# THE CLASSIC ENUMERATION OF GENERA OF EVEN DEFINITE LATTICES

MATHIEU DUTOUR SIKIRIĆ

Abstract. We revisit the enumeration of a genus of even positive definite lattices by Kneser neighbours, certified by the mass. We work at primes dividing the determinant, where the projective spaces are smallest, schedule the exploration of the neighbour graph by a random walk and by orders based on a Hecke bookkeeping, and compute canonical forms through the Weyl chamber of the root system. Genera of rank up to 19 with up to 40 617 classes are enumerated in minutes.

hexagon:2611.00337v1

## 1. Introduction

A genus of positive definite lattices is a finite set of isometry classes, and listing its classes is a basic task of the computational theory of quadratic forms: the classes of a genus are the input of the computation of spaces of modular forms (theta series, algebraic modular forms), of classifications of lattices with prescribed properties, and of the many tables built on them. The standard method is Kneser's [11]: starting from one lattice of the genus, build its $p$-neighbours, which are again in the genus, recognise the classes they belong to, and continue from the new classes. Schulze-Pillot [20] and Scharlau–Hemkemeier [19] made it a practical algorithm, and Voight [21] gives a modern account. The process stops when the classes found account for the whole mass of the genus, $\sum 1/|\mathrm{Aut}(L)|$, which is known in advance by the Smith–Minkowski–Siegel mass formula; this is what certifies the result.

The method is implemented in Magma [13], and among open source systems in Hecke.jl [10] and SageMath [18]; Section 8 compares the program described here with the latter two.

The cost of the method has three parts: the orbits of the automorphism group of a class on the lines of $L/pL$, one canonical form (or one series of isometry tests) per orbit to recognise the neighbour, and the automorphism group of each new class. Two features dominate. First, the number of lines is $(p^n-1)/(p-1)$, so the prime $p$ must be as small as possible; in rank 19 it is $5.2 \cdot 10^5$ at $p=2$ and $1.9 \cdot 10^{15}$ at $p=7$. Second, almost all of the work is wasted: in a systematic expansion more than 90% of the neighbours built are classes already known, and about half of the classes are expanded completely before the mass closes. The classic setting of the theory assumes that $p$ does not divide the determinant, which for the genera of even determinant excludes $p=2$ and makes most of them out of reach.

This note describes what was done to make the enumeration practical on genera of rank 14 to 19 with tens of thousands of classes. There are four parts.

(1) *Primes dividing the determinant* (Section 2). Kneser's construction, restricted to the vectors $v$ with $b(v,L) \not\subseteq p\mathbb{Z}$, stays in the genus at every prime. We count the lines that give neighbours, show that the neighbour relation is symmetric, and explain why the more general notion of neighbour can leave the genus when $p$ divides the determinant.

(2) *Scheduling the exploration* (Sections 3 and 4). The neighbour graph is not known in advance, and the task is to find a set of edges reaching every vertex at the least cost. We combine a random walk, which harvests most classes cheaply, with full expansions chosen by a Hecke bookkeeping that tells, for every class, how many of its neighbours are still unexplained.

*Date*: November 2026.

(3) *Canonical forms and automorphism groups* (Section 5). The lattices met have large root systems. Fixing a Weyl chamber removes the Weyl group from the problem, and the canonical form, the automorphism group and the isometry test are then computed on a small configuration.
(4) *The orbits on the projective space* (Section 6), which at $p = 2$ can be computed on bitmasks.

The test data, the measurements and the final runtimes are gathered in Section 7, which also reports the ideas that did not work. All the algorithms described here are implemented in the program `GENUS_Enumerate` of `polyhedral_common` [16], together with the canonical forms and automorphism groups of Section 5.

## 2. Genera and neighbours

2.1. **Genera.** A lattice is a free $\mathbb{Z}$-module $L$ of rank $n$ with a symmetric bilinear form $b : L \times L \to \mathbb{Z}$; it is positive definite if $b(x, x) > 0$ for $x \neq 0$, and even if $b(x, x) \in 2\mathbb{Z}$ for all $x$. With a basis $e_1, \dots, e_n$ it is given by its Gram matrix $A = (b(e_i, e_j))$, up to $A \mapsto PAP^T$ with $P \in \mathrm{GL}_n(\mathbb{Z})$, and its determinant $d = \det A$ does not depend on the basis. Two lattices are isometric, or in the same class, if there is a bijective linear map between them preserving $b$.

**Definition 1.** Two lattices $L$ and $L'$ are in the same *genus* if $L \otimes \mathbb{R} \cong L' \otimes \mathbb{R}$ and $L \otimes \mathbb{Z}_q \cong L' \otimes \mathbb{Z}_q$ for every prime $q$, the isometries being of the extended forms over $\mathbb{R}$ and over the $q$-adic integers $\mathbb{Z}_q$.

Isometric lattices are in the same genus, and a genus is a finite union of classes [15]. The rank, the signature, the parity and the determinant are invariants of the genus, but they do not determine it: the genus is a local invariant at every prime, and the determinant only records the product of the local determinants.

**Example 1.** $A_3 \oplus A_3$ and $A_1 \oplus A_1 \oplus D_4$ are both even, positive definite, of rank 6 and determinant 16, but their discriminant groups $L^\#/L$ are $(\mathbb{Z}/4)^2$ and $(\mathbb{Z}/2)^4$, so they are not in the same genus: $L \otimes \mathbb{Z}_2$ is not the same.

The *level* of an even lattice is the smallest positive integer $N$ such that $NA^{-1}$ is the Gram matrix of an even lattice; it is also an invariant of the genus, and DefLatDB records it in its labels. For even lattices, Nikulin [12] shows that the genus is determined by the rank, the signature and the discriminant form, the finite group $L^\#/L$ with the quadratic form $x \mapsto b(x, x) \bmod 2\mathbb{Z}$. Concretely, a genus is described by the Jordan decompositions of $L \otimes \mathbb{Z}_p$ at the primes $p \mid 2d$,

$$L \otimes \mathbb{Z}_p = U_0 \perp p\,U_1 \perp p^2\,U_2 \perp \cdots,$$

with $U_k$ unimodular, the component of scale $p^k$. Conway and Sloane [5] encode it in a symbol, which we use for the genera of the test data. For example $II_{19,0}\,2_7^1\,9^{-1}\,5^1$, or in the notation of DefLatDB $\{1\}_{II}^{-18}\{2\}_7^1\{9\}^{-1}\{5\}^1$, is the genus of the even positive definite lattices of rank 19 and determinant 90 whose 2-adic decomposition is an even unimodular component of rank 18 and sign $-$ plus a 2-modular component of rank 1 and oddity 7, with one component of scale 9 at 3 and one of scale 5 at 5.

2.2. **Deciding the genus.** The definition quantifies over all primes, but only finitely many matter, and each local condition is a finite computation. For a lattice $L$ with Gram matrix $A$ of determinant $d$:

(1) *Primes not dividing* $2d$. For $q \nmid 2d$, $L \otimes \mathbb{Z}_q$ is unimodular, and a unimodular $\mathbb{Z}_q$-lattice is determined by its rank and the square class of its determinant. So two lattices of the same rank and determinant are isometric at every such $q$, and the real condition is the signature.

(2) *Jordan decomposition at $p \mid 2d$.* Let $k = v_p(d) + 1$, and $k = v_2(d) + 3$ at $p = 2$. Work in $\mathbb{Z}/p^k\mathbb{Z}$, which determines $L \otimes \mathbb{Z}_p$. Repeatedly take an entry of $A$ of minimal $p$-adic valuation. If it can be taken on the diagonal, it splits off a block $(a)$: clear its row and column by symmetric elimination, which only divides by a unit. For $p$ odd this is always possible, since if $v(a_{ij}) < \min(v(a_{ii}), v(a_{jj}))$, replacing $e_i$ by $e_i + e_j$ gives a diagonal entry $a_{ii} + 2a_{ij} + a_{jj}$ of valuation $v(a_{ij})$. At $p = 2$ the minimum may be attained only off the diagonal; then the $2 \times 2$ block $\left(\begin{smallmatrix} a_{ii} & a_{ij} \\ a_{ij} & a_{jj} \end{smallmatrix}\right)$, whose determinant is $a_{ij}^2$ times a unit, splits off. The result is a block diagonal form whose blocks, grouped by their scale $p^j$, are the Jordan components $p^j U_j$.

(3) *Odd $p$.* Record for every scale $p^j$ the rank $n_j$ of $U_j$ and the Legendre symbol $\varepsilon_j = \left(\frac{\det U_j}{p}\right)$. Two lattices are isometric over $\mathbb{Z}_p$ if and only if these data agree [15, Theorem 92:2], [5, Ch. 15, §7].

(4) $p = 2$. Record for every scale $2^j$ the rank $n_j$, the sign $\varepsilon_j = +$ if $\det U_j \equiv \pm 1 \bmod 8$ and $-$ otherwise, the type (II if $U_j$ is even, I if it has an odd diagonal entry), and, for type I, the oddity, the trace of a diagonalisation of $U_j$ modulo 8. Unlike the odd case, these data depend on the decomposition: the oddities are only defined up to their sums over compartments, maximal runs of consecutive type I components, and signs can walk between components linked by a train. Conway and Sloane put the symbol in a canonical form by these two rules, and two lattices are isometric over $\mathbb{Z}_2$ if and only if their canonical 2-adic symbols are equal [5, Ch. 15, §7.3–7.6].

Two lattices are in the same genus exactly when they have the same rank, signature and determinant and the same local symbols at the primes dividing $2d$. For even lattices the discriminant form gives an equivalent test [12]. The cost is a few eliminations on $n \times n$ matrices modulo small prime powers, negligible next to an enumeration. In the program the genus of a neighbour is never tested (Section 2.5), but this is the test one would use, and Proposition 2 below reads the number of neighbour lines off the same decomposition.

The *mass* of the genus $G$ is

$$m(G) = \sum_{[M] \in G} \frac{1}{|\mathrm{Aut}(M)|},$$

where $\mathrm{Aut}(M) = \mathrm{O}(M)$ is the finite group of isometries of $M$. It is given by the Smith–Minkowski–Siegel mass formula as a product of local factors, without knowing the classes [6]. An enumeration has found all classes exactly when the masses of the classes found add up to $m(G)$.

2.3. **Kneser neighbours.** Let $L$ be even of rank $n$, with Gram matrix $A$, and let $p$ be a prime. The construction is Kneser's [11]; we follow the presentation of Scharlau–Hemkemeier [19, §2] and Voight [21, §3], who assume $p \nmid d$, and add the condition (a) below, which is automatic in that case and essential otherwise. A point of $\mathbb{P}^{n-1}(\mathbb{F}_p)$, the line of a vector $v \in L$ modulo $pL$, is *admissible* if

$$\text{(a) } b(v, L) \not\subseteq p\mathbb{Z}, \qquad \text{(b) } b(v, v) \in p\mathbb{Z} \text{ for } p \text{ odd}, \ b(v, v) \in 4\mathbb{Z} \text{ for } p = 2.$$

Both conditions depend only on the line: (a) is $Av \not\equiv 0 \pmod p$, and (b) says that $v$ is isotropic modulo $p$ (that $b(v, v)/2$ is even, at $p = 2$). This is what the program tests on each point.

**Lemma 1.** *An admissible line has a representative $v$ with $b(v, v) \in p^2\mathbb{Z}$ ($b(v, v) \in 8\mathbb{Z}$ at $p = 2$), and for any such representative the lattice*

$$N = L_v + \mathbb{Z}\frac{v}{p}, \qquad L_v = \{x \in L : b(x, v) \in p\mathbb{Z}\},$$

*is even, integral, and depends only on the line. Different lines give different lattices $N$.*

*Proof.* By (a) there is $e$ in the basis with $b(v, e) \not\equiv 0 \bmod p$. For $v' = v + pae$, $b(v', v') = b(v, v) + 2pa\, b(v, e) + p^2a^2 b(e, e)$. For $p$ odd, $b(v, v) = pc$ and $c + 2a\, b(v, e) \equiv 0 \bmod p$ has a solution $a$. For

$p = 2$, $b(v, v) = 4c$, $b(e, e)$ is even, and $b(v', v') \equiv 4(c + a\, b(v, e)) \bmod 8$, which vanishes for $a = c$. Condition (a) gives $[L : L_v] = p$, and the corrected norm makes $N$ integral and even: $b(v/p, x) \in \mathbb{Z}$ for $x \in L_v$, and $b(v/p, v/p) \in \mathbb{Z}$, in $2\mathbb{Z}$ at $p = 2$. Two corrected representatives of the same line are $v$ and $v' = \mu v + pw$ with $\mu$ prime to $p$ and $w \in L$. Multiplying $v$ by $\mu$ does not change $N$: $L_{\mu v} = L_v$, and $L_v + \mathbb{Z}\,\mu v/p$ contains $v \in L_v$ and $\mu v/p$, hence $v/p$, since $\mu$ and $p$ are coprime. So we may take $\mu = 1$; then the two norm conditions force $b(v, w) \equiv 0 \bmod p$, that is $w \in L_v$, and $L_v + \mathbb{Z}\, v'/p = L_v + \mathbb{Z}\, v/p$. Finally $N$ determines $L_v = L \cap N$ and the line of $v$, since $v/p$ generates $N/L_v$. □

We call $N$ the neighbour of the line. The program builds it exactly as in the proof: it tests (a) and (b) on the line, then corrects the representative.

In Kneser's general sense a $p$-neighbour of $L$ is an integral lattice $\Pi$ on $L \otimes \mathbb{Q}$ with $[L : L \cap \Pi] = [\Pi : L \cap \Pi] = p$. Such a $\Pi$ has the determinant of $L$.

2.4. **Why primes dividing the determinant matter.** The literature on neighbours assumes $p \nmid d$ ([11], [19, §2], [21, Definition 3.10]). Then condition (a) holds for every primitive $v$, the two notions of neighbour agree, the neighbours are in the genus because a unimodular $\mathbb{Z}_p$-lattice is determined by its rank, its determinant and its type, and for $n \geq 3$ the $p$-neighbour graph is connected on each spinor genus, by strong approximation. But an even lattice of odd rank has even determinant, and all the genera considered here have even $d$, so $p = 2$ always divides $d$. The smallest prime not dividing $d$ is 7 for $d = 30$, with $1.9 \cdot 10^{15}$ lines in rank 19, and 11 for $d = 210$, with $4.2 \cdot 10^{14}$ lines in rank 15. Everything that makes these genera tractable therefore happens at a prime dividing the determinant, and the three properties have to be reconsidered there: whether the neighbours stay in the genus, which lines give neighbours, and whether the graph is connected.

2.5. **Do the neighbours leave the genus?** It is often said that $p$-neighbours for $p \mid d$ can leave the genus. This is true for the general notion and false for the construction above, and the difference is condition (a).

**Proposition 1.** *Let $p$ be any prime and $N$ the neighbour of an admissible line, built from a representative $v$ as in Lemma 1. Then $N$ is in the genus of $L$. More precisely, $v$ and a vector $x \in L \otimes \mathbb{Z}_p$ with $b(x, v) = 1$ span a hyperbolic plane $H$ with $L \otimes \mathbb{Z}_p = H \perp M$, and $N \otimes \mathbb{Z}_p = H' \perp M$ with $H' = \mathbb{Z}_p v/p + \mathbb{Z}_p\, px \cong H$.*

*Proof.* Let $v$ be the corrected representative, so that $b(v, v) \in p^2\mathbb{Z}$ ($8\mathbb{Z}$ at $p = 2$). Evenness and the determinant follow from (a), the corrected norm and $[L : L_v] = [N : L_v] = p$. For a prime $q \neq p$ the indices are prime to $q$, so $N \otimes \mathbb{Z}_q = L \otimes \mathbb{Z}_q$; and $N \otimes \mathbb{R} = L \otimes \mathbb{R}$. At $p$, write $L_p = L \otimes \mathbb{Z}_p$; condition (a) gives $x \in L_p$ with $b(x, v) = 1$. The sublattice $H = \mathbb{Z}_p v + \mathbb{Z}_p x$ has Gram matrix

$$\begin{pmatrix} a & 1 \\ 1 & c \end{pmatrix}, \qquad a = b(v, v) \in p^2\mathbb{Z}_p,\ c = b(x, x),$$

of determinant $ac - 1 \in \mathbb{Z}_p^\times$. A unimodular sublattice splits off: $L_p = H \perp M$ with $M = H^\perp$. Since $M \perp v$, $M \subseteq (L_v)_p$, and for $h = \alpha v + \beta x \in H$ one has $b(h, v) = \alpha a + \beta \equiv \beta \bmod p$. Hence $(L_v)_p = (\mathbb{Z}_p v + \mathbb{Z}_p\, px) \perp M$ and

$$N_p = H' \perp M, \qquad H' = \mathbb{Z}_p \frac{v}{p} + \mathbb{Z}_p\, px, \qquad \operatorname{Gram} \begin{pmatrix} a/p^2 & 1 \\ 1 & p^2 c \end{pmatrix}.$$

$H'$ is integral (and even for $p = 2$, since $a \in 8\mathbb{Z}_2$) and unimodular of the same determinant $ac - 1$ as $H$. For $p$ odd a unimodular $\mathbb{Z}_p$-lattice is determined by its rank and the square class of its determinant, so $H' \cong H$. For $p = 2$, $H$ and $H'$ are even unimodular binary $\mathbb{Z}_2$-lattices, isometric to the hyperbolic plane or to the anisotropic plane, which are told apart by the square class of the determinant ($-1$ against 3); here both determinants are $\equiv -1 \bmod 16$, so $H \cong H'$ is the hyperbolic plane. In both cases $N_p \cong H \perp M = L_p$. □

**Remark 1.** *Schulze-Pillot* [20, property (v)] *proves the same for $p \parallel d$, through Eichler's maximal lattices; there condition (a) holds automatically for primitive $v$ with $p^2 \mid b(v,v)$. When $p^2 \mid d$ this fails: a primitive $v$ can satisfy $b(v,L) \subseteq p\mathbb{Z}$, and $\mathbb{Z}v/p + L$ then has determinant $d/p^2$. The program rejects such $v$: condition (a) is tested on every line.*

So the neighbour changes only the unimodular component of $L \otimes \mathbb{Z}_p$; the components of scale $p, p^2, \dots$ are kept, and the other primes are not affected. Conversely, a neighbour $\Pi$ in the general sense either is the neighbour of an admissible line, or $\Pi = (L \cap \Pi) + \mathbb{Z}v/p$ with $v \in L \cap pL^{\#} \setminus pL$, a vector that fails condition (a). Such vectors exist only when $p \mid d$, since otherwise $pL^{\#} = pL$. For them $L_v = L$, the intersection $L \cap \Pi$ is some sublattice of index $p$ of $L$, and the argument above, which needs the unimodular plane $H$, is not available: $\Pi$ has the determinant of $L$ but its components of scale $p^k$ can be redistributed, and it can lie in another genus of the same determinant. The program never builds these exceptional neighbours, so it never needs a genus test. The enumeration is in any case self-checking: a lattice from another genus would add a term $1/|\mathrm{Aut}|$ foreign to the genus, and the masses would not close.

2.6. **Which lines give neighbours.** Write $L \otimes \mathbb{Z}_p = U \perp M'$ with $U$ unimodular of rank $r$ and $M'$ of scale divisible by $p$; at $p = 2$ write further $M' = W \perp M''$ with $W$ the 2-modular component and $M''$ of scale divisible by 4. Since $L$ is even, $U$ is even at $p = 2$, and $q(x) = b(x,x)/2$ induces a nondegenerate quadratic form $\bar{q}$ on $U/2U$. On $W/2W$, $q$ modulo 2 is a linear form $\lambda$, nonzero exactly when $W$ is odd.

**Proposition 2.** *The number $n_p(L)$ of admissible points of $\mathbb{P}^{n-1}(\mathbb{F}_p)$ depends only on $L \otimes \mathbb{Z}_p$, so it is a constant $n_p(G)$ of the genus.*

1. *For $p$ odd, $n_p(G) = Z_p(U)\, p^{n-r}/(p-1)$, where $Z_p(U)$ is the number of nonzero isotropic vectors of $U/pU$.*
2. *For $p = 2$, $n_2(G) = Z_2(U)\, 2^{n-r}$ if $W$ is even, with $Z_2(U)$ the number of nonzero zeros of $\bar{q}$, and $n_2(G) = (2^r - 1)\, 2^{n-r-1}$ if $W$ is odd.*

*In particular $n_p(G) = 0$ exactly when $r \le 1$, or $r = 2$ and $U$ is anisotropic, the latter only if $W$ is even when $p = 2$.*

*Proof.* Write $v = u + m$ with $u \in U$, $m \in M'$. Condition (a) says $u \not\equiv 0 \bmod pU$, since $b(M', L) \subseteq p\mathbb{Z}_p$ and $U$ is unimodular. Condition (b) is $b(v,v) \equiv 0 \bmod p$, respectively $q(v) \equiv 0 \bmod 2$. For $p$ odd, $b(v,v) \equiv b(u,u) \bmod p$, which gives (1). For $p = 2$, $q(v) \equiv \bar{q}(u) + \lambda(w) \bmod 2$, where $w$ is the component of $v$ in $W$, since the cross terms vanish and $q$ is even on $M''$. If $\lambda = 0$ this is $\bar{q}(u) = 0$; if $\lambda \neq 0$, for each $u \neq 0$ exactly half of the choices of $w$ work. The count depends only on the Jordan decomposition of $L \otimes \mathbb{Z}_p$, hence only on the genus. □

For the genus $\{1\}_{II}^{-18}\{2\}_7^1\{9\}^{-1}\{5\}^1$ above, $r = 18$ and $W$ is odd of rank 1, so $n_2(G) = 2^{18} - 1 = 262\,143$ of the $2^{19} - 1$ points; this is the number the program finds for each of its 28 528 classes. With $W$ even, $\bar{q}$ of minus type would give $Z_2(U) = 2^{17} - 2^8 - 1$ instead.

2.7. **Symmetry of the relation.**

**Lemma 2.** *For every prime $p$, if $N$ is the neighbour of an admissible line of $L$, then $L$ is the neighbour of an admissible line of $N$.*

*Proof.* Let $v$ be the corrected representative. Take $x \in L$ with $b(x,v) \equiv 1 \bmod p$, which exists by (a), and $w = px \in L_v \subseteq N$. Then $b(w, v/p) = b(x,v)$ is prime to $p$, so $b(w,N) \not\subseteq p\mathbb{Z}$, and $b(w,w) = p^2 b(x,x) \in p^2\mathbb{Z}$, in $8\mathbb{Z}$ for $p = 2$ since $b(x,x)$ is even. So the line of $w$ is admissible for $N$, $w$ is already a corrected representative, and $N_w = L_v$ (both have index $p$ in $N$ and $L_v \subseteq N_w$), and $N_w + \mathbb{Z}w/p = L_v + \mathbb{Z}x = L$. □

2.8. **Connectivity.** The *neighbour graph* at $p$ has the classes of $G$ as vertices and an edge from $L$ to $M$ for every point of $L$ whose neighbour is isometric to $M$; by Lemma 2 its edges can be paired. For $p \mid d$ no connectivity theorem is known, and the graph can be empty: by Proposition 2, when $n_p(G) = 0$ no class has a neighbour at $p$ at all. On the test data the graph at $p = 2$ was connected whenever it was not empty (Section 7.2), but this reflects the genera of the database rather than a general fact. When the graph at a prime has neighbours but is not connected, its components are unions of spinor genera, of equal mass but not of equal size (Section 7.4). The enumeration does not rely on connectivity: when the mass does not close at one prime, the next prime is used.

2.9. **Recognition and expansion.** Every neighbour is brought to a canonical form, and a dictionary of the canonical forms of the classes found decides in one lookup whether it is new. For a new class the order of its automorphism group is computed and $1/|\mathrm{Aut}|$ is added to the running mass. *Expanding* a class $L$ at $p$ means computing the orbits of $\mathrm{Aut}(L)$ on $\mathbb{P}^{n-1}(\mathbb{F}_p)$, keeping one admissible representative of each orbit, and building and recognising its neighbour. Two points of one orbit give isometric neighbours, so the orbits only save work, and their sizes count the edges.

## 3. The Hecke bookkeeping

3.1. **The identity.** For classes $L$ and $M$ of $G$, let $T(L, M)$ be the number of points of $\mathbb{P}^{n-1}(\mathbb{F}_p)$ for $L$ whose neighbour is isometric to $M$, the number of edges from $L$ to $M$. The expansion of $L$ gives the row $T(L, \cdot)$ at no extra cost, from the sizes of the orbits.

**Proposition 3.** *For every prime $p$ and all classes $L$, $M$ of the genus,*

$$\frac{T(L,M)}{|\mathrm{Aut}(L)|} = \frac{T(M,L)}{|\mathrm{Aut}(M)|}.$$

*Proof.* Different points give different neighbours, so $T(L, M)$ is the number of neighbours of $L$ isometric to $M$. Let $\Omega$ be the set of pairs $(X, Y)$ of lattices on $V = L \otimes \mathbb{Q}$ with $X \cong L$, $Y \cong M$ and $Y$ a neighbour of $X$, and let $\mathrm{O}(V)$ act on it. Fixing the first lattice to be $L$, the orbits are those of $\mathrm{Aut}(L)$ on the neighbours of $L$ isometric to $M$, and $\sum_{\text{orbits}} 1/|\text{stabiliser}| = T(L, M)/|\mathrm{Aut}(L)|$. By Lemma 2, $Y$ is a neighbour of $X$ if and only if $X$ is one of $Y$, so fixing the second lattice to be $M$ gives $T(M, L)/|\mathrm{Aut}(M)|$ for the same sum. □

For $p \nmid d$ this is the classical self-adjointness of the Hecke operator for the inner product weighted by $1/|\mathrm{Aut}|$; the point is that it holds at $p \mid d$ too.

3.2. **The deficit.** Let $E$ be the set of classes already expanded at $p$. By Proposition 3, the edges from any class $L$ to the expanded classes are known without expanding $L$, and

$$\delta(L) = n_p(G) - |\mathrm{Aut}(L)| \sum_{M \in E} \frac{T(M,L)}{|\mathrm{Aut}(M)|}$$

counts the points of $L$ whose neighbours are not yet accounted for. If $\delta(L) = 0$, all neighbours of $L$ are expanded classes, hence known, and the expansion of $L$ can be skipped. If the mass has not closed and the graph at $p$ is connected, some missing class is a neighbour of a known class of positive deficit. The skip alone turns out to save little; the use of the deficit is to choose the next class to expand.

## 4. Scheduling the exploration

4.1. **The problem.** The neighbour graph is not known in advance: its vertices are found as the enumeration proceeds, and an edge is known only once it has been probed, at the cost of one neighbour and one canonical form. The goal is to find a set of edges that reaches every vertex, a spanning set of the graph, while probing as few edges as possible, and to know when to stop, which the mass tells. Two kinds of probe are available:

- a *full expansion* of a class probes all its edges, one per orbit of its automorphism group; it is exhaustive, but most of its edges lead to known classes;
- a *random draw* probes one random edge of a class; it needs no orbit computation, and early in the enumeration it very likely finds a new class.

A schedule decides which probes to make, and in which order. Its quality is measured by the number of canonical forms computed until the mass closes.

4.2. **Three schedules.**

**out-prime:** expand every class at one prime, the smallest prime not dividing $d$. This is Kneser's setting, with its connectivity theorem, but the projective spaces are huge.
**iterate:** work with an increasing list of primes $2, 3, 5, \ldots$, described below.
**random walk:** the random walk below, followed by the expansions of the iterate schedule.

The iterate schedule is not a sequence of independent passes, one per prime: the primes stay in play together, and the smaller ones always have priority.

**Algorithm 1** (Iterate)**.** Keep the list $p_1 = 2 < p_2 < \cdots < p_k$ of the primes brought in so far, and for each $p_i$ the set of the classes already expanded at $p_i$. Repeat, until the mass closes:

(1) find the smallest $i$ such that some known class is not yet expanded at $p_i$;
(2) if there is one, choose such a class by the order of the expansions (Section 4.4), with the deficits computed at $p_i$, and expand it at $p_i$, recording its new classes;
(3) if there is none, every known class is expanded at every prime in play: bring in the next prime $p_{k+1}$.

Three consequences matter in practice.

- *Back-expansion.* A class found at 3 is unexpanded at 2, so it is expanded at 2 before the expansions at 3 resume. The cheap prime keeps being exploited after a larger one has been brought in, and every class is eventually expanded at every prime in play: the classes found are the union of the components, for the graphs at $p_1, \ldots, p_k$ together, of the classes met.
- *When* 2 *gives nothing.* If $n_2(G) = 0$, the expansions at 2 build no neighbour. They are cheap: the orbits are computed, and since the deficit is 0 from the start, the Hecke bookkeeping skips the loop over the orbits right after. The schedule then reduces to working at 3, then 5, and the genera of Section 7.3 are enumerated this way.
- *Termination.* The run stops when the mass closes, that is when the whole genus has been enumerated. A new prime is brought in only when every known class has been expanded at every prime in play and the mass is still open, and $p_{k+1}$ is the next prime, whether or not it divides $d$. For $n \geq 3$ the primes not dividing $d$ have neighbours, and by Kneser's theorem each of them connects every spinor genus to the spinor genus given by the class of $p$ in the finite group of spinor genera. These classes run over the whole group as $p$ varies, so the primes in play eventually reach every spinor genus and the mass closes. The run also stops, as an error, if the masses found exceed the mass of the genus, which genuine neighbours cannot do.

The random-walk schedule uses the same list of primes and the same priority for its full expansions; only the walk in front of it is new.

4.3. **The random walk.**

**Algorithm 2** (Random walk)**.** Keep a list of pending classes, those not yet walked from, treated by decreasing $|\mathrm{Aut}|$. For a pending class $L$:

(1) let $b$ be the smallest integer with $|\mathrm{Aut}(L)| < 2^b$, and set the hit bound to $\max(1, \lceil c_h b \rceil)$;
(2) draw random points of $\mathbb{P}^{n-1}(\mathbb{F}_p)$ uniformly (at $p = 2$, a random nonzero vector of $\mathbb{F}_2^n$); a point that is not admissible counts as a failed draw, and at most $c_f b$ failed draws are allowed;

(3) recognise the neighbour; a new class is added to the pending list, a known class counts as a hit;
(4) stop when the hits reach the bound.

When no class is pending, run the full expansions. Every class they find is walked from at once, before the expansions resume.

A walk never stops for finding too many new classes: only the hits and the failed draws are bounded. The bound grows with $\log|\mathrm{Aut}(L)|$ since a class with a large group has few orbits, and its random neighbours concentrate on few classes. A small factor is best ($c_h = 0.25$, a single hit for $|\mathrm{Aut}| \leq 2^4$; Section 7.5): the walk is a cheap harvest of the bulk of the classes, and stops as soon as it starts meeting known ones. A walk that closes the mass on its own is possible with a large factor, but costs more than the systematic expansion. The full expansions remain necessary for the tail: the last classes, which are reached through few edges.

4.4. **The order of the expansions.** Once the walk is exhausted, or from the start in the iterate schedule, the classes are expanded one at a time, and the order decides how soon the mass closes. Four rules choose the next class among the unexpanded ones:

**creation:** the order of discovery, the classic order.
**deficit:** the largest deficit $\delta(L)$, ties to the larger $|\mathrm{Aut}|$. It goes to the classes whose neighbourhood is least explored, and if the mass has not closed, a missing class is adjacent to one of them.
**aut:** the largest $|\mathrm{Aut}(L)|$. Such classes have few orbits, so their expansion is cheap, and lattices with large root systems tend to be neighbours of each other: a missing class of large $|\mathrm{Aut}|$ is reached through few edges from generic classes but through many from other classes of large $|\mathrm{Aut}|$, by Proposition 3.
**mixed:** one pick by deficit, then one by $|\mathrm{Aut}|$, in turn.

All four are exact: they only change which classes are expanded before the mass closes. Each pure order has a blind spot. The deficit order sees the whole graph through the edges already counted, and is very effective in the bulk of the enumeration. But the classes it misses typically have high symmetry, and such classes are adjacent, in practice, only to classes of high symmetry: it makes sense to expand those in priority, which is what the $|\mathrm{Aut}|$ order does. The $|\mathrm{Aut}|$ order, in turn, misses the classes of ordinary $|\mathrm{Aut}|$ reached through few edges. The mixed order covers both tails; on the genus of 28 528 classes above, the deficit order took 1103 expansions, the $|\mathrm{Aut}|$ order missed four classes after 2 hours, and the mixed order needed 833 expansions and a quarter of the canonical forms of the deficit order (Section 7.6). It is our default.

4.5. **The limits of scheduling.** No schedule removes the randomness of the tail. When one class $M$ is missing, the missing mass is $1/|\mathrm{Aut}(M)|$, so $|\mathrm{Aut}(M)|$ is known, but the edges leading to $M$ are not. A random neighbour lands on $M$ with probability $(1/|\mathrm{Aut}(M)|)/m(G)$, which can be of order $10^{-4}$, and a run whose path does not pass close to $M$ may spend many expansions on it. The order of the orbit representatives decides which path a run follows, and changing it only reshuffles which runs are unlucky. Single runs should be compared with this variance in mind (Section 7.6).

## 5. Canonical forms and automorphism groups

Each neighbour needs a canonical form, and each new class its automorphism group. One family of methods serves for the canonical form, the isometry test and the automorphism group. All of them first reduce the Gram matrix by LLL, $A \mapsto PAP^T$, work on the reduced matrix, and bring the result back: $B \mapsto BP$ for a canonical basis, $g \mapsto P^{-1}gP$ for the generators of the group, $P_2^{-1}EP_1$ for an isometry. The canonical form does not depend on the basis, but its cost does, and every neighbour then gets exactly one reduction.

5.1. **Characteristic families and the graph method.** The canonical form of Dutour Sikirić, Haensch, Voight and van Woerden [8] set up the modern approach. A *characteristic family* is a finite set $V \subset L$ determined by the lattice alone, so that every isometry maps the family of $L$ onto that of its image. Examples are the vectors of norm at most the smallest $\lambda$ for which they span $L$, and the *iterated shortest vectors*: the shortest vectors of $L$ and, when they are not of full rank, the same construction applied to the orthogonal complement of their span in $L$. The latter family is of full rank and stays small even when one direction of the lattice is much longer than the others, but it spans only a sublattice of finite index; a variant completes it, by closest vector computations, into a family spanning $L$. The configuration $V$ is turned into a complete graph whose vertices are the vectors and whose edges are coloured by the values $b(v, w)$. A canonical labelling of this graph by nauty or traces orders $V$ canonically, and the Hermite normal form of the ordered family gives a canonical basis of the lattice it spans, hence a canonical Gram matrix of $L$ when $V$ spans $L$. The automorphism group of the coloured graph gives $\mathrm{Aut}(L)$, and an isometry test is a comparison of canonical forms. The cost grows with $|V|$, the graph having $|V|^2$ edges; for the lattices met here, of rank up to 19 with about 12 000 vectors of norm 4, the family is large.

5.2. **The Plesken–Souvignier algorithm.** Plesken and Souvignier [17] compute $\mathrm{Aut}(L)$ and test isometry by a backtrack that never builds anything quadratic in the family. Let $S$ be the set of vectors of norm at most $\max_i A_{ii}$, up to sign. It is invariant under $\mathrm{Aut}(L)$, and contains the basis vectors $e_1, \dots, e_n$, which is why the Gram matrix is reduced first: an LLL reduced basis keeps the bound, hence $S$, small. An automorphism maps $e_1, \dots, e_n$ to vectors $v_1, \dots, v_n$ of $S$ with

$$b(v_i, v_j) = b(e_i, e_j) \quad \text{for all } i, j,$$

and conversely such vectors define an automorphism, the matrix with rows $v_i$, since the $e_i$ form a basis. The search chooses $v_1$, then $v_2$, and so on, among the vectors of $S$ of the right norm and the right products with the images already chosen. Three devices make it work.

- *The fingerprint.* For each level $k$, the number $f_k$ of vectors of $S$ with the products of $e_k$ against $e_1, \dots, e_{k-1}$ is an invariant: an automorphism maps those candidate sets bijectively. The basis is first reordered so that the $f_k$ are as small as possible early on, and a partial assignment is abandoned unless the number of candidates at the next level is exactly $f_k$.
- *Vector sums.* At level $k$ every vector of $S$ carries the tuple of its products with the last few chosen images. A partial automorphism maps the classes of vectors with equal tuples onto each other, with the same multiplicities, and maps the sum of each class to the corresponding sum, so the Gram matrices of these sums must agree. Without this refinement, lattices of rank 14 to 16 of moderate symmetry already lead to a combinatorial explosion.
- *The stabiliser chain.* The group is assembled level by level along the chain of pointwise stabilisers of $e_1, e_2, \dots$: once a level is complete, the orbit of the image of $e_k$ under the group found so far is known, and the candidates in one orbit need be searched only once; Schreier generators found along the way complete the generating set. The order is the product of the orbit lengths.

The isometry test is the same search with the images taken in the set $S'$ of the second lattice. The algorithm gives no canonical form by itself. One is obtained by *orbit splitting*, once $\mathrm{Aut}(L)$ is known as a permutation group on $S$: a prefix of vectors spanning $\mathbb{Q}^n$ is chosen one vector at a time, each time from the orbit of the stabiliser of the earlier choices that minimises an isometry invariant key (orthogonality to the prefix, orbit size, norms, products with the prefix); ties are refined by the products with the whole family, and the remaining ties are branched, keeping the lexicographically smallest result. The prefix then pins every vector by its products, and the reordered family gives the canonical basis as in the graph method. This avoids the quadratic graph entirely, and works on families as large as the 98 280 minimal pairs of the Leech lattice, but it requires the automorphism group first.

5.3. **The root system.** The methods that win on the genera of this note use the root system. The *roots* of an even lattice are its vectors of norm 2; they form a root system $R$ of type ADE, whose reflections $s_r(x) = x - b(x,r)r$ are automorphisms of $L$. A positive system is chosen by a generic linear form (the roots whose first nonzero coordinate is positive), and the simple roots are the positive roots that are not a sum of two positive roots; distinct simple roots have product 0 or $-1$, which gives the Dynkin diagram, its components and their types, and $|W(R)|$ from the tables, with no group computation. The Weyl group $W(R)$, generated by the simple reflections, is a normal subgroup of $\mathrm{Aut}(L)$, and acts simply transitively on the chambers of $R$. With $\rho$ the Weyl vector of the chosen chamber,

$$\mathrm{Aut}(L) = W(R) \rtimes \mathrm{Aut}(L, \rho),$$

where $\mathrm{Aut}(L,\rho)$, the *residual group*, is the stabiliser of the chamber; it acts on the Dynkin diagram and on the orthogonal complement $R^\perp$ of the roots, which is root free. The lattice is an overlattice of $\mathbb{Z}R \oplus R^\perp$, of index the *glue index*. For the lattices met here $W(R)$ is the bulk of $\mathrm{Aut}(L)$: the last class of the genus of 28 528 classes, an overlattice of $A_{12} \oplus D_5 \oplus R^\perp$, has $|\mathrm{Aut}| = 2|W(R)|$. Removing $W(R)$ from the configuration is what makes the following methods fast.

**Vinberg:** The family is made of all the roots together with a characteristic family of $R^\perp$, computed in $R^\perp$, which is root free and of smaller rank, and lifted to $L$. It is invariant and of full rank, but spans only $\mathbb{Z}R \oplus R^\perp$, so the canonical form orders it by the graph method and then canonicalises the position of $L$ among the overlattices of the sublattice it spans (the glue). The automorphism group is computed as $W(R) \rtimes \mathrm{Aut}(L,\rho)$: the simple reflections generate $W(R)$, of known order, and $\mathrm{Aut}(L,\rho)$ is the automorphism group of the small family made of the simple roots and the characteristic family of $R^\perp$, since an automorphism preserving the simple roots preserves the chamber. An isometry test likewise reduces to the residual families: an isometry composed with the element of the Weyl group that brings the image chamber back is an isometry of the residual families.

**Weyl:** The same, with only the simple roots, with both signs, in place of all the roots [2]. The graph has $2 \cdot \mathrm{rank}(R)$ root vertices instead of $|R|$, and its symmetries no longer contain $W(R)$. The family depends on the chamber, but only up to isometry: an isometry carries a chamber to a chamber, and the element of $W(R)$ moving it back fixes $R^\perp$ pointwise. So the canonical form does not depend on the chamber chosen.

**Weyl chamber:** Let $V$ be a characteristic family spanning $L$. The family is made of the simple roots and of the vectors of $V$ that lie in the closed fundamental chamber and are not roots, with both signs [2]. Since $V$ is invariant under $W(R)$ and the chamber is a fundamental domain, this family still spans $L$ itself, so the canonical basis is directly the Hermite normal form of the canonically ordered family, with no glue step. The vectors of $V$ in the chamber are computed without forming $V$: the family $V$ is built by a recursion of closest vector problems in cosets $y + \mathbb{Z}R$, and the minimal vector of such a coset in the chamber is unique, reached from $y$ by reflecting into the chamber and subtracting a positive root $\delta$ whenever $b(y,\delta) \geq 2$, which shortens $y$, after a rounding of the component of $y$ in $\mathbb{Q}R$ to start close. For the automorphism group and the isometry test the simple roots are taken with one sign only: a symmetry of the family then preserves the simple roots, hence the chamber, and the symmetry group of the family is exactly $\mathrm{Aut}(L,\rho)$.

All the root-based methods fall back on the graph method for a root free lattice. On the genera of this note the Weyl-chamber method is the fastest for both the canonical form and the automorphism group, by a factor 2 over the next one and two orders of magnitude over Plesken–Souvignier (Section 7.8). The recognition of a neighbour by isometry tests against the known classes with the same invariants, instead of a canonical form, is kept for checking.

## 6. The orbits on $\mathbb{P}^{n-1}(\mathbb{F}_2)$

An expansion starts with the orbits of $\mathrm{Aut}(L)$ on the $(p^n-1)/(p-1)$ points, with their sizes. The generic computation walks the points, builds the vector of each, multiplies it by each generator ($n^2$ operations) and converts the image back to an index: at $p = 2$ and $n = 19$, about $4 \cdot 10^9$ operations per expansion. Once the canonical form is fast, this dominates the full expansion at rank 19.

At $p = 2$ a point is a nonzero vector of $\mathbb{F}_2^n$, stored as an integer $x \in [1, 2^n - 1]$ whose bits are its coordinates. A generator $g$ acts $\mathbb{F}_2$-linearly, so the image of $x$ is the XOR of the images of its set bits. For each generator and each byte position $k$ we tabulate the 256 images of the vectors supported on the bits $8k, \ldots, 8k + 7$; the image of $x$ is then the XOR of $\lceil n/8 \rceil$ table entries. The orbits are found by a traversal with a visited bitmap, and their sizes, which the Hecke bookkeeping needs, come for free. This makes the orbits a negligible part of an expansion (Section 7.9).

The generators can also be replaced by a few random products of them. They generate a subgroup, whose orbits refine those of the group, so the enumeration stays correct whatever happens; it only builds more neighbours if the orbits are finer.

## 7. Results

7.1. **Test data.** The test data is the database DefLatDB of S. Muller [7], which lists for 8676 genera of definite lattices of rank 3 to 21 a complete set of representatives with the orders of their automorphism groups. We use its 6333 genera of even lattices of even determinant. For each genus the seed is the first listed lattice, and the mass is the sum of $1/|\mathrm{Aut}|$ over the listed classes. All runs are on one core, with the rational arithmetic of FLINT [9], which makes the enumeration about 3.4 times faster than with GMP rationals.

7.2. **The prime 2 on DefLatDB.** We ran the iterate schedule with the creation order on the 6333 genera, with a cap of 60 s and then 10 min per genus. In this schedule every class found is expanded at $p = 2$; only if the mass is still open when all of them are expanded are the classes expanded at 3, then at 5, and so on, each new class being expanded at all the primes used so far. The table records the largest prime used when the mass closed. "Needs $p = 3$" thus means that the 2-neighbours of the classes reachable from the seed do not give the whole genus, and that the 3-neighbours do; it says nothing about whether 3 divides $d$, and the prime 2 always does.

| largest prime used when the mass closes (of 4551 genera counted) | genera |
|---|---|
| 2 | 4069 |
| 3 | 386 |
| 5 | 90 |
| 7 | 5 |
| 11 | 1 |

Table 1. The primes needed to close the mass, iterate schedule.

**Observation 1.** *When $p = 2$ fails, it fails completely: in every failing genus with $h > 1$, no line of any class gives a 2-neighbour at all, even when the classes found at 3 are expanded again at 2. Every failing genus has the anisotropic plane $\{1\}_{II}^{-2}$ as unimodular 2-adic Jordan component. When that component has rank at least 4, or is the hyperbolic plane, $p = 2$ always sufficed. Inside the anisotropic-plane class $p = 2$ still works in about 40% of the genera with $h > 1$.*

Proposition 2 explains the observation. The failures are the genera with $n_2(G) = 0$: $U$ is the anisotropic plane and the 2-modular component is even or absent. When $U$ is the anisotropic plane and $p = 2$ works, the 2-modular component must be odd, and its vectors of odd $q$ compensate those

of $U$. Conversely, in every genus counted with $n_2(G) > 0$ the 2-neighbour graph turned out to be connected on the whole genus: the mass closed from a single seed.

Table 2 gives the number of classes expanded before the mass closes, on the 3733 genera with $h > 1$ closed at $p = 2$ alone. The last class found is never expanded, since its arrival closes the mass.

| $h$ | genera | expanded, mean | expanded, max | fraction, mean | fraction, max |
|---|---|---|---|---|---|
| 2 | 377 | 1.0 | 1 | 0.50 | 0.50 |
| 3 | 332 | 1.5 | 2 | 0.49 | 0.67 |
| 4 | 275 | 2.1 | 3 | 0.52 | 0.75 |
| 5 | 225 | 2.6 | 4 | 0.53 | 0.80 |
| 6–10 | 761 | 4.2 | 9 | 0.54 | 0.90 |
| 11–20 | 742 | 8.1 | 18 | 0.55 | 0.95 |
| 21–50 | 672 | 19.4 | 46 | 0.59 | 0.97 |
| 51–100 | 343 | 43.4 | 90 | 0.62 | 0.96 |
| $> 100$ | 6 | 63.2 | 84 | 0.62 | 0.82 |

TABLE 2. Classes expanded at $p = 2$ before the mass closes, creation order.

Over all, the fraction is 0.55 on average, with median 0.50, minimum 0.125 and maximum 0.97, and 94% of the neighbours built are classes already known.

7.3. **The genera where $p = 2$ fails.** To see these genera completely, and not only those reached by the sweep within its time caps, we listed them from their symbols. By Proposition 2, $n_2(G) = 0$ exactly when the unimodular 2-adic component is the anisotropic plane and the 2-modular component is even or absent (a unimodular component of rank 0 does not occur in the database). Among the 6333 genera, 598 satisfy this, 493 of them with $h > 1$. For each of these we computed, from the complete DefLatDB list of classes, the neighbour graphs at 3, 5, 7, ..., and the number of connected components of the union of the graphs at the primes $2, 3, \ldots, q$, adding primes until the union is connected.

| primes needed | genera | $h$ max | $h$ median | rank |
|---|---|---|---|---|
| $2, 3$ | 396 | 191 | 4 | 3–12 |
| $2, 3, 5$ | 91 | 22 | 3 | 3–7 |
| $2, 3, 5, 7$ | 5 | 5 | 3 | 3–4 |
| $2, 3, 5, 7, 11$ | 1 | 2 | 2 | 3 |

TABLE 3. The 493 genera with $n_2(G) = 0$ and $h > 1$, by the primes needed to connect the neighbour graph.

The result is all or nothing at every prime. Each prime either gives no neighbour at all, $n_p(G) = 0$, and the number of components stays $h$, or it connects the whole genus at once: in no genus does a prime join only some of the classes. The primes that fail are exactly those where the unimodular component of $L \otimes \mathbb{Z}_p$ has rank at most 1 or is an anisotropic plane, as Proposition 2 says. In 161 of the 493 genera the prime that connects is the smallest prime not dividing $d$, the setting of Kneser's theorem; in the other 332 it divides $d$, but its unimodular component is large enough.

*The genus that needs* 11. It is the genus $\{1\}_{II}^{-2}\{4\}_1^1\{3\}^{-2}\{5\}^1\{7\}^{-1}$, of rank 3, determinant $1260 = 2^2 \cdot 3^2 \cdot 5 \cdot 7$ and level 420, with $h = 2$ classes, both with $|\mathrm{Aut}| = 8$, so $m(G) = 1/4$,

represented by

$$\begin{pmatrix} 18 & 12 & 9 \\ 12 & 12 & 6 \\ 9 & 6 & 22 \end{pmatrix}, \qquad \begin{pmatrix} 4 & 0 & 0 \\ 0 & 18 & 3 \\ 0 & 3 & 18 \end{pmatrix}.$$

Every prime below 11 divides $d$ and fails, for a local reason that can be read off the symbol:

- at 2 the unimodular component is the anisotropic plane, and there is no 2-modular component (the next scale is 4);
- at 3 the component of scale 3 has rank 2, so the unimodular component has rank 1;
- at 5 and at 7 the unimodular component has rank 2, and it is anisotropic.

So the number of components is 2 for $\{2\}$, $\{2,3\}$, $\{2,3,5\}$ and $\{2,3,5,7\}$. At 11, which does not divide $d$, every nonzero isotropic line of the ternary form gives a neighbour, $n_{11}(G) = (11^2-1)/10 = 12$, and

$$T_{11} = \begin{pmatrix} 8 & 4 \\ 4 & 8 \end{pmatrix}$$

connects the two classes.

*Why the failing genera are small.* The prime $p$ fails only if the unimodular component of $L \otimes \mathbb{Z}_p$ has rank at most 2, so that a component of rank at least $n-2$ has scale divisible by $p$, and $p^{n-2}$ divides $d$; at $p = 2$, with no 2-modular component, even $4^{n-2}$ does. For $p = 2$ to fail in rank $n$ the determinant must therefore be large, and this is what the database shows: the smallest determinant of a failing genus is 48 in rank 5, 512 in rank 9 and 1024 in rank 11 and 12. A genus that needs a prime $q$ must fail at every prime below $q$, so that $\prod_{p<q} p^{n-2}$ divides $d$: this pushes the genera that need 5 or more into rank 3 to 7, and those that need 7 or 11 into rank 3 and 4, where the class numbers are small. For $n \geq 3$, the smallest prime not dividing $d$ always has $n_p(G) > 0$, and by Kneser's theorem it connects each spinor genus; in the database it always connected the whole genus, so no genus needed a prime beyond it. The failing genera also have smaller class numbers than the other genera of the same rank (at most 191 in rank 5, against 1951 for the database in that rank, and 155 against 15 003 in rank 6); the determinant condition does not explain this by itself, and we leave it as an observation.

7.4. **Disconnected neighbour graphs.** In all the genera above, a prime that does not connect the genus gives no neighbour at all, so that the components are the $h$ single classes, all of size 1 but of unequal masses (for c02371 at $p = 3$, 1/24, 1/8 and 1/12). To see a prime with neighbours and several components, we looked at the genera with several spinor genera. Among the 4768 even genera of DefLatDB of rank at least 3 with 2 to 300 classes, SageMath finds 4761 with one proper spinor genus and 7 with two (and two improper spinor genera as well); all seven have rank 3 or 4 and 2 to 4 classes. We computed their complete neighbour graphs at the eight primes from 2 to 19 (Table 4).

The two situations are distinct.

- *A prime with* $n_p(G) = 0$ gives the $h$ single classes, of unequal masses. This is the case of 3 in all seven genera, and of 2 in c02463.
- *A prime with* $n_p(G) > 0$ either connects the genus or gives exactly two components, which are the two spinor genera. In these seven genera the primes 5, 11, 17, and 2 when $n_2(G) > 0$, connect, and the primes 7, 13, 19, all $\equiv 1 \bmod 3$, give the two components; this includes $p = 7$ for c02617, where 7 divides $d$ but $n_7(G) = 14$. The two components always have the same mass, but not always the same number of classes: in c02371, c02677 and c04148 they have 2 and 1 classes.

This agrees with the theory of spinor genera for $p \nmid d$: a $p$-neighbour lies in the spinor genus obtained from that of $L$ by the class of $p$ in the group of spinor genera, here of order 2, so that the components at $p$ are the cosets of the subgroup generated by that class, and the class seems to be

| genus | $n$ | $d$ | $h$ | $p=2$ | $p=3$ | $p\equiv 2\ (3)$ | $p\equiv 1\ (3)$ | sizes | masses |
|---|---|---|---|---|---|---|---|---|---|
| c02703 | 3 | 54 | 2 | 1 | $2^\circ$ | 1 | 2 | 1, 1 | 1/24, 1/24 |
| c02371 | 3 | 162 | 3 | 1 | $3^\circ$ | 1 | 2 | 2, 1 | 1/8, 1/8 |
| c02463 | 3 | 216 | 2 | $2^\circ$ | $2^\circ$ | 1 | 2 | 1, 1 | 1/24, 1/24 |
| c02465 | 3 | 216 | 2 | 1 | $2^\circ$ | 1 | 2 | 1, 1 | 1/8, 1/8 |
| c02617 | 3 | 378 | 4 | 1 | $4^\circ$ | 1 | 2 | 2, 2 | 1/6, 1/6 |
| c02677 | 3 | 486 | 3 | 1 | $3^\circ$ | 1 | 2 | 2, 1 | 1/8, 1/8 |
| c04148 | 4 | 729 | 3 | 1 | $3^\circ$ | 1 | 2 | 2, 1 | 1/48, 1/48 |

TABLE 4. Number of connected components of the neighbour graph of the seven genera with two spinor genera, at $p = 2$, $p = 3$, the primes $p = 5, 11, 17$ and the primes $p = 7, 13, 19$; $^\circ$ marks a prime with $n_p(G) = 0$, whose components are single classes. The last two columns give the sizes and the masses of the two components at $p \equiv 1 \bmod 3$, the same for 7, 13 and 19.

given here by the character $p \mapsto (p/3)$, which we read off the data rather than derive. The equality of the masses agrees with the classical fact that the spinor genera of a genus of rank at least 3 all have the same mass, which Hecke.jl uses to split the mass of a genus among its spinor genera; the class numbers of the spinor genera need not be equal, and here they are not. So when a neighbour graph with neighbours is not connected, its components are unions of spinor genera: equal in mass, not in size. That $p = 7$ behaves in the same way in c02617, where it divides $d$, is an observation on one genus.

7.5. **The random walk.** For the tuning of the walk and of the orders we used 60 genera with $h > 20$, drawn at random, 20 in each of the ranges $h = 21$–$50$, 51–100 and $h > 100$, among the genera that the sweep of Section 7.2 closed within 40 s. Counting the canonical forms of neighbours (Table 5), with the expansions after the walk in decreasing |Aut|:

| setting | canonical forms | time | mass closed by the walk alone |
|---|---|---|---|
| iterate | 101 722 | 755 s | — |
| walk, $c_h = 0$ | 64 747 | 561 s | — |
| walk, $c_h = 0.25$ | 65 716 | 513 s | 0/60 |
| walk, $c_h = 0.5$ | 80 548 | 662 s | 0/60 |
| walk, $c_h = 1$ | 104 365 | 971 s | 4/60 |
| walk, $c_h = 2$ | 148 408 | 1349 s | 23/60 |

TABLE 5. The random walk at $p = 2$ against iterate, 60 genera with $h > 20$. The last column was not recorded for $c_h = 0$; iterate has no walk. With $c_h = 0$ the hit bound is always 1.

With $c_h = 0.25$ the walk saves 35% of the canonical forms and 32% of the time against iterate, and 41% and 39% on the genera with $h > 100$. We take $c_f = 16$.

7.6. **The orders.** On the same 60 genera (Table 6), in the iterate schedule, the deficit order saves 45% of the canonical forms against creation and is better on 52 of the 60 genera. After the walk the deficit order is better on 38 genera and worse on 22, and costs 5% more over all: on these mid-sized genera the walk already finds most classes, and the order only rearranges a short tail.

Tables 7 and 8 were measured with the code of earlier stages of this work, before the final versions of the canonical form and of the orbit computation (Sections 5 and 6). They compare orders and schedules run with the same code, and their times are not comparable with those of Table 11. On

| schedule | order | $h = 21$–$50$ | 51–100 | 101–531 | total |
|---|---|---|---|---|---|
| iterate | creation | 5699 | 19 414 | 76 609 | 101 722 |
| iterate | deficit | 4138 | 10 606 | 41 370 | 56 114 |
| walk | aut | 5856 | 14 457 | 45 403 | 65 716 |
| walk | deficit | 5164 | 14 760 | 48 410 | 68 334 |

TABLE 6. Canonical forms by order, 60 genera with $h > 20$.

larger genera of determinant 30 and 210, with 10 minutes each, the walk followed by the deficit order is clearly best (Table 7): it completes 4 of the 6 genera and misses one class in each of the other two, while the walk with the |Aut| order completes one, and iterate with the deficit order none.

| genus | $h$ | walk + aut | iterate + deficit | walk + deficit |
|---|---|---|---|---|
| c02188 (det 30) | 548 | complete, 467 s | 545 | complete, 270 s |
| c02189 (det 30) | 565 | 564 | 564 | complete, 310 s |
| c01440 (det 210) | 2692 | 2681 | 2687 | 2691 |
| c01439 (det 210) | 2700 | 2693 | 2698 | complete, 513 s |
| c01437 (det 210) | 2797 | 2787 | 2790 | 2796 |
| c01438 (det 210) | 2813 | 2803 | 2810 | complete, 551 s |

TABLE 7. Classes found in 10 minutes, $c_h = 0.25$.

The genus c02216, $\{1\}_{II}^{-18}\{2\}_{7}^{1}\{9\}^{-1}\{5\}^{1}$ with 28 528 classes, shows why both deficit and |Aut| are needed. After the same walk (214 654 canonical forms):

| order | full expansions | canonical forms in them | result |
|---|---|---|---|
| deficit | 1103 | 872 732 | complete |
| aut | 2716 | 455 353 | 28 524 classes after 2 h |
| mixed | 833 | 223 006 | complete in 66 min |

TABLE 8. The orders on c02216.

The last class of the deficit run, 28 528, is an overlattice of $A_{12} \oplus D_5 \oplus M$, with $M$ of rank 2, determinant 4680 and minimum 36, glue index 52, and $|\mathrm{Aut}| = 2|W(A_{12})||W(D_5)| = 2.39 \cdot 10^{13}$, among the largest of the genus. It was found by the expansion of class 24 742 ($A_4A_8D_4$, $|\mathrm{Aut}| = 1.67 \cdot 10^{10}$) through 9 of its 262 143 points; conversely class 28 528 sends 12 870 points to 24 742, and $12\,870 \cdot 1.67 \cdot 10^{10}/2.39 \cdot 10^{13} = 9$, as Proposition 3 says. By the same identity, the classes reaching 28 528 most often are:

The $A_{16}$ class sends 2.4% of its points to the last class and has few orbits, but the deficit order never took it. The |Aut| order missed four classes of ordinary groups, of rank 5225 to 14 993 of 28 528 by |Aut|. The last class of the mixed run, of $|\mathrm{Aut}| = 663\,552$, one of those the |Aut| order missed, came from a deficit pick. We did not run the creation order on this genus.

The Hecke identity was also checked numerically on 300 other genera, 60 where $p = 2$ fails and 240 where it suffices, drawn at random among those the sweep closed within 60 s, expanding every class, with 5666 expansions at $p = 2, 3, 5, 7$, many at a prime dividing the determinant. The skip of the classes of deficit 0 saved 161 canonical forms on the 60 genera, 0.2% with iterate and 0.01% with the walk.

| class | roots | \|Aut\| | points leading to 28 528 |
|---|---|---|---|
| 28 528 | $A_{12}D_5$ | $2.4 \cdot 10^{13}$ | 6862 |
| 26 193 | $A_{16}$ | $7.1 \cdot 10^{14}$ | 6188 |
| 27 330 | $A_9D_7$ | $2.3 \cdot 10^{12}$ | 700 |
| 26 199 | $A_7A_9$ | $2.9 \cdot 10^{11}$ | 252 |
| 27 480 | $A_1A_4A_6E_6$ | $1.3 \cdot 10^{11}$ | 180 |
| 26 195 | $A_8D_8$ | $3.7 \cdot 10^{12}$ | 112 |
| 24 742 | $A_4A_8D_4$ | $1.7 \cdot 10^{10}$ | 9 |

*Variance.* On c01437 (2797 classes), with the walk and the mixed order, 10 seeds of the walk give 195 to 235 full expansions (25 to 28 s) in nine runs, and 409 (45 s) in one. In that run the second-to-last class came after 217 expansions, as in the others, and the 192 remaining expansions were all spent on the last class, an ordinary one ($|\mathrm{Aut}| = 5.8 \cdot 10^6$, missing mass $1/5\,806\,080$). A random 2-neighbour lands on it with probability about $9 \cdot 10^{-5}$, so about 12 000 draws, the order of the 16 000 neighbours of those 192 expansions.

7.7. **The neighbour graph.** To see what the orders are up against, we computed the whole neighbour graph at $p = 2$ of ten genera of the test data, of rank 15 to 19 and with 548 to 2813 classes, by expanding every class of the DefLatDB list: the matrix $T(L, M)$ in full. This is the only exhaustive computation of the note; it took 3 to 11 minutes per genus, while the genera with tens of thousands of classes would need weeks.

The random neighbour walk has the transition matrix $P = T/n_2(G)$. By Proposition 3 it is reversible, with stationary distribution

$$\pi(L) = \frac{1/|\mathrm{Aut}(L)|}{m(G)},$$

so $D^{1/2}PD^{-1/2}$, with $D = \mathrm{diag}(\pi)$, is symmetric with the spectrum of $P$, and $1 = \lambda_1 > \lambda_2 \geq \cdots \geq \lambda_h$. The spectral gap $1 - \lambda_2$ measures the expansion: the conductance $\Phi$ of the graph, the least proportion of the stationary flow leaving a set of stationary mass at most $1/2$, satisfies $(1 - \lambda_2)/2 \leq \Phi \leq \sqrt{2(1 - \lambda_2)}$ (Cheeger), and the walk mixes in at most $\log(4/\pi_{\min})/(1 - \lambda_2)$ steps. Table 9 gives these measures, together with the number of expansions needed to find every class from the seed, in the order of discovery and for a greedy oracle that knows the graph and always expands the found class reaching the most classes not yet found.

| genus | $n$ | $h$ | $\lambda_2$ | $\lambda_h$ | diam. | degree | $\pi(\max \lvert\mathrm{Aut}\rvert)$ | creation | oracle |
|---|---|---|---|---|---|---|---|---|---|
| c02188 | 19 | 548 | 0.502 | −0.004 | 4 | 96 | $2.8 \cdot 10^{-15}$ | 511 | 22 |
| c02189 | 19 | 565 | 0.502 | −0.011 | 4 | 95 | $1.5 \cdot 10^{-16}$ | 558 | 23 |
| c02089 | 17 | 972 | 0.505 | −0.010 | 5 | 103 | $4.2 \cdot 10^{-14}$ | 792 | 36 |
| c02088 | 17 | 1 475 | 0.505 | −0.012 | 4 | 135 | $3.2 \cdot 10^{-13}$ | 1 387 | 47 |
| c02091 | 17 | 2 311 | 0.505 | −0.002 | 5 | 175 | $4.6 \cdot 10^{-16}$ | 2 293 | 61 |
| c02090 | 17 | 2 351 | 0.505 | −0.012 | 5 | 168 | $2.1 \cdot 10^{-14}$ | 2 280 | 65 |
| c01440 | 15 | 2 692 | 0.511 | −0.015 | 5 | 137 | $3.3 \cdot 10^{-13}$ | 2 602 | 84 |
| c01439 | 15 | 2 700 | 0.510 | −0.015 | 6 | 133 | $3.3 \cdot 10^{-14}$ | 2 697 | 83 |
| c01437 | 15 | 2 797 | 0.510 | −0.013 | 5 | 130 | $4.7 \cdot 10^{-13}$ | 2 597 | 86 |
| c01438 | 15 | 2 813 | 0.511 | −0.013 | 5 | 132 | $4.7 \cdot 10^{-13}$ | 2 441 | 88 |

TABLE 9. The neighbour graphs at $p = 2$: second and last eigenvalue of the walk, diameter, median number of distinct neighbour classes, stationary probability of the class of largest |Aut|, and expansions to find every class from the seed.

Four facts stand out.

- *The graphs are excellent expanders.* The Hecke identity holds exactly on every pair of classes, every graph is connected, of diameter 4 to 6, and the spectral gap is 0.49 to 0.50 in every case. The spectrum is layered: besides $\lambda_1 = 1$ there are a few eigenvalues near $1/2$, then groups near $1/4$, $1/8$, $1/16$, and a bulk near 0, with $|\lambda_h| \le 0.015$. Such large Hecke eigenvalues are those of non-tempered automorphic representations, as for the Niemeier lattices [3]; we do not pursue their interpretation here.
- *The stationary distribution is extremely uneven.* The class of largest |Aut| has stationary probability $10^{-16}$ to $10^{-13}$, against $1/h \approx 10^{-3}$. A walk, however well it mixes, lands on it in proportion to $1/|\mathrm{Aut}|$: this is why the random walk alone never closes the mass, and why the order by |Aut| is needed in the tail. Good expansion and rare classes are not in conflict; the rare classes are rare by their weight, not by their position in the graph.
- *Few expansions suffice in principle.* An oracle finds every class after expanding 22 to 88 classes, 3 to 4% of the genus, while the order of discovery expands 80 to 99% of it. With the walk and the mixed order the program needs 29 to 409 full expansions on the same genera (Table 11), after a walk that has found most of the classes. The gap to the oracle is what an order could still gain.
- *The degrees are large.* A class has a median of 95 to 175 distinct neighbour classes, and the class of largest degree up to 544, so that a few well-chosen expansions cover the genus: the difficulty is to choose them without knowing the graph.

7.8. **Canonical forms and automorphism groups.** On the first 150 classes of c02189 (determinant 30, rank 19) and of c01437 (determinant 210, rank 15), the mean time per class:

| canonical form | c02189 | |
|---|---|---|
| Weyl chamber | 46 ms | |
| Weyl | 94 ms | |
| Vinberg | 249 ms | |
| Plesken–Souvignier | 4.8 s (max 43 s) | |
| **automorphism group** | **c02189** | **c01437** |
| Weyl chamber | 38 ms (max 56) | 16 ms (max 23) |
| Vinberg | 73 ms | 35 ms |
| iterated shortest | 229 ms | 110 ms |
| Plesken–Souvignier | 1.5 s (max 12 s) | 79 ms |
| graph | $> 9$ s | 1.0 s (max 74 s) |

TABLE 10. Methods for the canonical form and the automorphism group.

All methods that completed gave the automorphism group orders of DefLatDB. The Weyl-chamber method has no heavy tail.

7.9. **Profile and orbits.** Before the bitmask orbits, a profile of c02216 put 82% of the time of a full expansion at rank 19 in the orbit computation and 16% in the canonical forms; at rank 16 (c01914), 30% and 66%. The bitmask computation brought the orbits of an expansion at rank 19 from about 1.5 s to 14 ms. The canonical forms of the $\approx 3000$ neighbours of that expansion take about 120 s, so the orbits are now negligible. In the walk at rank 19, 90% of the time is in the canonical forms: the Weyl-chamber family 47%, the canonical labelling 24%, the LLL reduction 16%, the root system 10%; the automorphism groups of the new classes take 7%, and the construction of the neighbours 4%.

The automorphism groups have 10 to 20 generators on these genera, all distinct and nontrivial modulo 2. Two to four random products of 20 generators usually give the same orbits and make the orbit computation about 3 times faster, but this saves under 1% of a run, so the option is off by default.

7.10. **Final runtimes.** With the walk ($c_h = 0.25$), the mixed order, the Weyl-chamber method, the bitmask orbits and FLINT, on 31 genera of DefLatDB of rank 14 to 19 (Table 11). The time is the wall-clock time to the last class, which closes the mass; the CPU time equals it. All 31 genera close the mass at $p = 2$ alone, and every |Aut| found is one of DefLatDB.

| genus | $n$ | det | $h$ | time (min) | full expansions |
|---|---|---|---|---|---|
| c02188 | 19 | 30 | 548 | 0.2 | 29 |
| c02189 | 19 | 30 | 565 | 0.2 | 61 |
| c02089 | 17 | 90 | 972 | 0.2 | 49 |
| c02088 | 17 | 90 | 1 475 | 0.3 | 93 |
| c02091 | 17 | 90 | 2 311 | 0.5 | 131 |
| c02090 | 17 | 90 | 2 351 | 0.5 | 130 |
| c01440 | 15 | 210 | 2 692 | 0.5 | 226 |
| c01439 | 15 | 210 | 2 700 | 0.5 | 231 |
| c01437 | 15 | 210 | 2 797 | 0.8 | 409 |
| c01438 | 15 | 210 | 2 813 | 0.5 | 237 |
| c02215 | 19 | 90 | 16 700 | 7.8 | 567 |
| c02216 | 19 | 90 | 28 528 | 13.9 | 821 |
| c02217 | 19 | 90 | 28 959 | 15.9 | 985 |
| c01664 | 15 | 302 | 31 190 | 6.3 | 1867 |
| c01824 | 16 | 256 | 31 640 | 9.1 | 1683 |
| c01822 | 16 | 256 | 31 722 | 7.1 | 1337 |
| c01821 | 16 | 256 | 32 058 | 7.4 | 1389 |
| c01823 | 16 | 256 | 32 068 | 7.2 | 1343 |
| c01814 | 16 | 248 | 32 191 | 7.2 | 1505 |
| c01813 | 16 | 248 | 32 260 | 6.5 | 1353 |
| c01098 | 14 | 2048 | 33 566 | 14.0 | 2183 |
| c01866 | 16 | 260 | 33 819 | 7.6 | 1473 |
| c01867 | 16 | 260 | 33 940 | 6.8 | 1297 |
| c02213 | 19 | 82 | 36 267 | 13.2 | 913 |
| c01915 | 16 | 300 | 36 568 | 8.3 | 1525 |
| c01916 | 16 | 300 | 36 575 | 10.1 | 1749 |
| c01913 | 16 | 300 | 36 896 | 9.7 | 1743 |
| c01914 | 16 | 300 | 36 904 | 9.5 | 1684 |
| c01097 | 14 | 2048 | 39 036 | 12.0 | 1977 |
| c01876 | 16 | 272 | 40 617 | 10.4 | 1821 |
| c01877 | 16 | 272 | 40 617 | 10.1 | 1817 |
| total | | | | 204.3 | |

Table 11: Time to the last class, and number of full expansions at $p = 2$.

The genera of rank 19 need fewer expansions per class, but each expansion builds about 3000 neighbours. The genera c01437 and c01098 show the variance of the tail: their number of full expansions is about twice that of comparable genera.

7.11. **What did not work.**

**Large primes in the walk.:** Walking at primes in $[3, 20]$ or $[50, 200]$ instead of 2, on the 60 genera with $h > 20$: 60 378 and 62 982 canonical forms against 65 716, and 4 to 11% more time. The walk finds fewer new classes per neighbour as $p$ grows (18% at 2, then 16% and 14%), each neighbour costs a little more, and the hit rule stops the walk earlier. It stays as an option, since classes of high symmetry can be far apart at 2 and close at a large prime (the Niemeier lattice $D_{24}^+$ reaches the Leech lattice at $p = 47$).

**Deduplication by invariants.:** Keeping one lattice per value of a cheap invariant, with the mass as certificate, fails on both counts. On c02189 and c01437, the root system, the root decomposition and an isometry invariant together cost 48 and 19 ms, against 66 and 28 ms for the canonical form at the time, and they still merge 13% and 39% of the classes (9% and 33% with |Aut| added). The theta series up to norm 4 or 6 costs 15 to 300 times a canonical form.

**Skipping by the deficit alone.:** 0.2% of the canonical forms.

**Fewer generators.:** Under 1%.

**A better fixed order of the representatives.:** It only reshuffles which runs are unlucky.

## 8. Comparison with other programs

8.1. **The programs.** Magma [13] has a genus enumeration for definite lattices; its code is not available, and we do not discuss it further. Assaf, Chen, Garg and Wang [1] enumerate the lattices of given rank and determinant, listing the genus symbols in SageMath and computing the classes of each genus with Magma, by neighbours and by a descent from a genus of rank one higher in the manner of Chenevier and Taïbi [4]. The isometry and automorphism programs of Plesken and Souvignier [17], available for instance in PARI/GP, are the usual building blocks. The two open source enumerations of definite genera that we know of are the following; the descriptions are taken from their source code.

- *Hecke.jl* [10], part of the OSCAR computer algebra system, provides `enumerate_definite_genus` for definite integral lattices of rank at least 3. It first computes one representative of each spinor genus, and enumerates each spinor genus separately, at the smallest *Kneser prime*: a prime at which the genus is isotropic, which is not improperly automorphous, and at which $L \otimes \mathbb{Z}_p$ is maximal integral. At a prime dividing $d$, maximality holds exactly when $p$ divides the level only once and the component of scale $p$ has rank 1, or rank 2 with $p$ odd and the sign that makes it anisotropic; in particular it excludes $p = 2$ as soon as 4 divides the level. The neighbours come from the orbits of the automorphism group on the lines when there are fewer than $10^6$ of them, and from random lines otherwise. A neighbour is recognised by isometry invariants (minimum, root system, kissing number, |Aut|) and then by isometry tests against the known classes with the same invariants. Each spinor genus stops when its share of the mass, the mass divided by the number of spinor genera, is reached.
- *SageMath* [18] computes the classes of a genus with `Genus.representatives`. For a definite genus it takes one seed per spinor genus and iterates the neighbours at the smallest prime not dividing $d$, from the orbits on the lines when $p^n \leq 2^{18}$ and from random lines otherwise, until the mass is reached; a neighbour is compared by an equivalence test with every class found. For definite genera of rank above 6 it calls Magma by default.

The program of this note differs from both in three ways: it works on the whole genus from one seed, at the primes $2, 3, 5, \ldots$ in turn whether or not they divide the determinant, and with every admissible line, whether or not $L \otimes \mathbb{Z}_p$ is maximal; it recognises the neighbours by a canonical form, one dictionary lookup each, instead of isometry tests; and it schedules the exploration by a random walk and the Hecke bookkeeping.

8.2. **Benchmark.** We ran the three programs on the same genera of DefLatDB, from the same seed, the first listed lattice: our program with the random walk and the default settings, Hecke.jl 0.40.1 (`enumerate_definite_genus` with its defaults) and SageMath 10.9 (`Genus.representatives` with its own backend). Each run had a cap of 30 minutes and 10 GB; a program that hit the cap or failed was not run on the larger genera of the same group. Every run that finished found the class number of DefLatDB. The times of Hecke.jl and SageMath are those of the enumeration call, without the loading of Julia or Sage (about 50 s for Julia), while ours is the whole process, so that times below 2 s are dominated by the start of the program.

| genus | $n$ | $d$ | $h$ | ours | Hecke.jl ($p$) | SageMath |
|---|---|---|---|---|---|---|
| c06165 | 6 | 2880 | 45 | 1 s | 1.2 s (3) | 171 s |
| c00178 | 10 | 3840 | 46 | 1 s | 19 s (3) | 956 s |
| c01129 | 14 | 256 | 51 | 1 s | 290 s (3) | $>$ 1800 s |
| c00208 | 10 | 432 | 101 | 1 s | 304 s (5) | — |
| c01002 | 14 | 128 | 107 | 1 s | 772 s (3) | — |
| c00591 | 12 | 576 | 210 | 2 s | 566 s (3) | — |
| c01018 | 14 | 144 | 288 | 3 s | $>$ 1800 s (5) | — |

TABLE 12. Genera of even determinant. In brackets the prime used by Hecke.jl, its smallest Kneser prime; — not run, the program having timed out on a smaller genus.

| genus | $n$ | $d$ | $h$ | ours | Hecke.jl | SageMath |
|---|---|---|---|---|---|---|
| c04293 | 4 | 945 | 25 | 1 s | 1.0 s | 2.2 s |
| c07753 | 8 | 2025 | 20 | 1 s | 1.6 s | 2.6 s |
| c00623 | 12 | 81 | 24 | 2 s | 1.9 s | 213 s |
| c01130 | 14 | 27 | 25 | 1 s | 1.9 s | failed |
| c02112 | 18 | 11 | 33 | 1 s | 20 s | — |
| c02123 | 18 | 15 | 51 | 2 s | 69 s | — |
| c02127 | 18 | 19 | 111 | 3 s | 202 s | — |
| c02133 | 18 | 23 | 177 | 4 s | 121 s | — |
| c01942 | 16 | 49 | 271 | 4 s | 111 s | — |

TABLE 13. Genera of odd determinant, where all three programs work at $p = 2$. SageMath failed on c01130 by an overflow of the default PARI stack (1 GB) in the computation of an automorphism group.

The two groups separate the effects. When 2 divides $d$ (Table 12), Hecke.jl never uses $p = 2$: for all these genera $L \otimes \mathbb{Z}_2$ is not maximal integral, so 2 is not a Kneser prime (Hecke.jl's own test, `is_maximal_integral_bilinear`, confirms it on each of them). It works at its smallest Kneser prime, 3 or 5; in rank 14 the $2.4 \cdot 10^6$ lines at 3, and the $1.5 \cdot 10^9$ lines at 5 for c01018, exceed its threshold of $10^6$, so that it draws random lines. SageMath works at the smallest prime not dividing $d$, here 7, 7 and 3 on the three genera it ran. The factor between our program and Hecke.jl is from about 20 to several hundred from rank 10 on, and Hecke.jl timed out at 288 classes.

When $d$ is odd (Table 13), the three programs work at the same prime, and from the orbits on the lines, $2^n \leq 2^{18}$. On the small genera, up to about 25 classes, the three are comparable, apart from SageMath from rank 12 on. On the genera of rank 16 and 18 with 33 to 271 classes the factor between our program and Hecke.jl is 20 to 70. This part of the gap does not come from the prime: it comes from the recognition, one canonical form and a dictionary lookup against invariants followed

by isometry tests in Hecke.jl and by equivalence tests against every known class in SageMath, from the scheduling, and from the implementation (the orbits at $p = 2$ on bitmasks, Section 6). The benchmark does not separate these three contributions. The use of $p = 2$ when it divides $d$ thus adds to an advantage that exists without it, and it is what makes the genera of rank 15 to 19 and even determinant reachable at all.

## 9. Open questions

The order in which the graph is explored changes what is obtained, and how fast: the same genus is closed after 833 or 1103 expansions, or not at all in two hours, depending on the order alone, and two runs of the same schedule differing only in the seed of the walk can differ by a factor 2. This raises several questions.

**Question 1.** *How far are the orders from the best possible? An oracle that knows the graph needs far fewer expansions (Section 7.7). Is there an online rule, using only the classes found, their automorphism groups and the Hecke rows already computed, with a guaranteed ratio to that optimum?*

**Question 2.** *The mixed order alternates deficit and* |Aut| *picks in a fixed proportion. Should the proportion adapt during the run, for instance by rewarding the rule whose last picks found new classes, as a bandit problem?*

**Question 3.** *Within one expansion, the orbits are taken in a fixed order, and the expansion stops when the mass closes. Would taking the orbits by increasing size, or by a predicted chance of novelty, shorten the last expansions? Similarly, when should the random walk stop and the expansions start, and is it worth restarting the walk from the classes of large deficit at the end?*

**Question 4.** *The tail of an enumeration consists of a few classes reached through very few points. The missing mass gives* |Aut| *of the missing class when one class is missing, and the Hecke identity makes classes of large* |Aut| *likelier to reach it, but $T(M, L)$ is unknown for the missing $M$. Is there a better guide than the deficit and* |Aut| *to choose the classes to expand at the end?*

## Acknowledgments

I thank Simon Brandhorst and John Voight for useful conversations.

## Tool and computational resource disclosure

Following the Leiden Declaration on Artificial Intelligence and Mathematics [14], we describe the automated tools used.

*Large language model.* Claude Code, with the model Claude Opus 5.5 of Anthropic, was used throughout this work, under the direction of the author: to implement and test the changes to `polyhedral_common` described here (the random walk, the Hecke bookkeeping, the orders of expansion, the dispatch of the lattice methods, the bitmask orbits), to run the benchmarks and the computations of Section 7 and analyse their output, and to draft this manuscript, including its tables and the first versions of the proofs of Lemma 1, Proposition 2, Lemma 2 and Proposition 3. The author takes responsibility for the content.

*Mathematical software.* `polyhedral_common` [16] for all the lattice computations, with FLINT [9] and GMP for the arithmetic and nauty and traces for the canonical labellings; Julia with its standard linear algebra for the spectra of Section 7.7; Hecke.jl and SageMath for the comparison of Section 8; Python for the preparation and the analysis of the data. No proof assistant was used.

*Data and computational resources.* The test data is DefLatDB [7]. All computations ran on a single desktop computer, one process at a time on one core, with a memory cap of 10 GB; the longest single run, the complete neighbour graph of a genus of 2351 classes in rank 17, took about 11 minutes, and the benchmark of Table 11 204 minutes.

## References


[1] E. Assaf, V. Chen, R. Garg and B. Wang, *Efficient enumeration of quadratic lattices*, arXiv:2601.18990 (2026).
[2] S. Brandhorst and T. Hofmann, *Automorphisms and canonical forms of integer lattices*, arXiv:2610.16753 (2026).
[3] G. Chenevier and J. Lannes, *Automorphic forms and even unimodular lattices*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) **69**, Springer, 2019.
[4] G. Chenevier and O. Taïbi, *Unimodular lattices of rank* 29 *and related even genera of small determinant*, preprint, `https://otaibi.perso.math.cnrs.fr/hdiscp.pdf`.
[5] J. H. Conway and N. J. A. Sloane, *Sphere packings, lattices and groups*, 3rd ed., Springer, 1999.
[6] J. H. Conway and N. J. A. Sloane, *Low-dimensional lattices. IV. The mass formula*, Proc. Roy. Soc. London Ser. A **419** (1988), 259–286.
[7] S. Muller, *DefLatDB: a database of genera of definite integer lattices*, `https://github.com/StevellM/DefLatDB`.
[8] M. Dutour Sikirić, A. Haensch, J. Voight and W. P. J. van Woerden, *A canonical form for positive definite matrices*, Proceedings of ANTS XIV, Open Book Series **4** (2020), 179–195.
[9] The FLINT team, *FLINT: Fast Library for Number Theory*, `https://flintlib.org`.
[10] C. Fieker, W. Hart, T. Hofmann and F. Johansson, *Nemo/Hecke: computer algebra and number theory packages for the Julia programming language*, Proceedings of ISSAC '17, ACM (2017), 157–164.
[11] M. Kneser, *Klassenzahlen definiter quadratischer Formen*, Arch. Math. **8** (1957), 241–250.
[12] V. V. Nikulin, *Integral symmetric bilinear forms and some of their applications*, Math. USSR Izv. **14** (1980), 103–167.
[13] W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), 235–265.
[14] *Leiden Declaration on Artificial Intelligence and Mathematics*, 2026, `https://leidendeclaration.ai/`.
[15] O. T. O'Meara, *Introduction to quadratic forms*, Springer, 1963.
[16] M. Dutour Sikirić, *polyhedral_common*, `https://github.com/MathieuDutSik/polyhedral_common`.
[17] W. Plesken and B. Souvignier, *Computing isometries of lattices*, J. Symbolic Comput. **24** (1997), 327–334.
[18] The Sage Developers, *SageMath, the Sage Mathematics Software System*, `https://www.sagemath.org`.
[19] R. Scharlau and B. Hemkemeier, *Classification of integral lattices with large class number*, Math. Comp. **67** (1998), 737–749.
[20] R. Schulze-Pillot, *An algorithm for computing genera of ternary and quaternary quadratic forms*, Proc. ISSAC '91, ACM (1991), 134–143.
[21] J. Voight, *Kneser's method of neighbors*, arXiv:2308.11566 (2023).



Mathieu Dutour Sikirić, MSM-programming, Karlovacka Cesta 28B, 10452 Klinca Selo, Croatia
*Email address*: `mathieu.dutour@gmail.com`