B. Souvignier: Computing isometries of lattices. Preprint 1993.

[Que93] H.-G. Quebbemann: Modular Lattices in Euclidean Spaces. Universität Bielefeld, SFB 343, Preprint 93–031. To appear in J. Number Theory.

[SchVe94] R. Scharlau, B.B. Venkov: The genus of the Barnes-Wall Lattice. Comment. Math. Helvetici **69** (1994), 322–333.

[SPi91] R. Schulze-Pillot: An algorithm for computing genera of ternary and quaternary quadratic forms. Proc. of the Int. Symp. on Symbolic and Algebraic Computation, Bonn 1991.

[Ven80] B.B. Venkov: On the classification of integral even unimodular 24-dimensional quadratic forms. Proc. Steklov Inst. Math. **4** (1980), 63–74, also reprinted as chapter 18 in [CoSl88a].

Addresses:

Universität Dortmund
Fachbereich Mathematik
44221 Dortmund
Internet: Rudolf.Scharlau@Mathematik.Uni–Dortmund.DE
and Boris.Hemkemeier@Mathematik.Uni–Dortmund.DE