Automorphism Groups of Lattices in Large Genera

Rudolf Scharlau

Technische Universität Dortmund

BIRS, Banff, 14. November 2011

Lattices and their genera
Automorphism groups
Explicit enumeration of large genera

Rudolf Scharlau Groups in Large Genera

Lattices

Definition 1.1

A (full) **lattice** on a quadratic vector space (V, b) over $\mathbb{Q}$ is a subset of the shape

$$\begin{aligned} L &= \{x_1v_1 + x_2v_2 + \cdots + x_nv_n \mid x_1, \ldots, x_n \in \mathbb{Z}\} \\ &= \mathbb{Z}v_1 \oplus \mathbb{Z}v_2 \oplus \ldots \oplus \mathbb{Z}v_n \end{aligned}$$

for some basis $v_1, v_2, \ldots, v_n$ of V.

The associated integral quadratic form is

$$Q(x_1, \ldots, x_n) = \tfrac{1}{2}\sum_{i,j} b(v_i, v_j)\, x_ix_j.$$

Lattices and their genera
Automorphism groups
Explicit enumeration of large genera
Lattices
Genera of lattices

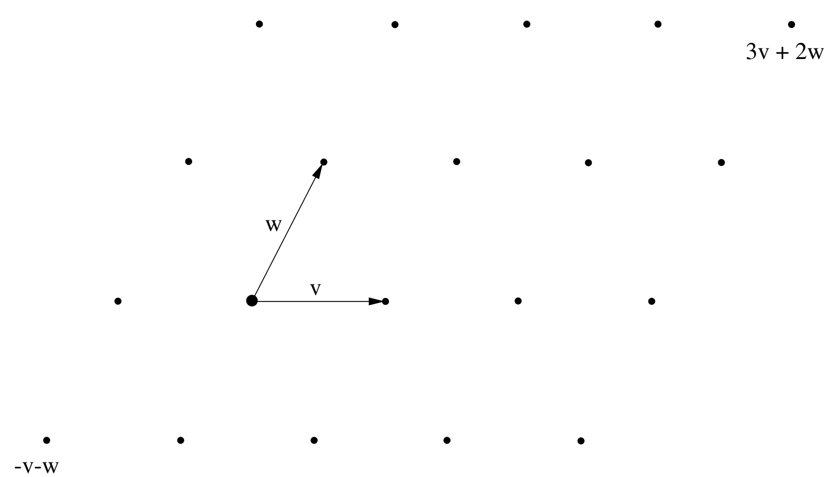

Fig. 1: A lattice in dimension 2

Rudolf Scharlau Groups in Large Genera

Definition 1.2

The **Gram matrix** of a lattice L w.r.t. a basis $v_1, \ldots, v_n$ is the symmetric $n \times n$-matrix $(b(v_i, v_j))$.

The **determinant** $\det L$ of L is the determinant of any Gram matrix of L.

A quadratic lattice is called an **integral lattice** if $b(L, L) \subseteq \mathbb{Z}$.

Theorem 1.1 (Finiteness of Class Number)

For a given determinant d, the number of isometry classes of (positive definite) integral lattices with determinant d is finite.

This is a consequence of reduction theory, which gives a lattice basis with $b(v_i, v_i) \leq C\, d^{1/n}$ for some constant C.

Genera of lattices

Let p be a prime number. Every quadratic vector space (V, b) over $\mathbb{Q}$ embeds into a quadratic vector space (V_p, b) over $\mathbb{Q}_p$, its **completion** at the prime p, where $V_p := V \otimes_{\mathbb{Q}} \mathbb{Q}_p$, and the natural extension $b_p : V_p \times V_p \to \mathbb{Q}_p$ is simply denoted by b again. This definition extends to $p = \infty$ with $\mathbb{Q}_\infty := \mathbb{R}$.

The (weak) local-global principle of Minkowski and Hasse for quadratic spaces says that (V, b) is determined up to isomorphism by all its completions.

Similarly, a quadratic lattice L embeds into its **completion** $L_p := L \otimes_{\mathbb{Z}} \mathbb{Z}_p$. One also sets $L_\infty = V_\infty$.

The local-global principle of Minkowski and Hasse in general does not hold for quadratic lattices. Therefore, the following notion is introduced.

Definition 1.3

Two lattices L and M are in the same **genus** if $L_p \cong M_p$ for all $p \in \mathbb{P} \cup \{\infty\}$.

Lattices in the same genus have the same determinant. Thus:

The number $h(\mathcal{G})$ of isometry classes in a genus $\mathcal{G}$ is finite. It is called the **class number** of the genus.

Basic task: Given a genus in terms of local data (e.g. modular decomposition, genus symbol, discriminant quadratic form on the discrimiminant group $L^{\#}/L$), determine a set of representatives, in particular the class number of $\mathcal{G}$.

Automorphism groups

Mass and class number of a genus

For a lattice L in a quadratic vector V space over $\mathbb{Q}$, we denote by $\mathrm{Aut}\, L := \mathrm{Aut}(L,b) \subset \mathrm{O}(V,b)$ its automorphism group. We always aussume that b is positive definite, then

$$a(L) := |\,\mathrm{Aut}\, L| < \infty.$$

Every finite rational matrix group can be embedded into a group $\mathrm{Aut}(L,b)$. Any maximal f.r.m.g. can be realized as a group $\mathrm{Aut}\, L$.

Definition 2.1 (The mass of a genus)

Let $L = L_1, \ldots, L_h$ be a system of representatives for a genus $\mathcal{G}$ of positive definite lattices of dimension n. The sum of the inverses of the orders of their automorphism groups is called the **mass** of $\mathcal{G}$:

$$\mathrm{mass}(\mathcal{G}) := \sum_{j=1}^{h} \frac{1}{a(L_j)}.$$

The notion goes back to G. Eisenstein; also H.J.S Smith used it before Minkowski developed his theory.

Theorem 2.1 (Minkowski's mass formula)

Let $L = L_1, \ldots, L_h$ be a system of representatives for a genus $\mathcal{G}$ of positive definite lattices of dimension n. The mass of $\mathcal{G}$ is the product of certain **representation densities** *$\alpha_p(L_p, L_p)$, where p runs over all primes, with a certain factor "at infinity":*

$$\mathrm{mass}(\mathcal{G}) = \sum_{j=1}^{h} \frac{1}{|\,\mathrm{Aut}(L_j)|} = \gamma(n) \prod_{p} \alpha_p^{-1}(L_p, L_p).$$

We want to study automorphism groups of lattices in a given genus $\mathcal{G}$.

Notation:

- $\mathcal{G}_0 := \{L \in \mathcal{G} \mid \mathrm{Aut}\, L = \{\pm \mathrm{id}\}$
- $\mathcal{G}_1 := \{L \in \mathcal{G} \mid \mathrm{Aut}\, L \neq \{\pm \mathrm{id}\}$
- $h_0(\mathcal{G}) := \mathrm{card}\, \mathcal{G}_0$, $h_1(\mathcal{G}) := \mathrm{card}\, \mathcal{G}_1$
- $\mathrm{mass}(\mathcal{G}) =: m(\mathcal{G})$, define $m_0(\mathcal{G})$, $m_1(\mathcal{G})$ in the obvious way

Obvious facts:

- $h(\mathcal{G}) = h_0(\mathcal{G}) + h_1(\mathcal{G}), \quad m(\mathcal{G}) = m_0(\mathcal{G}) + m_1(\mathcal{G})$
- $h_0(\mathcal{G}) = 2m_0(\mathcal{G})$
- $h(\mathcal{G}) \geq 2m(\mathcal{G})$

Theorem 2.2 (Minkowski)

The order of finite subgroups of $\mathrm{GL}_n(\mathbb{Z})$ *is bounded by*

$$\tilde{a}(n) := \prod_{p \leq n+1} p^{\mu(n,p)},$$

where

$$\mu(n,p) = \sum_{j \geq 0} \left[\frac{n}{(p-1)p^j} \right]$$

Minkowski obtained his bound by reducing the group modulo p (respectively modulo 4, if $p = 2$).

Example:
$$\begin{aligned} \tilde{a}(16) &= 2^{31} \cdot 3^{10} \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \\ a(I_{16}) &= 2^{31} \cdot 3^6 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13 \\ a(2E_8) &= 2^{29} \cdot 3^{10} \cdot 5^4 \cdot 7^2 \end{aligned}$$

Now we have an (again very crude) estimate between class number and mass in the converse direction:

$$h(\mathcal{G}) \leq \tilde{a}(m) \cdot m(\mathcal{G}).$$

Notice that the bound $\tilde{a}(n)$ grows very fast (roughly like n^n). Clearly $2^n \cdot n! = a(I_n)$ is a lower bound.

Theorem 2.3 (W. Magnus, 1937, H. Pfeuffer, 1971)

For genera $\mathcal{G}$ *of positive definite lattices of dimension* $n \geq 6$ *and determinant* d*, one has*

$$\mathrm{mass}(\mathcal{G}) > 2^{-n+1} \cdot \prod_{k=1}^{n} \frac{\Gamma(k/2)}{\pi^{k/2}} \cdot d^{\frac{1}{26}},$$

similarly for $3 \leq n \leq 5$.

Therefore, the mass, and thus also the class number $h(\mathcal{G})$, goes to infinity with the dimension (very rapidly), and also with the determinant.

Theorem 2.4 (Jürgen Biermann, 1980)

For genera $\mathcal{G}$ of positive definite lattices **in fixed dimension** *$n \geq 3$, one has*

$$\frac{h_0(\mathcal{G})}{h(\mathcal{G})} \to 1, \quad \textit{if } \det \mathcal{G} \to \infty.$$

With $h(\mathcal{G}) = h_0(\mathcal{G}) + h_1(\mathcal{G})$ one rewrites this as

$$\frac{h_1(\mathcal{G})}{h(\mathcal{G})} \to 0, \quad \text{if } \det \mathcal{G} \to \infty.$$

"Most lattices have trivial automorphism group."

Theorem 2.5 (Etsuko Bannai, 1988)

For the genus $\mathcal{E}_n$ of even or odd unimodular positive definite lattices dimension n, one has

$$\frac{m_1(\mathcal{E}_n)}{m(\mathcal{E}_n)} \to 0, \quad \textit{if } n \to \infty.$$

More precisely

$$\frac{m_1(\mathcal{E}_n)}{m(\mathcal{E}_n)} \leq 2 \cdot \frac{(8\pi)^{n/2}}{\Gamma(n/2)} \quad \text{if } n \geq 144.$$

Thus, "many" lattices with trivial group exist, for growing dimension.

Trying to transform Bannai's estimate into an estimate of class numbers, using the above upper and lower bounds, leads to

$$\frac{h_1}{h} \leq \frac{\tilde{a}(n) \cdot m_1}{2 \cdot m} \leq \tilde{a}(n) \cdot \frac{(8\pi)^{n/2}}{\Gamma(n/2)}.$$

Since $\tilde{a}^n > n!$, the right hand side tends to infinity.

Therefore, in order to prove that again "most lattices have trivial automorphism group", better upper estimates for the class number h_1 of lattices with non-trivial group are needed.

Explicit classification of large genera
A general strategiy for classification

We want to look at the actual distribution of (orders of) automorphism groups among all the lattices of some (arithmetically interesting) large genera.

Enumerate a set of representatives for a specified genus $\mathcal{G}$, following these steps:

1. Generate lattices in $\mathcal{G}$ by some algebraic procedure
2. Test for isometry with lattices already constructed
3. Verify the completeness of the list

Step 1 is typically handled by Kneser's method of neighbouring lattices: L and L' are neighbors, if their intersection $L \cap L'$ is of index 2 in both of them.
All neigbours of L can be efficiently generated from (certain) classes of $L/2L$.
Step 2 is a matter of invariants (theta series, order of automorphism group, successice minima, ...) and of sophisticated algorithms for testing isometry of a given pair of lattices (improved backtracking), by Plesken and Souvignier.
Step 3 is handled best by the mass formula.

Some genera of level 2, 5, 7, 11

The following is joint work with Boris Hemkemeier.

Theorem 3.1 (Level 11, dimension 12)

The genus $II_{12}(11^6)$ *has class number* 67323. *It contains precisely*

- 27193 *lattices with minimum* 2
- 40036 *lattices with minimum* 4
- 94 *lattices with minimum* 6
- *no lattice with minimum* 8.

This reproves the absence of "extremal" 11-modular lattices in this genus, first shown by Nebe and Venkov using Siegel modular forms.

The automorphism groups for the genus $II_{12}(11^6)$:
recall $a(L) := |\mathrm{Aut}(L)|$:

Among the 67323 lattices, there exist

- 16613 lattices (24.7%) with trivial group, i.e. $a(L) = 2$
- 6065 lattices for which $3 \mid a(L)$
- 421 lattices for which $5 \mid a(L)$
- 0 lattices for which $7 \mid a(L)$ or $13 \mid a(L)$
- 1 lattice for which $11 \mid a(L)$

Theorem 3.2 (Level 14, dimension 14)

The genus $II_{14}(7^7)$ *has class number* 83006. *It contains precisely*

- 46574 *lattices with minimum* 2
- 36431 *lattices with minimum* 4
- 1 *lattice with minimum* 6.

The unique extremal 7-modular lattice was not known before.

The automorphism groups for the genus $II_{14}(7^7)$:
recall $a(L) := |\operatorname{Aut}(L)|$:

Among the 83006 lattices, there exist

12827 lattices (15.4%) with trivial group, i.e. $a(L) = 2$
11797 lattices for which $3 \mid a(L)$
353 lattices for which $5 \mid a(L)$
82 lattices for which $7 \mid a(L)$
0 lattices for which $11 \mid a(L)$ or $13 \mid a(L)$

$\mathcal{G}$	$20, 2^{10}$	$16, 5^4$	$16, 5^6$	$16, 5^8$	$14, 7^5$	$14, 7^7$	$12, 11^6$
mass	.00117	.08047	1219.1	30325.2	284.1	13921.7	15096.9
h	546	848	34394	≥ 229467	8664	83006	67323
$avg(a)$	18.83	13.36	4.81	2.91	4.93	2.57	2.15
$a = 2$	–	–	174	≥ 23398	24	12827	16613
$a = 4$	–	–	1184	≥ 39442	242	17238	17659
$a = 8$	–	–	2700	≥ 41676	644	16349	13069
$3 \mid a$	537	839	19085	≥ 41800	5261	11797	6065
$5 \mid a$	295	529	2182	≥ 2198	631	353	421
$7 \mid a$	95	155	156	≥ 83	84	82	0

Table: Orders of automorphism groups of lattices in large genera

Conclusion

- For genera of small level and dimension $12 \leq n \leq 20$, small masses ($<< 1$) occur with class numbers of several hundreds, thus only large groups.
- For many genera with larger mass ($\sim \ldots 10^4$), the class number remains computable ($\sim \ldots 10^5$), the average group order goes down to less than 10.
- In large cases, the "typical" automorphism group is a 2-group of "small" order (e.g. ≤ 64).
- Trivial groups occur, but are not the majority; their proportion goes up from less than 1/100 to about 1/4.

Outlook: A structure theory and a mass formula for orthogonal representations of the cyclic group C_ℓ, ℓ an odd prime or $\ell = 4$ should give more precise estimates of h_1 and thus clarify the asymptotic behaviour of h_1/h.

Work in progress by Björn Hoffmann, Stefan Höppner, Timo Rosnau (PhD thesis project).

- E. Bannai: Positive definite unimodular lattices with trivial automorphism groups. Mem. Amer. Math. Soc. **85** (1990) no. 429, iv+70pp.
- J. Biermann: Gitter mit kleiner Automorphismengruppe in Geschlechtern von **Z**-Gittern mit positiv-definiter quadratischer Form. Dissertation, Göttingen 1981.

Lattices and their genera
Automorphism groups
Explicit enumeration of large genera
A general strategy for classification
Some genera of level 2, 5, 7, 11

- G. Nebe, B.B. Venkov: Non-existence of extremal lattices in certain genera of modular lattices. J. of Number Theory, **60**, No. 2 (1996), 310–317.
- W. Plesken, B. Souvignier: Computing isometries of lattices. J. Symbolic Comp. **24**, no. 3/4 (1997), 327–334.
- R. Scharlau, B. Hemkemeier: Classification of integral lattices with large class number. Math. of Comput. (1998).
- R. Scharlau, R. Schulze-Pillot: Extremal Lattices, In *Algorithmic Algebra and Number Theory*, edited by B.H. Matzat, G.-M. Greuel, G. Hiss, Springer Verlag 1999.

Rudolf Scharlau
Groups in Large Genera