Automorphism groups of lattices with roots

Improving on Plesken-Souvignier in certain cases

Olivier Taïbi

CNRS, UMPA/ENS Lyon

Atelier PARI/GP 2024 (ENS Lyon, January 8-12 2024)

Lattices

Definition

A lattice is a finite free $\mathbb{Z}$-module L together with a symmetric bilinear form $L \times L \to \mathbb{Z}, (v_1, v_2) \mapsto v_1 \cdot v_2$ which is positive-definite: for all $v \in L \smallsetminus \{0\}$ we have $v \cdot v > 0$.

Remark

The category $\mathcal{L}$ of lattices is equivalent to its full subcategory of objects for which $L = \mathbb{Z}^n$ for some integer n: the set of objects is the disjoint union over $n \geq 0$ of the set of symmetric positive definite $S \in M_n(\mathbb{Z})$ and

$$\mathrm{Hom}(S_1, S_2) = \{M \in M_{n_2,n_1}(\mathbb{Z}) \,|\, {}^t M S_2 M = S_1\}.$$

Lattice genera

Definition

Two lattices L_1, L_2 are in the same genus if for every prime p we have $\mathbb{Z}_p \otimes_{\mathbb{Z}} L_1 \simeq \mathbb{Z}_p \otimes_{\mathbb{Z}} L_2$ (as quadratic spaces over $\mathbb{Z}_p$).

This partitions the category $\mathcal{L}$ of lattices into full subcategories (groupoids) called genera.

Theorem

Each genus only has finitely many isomorphism classes.

So each genus is (abstractly) equivalent to a finite collection of finite groups.

Lattice genera and automorphic forms

Proposition

Let $\mathcal{X}$ be a genus, L a lattice in $\mathcal{X}$. Let G be the corresponding linear algebraic group: $G(R) \simeq \{M \in \mathrm{GL}_n(R) \,|\, {}^tMSM = S\}$. Then $\mathcal{X}$ is equivalent to the quotient of $G(\mathbb{A}_f)/G(\widehat{\mathbb{Z}})$ by the left action of $G(\mathbb{Q})$:

- *Natural bijection between $\mathcal{X}/\sim$ and $G(\mathbb{Q})\backslash G(\mathbb{A}_f)/G(\widehat{\mathbb{Z}})$.*
- *If $[L] \in \mathcal{X}/\sim$ corresponds to $[x] \in G(\mathbb{Q})\backslash G(\mathbb{A}_f)/G(\widehat{\mathbb{Z}})$ then $\mathrm{Aut}(L) \simeq G(\mathbb{Q}) \cap xG(\widehat{\mathbb{Z}})x^{-1}$.*

Concrete description of the space of automorphic forms for $G_{\mathbb{Q}}$, level $G(\widehat{\mathbb{Z}})$ and weight some algebraic representation V of $G(\mathbb{Q})$:

$$\bigoplus_{[L]\in\mathcal{X}/\sim} V^{\mathrm{Aut}(L)}.$$

Lattice genera: examples

Example

For $n \geq 1$, lattices in dimension $8n$ which are even (the diagonal of S is even) and unimodular ($\det S = 1$) form a single (non-empty) genus $\mathcal{X}^e_{8n,1}$. Denoting $c(8n) = |\mathcal{X}^e_{8n,1}/\sim|$:

$$c(8) = 1,\ c(16) = 2,\ c(24) = 24 \textit{(Niemeier)},\ c(32) > 10^9 \textit{(King)}.$$

Example (ramified at 2)

For $n \geq 1$, genus $\mathcal{X}^o_{n,1}$ of $S = I_n$ consists of all odd (=not even) unimodular lattices. 2020: $n = 26, 27$ (Chenevier), $n = 28$ (Allombert-Chenevier). $|\mathcal{X}^o_{28,1}/\sim| = 374,062$.

Lattice genera: main example for this talk

Example (ramified at 3)

Lattices in dimension 27 which are even of determinant 6 form a single genus $\mathcal{X}^e_{27,6}$.

Computed a month ago (joint work with Gaëtan Chenevier). There are $285,825$ (isomorphism classes of) lattices in this genus.

Computing a genus

To compute a genus $\mathcal{X}$ (even just as a list of objects), have to:

- Generate lattices in $\mathcal{X}$ (Kneser neighbours, or from lattices in some other genus).
- Decide which are isomorphic (`qfisom`, or better: good invariant discriminating non-isomorphic lattices).
- When are we done / does this invariant really discriminate non-isomorphic lattices?

Theorem (Smith-Minkowski-Siegel mass formula ∼ Tamagawa numbers for special orthogonal groups)

Let $\mathcal{X}$ be a genus of lattices. There is an explicit ("easily" computable) formula for its mass $\sum_{[L]\in\mathcal{X}/\sim}|\mathrm{Aut}(L)|^{-1}$.

This allows us to check if we are done, provided we can compute automorphism groups.

Given $S \in M_n(\mathbb{Z})$ symmetric positive definite, defining an inner product $(v_1, v_2) \mapsto v_1 \cdot v_2$ on $L = \mathbb{Z}^n$, want to compute the group

$$G = \mathrm{Aut}(L) \simeq \{M \in M_n(\mathbb{Z}) \,|\, {}^tMSM = S\}.$$

Plesken-Souvignier 1997, `qfauto` in GP.

Plesken-Souvignier: basic idea

Let $m = \text{maxdiag}(S) = \max\{e_i \cdot e_i \,|\, 1 \leq i \leq n\}$. Compute $A = \{v \in L \,|\, v \cdot v \leq m\}$ (Fincke-Pohst, `qfminim` in GP). Have an embedding

$$\begin{aligned} G &\longrightarrow A^n \\ g &\longmapsto (g(e_i))_{1 \leq i \leq n} \end{aligned}$$

Recursive (backtracking) algorithm to enumerate all $g \in G$:

- Compute list of candidates for $g(e_1)$: $\ell_1 := \{e_1' \in L \,|\, e_1' \cdot e_1' = e_1 \cdot e_1\} \subset A$.
- For each $e_1' \in \ell_1$, compute list of candidates for $g(e_2)$:

$$\ell_2(e_1') := \{e_2' \in L \,|\, e_2' \cdot e_2' = e_2 \cdot e_2 \text{ and } e_2' \cdot e_1' = e_2 \cdot e_1\} \subset A$$

- etc

Plesken-Souvignier: refinements

Refinements (crucial):

- Only compute generators for G, which can be very big (e.g. $\mathrm{Leech} \in \mathcal{X}^e_{24,1}$ has $8,315,553,613,086,720,000$ automorphisms). Letting $G_i = \mathrm{Stab}_G(e_1, \dots, e_{i-1})$, compute generators for G_n (trivial), G_{n-1} (slightly harder), $\dots$, up to $G_1 = G$. Knowing G_{i+1}, compute $G_i \cdot e_i$ and generators for G_i.
- Fingerprint: optimize $(|\ell_i(e'_1, \dots, e'_{i-1})|)_{1 \leq i \leq n}$
- Vector sums
- Bacher polynomials (for very symmetric lattices)

Back to example: $\mathcal{X}^e_{27,6}$

Recall: genus $\mathcal{X}^e_{27,6}$ has $285,825$ (isomorphism classes of) lattices. For almost all of them, there is a basis such that $\mathrm{maxdiag}(S) = 4$, and for these `qfauto` computes $\mathrm{Aut}(L)$ in about 3.5s.

Problem: 28 of them are not generated by vectors of length ≤ 4, they have about $13 \cdot 10^6$ vectors of length 6.
One of them is not generated by vectors of length ≤ 6, it has about $5 \cdot 10^8$ vectors of length 8.

The root system of a lattice

Proposition

Let L be a lattice. Then $R = \{v \in L \mid v \cdot v = 2\}$ is a simply-laced root system (in the span of R in the $\mathbb{Q}$-vector space $\mathbb{Q}L$). In particular it decomposes uniquely as an orthogonal disjoint union of root systems isomorphic to one of A_n for $n \geq 1$, D_n for $n \geq 4$ and E_n for $n \in \{6, 7, 8\}$.

Main point: for $\alpha \in R$, the symmetry

$$\begin{aligned} s_\alpha : \mathbb{Q}L &\longrightarrow \mathbb{Q}L \\ v &\longmapsto v - (\alpha \cdot v)\alpha \end{aligned}$$

stabilizes R, because it stabilizes L.
The root system R generates a sublattice $Q(R)$ of L. The Weyl group $W(R) = \langle s_\alpha, \alpha \in R \rangle$ embeds in $\mathrm{Aut}(L)$, and is "well-known".

Based root systems in lattices

Proposition

Let L be a lattice, R its root system. Fix an order R^+ of the root system R (in particular $R = R^+ \sqcup -R^+$). We have an isomorphism $\mathrm{Aut}(L) \simeq W(R) \rtimes \mathrm{Aut}(L, R^+)$. The morphism $\mathrm{Aut}(L, R^+) \to \mathrm{Aut}(R, R^+) \times \mathrm{Aut}(R^{\perp, L})$ is injective.

Let $\Delta \subset R^+$ be the set of simple roots (in particular Δ is a basis of $Q(R)$). The group $\mathrm{Aut}(R, R^+)$ is well-known (as a subgroup of $\mathfrak{S}_\Delta$): if $R \simeq \bigsqcup m_i R_i$ with R_i irreducible then

$$\mathrm{Aut}(R, R^+) \simeq \prod_i \mathrm{Aut}(R_i)^{m_i} \rtimes \mathfrak{S}_{m_i}.$$

Example: worst lattice in $\mathcal{X}^e_{27,6}$

The unique lattice L in $\mathcal{X}^e_{27,6}$ which is not generated by its vectors of length ≤ 6 has root system $R \simeq D_{26}$ and

- $Q(R) \simeq \{(x_1, \ldots, x_{26}) \in \mathbb{Z}^{26} \mid \sum_i x_i \text{ even}\}$ (with standard inner product), $W(R) \simeq \{\pm 1\}^{25} \rtimes \mathfrak{S}_{26}$ and $\mathrm{Aut}(R, R^+) \simeq \mathfrak{S}_2$,
- $R^{\perp, L}$ has Gram matrix (6),
- $Q(R) \oplus R^{\perp, L}$ has index 2 in L.

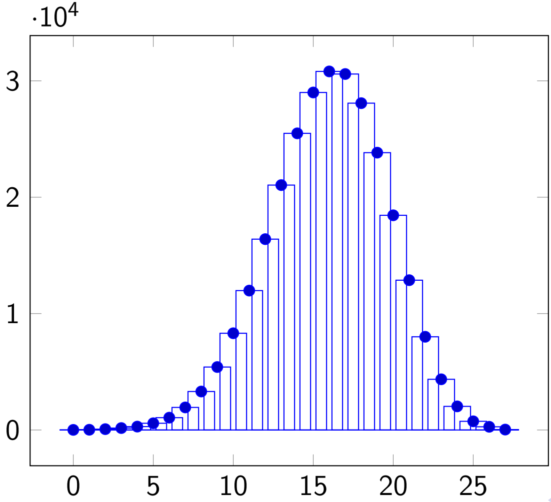
So $\mathrm{Aut}(L, R^+)$ is the stabilizer of L in $\mathrm{Aut}(R, R^+) \times \{\pm 1\}$, and may be computed with pen and paper ...

Root systems of the 27 lattices in $\mathcal{X}^e_{27,6}$ which are generated by vectors of length ≤ 6 but not 4:

$A_{20}E_6$	$A_9D_{11}D_6$	$A_{11}D_9E_7$	$A_5^3D_{12}$	$A_{15}D_{11}$	$A_3A_9D_{14}$
$A_1^2D_{16}D_8$	$D_{12}D_{14}$	$A_2D_{18}E_7$	$D_{20}D_6$	$A_5D_{15}E_6$	$A_1A_7D_{13}D_5$
A_9D_{17}	$A_{11}D_9E_6$	$A_7^2D_5D_7$	$D_{14}D_6^2$	$D_{12}E_7^2$	$D_{18}E_8$
$A_9^2D_8$	$D_{10}D_8^2$	$D_{12}E_7^2$	$D_6^3D_8$	$A_5^4D_6$	$D_4^5D_6$
$A_3^7D_5$	$A_1^{22}D_4$	A_3			

Rank is 26 or 27, except for A_3.

Restrict to lattices L in $\mathcal{X}^e_{27,6}$ which do not factor as $Q(A_1) \oplus L'$.
Number of isomorphism classes of lattices by rank of the root system:



An invariant

Goal: modify Plesken-Souvignier to compute $\mathrm{Aut}(L, R^+)$.

Definition

For $v \in L$, $\mathrm{inv}(v, R^+) := \mathrm{Aut}(R, R^+) \cdot (\alpha \cdot v)_{\alpha \in \Delta}$.

The group $\mathrm{Aut}(L, R^+)$ preserves these invariants, in particular $g \in \mathrm{Aut}(L, R^+)$ maps e_i to an element of

$$\{v \in L \,|\, v \cdot v = e_i \cdot e_i \text{ and } \mathrm{inv}(v, R^+) = \mathrm{inv}(e_i, R^+)\}.$$

This invariant is computable: can choose representatives for each orbit and map an element of $\mathbb{Z}^\Delta$ to the corresponding representative (sorting for certain lexicographic orders).

Bonus

- Root system gives a number of (linearly independent) vectors invariant under $\mathrm{Aut}(L, R^+)$, e.g. a factor A_r^m gives $\lfloor (r+1)/2 \rfloor$ invariant vectors and a factor D_r^m gives $r-1$ invariant vectors. When the set I of such invariant vectors is large it is cheaper to enumerate each

$$\{v \in L \,|\, v \cdot v = e_i \cdot e_i \text{ and } \forall w \in I,\ v \cdot w = e_i \cdot w\}$$

  (reduces to translated Fincke-Pohst in dimension $n - |I|$) than to filter the enumeration of all short vectors according to $\mathrm{inv}(-, R^+)$.
- The sum of all $v \in L$ having given norm (≥ 4) and invariant with respect to R^+ is also invariant under $\mathrm{Aut}(L, R^+)$, this often yields new (linearly independent) invariant vectors.