A Focus on Hermite Constant 11

THE CERTIFICATES AND MACADAMIA 0052

Rémi Géraud-Stewart[1] and David Naccache[1,2]

[1] ENS, CNRS, PSL Research University, Paris, France
remi.geraud@ens.fr, david.naccache@ens.fr
[2] Fakultet inženjerskih nauka, Univerziteta u Kragujevcu
6 Sestre Janjić, 34000 Kragujevac, Serbia
david@kg.ac.rs

Abstract. This paper assembles the dimension-eleven argument in a series on the Hermite constants in dimensions ten, eleven and twelve. The root paper reduces a hypothetical lattice of minimum 4 and determinant below 972 to a chain of sections of ranks eleven, ten and nine. Its rank-nine section is marked by a perfect form below an explicit determinant cutoff. The global finite computation leaves $4\,487\,813$ candidate forms and excludes all but ten by certificates. We state the mathematical content of these certificates, describe their data and checking rules, and prove why every valid certificate excludes the corresponding form. The four formats are trace, domain, glue and tree certificates; each tree must cover its entire stated domain. One of the ten remaining cases, `0052:005247066`, is treated here by a complete gluing cover. Five companion papers settle the other nine. We also prove the common inequalities used by those local arguments. The resulting bound is $\gamma_{11} = 4/\sqrt[11]{972}$, conditional on the attributed rank-nine classification, the rank-ten census and the stated global and local finite checks.

Keywords: Hermite constant · Lattice packings · Perfect forms · Voronoi domain · Exact certificates · Branch and bound · Verified computation

1 Introduction

This paper is the second of a series of seven papers, made public concurrently, whose aim is to establish the Hermite constants γ_{10}, γ_{11} and γ_{12}. The root paper of the series [2] recalls the problem, proves γ_{10} in full, derives γ_{12} from γ_{11} and reduces γ_{11} to a statement about perfect forms of rank 9: a hypothetical lattice of rank 11 with minimum 4 and determinant below 972 would contain a chain of sections of ranks 10 and 9, and the section of rank 9 would lie, in the sense of Voronoi, over one of $4\,487\,813$ explicitly known perfect forms. The present paper proves what remains for all these forms but ten, settles one of the ten (the form `0052:005247066`, Appendix E) and points to the five companion papers [3,4,5,6,7] that settle the other nine, grouped by the method that cracks them.

Theorem 1. *Assume Hypothesis 2, the rank-ten result of [2], Computational results 5, 19 and 46, and the finite verification statements of the five companion papers. Every*

lattice of rank 11 *with minimum* 4 *has determinant at least* 972. *Hence*

$$\gamma_{11} = \frac{4}{\sqrt[11]{972}} = 2.1401980\ldots,$$

attained by the lattice K_{11}.

Theorem 1 is Theorem 14 of [2]. Its proof combines the root paper's reduction, the global certificate database, and local rank-eleven arguments for the ten residual forms. Appendix E treats one residual form; the five companion papers treat the other nine. Section 8 assembles these ingredients.

The strategy. A certificate is a finite rational witness whose exact verification establishes a bound throughout a specified region. Section 5 gives the rule for each certificate format and proves its implication. A finite covering tree joins the regional bounds into a global one. Section 7 describes the reproduction procedure and the saved evidence.

Organisation. Section 2 recalls what is taken from [2]: the chain, the constants, the survivors and the way a form is named. Section 3 describes how the candidate forms were selected from the data of [1] and fixes the thresholds against which every certificate is measured. Section 4 states what must be proved for a survivor and the two levels (rank 10, rank 11) at which it can be proved. Section 5 is the heart of this paper: for each kind of certificate, the lemma it rests on, the data it contains, the algorithm that checks it and why a checked certificate excludes the form. Section 6 describes the database, its tables and its counts, and the ten rows that read as separate proofs. Section 7 describes the verifier and the reproduction pack. Section 8 assembles the proof of Theorem 1, states the theorem that the root paper imports from this paper, and lists the hypotheses inherited from [2]. Appendices A–C give the integer form of the thresholds, the layout of the certificates and a snippet that reads the database. The last two appendices leave the certificates for the rank-11 arguments: Appendix D states and proves once the common coordinate system and the common inequalities that the five companion papers use, and Appendix E settles the form `0052:005247066` by a direct certificate for every gluing. Figure 1 shows the whole elimination at a glance.

2 What is taken from the root paper

We recall the definitions of [2, Section 2] and the results of its Sections 5 and 6 used here.

2.1 Definitions

A *lattice* of rank k is $L = B\mathbb{Z}^k$, B a real matrix of rank k; its *Gram matrix* is $Q = B^{\mathsf{T}}B$, its determinant $\det L = \det Q$, its minimum $\min L$ the least squared length of a nonzero vector, and its dual L^* has Gram matrix Q^{-1} in the dual basis. For positive definite Q, $Q[x] = x^{\mathsf{T}}Qx$, $\min Q = \min\{Q[x] : x \in \mathbb{Z}^k \setminus \{0\}\}$ and $\operatorname{Min} Q = \{x \in \mathbb{Z}^k \setminus \{0\} : Q[x] = \min Q\}$. Matrices Q and $U^{\mathsf{T}}QU$ are *equivalent* when U is an integer

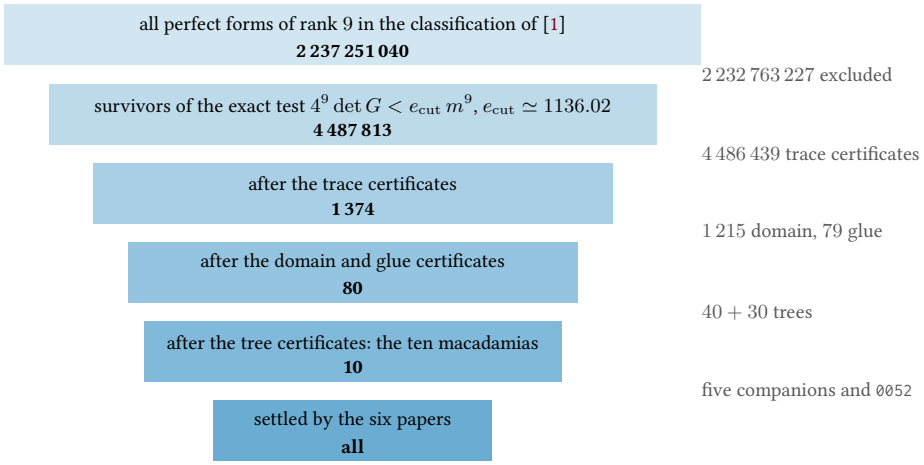

Fig. 1. The elimination of the rank-9 perfect forms (the counts of [2, Table 3]). Each band is one stage; the grey label on the right of a band says how many forms the stage above it excluded, and by which certificates. The test of the second band is decided exactly, as $(4^9 \det G)^{55} < 2^{246}3^{197}m^{495}$ (Section 3); the certificates are those of Section 5, and the database and the verifier of Sections 6 and 7 check every one of them. The ten macadamias are settled in Appendix E (`0052`) and in the five companion papers [3,4,5,6,7].

matrix of determinant ± 1, written $U \in GL_k(\mathbb{Z})$. A positive definite P is *perfect* if the matrices cc^{T}, $c \in \operatorname{Min} P$, span Sym_k, the space of symmetric $k \times k$ matrices. The *Voronoi domain* of a perfect P is the cone

$$\mathcal{D}(P) = \operatorname{cone}\{cc^{\mathsf{T}} : c \in \operatorname{Min} P\} \subset \operatorname{Sym}_k,$$

and Voronoi's theorem [11] (see [8]) says that the domains of the perfect forms of rank k cover the cone of positive definite matrices. Here a cone consists of all finite nonnegative linear combinations of its generators. We scale the initial lattice to minimum 4: by [2, equation (1)], $\gamma_n \le c$ if and only if every lattice of rank n with minimum 4 has determinant at least $(4/c)^n$, and $\gamma_{11} = 4/\sqrt[11]{972}$ is the statement of Theorem 1.

Matrix notation. Write I_k for the identity, e_i for coordinate vectors and $\mathbf{1}$ for the all-one vector. For symmetric matrices, $A \succeq 0$ means $x^{\mathsf{T}}Ax \ge 0$ for every x; $A \succ 0$ means strict positivity for $x \ne 0$, and $A \preceq B$ means $B - A \succeq 0$. The superscript T denotes transpose. The trace $\operatorname{tr} A$ is the sum of the diagonal entries; $\|A\|_F^2 = \operatorname{tr}(A^{\mathsf{T}}A)$ is the squared Frobenius norm, and $\|A\|_{\mathrm{op}} = \sup_{|x|=1} |Ax|$ is the operator norm. For $A \succ 0$, $A^{1/2}$ is its positive definite symmetric square root. We use $(x)_+ = \max(x, 0)$; subscripts $-$ and $+$ on a box coordinate denote its lower and upper endpoints. A primitive sublattice is $M = L \cap \operatorname{span} M$; a primitive vector generates one of rank one.

2.2 The hypothesis and the result for dimension 10

Hypothesis 2 ([2, Hypothesis 2]). The data set of [1] contains, for every perfect positive definite 9×9 matrix, an integral Gram matrix equivalent to a positive multiple of it.

The arguments of this paper use Hypothesis 2 only for the perfect matrices whose determinant at minimum 4 is below e_{cut} (below).

Theorem 3 ([2, Theorem 3]). *Assume Hypothesis 2 and Computational result 9 of [2]. Every lattice of rank* 10 *with minimum* 4 *has determinant at least* 768.

2.3 The chain

Let

$$d_{\mathrm{cut}} = 4\,\sqrt[11]{972^9} = 1113.048\ldots,$$
$$e_{\mathrm{cut}} = \frac{4\,\sqrt[10]{d_{\mathrm{cut}}^9}}{\sqrt[10]{768}} = \sqrt[55]{2^{246}3^{197}} = 1136.021\ldots$$

Proposition 4 (the chain; [2, Proposition 15]). *Assume Theorem 3. Let* L_0 *have rank* 11*, minimum* 4 *and determinant* $D_0 < 972$*. There are a lattice* L *of rank* 11 *with minimum* 4 *and determinant* $\Delta < 972$*, a shortest vector* n_{11} *of* L^* *and a shortest vector* n_{10} *of* M^**, where* $M = L \cap n_{11}^{\perp}$ *and* $N = M \cap n_{10}^{\perp}$ *are sublattices of ranks* 10 *and* 9*, with*

$$\min M \geq 4, \qquad 768 \leq d := \det M < d_{\mathrm{cut}},$$
$$\Delta \geq \frac{3d}{4u} \quad \text{where } u = |n_{10}|^2 = \min M^*,$$
$$\min N \geq 4, \qquad \det N = ud < e_{\mathrm{cut}}.$$

Let $n_{11} \in L^*$ and $n_{10} \in M^*$ be the successive shortest dual normals. We use

$$\Delta = \det L, \qquad d = \det M, \qquad e = \det N,$$
$$v = |n_{11}|^2 = \min L^*, \qquad u = |n_{10}|^2 = \min M^*, \qquad t = \min N^*.$$

An adapted basis gives $d = v\Delta$ and $e = ud$. Rounding a lift across either cut gives $v \leq 4u/3$ and $u \leq 4t/3$; hence

$$\Delta \geq \frac{3d}{4u}, \qquad u \leq \frac{4}{3}t. \tag{1}$$

These identities and inequalities concern the actual chain and are independent of its basis.

The perfect form over N. Let Q be a Gram matrix of N and $X = Q^{-1}$. By Voronoi's theorem X lies in the domain of a perfect form P of rank 9, which we scale to $\min P = 4$. Write $X = \sum_c \lambda_c\, cc^{\mathsf{T}}$ over one representative c of each pair $\pm c$ of $\operatorname{Min} P$, $\lambda_c \geq 0$. Then (as in [2, Proposition 7])

$$\operatorname{tr}(XP) = \sum_c \lambda_c P[c] = 4 \sum_c \lambda_c \leq 9 \qquad \text{and} \qquad \det P \leq \det Q = e, \tag{2}$$

because $9 = \operatorname{tr}(XQ) = \sum_c \lambda_c Q[c] \geq 4 \sum_c \lambda_c$ (every c is a nonzero vector of N, so $Q[c] \geq 4$), and because the nine eigenvalues of $Q^{-1/2} P Q^{-1/2}$ are positive with sum $\operatorname{tr}(XP) \leq 9$, so their product $\det P / \det Q$ is at most 1. We say that the chain, or N, *lies over* P. Thus every chain of Proposition 4 lies over a perfect form P of rank 9 with $\min P = 4$ and $\det P \leq e < e_{\mathrm{cut}}$. By Hypothesis 2, P is equivalent to $(4/\min G)\, G$ for a matrix G of the data set of [1]; if m is the least diagonal entry of G, then $\min G \leq m$ and

$$e_{\mathrm{cut}} > \det P = \frac{4^9 \det G}{(\min G)^9} \geq \frac{4^9 \det G}{m^9}, \tag{3}$$

a condition tested exactly, in integers, as $(4^9 \det G)^{55} < 2^{246} 3^{197} m^{495}$. The matrices G that pass this test are the *survivors*, and Section 3 counts them: there are 4 487 813. For each survivor the minimum $s = \min G$ is computed exactly and the survivor is taken as the form $P = (4/s)\, G$ of minimum 4. Replacing Q by the equivalent Gram matrix $U^{-\mathsf{T}} Q U^{-1}$, where $P = U^{\mathsf{T}} P_{\mathrm{data}} U$, we may and do assume that P *is* the survivor $(4/s)\, G$ in a chosen basis: the quantities Δ, d, e, u, t, v are basis-invariant.

How a form is named. We refer to a survivor by its index in the data set of [1], written `file:row`. The data set (Zenodo record 15707640) is distributed as 64 files `perfect_0000.nc`, …, `perfect_0063.nc` in NetCDF format; each file holds a list of records, and a record consists of an integral Gram matrix G (its 45 entries G_{ij}, $i \leq j$), its scale, its minimum, the number of its neighbours in Voronoi's graph and a few more fields. In `file:row`, `file` is the four-digit number of the file and `row` the position of the record in that file, counted from 0, as the reader distributed with the data addresses it, written with nine digits. Thus `0030:030301719` is the record at position 30 301 719 of the file `perfect_0030.nc`, and the matrix G of that record, scaled to minimum 4, is the form. The three forms of [2, Section 5] are `0030:030301719` (P_Λ, the form of Λ_9), `0019:030884313` (P_S) and `0017:001746552` (P_K, the form KAPPA9.2 of [9]).

2.4 Gluings, and the hypotheses the certificates use

Fix a survivor P, with C one representative of each pair of $\operatorname{Min} P$, and a chain over P with the notation above, in a basis of N in which $X = Q^{-1} \in \mathcal{D}(P)$. Then $M = N \oplus \mathbb{Z} g$ for a vector g whose orthogonal projection onto $N \otimes \mathbb{R}$ has coordinates $\tau \in \mathbb{R}^9$ in that basis and whose component orthogonal to N has squared length $1/u$ (choose the sign of n_{10} so that $n_{10} \cdot g = 1$).

The class of τ modulo $\mathbb{Z}^9$ is the *first gluing*; M is determined by (N, τ, u). Likewise $L = M \oplus \mathbb{Z} g'$, the projection of g' onto $M \otimes \mathbb{R}$ has coordinates $\varphi \in \mathbb{R}^{10}$ in the basis (N, g) of M, the component orthogonal to M has squared length $1/v$, and the class of

φ modulo $\mathbb{Z}^{10}$ is the *second gluing*. For $x \in \mathbb{R}$ let $\|x\|$ be the distance from x to the nearest integer. The certificate rules use the following consequences of the chain.

- **(Domain)** $X = \sum_c \lambda_c\, cc^{\mathsf{T}}$ over $c \in C$ with $\lambda_c \geq 0$, $\sum_c \lambda_c \leq 9/4$ and $\lambda_c \leq 1/4$. (The first bound is (2); for the second, $\lambda_c\, cc^{\mathsf{T}} \preceq X$ applied to the vector Qc gives $\lambda_c Q[c]^2 \leq Q[c]$, so $\lambda_c \leq 1/Q[c] \leq 1/4$.) Hence, for every positive semidefinite G',
$$\operatorname{tr}(XG') = \sum_c \lambda_c G'[c] \leq \frac{S_9(G')}{4}, \tag{4}$$
where $S_9(G')$ is the sum of the nine largest values $G'[c]$, $c \in C$ (at most nine of the λ_c can be as large as $1/4$, and their sum is at most $9/4$).
- **(T)** Every nonzero $z \in \mathbb{Z}^9$ is a nonzero vector of N^* in the dual basis, so $X[z] \geq t$.
- **(L2)** Every nonzero vector of M^* has norm at least u. In coordinates: a vector $z \in \mathbb{Z}^9$ of N^* lifts to the vectors $z + (k - z\cdot\tau)\, n_{10}$ of M^*, $k \in \mathbb{Z}$ (they have integer products with N and with g, and $n_{10}\cdot g = 1$), so for $z \in \mathbb{Z}^9$ and $k \in \mathbb{Z}$ not both zero,
$$X[z] + u\,(k - z\cdot\tau)^2 \geq u, \qquad \text{in particular} \qquad X[z] \geq u\left(1 - \|z\cdot\tau\|^2\right)\ (z \neq 0).$$
- **(L3)** Every nonzero vector of L^* has norm at least v: for $\zeta = (z, k) \in \mathbb{Z}^{10}$ and $k' \in \mathbb{Z}$ not all zero, $X[z] + u\,(k - z\cdot\tau)^2 + v\,(k' - \zeta\cdot\varphi)^2 \geq v$ (the same lifting, one level up).
- **(M)** Every nonzero vector of M has norm at least 4; in coordinates, for $(x, k) \in \mathbb{Z}^{10} \setminus \{0\}$, $Q[x + k\tau] + k^2/u \geq 4$. Every nonzero vector of N has norm at least 4.
- **(u)** $\det P/d_{\mathrm{cut}} \leq u \leq \sqrt[5]{4/3}$. The lower bound: $e \geq \det P$ by (2) and $e = ud$ with $d < d_{\mathrm{cut}}$. The upper bound is Theorem 3 applied to M^*, as in the proof of Proposition 4: $u\,\sqrt[10]{d} \leq 4/\sqrt[10]{768}$ and $d \geq 768$. Also $v \leq 4u/3$.
- **(Symmetry)** For $V \in \mathrm{Aut}(P) = \{V \in GL_9(\mathbb{Z}) : VPV^{\mathsf{T}} = P\}$, the change of basis V maps chains over P to chains over P with the same d, Δ, u, v and first gluing $V^{-\mathsf{T}}\tau$; and τ is defined modulo $\mathbb{Z}^9$. The affine group Γ generated by these changes of basis and the integer translations acts on first gluings and preserves the chain conditions.

The conventions of the data: a matrix G acts on row vectors, $G' = UGU^{\mathsf{T}}$ is the form in the basis U, and Aut is written accordingly.

3 The candidate forms

The exact selection input. For a raw form G, write $\delta_G = \det G$ and $m = \min_i G_{ii}$. The exact rank-eleven test is $(4^9\delta_G)^{55} < 2^{246}3^{197}m^{495}$, as in (3). Integer elimination computes δ_G exactly. Since $\min G \leq m$, the test retains every form below e_{cut}. The selection is computed exactly, record by record, by the reproduction pack of Section 7.1; the next paragraph describes how.

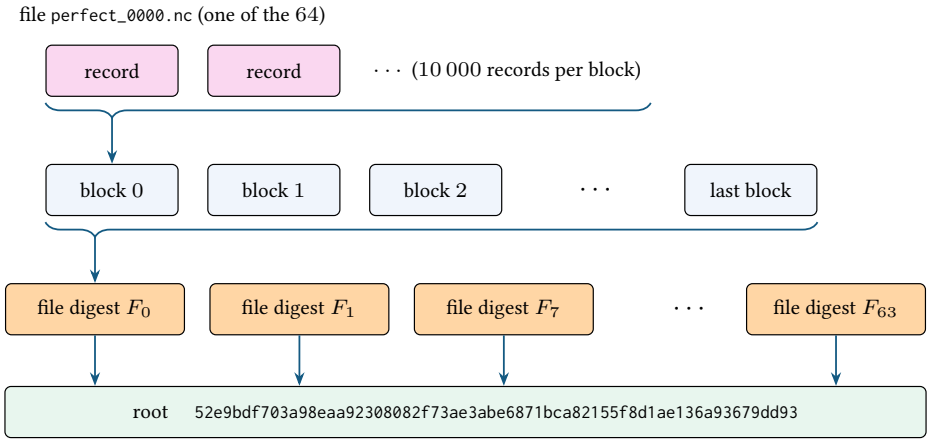

Fig. 2. The hashed transcript of the exact census. The phases **ten** and **verify B** of the reproduction pack (Section 7.1) both write it, and their roots are equal: the two scans read the same records and take the same decisions. A reader can recheck any part of the census without rerunning it. **One record** contributes the line `file:row:m:scale:det:t814:tc9` (its exact decisions) and its 90 raw bytes. **One block** of 10 000 consecutive records gives one SHA-256 digest (the last block of a file may hold fewer records). **The file digest** hashes the block digests of a file; **the root** hashes the 64 file digests. **Checking:** `exact_census.py check` recomputes chosen blocks (for instance 50 at random) from the data set and compares them, checks that each file digest hashes its block digests, and recomputes the root from the file digests: one block takes under a second, a file minutes.

3.1 The scan of the data set

The data set of [1] holds 2 237 251 040 records in the 64 files of Section 2.3. Each file is a NetCDF file with one unlimited dimension, `number_ctype`, and, among its variables, `form` (45 signed 16-bit integers per record: the *lower* triangle of G, row by row, that is G_{11}; G_{21}, G_{22}; G_{31}, G_{32}, G_{33}; . . .), `scale`, `minQ` (the number of pairs of minimal vectors), `uid`, `autQ` and `neighbours`. (The database of Section 6 stores the same 45 entries in the other order, the *upper* triangle row by row.) The scan decides every record exactly: the module `exact_census.py` of the reproduction pack computes δ_G by fraction-free (Bareiss) elimination in integers of unbounded size and compares the two sides of (3) as integers; no floating-point value takes part in any decision. Every record also enters a hashed transcript: the line `file:row:m:scale:det:t814:tc9` of its decisions and the 90 bytes of the record are fed to SHA-256, one digest is kept per block of 10 000 consecutive records, the digests of a file are hashed into the file digest and the 64 file digests into the root (Figure 2). The run of Section 7.1 has root `52e9bdf703a98eaa92308082f73ae3abe6871bca82155f8d1ae136a93679dd93`; any block is recomputed and compared in under a second, a file in minutes. An independent implementation of the same exact scan gave the same root. Exactly 4 487 813 records pass the test, and they are the keys of the database (Computational result 19).

Computational result 5. Exactly $4\,487\,813$ of the $2\,237\,251\,040$ records of [1] pass the test (3). For each of them the minimum $s = \min G$ was computed exactly (LLL reduction followed by Fincke–Pohst enumeration in integers). The keys `file:row` of these records are the keys of the database of Section 6.

The scan is the only step of the paper that touches the data set, and its filtering is repeated by the verifier (Section 7), which also checks that the survivors are exactly the keys of the database: the same number, the same keys, the same Gram matrices. The list of survivors was selected with the field `scale` of each record, which equals $\min G$ on every record selected; the verifier applies the test with the least diagonal entry m as in (3), which needs no minimum, and compares the field `scale` with the database. The two selections give the same $4\,487\,813$ keys (Computational result 19).

3.2 The thresholds, in integers

Three irrational constants appear in the certificates:

$$d_{\mathrm{cut}} = 4\,\sqrt[11]{972^9} \simeq 1113.0488, \qquad T_Q = \frac{16}{3}\,\sqrt[11]{972^9} \simeq 1484.0651,$$
$$T_1 = T_Q\Big(\frac{9}{10}\Big)^{10} \simeq 517.4615.$$

d_{cut} is the bound on d of Proposition 4; $T_Q = 4d_{\mathrm{cut}}/3$ is the bound on e/t of (1); and T_1 is T_Q divided by the factor $(10/9)^{10}$ of the trace lemma (Section 5.2). The eleventh powers $d_{\mathrm{cut}}^{11} = 4^{11}972^9$ and $T_Q^{11} = (16/3)^{11}972^9$ are rational, and T_1^{11} is rational too. So every comparison of a positive rational $x = n/m$ with one of them is a comparison between integers:

$$\begin{aligned} x \ge d_{\mathrm{cut}} &\iff n^{11} \ge 4^{11}\,972^9\,m^{11}, \\ x \ge T_Q &\iff (3n)^{11} \ge 16^{11}\,972^9\,m^{11}, \\ x \ge T_1 &\iff n^{11}\,3^{11}\,10^{110} \ge m^{11}\,16^{11}\,972^9\,9^{110}, \end{aligned} \tag{5}$$

and for the third level (Section 5.9) $x \ge 972 \iff n \ge 972\,m$. We write $\mathrm{ge}_{d_{\mathrm{cut}}}(n,m)$, $\mathrm{ge}_{T_Q}(n,m)$, $\mathrm{ge}_{T_1}(n,m)$ and $\mathrm{ge}_{972}(n,m)$ for these four tests. Likewise $e_{\mathrm{cut}}^{55} = 2^{246}3^{197}$ in (3), and the bounds of (u) are tested as $(4u_0)^{11}\,972^9 \le (\det P)^{11}$ and $3u_1^5 \ge 4$. These certificate comparisons use exact arithmetic; floating point may be used to *find* certificates.

4 What must be proved for a survivor

By Proposition 4 and Section 2.3, Theorem 1 follows once the following is shown for each survivor P.

> **(E)** Every chain $L \supset M \supset N$ over P with $\min L = 4$ (Section 2.4) has $\Delta \ge 972$.

Indeed, a lattice of rank 11 with minimum 4 and determinant below 972 gives, by Proposition 4, a chain with $\Delta < 972$, which lies over some survivor. There are two levels at which (E) can be proved, as explained in [2, Section 6.2].

At rank 10. One shows that *no lattice M of the chain lies over P at all*: every chain over P has $d \geq d_{\mathrm{cut}}$ (or, stronger, every N over P has $e/t \geq T_Q$), which contradicts Proposition 4 or (1). This is a statement about M and N only; it does not involve the second gluing, and the lemmata of Section 5 give it the form of exact certificates: a trace or a domain certificate proves $e/t \geq T_Q$ for every N over P (whatever M is), a glue certificate proves $d \geq d_{\mathrm{cut}}$ for every chain over P, and a tree certificate proves $d \geq d_{\mathrm{cut}}$ region by region over a finite cover of the first gluings.

At rank 11. For ten survivors no statement at rank 10 can be true, because an actual lattice M of rank 10 with minimum 4 and determinant below d_{cut} lies over them (Λ_{10} over Λ_9, sections of K_{11}, and so on; Table 3). For these, (E) must be proved at the level of L, where the bound 972 is attained by K_{11}. The database can hold certificates at this level too (the leaves of kind `three` of Section 5.9 prove $\Delta \geq 972$ on a region of first gluings, whatever the second gluing), but for the ten macadamias the proof is given outside the database: in Appendix E for `0052:005247066` and in the five companion papers [3,4,5,6,7] for the other nine; the database records this (Section 6.4).

Lemma 6. *Let P be a survivor. Each of the following implies (E):*

- a *every positive definite Q with $\min Q \geq 4$ and $Q^{-1} \in \mathcal{D}(P)$ has $\det Q \geq T_Q \min Q^{-1}$;*
- b *every chain over P has $d \geq d_{\mathrm{cut}}$;*
- c *every chain over P has $d \geq d_{\mathrm{cut}}$ or $\Delta \geq 972$.*

Proof. A chain over P with $\Delta < 972$ has $d < d_{\mathrm{cut}}$ (Proposition 4) and $e/t < T_Q$ (equation (1)), and its N has a Gram matrix Q with $\min Q \geq 4$, $Q^{-1} \in \mathcal{D}(P)$, $\det Q = e$ and $\min Q^{-1} = t$. Each of a, b, c contradicts one of these. □

The certificates of kinds trace and domain prove a, those of kinds glue and tree prove b, and a tree with leaves of the third level proves c.

5 The taxonomy of certificates

Figure 3 lists the kinds side by side.

5.1 Conventions common to all kinds

Exact short-vector enumeration. For a rational positive definite Gram matrix A, a factorisation $A = LDL^{\mathsf{T}}$, with L unit lower triangular and D positive diagonal, writes

$$A[z] = \sum_i D_{ii}\big(z_i + \sum_{j>i} L_{ji} z_j\big)^2.$$

Given $A[z] \leq R$, choose $z_n, z_{n-1}, \ldots, z_1$ in that order. At each stage the remaining nonnegative terms give a finite interval for the next integer coordinate. Enumerating those intervals and testing the resulting vectors gives the complete list. This is the bounded enumeration used here (Fincke–Pohst enumeration). The preceding LLL

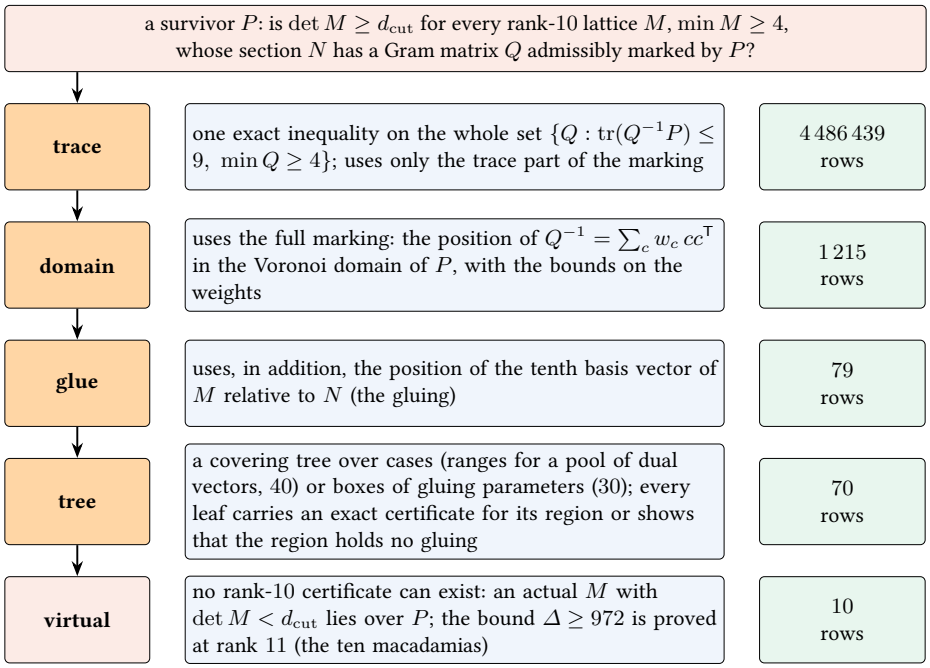

Fig. 3. The kinds of certificate of the database (this section and [2, Section 6.2]), each with what it uses and the number of rows of that kind (Table 2).

(Lenstra–Lenstra–Lovász) basis reduction is a change of basis by an integer matrix of determinant ± 1; all reported basis changes are checked exactly. See [8] for these lattice algorithms.

Every certificate refers to the survivor through the record (G, s) of the data, $s = \min G$, and names an integer matrix U with $|\det U| = 1$; the form is used in the basis U, that is, as $G' = UGU^{\mathsf{T}}$ and $P = (4/s)\, G'$, and C is the set of minimal vectors of G', one per pair $\pm c$, recomputed exactly by the checker from G' alone (LLL reduction, then Fincke–Pohst enumeration in integers). The vectors z_i of a certificate are integer vectors of $\mathbb{Z}^9$, read as vectors of N^* in the dual of the basis U; the quadratic form Y of a certificate is given as $Y = H/D$ with an integer symmetric matrix H and an integer $D > 0$, and its weights as $w_i = c_i/D$ with integers $c_i \geq 0$. For a certificate (Y, w) and $c \in C$ let

$$g(c) = Y[c] + \sum_i w_i\, (z_i \cdot c)^2, \qquad S_9 = S_9(Y, w).$$

Here S_9 is the sum of the nine largest values $g(c)$, so $D\, g(c) = H[c] + \sum_i c_i (z_i \cdot c)^2$ is an integer and $\Sigma := D\, S_9$ is the sum of the nine largest of these integers. For an integer symmetric matrix, "positive definite with determinant δ" is decided by fraction-free (Bareiss) elimination without pivoting: the pivots are the leading principal minors, all of which must be positive (Sylvester's criterion), the last one being δ. The tests $\mathrm{ge}_{d_{\mathrm{cut}}}$, ge_{T_Q}, ge_{T_1}, ge_{972} are those of (5). The first step of every verification but that of

Algorithm 1 Verification of a trace certificate

Input: G, s, $\{U, z, c, D, (x)\}$

1: **reject** unless $|\det U| = 1$, $D > 0$, every $c_i \in \mathbb{Z}_{>0}$, every $z_i \in \mathbb{Z}^9 \setminus \{0\}$
2: **reject** unless $\min_i G_{ii} \le s$, or $x \neq 0$ is given with $G[x] \le s$ ▷ some vector has norm $\le s$
3: $H \leftarrow D\,UGU^{\mathsf T} - \sum_i c_i z_i z_i^{\mathsf T}$ ▷ integers
4: **reject** unless H is positive definite; $\delta \leftarrow \det H$
5: **accept** iff $\mathrm{ge}_{T_1}\left(4^{10}(\sum_i c_i)\,\delta,\ s^{10}D^{10}\right)$ ▷ $W \det R \ge T_1$, so $e/t \ge (10/9)^{10} W \det R \ge T_Q$

a trace certificate is the same ("Algorithm 0" below): reject unless $|\det U| = 1$ (exact determinant); let $G' = UGU^{\mathsf T}$ and reject unless $\min G = s$ exactly; compute C, the set of all $c \in \mathbb{Z}^9$ with $G'[c] = s$, one per pair $\pm c$, by exact enumeration, and reject unless $|C| \ge 9$.

5.2 Trace certificates

The lemma. This is Lemma 11 of [2], with $t = \min Q^{-1}$ in place of the u of that paper.

Lemma 7 (trace lemma; [2, Lemma 11]). *Let P, Q be positive definite 9×9 matrices with $\mathrm{tr}(Q^{-1}P) \le 9$, and $t = \min Q^{-1}$. Let $z_i \in \mathbb{Z}^9 \setminus \{0\}$ and $\omega_i > 0$ ($i = 1, \dots, k$), let $W = \sum \omega_i$, and suppose $R = P - \sum \omega_i z_i z_i^{\mathsf T}$ is positive definite. Then $\det Q \ge (10/9)^{10}\, W \det R \cdot t$.*

The certificate. `zlib`(JSON {`"U"`, `"z"`, `"c"`, `"D"`}, optionally `"x"`): the basis U, vectors z_i, positive integers c_i and a positive integer D such that, in the coordinates $G' = UGU^{\mathsf T}$,

$$D\,G' = H + \sum_i c_i\, z_i z_i^{\mathsf T}, \qquad H \text{ positive definite.}$$

Then $P = R + \sum_i w_i z_i z_i^{\mathsf T}$ with $R = \frac{4}{sD} H$ and $w_i = \frac{4c_i}{sD}$, and

$$W \det R = \frac{4^{10}\,(\sum_i c_i)\,\det H}{s^{10} D^{10}}.$$

The certificates were found by maximising $\log(\sum w_i) + \log\det(P - \sum w_i z_i z_i^{\mathsf T})$ over short vectors z_i of G' in floating point and rounding the weights to integers with a margin.

The check (Algorithm 1; the function `verify_trace` of the verifier, about thirty lines of Python that need no library). The role of s deserves a word: the value $W \det R$ above decreases when s is replaced by a larger number, so the check is valid as soon as *some* nonzero vector of G has norm at most s; the checker does not compute $\min G$ for this kind. If no diagonal entry of G is at most s, the certificate names a vector x with $G[x] \le s$.

Algorithm 2 Verification of a domain certificate

Input: G', C (Algorithm 0), $\{H, D, z, c\}$

1: **reject** unless $D > 0$, H positive definite ($\delta = \det H$), all $c_i > 0$, all $z_i \neq 0$, $|C| \geq 9$
2: **for** $c \in C$ **do** $\gamma(c) \leftarrow H[c] + \sum_i c_i (z_i \cdot c)^2$ ▷ integer $= D\, g(c)$
3: **end for**
4: $\Sigma \leftarrow$ sum of the nine largest $\gamma(c)$ ▷ $= D\, S_9$
5: **accept** iff $\mathrm{ge}_{T_Q}\left(40^{10}(\sum_i c_i)\,\delta,\ \Sigma^{10}\right)$ ▷ $(40/S_9)^{10} W \det Y \geq T_Q$

Why it excludes the form. Let $s' = \min G \leq s$, so that the survivor is $P = (4/s')G'$. Then $P = R' + \sum_i w_i' z_i z_i^{\mathsf{T}}$ with $R' = \frac{4}{s'D} H \succ 0$, $w_i' = \frac{4c_i}{s'D} > 0$, and $W' \det R' = \frac{4^{10}(\sum c_i)\det H}{s'^{10} D^{10}} \geq \frac{4^{10}(\sum c_i)\det H}{s^{10} D^{10}} \geq T_1$.
For every N over P with Gram matrix Q, $\mathrm{tr}(Q^{-1}P) \leq 9$ by (2), so Lemma 7 gives $e/t \geq (10/9)^{10} T_1 = T_Q$: this is Lemma 6 a.

5.3 Domain certificates

The lemma. The trace lemma uses $\mathrm{tr}(Q^{-1}P) \leq 9$ only. The domain lemma uses the finer information (Domain) that $X = Q^{-1}$ lies in the Voronoi domain of P, through (4).

Lemma 8 (domain lemma). *Let P be a survivor, C its minimal vectors (one per pair). Let Y be positive definite, $z_i \in \mathbb{Z}^9 \setminus \{0\}$, $w_i \geq 0$ with $W = \sum_i w_i > 0$, and $S_9 = S_9(Y, w)$. Then every positive definite Q with $\min Q \geq 4$ and $Q^{-1} \in \mathcal{D}(P)$ satisfies, with $e = \det Q$ and $t = \min Q^{-1}$,*

$$\frac{e}{t} \;\geq\; \left(\frac{40}{S_9}\right)^{10} W \det Y.$$

Proof. Let $G' = Y + \sum_i w_i z_i z_i^{\mathsf{T}} \succeq 0$; then $G'[c] = g(c)$ and $S_9(G') = S_9$. By (4), $\mathrm{tr}(XY) + \sum_i w_i X[z_i] = \mathrm{tr}(XG') \leq S_9/4$, and by (T) $\sum_i w_i X[z_i] \geq tW$. The nine eigenvalues of $X^{1/2} Y X^{1/2}$ and the number tW are ten positive numbers with sum at most $S_9/4$ and product $\det X \det Y \cdot tW = t\, W \det Y / e$. By AM–GM the product is at most $(S_9/40)^{10}$. □

The certificate. `zlib`(JSON {`"basis_U"`, `"H"`, `"D"`, `"vectors"`, `"weights"`}): $Y = H/D$ and $w_i = c_i/D$ on the vectors z_i. The certificates were found by solving the convex program "maximise $\log\det Y + \log\sum w_i$ subject to $S_9(Y, w) \leq 40$" by an interior-point method and rounding to $D = 10^{12}$.

The check (Algorithm 2; functions `verify_certificate2` and `cert2_value`). The value of the lemma is computed as one fraction of integers:

$$\left(\frac{40}{S_9}\right)^{10} W \det Y = \left(\frac{40D}{\Sigma}\right)^{10} \frac{\sum_i c_i}{D} \frac{\delta}{D^9} = \frac{40^{10}(\sum_i c_i)\,\delta}{\Sigma^{10}}.$$

Why it excludes the form. Lemma 8 gives $e/t \geq T_Q$ for every Q of Lemma 6 a.

5.4 Glue certificates

The lemma. The glue lemma uses the position of the tenth basis vector g of M relative to N: the first gluing τ enters through (L2), $X[z] \geq u(1 - \|z \cdot \tau\|^2)$.

Lemma 9 (glue lemma). *Let P, C, Y, z_i, w_i, S_9 be as in Lemma 8, and let $m > 0$ be a number such that*

$$m \;\leq\; \sum_i w_i\big(1 - \|z_i \cdot \tau\|^2\big) \qquad \text{for every } \tau \in \mathbb{R}^9. \tag{6}$$

Then every chain over P has $d = \det M \geq (40/S_9)^{10}\, m \det Y$.

Proof. As in Lemma 8, $\operatorname{tr}(XY) + \sum_i w_i X[z_i] \leq S_9/4$; by (L2) the second term is at least $u\sum_i w_i(1 - \|z_i \cdot \tau\|^2) \geq um$. The nine eigenvalues of $X^{1/2}YX^{1/2}$ and the number um have sum at most $S_9/4$ and product $\det X \det Y \cdot um = m \det Y/d$, since $\det X = 1/e = 1/(ud)$. AM–GM. □

Lemma 10 (a valid m). *Let $\mathcal{T}$ be a set of triples $T = (i, j, k)$, $i < j < k$, with $z_i \pm z_j \pm z_k = 0$ for some choice of signs, let $\alpha_T \geq 0$, and $\beta_i = \max\big(0,\, w_i - \sum_{T \ni i} \alpha_T\big)$. Then*

$$m = W - \frac{1}{2}\sum_T \alpha_T - \frac{1}{4}\sum_i \beta_i$$

satisfies (6).

Proof. Let $r_i = \|z_i \cdot \tau\|^2 \leq 1/4$. For $T = (i, j, k)$, $z_k \cdot \tau \equiv \pm z_i \cdot \tau \pm z_j \cdot \tau$ modulo 1, and $\|x\|^2 + \|y\|^2 + \|x \pm y\|^2 \leq 1/2$ for real x, y; so $r_i + r_j + r_k \leq 1/2$.
Since $w_i \leq \beta_i + \sum_{T \ni i} \alpha_T$, $\sum_i w_i r_i \leq \sum_i \beta_i r_i + \sum_T \alpha_T (r_i + r_j + r_k) \leq \frac{1}{4}\sum_i \beta_i + \frac{1}{2}\sum_T \alpha_T$. □

The certificate. `zlib`(JSON) with the keys `"basis_U"`, `"H"`, `"D"`, `"vectors"`, `"weights"`, `"triangles"`, `"alpha"`: $Y = H/D$, $w_i = c_i/D$, the list $\mathcal{T}$ of triangles as index triples, and $\alpha_T = a_T/D$ with integers $a_T \geq 0$. (Some rows also carry the value found by the search; the checker recomputes it and does not read it.) The certificates were found by a joint convex program in (Y, w, α).

The check (Algorithm 3; `verify_glue_certificate`, `glue_value`). With $m_4 = 4\sum c_i - 2\sum a_T - \sum \beta_i$ (integers), $m = m_4/(4D)$ and the exact value is $40^{10} m_4\, \delta/(4\Sigma^{10})$.

Why it excludes the form. Lemmata 10 and 9 give $d \geq d_{\mathrm{cut}}$ for every chain over P: Lemma 6 b.

Algorithm 3 Verification of a glue certificate

Input: $G', C, \{H, D, z, c, \mathcal{T}, a\}$

reject unless $D > 0$, $c_i \geq 0$, $a_T \geq 0$, $z_i \neq 0$, H positive definite (δ)
for $T = (i, j, k) \in \mathcal{T}$ **do reject** unless $i < j < k$ and $z_i \pm z_j \pm z_k = 0$ for some signs
    $\mathrm{cov}_i \mathrel{+}= a_T$, $\mathrm{cov}_j \mathrel{+}= a_T$, $\mathrm{cov}_k \mathrel{+}= a_T$
end for
$\beta_i \leftarrow \max(0, c_i - \mathrm{cov}_i)$; $m_4 \leftarrow 4\sum_i c_i - 2\sum_T a_T - \sum_i \beta_i$; **reject** unless $m_4 > 0$
$\Sigma \leftarrow$ sum of the nine largest $H[c] + \sum_i c_i (z_i \cdot c)^2$, $c \in C$
accept iff $\mathrm{ge}_{d_{\mathrm{cut}}}\left(40^{10} m_4\, \delta,\ 4\, \Sigma^{10}\right)$ ▷ $(40/S_9)^{10} m \det Y \geq d_{\mathrm{cut}}$

5.5 Trees: the general shape

A single glue certificate must work for every first gluing at once. A *tree certificate* cuts the space of first gluings into regions and gives each region its own certificate. Two families are used: *trees of cases*, whose regions are ranges of the numbers $r_i = \|z_i \cdot \tau\|$ for a pool of dual vectors z_i, and *trees of boxes*, whose regions are boxes of first gluings τ in suitable coordinates. In both, a tree is a binary tree: an inner node splits its region by a hyperplane into two closed regions that cover it, and a leaf carries a certificate valid on its region, or a proof that the region contains no gluing at all. The root region contains a representative of the first gluing of every chain over P (modulo the symmetries used, Section 5.8).

Lemma 11 (tree argument). *Suppose the leaves of a tree cover the root region, and every leaf carries one of: a proof that its region contains no first gluing of a chain over P; a certificate that every chain over P with first gluing in the region has $d \geq d_{\mathrm{cut}}$; or a certificate that every such chain has $\Delta \geq 972$. Then every chain over P has $d \geq d_{\mathrm{cut}}$ or $\Delta \geq 972$, so (E) holds for P.*

Proof. A chain over P has its first gluing (or a symmetric image of it) in the root region, hence in some leaf. The leaf is not of the first kind, so the chain satisfies the certificate of the leaf. Lemma 6 c. □

The certificates on the regions quantify over *all* N with $X \in \mathcal{D}(P)$, all u and v: every lemma below uses X only through (Domain), so one leaf is valid for every X. The tree splits the first gluing only. A tree is accepted only if a the cuts are checked to split each region into two regions that cover it, b every leaf verifies on its region and c the number of leaves equals the number recorded in the head of the certificate.

5.6 Trees of cases

Regions. A region is a vector of intervals $a_i \leq r_i \leq b_i$, $r_i = \|z_i \cdot \tau\| \in [0, \frac{1}{2}]$, with a_i, b_i multiples of $\frac{1}{64}$; the root region is $[0, \frac{1}{2}]$ for every pool vector. An inner node $\{$`"v"`$: i,$ `"at"`$: x,$ `"le"`, `"ge"`$\}$ splits the region by $r_i \leq x$ and $r_i \geq x$.

The lemma. In a region, every τ satisfies: a $a_i \le r_i \le b_i$; b for every triangle $T = (i,j,k)$ of the pool, the *perimeter row* $r_i + r_j + r_k \le 1$ and the three rows $r_i \le r_j + r_k$, $r_j \le r_i + r_k$, $r_k \le r_i + r_j$ (because $z_i \cdot \tau \equiv \pm z_j \cdot \tau \pm z_k \cdot \tau$, $\|x+y\| \le \|x\| + \|y\|$ and $\|x\| + \|y\| + \|x+y\| \le 1$); c $r_i^2 \le (a_i + b_i) r_i - a_i b_i$ (the chord lies above the parabola on $[a_i, b_i]$).

Lemma 12 (bound on a region). *Let $\nu_{\mathrm{row}} \ge 0$ be multipliers on the rows of b, $\mu_i^- \ge 0$, let $\mathrm{cov}_i = \sum_{\mathrm{rows}} \nu_{\mathrm{row}} \cdot$ (coefficient of r_i in the row) and $\mu_i^+ = \max\bigl(0,\ w_i(a_i + b_i) + \mu_i^- - \mathrm{cov}_i\bigr)$. Then*

$$m = \sum_i w_i (1 + a_i b_i) - \sum_i \mu_i^+ b_i + \sum_i \mu_i^- a_i - \sum_{\text{perimeter rows}} \nu_{\mathrm{row}}$$

satisfies $m \le \sum_i w_i (1 - r_i^2)$ for every τ of the region; hence, if $m > 0$, Lemma 9 gives $d \ge (40/S_9)^{10} m \det Y$ for every chain over P whose first gluing lies in the region.

Proof. By c, $\sum_i w_i r_i^2 \le \sum_i w_i (a_i + b_i) r_i - \sum_i w_i a_i b_i$. Since $\mu_i^+ \ge w_i(a_i + b_i) + \mu_i^- - \mathrm{cov}_i$ and $r_i \ge 0$, $\sum_i w_i (a_i + b_i) r_i \le \sum_i (\mu_i^+ - \mu_i^- + \mathrm{cov}_i) r_i$. Now $\sum_i \mathrm{cov}_i r_i = \sum_{\mathrm{rows}} \nu_{\mathrm{row}} (\mathrm{row} \cdot r) \le \sum_{\text{perimeter rows}} \nu_{\mathrm{row}}$ by b, $\mu_i^+ r_i \le \mu_i^+ b_i$ and $-\mu_i^- r_i \le -\mu_i^- a_i$ by a. Collecting terms gives the claim. The last sentence is Lemma 9, whose proof uses (6) only at the τ of the chain. □

The short-vector improvement. Applying the minimum-four condition to one vector of N or M strengthens Lemma 9 by an explicit factor.

Lemma 13 (short-vector improvement). *In the setting of Lemma 9 (a certificate (Y, w) and a number $m > 0$ satisfying (6) on a set of first gluings), let $(x, k) \in \mathbb{Z}^{10} \setminus \{0\}$ and, for a chain whose first gluing τ lies in the set, let $s = S_9 / \bigl(10\,(Y[x + k\tau] + mk^2)\bigr)$. If $s \ge 1$ then*

$$d \ \ge\ \Bigl(\frac{40}{S_9}\Bigr)^{10} m \det Y \cdot E(s), \qquad E(s) = s\Bigl(\frac{9}{10 - \frac{1}{s}}\Bigr)^9 = \frac{9^9 s^{10}}{(10s - 1)^9}.$$

$E(1) = 1$ and E increases with s. For $k = 0$ and $x = c \in C$ this reads $s = S_9/(10\,Y[c])$, independent of τ.

Proof. Let $\sigma = S_9/4$, $\mathsf{D} = \mathrm{diag}(X, u)$ (so $\det \mathsf{D} = u \det X = 1/d$) and $\mathsf{D}_0 = (\sigma/10)\,\mathrm{diag}(Y^{-1}, 1/m)$. The proof of Lemma 9 gives $\mathrm{tr}(\mathsf{D}_0^{-1}\mathsf{D}) = (\mathrm{tr}(YX) + um)\,10/\sigma \le 10$. Let $Z = \mathsf{D}_0^{-1/2} \mathsf{D} \mathsf{D}_0^{-1/2}$, so $\mathrm{tr}\, Z \le 10$, and $y = \mathsf{D}_0^{-1/2}(x + k\tau, k)$. Then $|y|^2 = (10/\sigma)(Y[x + k\tau] + mk^2) = 4/s$ and $y^{\mathsf{T}} Z^{-1} y = Q[x + k\tau] + k^2/u$, the norm of a nonzero vector of M, which is at least $4 = s|y|^2$ by (M). So Z^{-1} has an eigenvalue at least s and Z an eigenvalue $\zeta \le 1/s \le 1$. The other nine eigenvalues of Z have sum at most $10 - \zeta$, so $\det Z \le \zeta\bigl((10 - \zeta)/9\bigr)^9 \le (1/s)\bigl((10 - 1/s)/9\bigr)^9$, as $x(10 - x)^9$ increases on $(0, 1]$. Finally $\det \mathsf{D} = \det \mathsf{D}_0 \det Z$ with $\det \mathsf{D}_0 = (S_9/40)^{10}/(m \det Y)$. □

The programs take for c the minimal vector of P with the least $Y[c]$; in a tree of boxes a leaf may name a vector (x, k) of M instead (Section 5.7). $E(s)$ is a rational function of the integers of the certificate and is evaluated exactly.

Algorithm 4 Verification of a tree of cases

Input: G', C; pool Z (nonzero vectors), $\mathcal{T}$ (each a true relation, $i<j<k$); the tree

function CHECK(node, a, b)
  if node is a certificate $\{H, D, w, \nu, \mu^-\}$ **then**
    require $0 \le a_i \le b_i \le \frac{1}{2}$, $D>0$, $H \succ 0$ (δ), all integers ≥ 0; compute exactly the m of Lemma 12 as a fraction; **require** $m>0$
    $\Sigma \leftarrow$ sum of the nine largest $H[c]+\sum_i c_i(z_i\cdot c)^2$; $q \leftarrow 10\min_{c\in C} H[c]$
    $E \leftarrow 9^9\Sigma^{10}/\big(q\,(10\Sigma-q)^9\big)$ if $\Sigma>q$, else 1 ▷ Lemma 13 with $s=\Sigma/q$
    return $\mathrm{ge}_{d_{\mathrm{cut}}}\big((40/S_9)^{10}\, m \det Y\cdot E\big)$ ▷ as a fraction in integers
  else if node is {empty: S} **then return** $|\det(z_i)_{i\in S}|=1$ and the region contains no gluing (the 256-sign test above)
  else if node is $\{v{:}\,i,\ at{:}\,x,\ le,\ ge\}$ with $a_i\le x\le b_i$ **then**
    return CHECK(le, a, $b|_{b_i=x}$) **and** CHECK(ge, $a|_{a_i=x}$, b)
  else return false ▷ an open node is not a certificate
  end if
end function
accept iff CHECK(root, 0, $\frac{1}{2}$) and the number of leaves equals the number recorded

Empty regions. The bounds of a region need not be compatible with the fact that $\tau\mapsto z\cdot\tau$ is a homomorphism $\mathbb{Z}^9\to\mathbb{R}/\mathbb{Z}$. A leaf $\{$`"empty"`$: S\}$ names nine pool vectors $z_{S_1},\dots,z_{S_9}$ forming a basis of $\mathbb{Z}^9$ ($|\det|=1$); write $z_i=\sum_j\gamma_{ij}z_{S_j}$ with integers γ_{ij}. A τ of the region has $z_{S_j}\cdot\tau\equiv\epsilon_j t_j$ modulo 1 with $\epsilon_j=\pm1$ and $t_j=r_{S_j}\in[a_{S_j},b_{S_j}]$; since $-\tau$ lies in the same region, $\epsilon_1=+1$ may be assumed. For each of the 256 choices of signs, $z_i\cdot\tau\equiv\sum_j\gamma_{ij}\epsilon_j t_j$ lies in an interval computed exactly; if for some i that interval contains no number x with $a_i\le\|x\|\le b_i$, no τ of the region has these signs. If this happens for all 256 choices, the region contains no τ at all and needs no certificate (`empty_region_test`).

The certificate. The blob of a tree row is the bytes of a gzip file holding one JSON object (Appendix B): a head with `"basis_U"`, the pool `"vectors"`, the `"triangles"` (index triples, checked to be true relations) and the number of `"leaves"`, then the tree. A leaf is a certificate $\{$`"H"`, `"D"`, `"w"`, `"nu"`, `"mum"`$\}$ of Lemma 12 (`"w"`: pairs $[i,c_i]$; `"nu"`: pairs $[\mathrm{row},\nu]$ with row $4t$ the perimeter row of triangle t and rows $4t+1,4t+2,4t+3$ its three other rows; `"mum"`: pairs $[i,\mu_i^-]$; all integers, in units of $1/D$ and $1/64$), or $\{$`"empty"`$: S\}$. The trees were found by branch and bound: at each region a convex program proposes a certificate, which is rounded and checked; if it fails, the region is split on the vector carrying the largest uncertainty.

The check. Algorithm 4; the functions are `verify_tree_certificate`, `bb_leaf_value` and `empty_region_test`.

Why it excludes the form. Every $\tau\in\mathbb{R}^9$ has (r_i) in the root region, and the cuts cover; every leaf proves $d\ge d_{\mathrm{cut}}$ on its region (Lemmata 12 and 13) or that the region is empty. Lemma 11.

5.7 Trees of boxes

Coordinates. The pool contains nine vectors $b_1, \dots, b_9$ (`"box_basis"`) forming a basis of $\mathbb{Z}^9$, and $z_i = \sum_j A_{ij} b_j$ with an integer matrix A. A first gluing is given by $s_j = b_j \cdot \tau$ modulo 1, and $z_i \cdot \tau = \sigma_i := \sum_j A_{ij} s_j$. In the data, $\tau = M_i L t$ where M_i is the inverse of the matrix of the b_j, $L = L_{\mathrm{int}}/D_L$ is a lower triangular rational matrix with ones on the diagonal (`"box_L"`, `"box_DL"`; checked by `box_L_valid`) and $t \in \mathbb{R}^9$ is the coordinate of the box; so $\sigma = ALt$, and everything is linear in t. The coordinates t are integers in units of $1/4096$ (`"unit"`), σ and τ in units of $1/UU$, $UU = 4096 D_L$. The matrix L comes from Gram–Schmidt in the metric of P and makes the edges of the boxes nearly orthogonal; it plays no role in the proof.

The root box. Without symmetry the root box is $R_0 = [0, \frac{1}{2}] \times [0,1]^8$ in t. It contains a representative of every first gluing: s is defined modulo $\mathbb{Z}^9$, changing s by $n \in \mathbb{Z}^9$ changes t by $L^{-1}n$, and L^{-1} is lower triangular with ones on the diagonal, so $n_1, n_2, \dots$ can be chosen in turn to bring $t_1, t_2, \dots$ into $[0,1)$; and as $t_1 = s_1$, replacing τ by $-\tau$ replaces t_1 by $1 - t_1$ modulo 1. The chain with first gluing $-\tau$ is the same chain with g replaced by $-g$ ($M = N \oplus \mathbb{Z}g = N \oplus \mathbb{Z}(-g)$), so every statement about chains is invariant under $\tau \mapsto -\tau$ and $t_1 \in [0, \frac{1}{2}]$ may be assumed. With symmetry the root box is the box `"sym.root"` of Section 5.8. An inner node $\{$`"v"`$: j,$ `"at"`$: x,$ `"le"`, `"ge"`$\}$ with $\ell_j < x < h_j$ splits the box $[\ell, h]$ by $t_j \le x$ and $t_j \ge x$.

m on a box. For a box $[\ell, h]$ and weights w_i, σ_i ranges over the interval $[L_i, H_i] = \sum_j (AL)_{ij} [\ell_j, h_j]$ (exact integers). If $[L_i, H_i] \subset [k_i - \frac{1}{2}, k_i + \frac{1}{2}]$ for an integer k_i (case `quad`), then $\|\sigma_i\|^2 \le (\sigma_i - k_i)^2$; otherwise (case `const`) $\|\sigma_i\|^2 \le \rho_i^2$, ρ_i the largest distance to $\mathbb{Z}$ of a point of $[L_i, H_i]$. The function

$$F(t) = \sum_{\texttt{quad}} w_i (\sigma_i(t) - k_i)^2 + \sum_{\texttt{const}} w_i \rho_i^2$$

is convex in t, so its maximum over the box is attained at one of the 2^9 vertices, and

$$m = \sum_i w_i - \max_{v \text{ vertex}} F(v) \;\le\; \sum_i w_i \big(1 - \|z_i \cdot \tau\|^2\big) \quad \text{for every } \tau \text{ of the box:} \tag{7}$$

2^9 evaluations in integers. No triangle is needed: a box knows that $\tau \mapsto z \cdot \tau$ is a homomorphism. Lemma 9 with this m gives $d \ge (40/S_9)^{10} m \det Y$ for every chain whose first gluing lies in the box, and Lemma 13 improves it. For a vector (x, k) of M, $Y[x + k\tau]$ is convex in τ, so its maximum over the box is attained at a vertex, and the least s of Lemma 13 over the box is computed from the vertices.

The leaf kinds. The leaf kinds of a tree of boxes are listed in Table 1; the head of the certificate carries, besides the keys of a tree of cases, `"box_basis"`, `"unit"`, `"box_L"`, `"box_DL"` and optionally `"sym"`. The trees were found by a depth-first search over boxes (one search per part of the root box, joined afterwards), which at each box tries, in order, the certificates inherited from the parent box, a `pattern` leaf, the box program with the best vector of M, a `uspec` or `spec` leaf, and, for a form under a real lattice, a `three` leaf, and splits the box when all fail.

Table 1. The leaves of a tree of boxes, their data (besides `"H"`, `"D"`, `"w"`) and what each proves on its box.

kind	data	proves on the box	checker
`box`	`["x"]`	$d \geq d_{\text{cut}}$ (Lemmata 9, 13, eq. (7))	`box_leaf_value`
`pattern`	`"nu"`, `"mum"`	$d \geq d_{\text{cut}}$ (Lemma 12 on the ranges of the box)	`bb_leaf_value`
`spec`	`"vec"`, `"vw"`, `"vd"`, `"gam"`, `"M"`, `"s"`, `"ab"`, `"abd"`	$d \geq d_{\text{cut}}$ (Lemma 14, several vectors of M)	`spec_leaf_value`
`pspec`	as `pattern`, plus as `spec`	$d \geq d_{\text{cut}}$ (Lemma 14, several vectors of N)	`pspec_leaf_value`
`uspec`	`"pieces"`: a list of {`"lo"`, `"hi"`, spec data}	$d \geq d_{\text{cut}}$ (Lemma 14, piecewise in u)	`uspec_leaf_pair`
`outside`	`"g"`	the box contains no point of F (Section 5.8)	Algorithm 6
`three`	`"v2"`, `"v3"`, `"tri"`	$\Delta \geq 972$, whatever the second gluing (Section 5.9)	`three_leaf_value`

Leaves of kind `box`. The glue lemma on the box with (7), and Lemma 13 with the better of two vectors: the minimal vector c of P with the least $H[c]$, and, if the leaf names a vector x (nine integers, $k = 1$, or ten integers (x, k)), the vector $(x + k\tau, k)$ of M, with $Y[x + k\tau] + mk^2$ maximised over the 512 vertices.

Leaves of kind `pattern`. The certificate of a tree of cases, on the region $a_i \leq r_i \leq b_i$ given by the exact range of $\|\sigma_i\|$ over the box, rounded outwards to multiples of $\frac{1}{64}$ (`box_pattern_bounds`): every gluing of the box lies in that region, and Lemma 12 applies. On a large box most vectors are `const` and the triangles of the case analysis are worth more than the vertices.

Leaves of kinds `spec`, `pspec`, `uspec`: *several vectors at once.* Lemma 13 uses one vector of M. The following lemma uses many at once. Fix a leaf (Y, w, m) with $m > 0$ valid on a box, so that $\operatorname{tr}(YX) + mu \leq S_9/4$ for every chain whose first gluing lies in the box. Let

$$K = \frac{40}{S_9} \operatorname{diag}(Y, m), \qquad \mathsf{D} = \operatorname{diag}(X, u), \qquad Z = K^{1/2} \mathsf{D} K^{1/2}, \qquad W = Z^{-1}.$$

Then $\operatorname{tr} Z \leq 10$, W is positive definite and block diagonal with blocks of sizes 9 and 1, and $d = 1/\det \mathsf{D} = \det K \det W$. A vector of M with coordinates $(x, k) \in \mathbb{Z}^{10} \setminus \{0\}$ has norm $\hat{y}^{\mathsf{T}} \mathsf{D}^{-1} \hat{y} = \tilde{y}^{\mathsf{T}} W \tilde{y} \geq 4$ with $\hat{y} = (x + k\tau, k)$ and $\tilde{y} = K^{1/2} \hat{y}$. For weights $\nu_y \geq 0$ on finitely many such vectors y, $\operatorname{tr}(\mathcal{A}W) \geq 4 \sum_y \nu_y$ with $\mathcal{A} = \sum_y \nu_y \tilde{y} \tilde{y}^{\mathsf{T}}$, and, W being block diagonal, the same holds for the block-diagonal part $\mathcal{A}_b$ of $\mathcal{A}$.

Lemma 14 (spectral lemma; several vectors). *Let* $\mathsf{M} \geq 1$, $\gamma \geq 0$, *and* $\phi(q) = \min_{1/10 \leq w \leq \mathsf{M}} \big(\log w - qw + \gamma/w\big)$. *Then*

$$\log\det W \;\geq\; \min\Big(\log g(\mathsf{M}),\; \sum_{i=1}^{10} \phi(a_i) + 4\sum_{y} \nu_y - 10\gamma\Big),$$
$$g(\mathsf{M}) = \mathsf{M}\Big(\frac{9}{10 - \frac{1}{\mathsf{M}}}\Big)^{9},$$

where $a_1 \leq \cdots \leq a_{10}$ *are the eigenvalues of* $\mathcal{A}_b$ *(those of its* 9×9 *block, and its last entry).* ϕ *is decreasing, so the* a_i *may be replaced by upper bounds, and* $\mathcal{A}_b$ *by any block-diagonal matrix that dominates it. Consequently* $d \geq (40/S_9)^{10} m \det Y \cdot \min\big(g(\mathsf{M}), \exp(\sum\phi(a_i) + 4\sum\nu_y - 10\gamma)\big)$.

Proof. The eigenvalues $w_1 \leq \cdots \leq w_{10}$ of W satisfy $\sum 1/w_i = \operatorname{tr} Z \leq 10$, so $w_i \geq 1/10$. If some $w_i \geq \mathsf{M}$, the other nine have $\sum_{j\neq i} 1/w_j \leq 10 - 1/w_i$, hence product at least $(9/(10-1/w_i))^9$ by AM–GM, and g increases on $[1,\infty)$: $\det W \geq g(w_i) \geq g(\mathsf{M})$. Otherwise all w_i lie in $[1/10, \mathsf{M}]$; by von Neumann's trace inequality $\operatorname{tr}(\mathcal{A}_b W) \leq \sum_i a_i w_i$ with both families sorted increasingly, so $\sum_i a_i w_i \geq 4\sum\nu_y$, and $\sum_i \log w_i \geq \sum_i (\log w_i - a_i w_i + \gamma/w_i) + 4\sum\nu_y - 10\gamma \geq \sum_i \phi(a_i) + 4\sum\nu_y - 10\gamma$. □

On a box. The 9×9 block of $\sum_y \nu_y \hat{y}\hat{y}^{\mathsf{T}}$ is a quadratic polynomial in τ with leading term $\kappa\tau\tau^{\mathsf{T}}$, $\kappa = \sum_y \nu_y k_y^2$: completing the square, $B(\tau) = B_0 + \kappa(\tau-\tau_0)(\tau-\tau_0)^{\mathsf{T}}$. Hence the 9×9 block of $\mathcal{A}_b$ is $\mathcal{A}_0 + \kappa z_\tau z_\tau^{\mathsf{T}}$, where $z_\tau = K_1^{1/2}(\tau - \tau_0)$ and $K_1 = \frac{40}{S_9} Y$. For $\rho \geq 0$ and a unit vector ξ, the eigenvalues of $\mathcal{A}_0 + \rho\xi\xi^{\mathsf{T}}$ are majorised by those of $\mathcal{A}_0$ with ρ added to the largest one. Here $x \preccurlyeq_{\mathrm{maj}} y$ means that the sums of the j largest entries satisfy $\sum_{i=1}^{j} x_i^{\downarrow} \leq \sum_{i=1}^{j} y_i^{\downarrow}$ for every j, with equality for the total sum; the superscript $\downarrow$ denotes decreasing order. Ky Fan's inequality gives $\lambda(A+B) \preccurlyeq_{\mathrm{maj}} \lambda^{\downarrow}(A) + \lambda^{\downarrow}(B)$. For concave ϕ, majorisation implies $\sum_i \phi(x_i) \geq \sum_i \phi(y_i)$, the property called Schur concavity. These spectral inequalities are treated in [12]. Since ϕ is also decreasing, increasing the last entry lowers this sum. So on a set of gluings with $K_1[\tau - \tau_0] \leq R^2$, $\sum_{i\leq 9}\phi(a_i(\tau)) \geq \phi(a_1) + \cdots + \phi(a_8) + \phi(a_9 + \kappa R^2)$, $a_1 \leq \cdots \leq a_9$ the eigenvalues of $\mathcal{A}_0$; the set enters only through R^2, which for a box is the largest of $K_1[\tau_v - \tau_0]$ over the vertices.

The last entry of $\mathcal{A}_b$ is $K_2\kappa$, $K_2 = \frac{40}{S_9} m$, and does not depend on the gluing. A leaf of kind `spec` carries vectors $y = (x, k)$ (`"vec"`) with weights $\nu_y = \mathtt{vw}_y/\mathtt{vd}$, the numbers γ (`"gam"`), M (`"M"`) and a number $s > 0$ (`"s"`) with which the centre τ_c of the box is used in place of τ_0 ($(b_c+\delta_\tau)(b_c+\delta_\tau)^{\mathsf{T}} \preceq (1+s) b_c b_c^{\mathsf{T}} + (1+1/s)\delta_\tau\delta_\tau^{\mathsf{T}}$ with $b_c = \tau_c - \tau_0$, $\delta_\tau = \tau - \tau_c$, so that $B(\tau) \preceq B_s + \kappa(1+1/s)\delta_\tau\delta_\tau^{\mathsf{T}}$, $B_s = B_0 + \kappa(1+s) b_c b_c^{\mathsf{T}}$, and the last term adds at most $\kappa(1+1/s)R^2$ to the largest eigenvalue, R^2 the largest $K_1[\tau_v - \tau_c]$ over the vertices), and nine rational numbers $\mathtt{ab}_1 \leq \cdots \leq \mathtt{ab}_9$ over a common denominator $\mathtt{abd}$, upper bounds of the eigenvalues $a_1 \leq \cdots \leq a_9$ of the 9×9 block $K_1^{1/2} B_s K_1^{1/2}$ of $\mathcal{A}_b$, which the checker verifies by inertia: with $B_s = \mathcal{B}/b$ ($\mathcal{B}$ an integer matrix, $b > 0$), $H = DY$ and $\Sigma = DS_9$, the integer matrix $40\,\mathtt{abd}\,H\mathcal{B}H - \mathtt{ab}_i\,\Sigma\,b\,H$ is congruent to $B_s - (\mathtt{ab}_i/\mathtt{abd})K_1^{-1}$, so its number of positive eigenvalues is the number of eigenvalues of the block exceeding $\mathtt{ab}_i/\mathtt{abd}$; the checker counts them from the signs of the leading

Algorithm 5 Verification of the leaves box, spec, pspec, uspec

Input: the box $[\ell, h]$ (within ± 64 units of the root), the leaf

require $D > 0$, $H \succ 0$ (δ), weights ≥ 0 on valid pool indices; $m \leftarrow$ the exact m of (7) (for pspec: of Lemma 12 on the rounded ranges); **require** $m > 0$

$\Sigma \leftarrow$ sum of the nine largest $H[c] + \sum c_i (z_i \cdot c)^2$

if box **then** $s \leftarrow \Sigma / (10 \min_c H[c])$; if $x = (x, k)$ is given, also $s' \leftarrow \Sigma / \big(10 \max_v (H[x + k\tau_v] + D\, m\, k^2)\big)$ over the 512 vertices; value $\leftarrow (40/S_9)^{10} m \det Y\, E(\max(s, s'))$

else ▷ spec, pspec, uspec: Lemma 14

  $B_s \leftarrow \sum \nu_y\, yy^{\mathsf{T}}$ (integers), corrected for the box by the rank-one term and the penalty $\rho = \kappa(1 + 1/s)R^2$, R^2 the exact maximum of the metric over the vertices

  for $i = 1..9$ **do require** that at most $9 - i$ eigenvalues of the 9×9 block exceed $\mathsf{ab}_i/\mathsf{abd}$ ▷ signs of leading principal minors

  end for

  $q_i \leftarrow \mathsf{ab}_i/\mathsf{abd}$, $q_9 \leftarrow q_9 + \rho$, $q_{10} \leftarrow K_2\kappa$; $F \leftarrow 4\sum\nu - 10\gamma + \sum_{i \leq 9} \underline{\phi}(q_i) + \underline{\phi}_{10}$ ($\underline{\phi}$: exact rational lower bounds of $\min_{w \in [1/10, \mathsf{M}]} (\log w - qw + \gamma/w)$; for a uspec piece $[u_{\mathrm{lo}}, u_{\mathrm{hi}}]$, $\underline{\phi}_{10}$ over $w \in [\max(\frac{1}{10}, \frac{1}{K_2 u_{\mathrm{hi}}}), \min(\mathsf{M}, \frac{1}{K_2 u_{\mathrm{lo}}})]$)

  value $\leftarrow (40/S_9)^{10} m \det Y \cdot \min\big(g(\mathsf{M}), \underline{\exp}(F)\big)$ ▷ $\underline{\exp}$: a rational lower bound of exp

end if

uspec: **require** the pieces to cover an interval $[u_0, u_1]$ with $(4u_0)^{11}\, 972^9 \leq (\det P)^{11}$ and $3u_1^5 \geq 4$, and every piece to reach d_{cut}

accept iff $\mathrm{ge}_{d_{\mathrm{cut}}}(\mathrm{value})$

principal minors (Jacobi's rule, by fraction-free elimination; a zero minor rejects the leaf) and requires at most $9 - i$ of them, that is $a_i \leq \mathsf{ab}_i/\mathsf{abd}$, for $i = 1, \ldots, 9$. The bound $\kappa(1 + 1/s)R^2$ is added to the ninth, and the tenth entry is $K_2\kappa$. A leaf of kind pspec is the same with vectors of N only ($k = 0$, no dependence on the gluing) on top of a pattern certificate. A leaf of kind uspec carries *pieces* $[u_{\mathrm{lo}}, u_{\mathrm{hi}}]$, each with its own spec data, and bounds the tenth term only for $u \in [u_{\mathrm{lo}}, u_{\mathrm{hi}}]$: the last entry of W is $w_{10} = 1/(K_2 u)$ exactly, so its range is $[1/(K_2 u_{\mathrm{hi}}), 1/(K_2 u_{\mathrm{lo}})]$; the pieces must cover $[\det P/d_{\mathrm{cut}}, \sqrt[5]{4/3}]$, which contains u for every chain with $d < d_{\mathrm{cut}}$ by (u), and every piece must reach d_{cut}.

5.8 Symmetry data and outside leaves

A tree may search only a fundamental domain of the automorphisms of P. By (Symmetry), $\Gamma = \mathrm{Aut}(P) \ltimes \mathbb{Z}^9$ acts on first gluings by the affine maps $g : \tau \mapsto A\tau + n$, $A = V^{-\mathsf{T}}$, $V \in \mathrm{Aut}(P)$, $n \in \mathbb{Z}^9$, and these maps are isometries of the metric G' (because $VG'V^{\mathsf{T}} = G'$). Fix a rational point p_0 and let

$$F = \{\tau : |\tau - p_0| \leq |g\tau - p_0| \text{ for all } g \in \Gamma\} \qquad \text{(distances in the metric } G').$$

Proposition 15 (fundamental domain). *Every Γ-orbit of first gluings meets F. F is cut out by the half-spaces $f_g(\tau) \leq 0$, $f_g(\tau) = |\tau - p_0|^2 - |g\tau - p_0|^2$, which are*

Algorithm 6 Verification of the symmetry data (`sym_check`) and of an `outside` leaf

Input: G', `"sym"` $= \{p_0, V, \text{root}, \text{faces}\}$

1: **for** every V **do require** $VG'V^{\mathsf{T}} = G'$ (exact integers)
2: **end for**
3: **require** $p_0 \in \mathbb{Q}^9$, root corners integers within ± 64 units
4: **for** each of the 18 faces **do require** the Farkas certificate: $\lambda \geq 0$ and the identity $\sum_g \lambda_g f_g(t) \equiv (\text{face function})(t) + \text{const}$ with the right sign (exact rationals), so that $\{f_g \leq 0\} \subseteq$ root
5: **end for**

Input: the box $[\ell, h]$, an `outside` leaf, the verified maps

6: $f \leftarrow \sum y_g f_g$ (one term with $y = 1$ for a single map), $y_g \geq 0$ rational; $f(t) = \kappa - a \cdot t$
7: **accept** iff $\kappa - \sum_j \max(a_j l_j, a_j h_j) > 0$ ▷ the least value of f on the box

affine functions of τ. Consequently, if a box R contains the polytope $\{f_g \leq 0 : g \in S\}$ for a finite set $S \subset \Gamma$, then R contains a representative of the first gluing of every chain over P, and a box on which some f_g, $g \in S$, or some nonnegative combination $\sum_g y_g f_g$, is positive contains no point of F.

Proof. An orbit is a finite union of translates of $\mathbb{Z}^9$, hence discrete, so it has a point closest to p_0, which lies in F by definition. f_g is affine because g is an isometry: $|g\tau - p_0|^2 = |\tau - g^{-1}p_0|^2$ differs from $|\tau - p_0|^2$ by an affine function. The polytope contains F, and a positive combination of the f_g is positive nowhere on F. □

The head of such a tree carries `"sym"` $= \{$`"p0"`, `"V"`, `"root"`, `"faces"`$\}$: the point p_0, the integer matrices V used, the root box, and for each of the 18 faces of the root box a *Farkas certificate*, nonnegative multipliers λ_g with $\sum_g \lambda_g f_g \equiv (\text{face function}) + \text{const}$ with the right sign, which proves that the polytope lies on the inner side of the face. An `outside` leaf carries one map $[v, n_1, \ldots, n_9]$ or a list of terms $[v, n, y_{\text{num}}, y_{\text{den}}]$. The maps S were chosen as the maps g with gp_0 nearest to p_0 (about 6000 of them); the Farkas certificates and the `outside` leaves were found by linear programming and made exact on their support.

5.9 Leaves of the third level

A leaf of kind `three` proves $\Delta \geq 972$ for every chain whose first gluing lies in the box, *whatever the second gluing*. It adds to the level-2 terms (z_i, n_i, w_i) of the box ($z_i \in \mathbb{Z}^9 \setminus \{0\}$, $n_i \in \mathbb{Z}$, $w_i \geq 0$; by (L2), $X[z_i] \geq u(1 - (n_i - z_i \cdot \tau)^2)$) *level-3 terms* (ζ_j, ω_j), $\zeta_j = (z_j, k_j) \in \mathbb{Z}^{10} \setminus \{0\}$, $\omega_j \geq 0$ (by (L3), $X[z_j] + u(k_j - z_j \cdot \tau)^2 \geq v(1 - \|\zeta_j \cdot \varphi\|^2)$), and *triangles* $T = (j_1, j_2, j_3)$ with $\pm\zeta_{j_1} \pm \zeta_{j_2} \pm \zeta_{j_3} = 0$ in $\mathbb{Z}^{10}$, with multipliers $\mu_T \geq 0$.

Lemma 16 (eleven numbers). *Let $B_u(\tau) = \sum_i w_i\big(1 - (n_i - z_i \cdot \tau)^2\big) - \sum_j \omega_j (k_j - z_j \cdot \tau)^2$, $B_v(\varphi) = \sum_j \omega_j \big(1 - \|\zeta_j \cdot \varphi\|^2\big)$, and S_9 the sum of the nine largest $g(c) = Y[c] + \sum_i w_i (z_i \cdot c)^2 + \sum_j \omega_j (z_j \cdot c)^2$, $c \in C$. If $0 < m_u \leq B_u$ on the box and*

Algorithm 7 Verification of a third-level leaf

Input: the box, $\{H, D, w, v2, v3, tri\}$

1: **require** $H \succ 0$ (δ), weights ≥ 0, every triangle a true relation in $\mathbb{Z}^{10}$
2: $\Sigma \leftarrow$ nine largest of $H[c] + \sum_i c_i (z_i \cdot c)^2 + \sum_j \omega_j (z_j \cdot c)^2$
3: $m_u \leftarrow \min_v \big(\sum_i c_i (UU^2 - e_i(v)^2) - \sum_j \omega_j e_j(v)^2 \big)$ over the 512 vertices, e_i, e_j exact integers ▷ m_u concave
4: $\sigma_j \leftarrow \max\big(0, \omega_j - \sum_{T \ni j} (\mu_T + \nu_{T,j} - \sum_{b \in T, b \neq j} \nu_{T,b})\big)$; $m_4 \leftarrow 4\sum\omega_j - \sum\sigma_j - 2\sum\mu_T$ ▷ $m_4 = 4Dm_v$
5: **accept** iff $\mathrm{ge}_{972}\left(44^{11}\delta\, m_u\, m_4,\ 4\,\Sigma^{11} UU^2\right)$ ▷ $\Delta \geq (44/S_9)^{11} \det Y\, m_u m_v \geq 972$

$0 < m_v \leq B_v$ *for every* $\varphi \in \mathbb{R}^{10}$*, then every chain over* P *with first gluing in the box has*

$$\Delta \;\geq\; \left(\frac{44}{S_9}\right)^{11} \det Y\, m_u\, m_v.$$

Proof. As in Lemma 9 with eleven numbers: the nine eigenvalues of $X^{1/2} Y X^{1/2}$, uB_u and vB_v. Their sum is at most $\mathrm{tr}(XG') \leq S_9/4$ by (L2), (L3) and (4), with $G' = Y + \sum w_i z_i z_i^{\mathsf{T}} + \sum \omega_j z_j z_j^{\mathsf{T}}$; their product is $\det Y \cdot uvB_uB_v/(ud) = \det Y\, B_uB_v/\Delta$, since $d = v\Delta$. AM–GM. □

The lower bound m_v that the checker computes (Algorithm 7, line 4) uses multipliers $\nu_{T,j}$ on the rows $\|x\| \leq \|y\| + \|z\|$ of the triangles as well as μ_T on their perimeter rows; it is the bound of Lemma 47 (Appendix E), which is this lemma with that explicit m_v, and its rows are shown there to be valid on $\mathbb{R}/\mathbb{Z}$.

Lemma 17 (all second gluings). *With* $\sigma_j = \max\big(0, \omega_j - \sum_{T \ni j} \mu_T\big)$*, the value* $m_v = \sum_j \omega_j - \frac{1}{4}\sum_j \sigma_j - \frac{1}{2}\sum_T \mu_T$ *satisfies* $m_v \leq B_v(\varphi)$ *for every* $\varphi \in \mathbb{R}^{10}$*.*

Proof. Exactly as Lemma 10, with $\zeta_j \cdot \varphi$ in place of $z_i \cdot \tau$. □

B_u is concave in τ (each term is), so m_u may be taken as its minimum over the 512 vertices of the box. The leaf carries `"v2"` (the level-2 terms), `"v3"` (the level-3 terms) and `"tri"` (the triangles with their multipliers), all integers with denominator 10^8; the leaves were found by cutting planes on the vertices of the box, maximising $11 \log \frac{44}{S_9} + \log\det Y + \log m_u + \log m_v$ in floating point and rounding down.
The lemma that the checker implements, with multipliers $\nu_{T,j}$ on the rows $\|x\| \leq \|y\| + \|z\|$ of the triangles as well as μ_T on their perimeter rows, is Lemma 47 of Appendix E (its $\omega_{T,j}, \tau_T$ and σ_i are the $\nu_{T,j}, \mu_T$ and σ_j here): it gives $m_v = \sum_j \omega_j - \frac{1}{4}\sum_j \sigma_j - \frac{1}{2}\sum_T \mu_T$ with σ_j computed as in line 4, and line 4 is four times this value in the integer units of the leaf (ω_j, σ_j, μ_T scaled by D).

Why a tree with such leaves excludes the form.

Proposition 18 (mixed tree). *A tree of boxes over the root box (with or without symmetry) whose leaves verify, each by the algorithm of its kind, proves that every chain over* P *has* $d \geq d_{\mathrm{cut}}$ *or* $\Delta \geq 972$*, hence (E).*

Algorithm 8 Verification of a tree of boxes

Input: G', C; pool Z (nonzero), A, M_i from `"box_basis"`; L valid (lower triangular, D_L on the diagonal); triangles true relations

if the certificate has `"sym"` **then** run Algorithm 6; $R_0 \leftarrow$ `"sym.root"`
else $R_0 \leftarrow [0, 2048] \times [0, 4096]^8$
end if
stack $\leftarrow [(\text{root}, R_0)]$; $n \leftarrow 0$
while stack not empty **do**
    (node, $[\ell, h]$) $\leftarrow$ pop
    if node is a leaf **then** $n \leftarrow n + 1$; **reject** unless the leaf verifies on $[\ell, h]$ by the algorithm of its kind (`box`, `pattern`, `spec`, `pspec`, `uspec`: Algorithm 5, value $\geq d_{\text{cut}}$; `outside`: Algorithm 6; `three`: Algorithm 7, value ≥ 972)
    else if node $= \{v{:}\, j,\ at{:}\, x,\ le,\ ge\}$ with $\ell_j < x < h_j$ **then** push $(le, [\ell, h|_{h_j = x}])$ and $(ge, [\ell|_{\ell_j = x}, h])$
    else reject
    end if
end while
accept iff n equals the number of leaves recorded

Proof. By the paragraph "the root box" or by Proposition 15, the root box contains a representative of the first gluing of every chain over P, and the chain with that representative has the same d and Δ; the leaves cover the root box (checked at every inner node); an `outside` leaf contains no such representative; a leaf of kind `box`, `pattern`, `spec`, `pspec` or `uspec` gives $d \geq d_{\text{cut}}$ on its box (Lemmata 9, 13, 12, 14); a leaf of kind `three` gives $\Delta \geq 972$ on its box (Lemmata 16 and 17). Lemma 11. □

6 The database

6.1 The files

The certificates are gathered in one SQLite 3 file of 1 918 717 952 bytes (1.9 GB), the *database*: the file `k11_certificates_v3.sqlite`, of SHA-256 `982eaf73232af64c cf3ad2123d5e1f3eef169976cb1a90b2f45eaae4389c59e8`. It ships with the verifier of Section 7, its library and its manifest (`MANIFEST_k11_certificates_v3.json`: the SHA-256 and size of the file, the counts by kind, the result of the last full verification and the SHA-256 of every tree certificate). The certificates occupy 1 195 MB of the file (62%), the keys 63 MB and the Gram matrices 404 MB; the rest is the index on the keys and page overhead. The database is self-contained: every certificate is inside it, in the column `cert` of the table `form`. It has one row per survivor. Section 7 rebuilds this file from the shipped database (phase **scrub**) and checks every row of the result (phase **verify**).

6.2 The tables

Figure 4 shows the tables and their links.

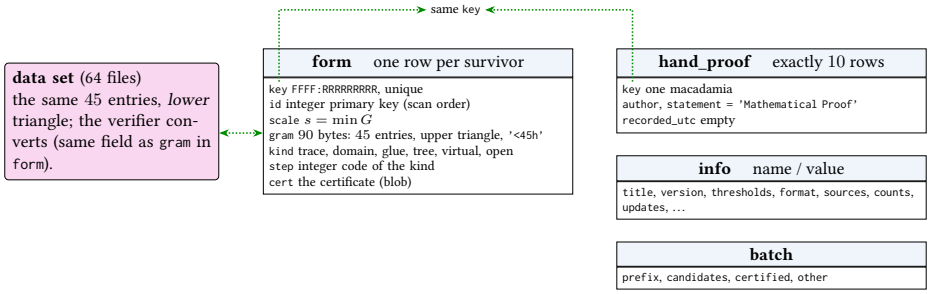

Fig. 4. The tables of the certificate database. Every certificate is inside the file, in the column `cert` of `form`. **Rows by kind:** trace 4 486 439; domain 1 215; glue 79; tree 70; virtual 10; open 0 (total 4 487 813). A `virtual` row is accepted only if three conditions hold: the real-lattice check of its data passes ($\min M = 4$ and $\det M < d_{\text{cut}}$); its `hand_proof` row is byte-exactly the canonical mention; and its key is in the list `VIRTUAL_KEYS` hard-coded in the verifier, not read from the database. A fifth table, `pending`, is empty.

Table `form`*: one row per survivor.* Columns: `id` (integer primary key, the order of the scan); `key` (text `FFFF:RRRRRRRRR`, the name of the form, Section 2.3; unique); `scale` (the integer $s = \min G$); `gram` (a blob of 90 bytes: the 45 entries G_{ij}, $i \le j$, that is the *upper* triangle of G row by row, $G_{11}, \ldots, G_{19}$; $G_{22}, \ldots, G_{29}$; ..., as signed 16-bit little-endian integers, Python `struct` format `'<45h'`; the data set stores the lower triangle row by row, Section 3, and the verifier converts); `kind` (one of `trace`, `domain`, `glue`, `tree`, `virtual`, `open`); `step` (an integer code of the kind, kept for the programs: 6 for `trace`, 7 for `domain`, 8 for `glue`, 9, 10 or 12 for `tree`, 0 otherwise); `cert` (the certificate, a blob whose format depends on the kind, Section 5 and Appendix B; NULL for `open`).

Table `info`*: name / value.* `title`, `created_utc`, `made_by`, `version`, `thresholds` (the constants of Section 3.2), `format` (a description of the rows), `sources` (where the certificates came from), `announced_by_the_logs` (the counts announced by the logs of the searches, compared with what was found), `problems_met`, `counts` (JSON: the number of rows of each kind and the total; the verifier compares its own counts with these), `updated_utc`, `updated_by` and `updates` (JSON: the log of the modifications of the file).

Table `batch`. Columns `prefix`, `candidates`, `certified`, `other`: the batches of the scan, with the number of survivors of each batch, how many of them were settled by a trace certificate and how many went further. (The file also contains a table `pending`, which is empty.)

Table `hand_proof`. Columns `key`, `author`, `statement`, `recorded_utc`: the forms proved outside the database. It has exactly ten rows, one per key of Table 3, and each row is the same canonical mention: `author` and `statement` both equal to the string `'Mathematical Proof'` and `recorded_utc` empty. The verifier checks this marker byte by byte; the corresponding mathematical proofs are cited in Section 6.4. The row of the form in `form` keeps its kind (`virtual`). Section 6.4 says what the rows mean.

Table 2. The rows of the database by kind.

kind	rows	what the row proves
`trace`	4 486 439	$e/t \geq T_Q$ for every N over the form; Lemma 6 a
`domain`	1 215	$e/t \geq T_Q$ for every N over the form; Lemma 6 a
`glue`	79	$d \geq d_{\mathrm{cut}}$ for every chain over the form; Lemma 6 b
`tree`	70	$d \geq d_{\mathrm{cut}}$ region by region (40 trees of cases, 30 of boxes); Lemma 6 b
`virtual`	10	nothing: a lattice M over the form; no rank-10 certificate exists
`open`	0	–
total	4 487 813	

Algorithm 9 Verification of a virtual row: the real-lattice check (`real_chain_check`)

Input: G, s, $\{\tau, u, \det\}$

1: build the Gram matrix of $M = N + \mathbb{Z}(\tau + f/\sqrt{u})$ on the basis $(b_1, \ldots, b_9, \tau + f/\sqrt{u})$, N the form scaled to minimum 4 (exact rationals)
2: **require** $M \succ 0$; $\min M = 4$ and $\min M^* = u$ (exact enumeration) ▷ then $w = \sqrt{u}\, f \in M^*$ is shortest and $M \cap w^{\perp} = N$
3: **require** $P^{-1} = \sum_{c \in C} \rho_c\, cc^{\mathsf{T}}$ with rational $\rho_c \geq 0$ ▷ the form lies in its own domain
4: **accept** iff $\det M = \det N/u < d_{\mathrm{cut}}$ (exact) and $\det M$ equals the recorded value

6.3 Counts

Table 2 gives the number of rows of each kind in the database. Every row of kind `trace`, `domain`, `glue` or `tree` is a certificate that proves (E) for its form by Lemma 6 and Section 5; the rows of kind `virtual` are the ten macadamias (Section 6.4); there is no row of kind `open`.

6.4 The ten rows that read as separate proofs

For ten survivors the database holds no certificate, and it says why: a row of kind `virtual` records an actual lattice M of rank 10 that lies over the form. (The row is a *virtual certificate*: a row in the place of a certificate that cannot exist.)

The row. `zlib`(JSON {`"tau"`, `"u"`, `"det"`, `"name"`}): a rational point $\tau \in \mathbb{Q}^9$ (as pairs numerator, denominator), a rational u, the rational $\det M$ and a name. Its meaning: with N the form scaled to minimum 4 and f a unit vector orthogonal to N,

$$M = N + \mathbb{Z}\Big(\tau + \frac{f}{\sqrt{u}}\Big)$$

is a lattice of rank 10 with $\min M = 4$, $\min M^* = u$, whose section by a shortest vector of M^* is N, with the form in its own Voronoi domain, and $\det M = \texttt{det} < d_{\mathrm{cut}}$. The row still carries these data so that the reader can check that an actual lattice lies over the form, and hence that no certificate of the four kinds can exist for it.

What the row shows. The pair (N, M) satisfies every hypothesis of Section 2.4 that a certificate at rank 10 uses: (Domain) by step 3, (L2) and (M) because M is a lattice with $\min M = 4$ and $\min M^* = u$, (u) because $d = \det M < d_{\text{cut}}$ and Theorem 3 applies to M; and $e/t \leq 4d/3 < T_Q$ by (1). A valid certificate of kind `trace`, `domain`, `glue`, or `tree` without leaves of the third level would prove $e/t \geq T_Q$ or $d \geq d_{\text{cut}}$ for this pair: so *no such certificate exists* for the form, and the row is not a certificate. The verifier checks the row exactly (Algorithm 9) and counts it as "not excluded".

What the verifier accepts. A row of kind `virtual` is accepted only if three conditions hold:

a the real-lattice check passes (Algorithm 9: the recorded M has minimum 4 and determinant below d_{cut} over the form);

b its row of `hand_proof` is byte-exactly the canonical mention (`author` and `statement` equal to `'Mathematical Proof'`, `recorded_utc` empty);

c its key is in a closed list of ten keys hard-coded in `verify_database.py` (the constant `VIRTUAL_KEYS`), not read from the database:

`0030:030301719`, `0019:030884313`, `0017:001746552`, `0008:022143116`, `0015:030291998`, `0001:010488327`, `0014:001749549`, `0059:016902802`, `0050:024468269`, `0052:005247066`.

Any other row carrying the mention fails; a row of `hand_proof` with the mention and no row of the database fails. The smoke test of the verifier rejects three forgeries: a virtual row whose key is outside the list; the mention attached to a row that is not virtual; and the mention misspelt. Thus the set of forms that the database leaves to a mathematical proof is fixed in the verifier's code, where a reader sees it, and cannot grow by editing the database.

The mathematical proof behind a virtual row. For each of the ten forms the proof is the one that Table 3 names: Appendix E of this paper for `0052:005247066`, and one of the five companion papers [3,4,5,6,7], grouped by method, for the other nine; each proves (E) for its forms by arguments at rank 11 specific to the form, and states the hypotheses it inherits.
A lattice of rank 10 can lie over several survivors (macadamias 4 and 5, 7 and 8); each form still needs its own proof, since the chains over two forms are different sets [2]. The determinant $\det P$ of the form itself is $u \det M$: 512, $5120/9$, 768, 864, 972, $2^{18}/3^5$, 1024, 1024, $8192/9$ and 972 for macadamias 1 to 10.

7 The verifier

7.1 The reproduction pack, and what it does

The global certificate database and its checker are distributed as `hermite11_rank9_reproduction.zip`. It is deposited in the Zenodo record doi:10.5281/zenodo.23979316 of the series and has SHA-256 `22a9336ef6677171a1e9d6760f0ca21c11abf3b0cc9e3c62cfe009e1a6982776` (1.44 GB). Running it proves every global finite assertion of this paper (Computational results 5 and 19) and Computational result 9 of [2]: its scans are

Table 3. The ten macadamias, numbered as in [2, Table 4]: the lattice M of rank 10 recorded in the `virtual` row, its determinant and dual minimum, and the paper that settles the form (contacts: contact geometry [3]; sections: reduction by sections [4]; spectral: finite spectral relaxation [5]; blocks: one selected contact, two linked blocks [6]; triangles: unequal triangles and adapted references [7]).

no.	form	lattice M over it	det M	min M^*	paper
1	`0030:030301719`	Λ_{10} (the form is $\Lambda_9 = P_\Lambda$)	768	$2/3$	blocks [6]
2	`0019:030884313`	the lattice over P_S; 294 min. vectors	$25600/27$	$3/5$	sections [4]
3	`0017:001746552`	the lattice over P_K; 270 min. vectors	1024	$3/4$	sections [4]
4	`0008:022143116`	section of K_{11}; 276 min. vectors	972	$8/9$	spectral [5]
5	`0015:030291998`	section of K_{11}; 270 min. vectors	972	1	contacts [3]
6	`0001:010488327`	rescaled dual of the 270-vector section	$2^{18}/3^5$	1	contacts [3]
7	`0014:001749549`	a lattice M_{260} with 260 min. vectors	1024	1	contacts [3]
8	`0059:016902802`	M_{260} of macadamia 7 (a second section)	1024	1	contacts [3]
9	`0050:024468269`	an unnamed lattice with 180 min. vectors	$3328/3$	$32/39$	triangles [7]
10	`0052:005247066`	an unnamed lattice with 164 min. vectors	$7776/7$	$7/8$	here, App. E

exact on every record. A complete run of its programs on a node with 160 hardware threads (Intel Xeon Platinum 8380, 5–6 November 2026) printed every verdict below and ended with `RESULT: EVERYTHING PASSED.`; its logs, transcripts and statistics are the verification report `hermite11_verification_report.zip` of the same record. The reader unzips it and runs, from its top directory,

```
$ bash reproduce.sh
```

(Figure 5 shows its contents.)

The script runs six named phases, `env`, `download`, `ten`, `scrub`, `verify`, `stats` (Figure 6; its progress banners count five, `PHASE 1/5` to `5/5`, the phase **ten** being printed as the last step, 2c, of the download banner), each resumable (a phase that was interrupted restarts where it stopped, and a phase already completed is skipped); the times are the wall times of the verification run, on one node with 160 hardware threads (Intel Xeon Platinum 8380, 2.3 GHz, 256 GB, 156 processes; 15 h 44 min in all):

1. **env**: a Python environment is created with `micromamba`, without root privileges; no other software is assumed.
2. **download**: the 64 files `perfect_0000.nc`, …, `perfect_0063.nc` of the Zenodo record 15707640 [1] are downloaded (160.33 GB), and the MD5 of every file is checked against the record (1 h 18 min).
3. **ten**: `result9.py` decides $4^9 \det G < 814\, m^9$ exactly for each of the 2 237 251 040 forms (the module `exact_census.py` of Section 3), finds the three survivors, identifies them with the three forms of [2, Section 5] by explicit unimodular matrices U checked exactly (so that $\min G = m$ follows from the minimum 4 of the reference forms), determines the runner-up exactly over all forms ($22528/27$, the form `0060:012815567`), and writes the transcript `result9_transcript.json`; the last line is `VERDICT: RESULT 9 HOLDS` (27 min).
4. **scrub**: every certificate of the shipped database is replayed in exact arithmetic and a new file, `k11_certificates_v4.sqlite`, is written with the same 4 487 813 rows,

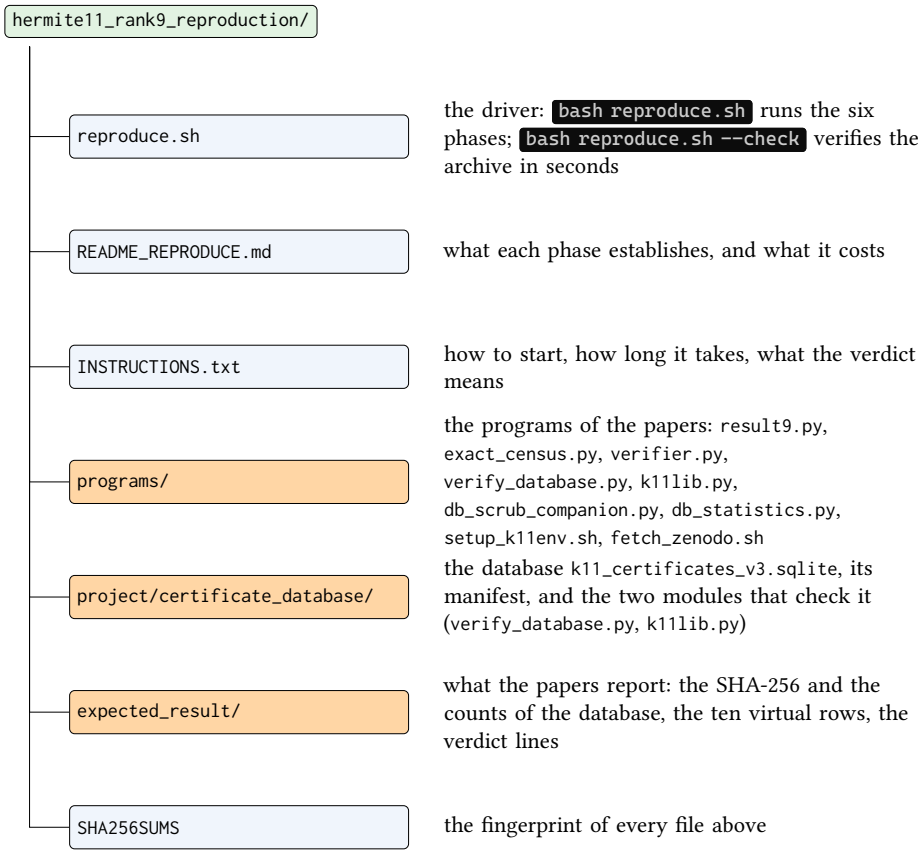

Fig. 5. What is inside the reproduction pack `hermite11_rank9_reproduction.zip` (1.44 GB). The light green box is the top folder of the pack, the orange boxes are folders and the blue boxes are single files. The 64 files of the classification are not in it: the phase **download** fetches them from Zenodo record 15707640 and checks their MD5.

the ten virtual rows and the canonical rows of `hand_proof`, and a new manifest: 0 failures (3 h 21 min).

5. **verify**, in three phases of `verifier.py` (B, C, D), on the rebuilt file. Phase B scans the 2 237 251 040 records of the data set as described in Section 3 (Computational result 5), exactly on every record, matches every survivor to a row of the database and every row's matrix and scale to the data set: the 4 487 813 survivors are the database, keys `EQUAL`, 0 missing, 0 extra, 0 matrices differing, 0 scales differing (42 min). It writes `phaseB_transcript.json`, whose root is the root of phase **ten**: the two scans read the same records and take the same decisions. Phase C re-checks every certificate in exact arithmetic, by the algorithm of Section 5 for its kind (Algorithms 1–8) or by the three conditions of Section 6.4 for a `virtual` row: 0 failures (3 h 17 min of wall time, 5 h 30 min of processor time). Phase C computes $\min G$ exactly and checks $\min G = s$ for every row not of kind `trace`; a `trace` row

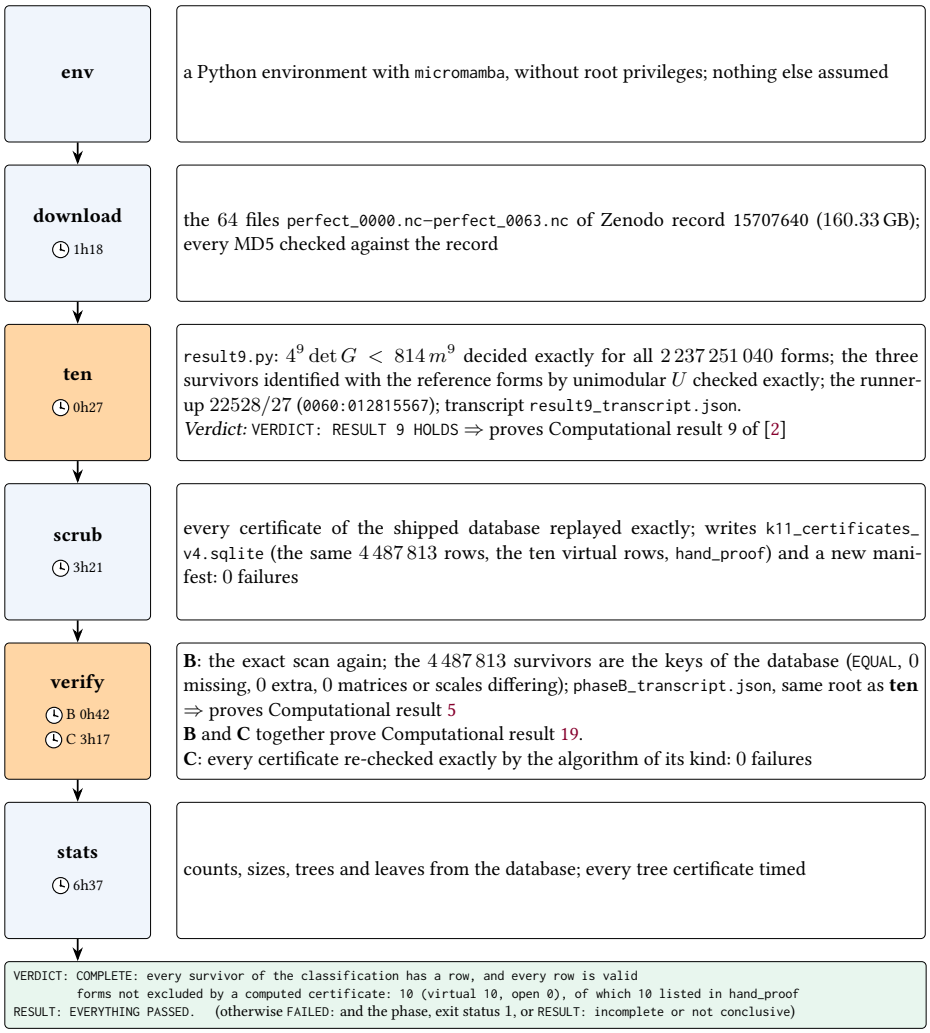

Fig. 6. What `bash reproduce.sh` does. Each phase is resumable; the clocks give the wall time of each phase in the verification run (one node, Intel Xeon Platinum 8380, 156 processes); env takes seconds. The two orange phases contain the exact scans of the data set (**ten** and **verify B**); their transcripts have the same root (Figure 2). The blue phases do not scan the data set.

needs only a vector of G of norm at most s (Section 5.2). Phase D prints the report (the counts by kind, the rows of `hand_proof`, the SHA-256 and size of the database, the time of each phase), writes `verifier_report.json` and gives the verdict below.

6. **stats**: the counts, the sizes, the trees and their leaves (Section 7.4) are computed from the database, and every tree certificate is timed separately (6 h 37 min, of which 3 h 19 min for the largest tree).

The run ends with the verdict and the result (the verifier prints each `VERDICT` line on one line; they are cut here at ↩):

```
VERDICT: COMPLETE: every survivor of the classification has a row, and ↩
         every row is valid
         forms not excluded by a computed certificate: 10 ↩
         (virtual 10, open 0), of which 10 listed in hand_proof
RESULT: EVERYTHING PASSED.
```

Otherwise it stops with `FAILED:` and the name of the phase (exit status 1), or ends with `RESULT: incomplete or not conclusive` and points to the logs. The tree of `0060:012815567` has 763 594 leaves and takes 3 h 19 min on one process. For a run spanning several cluster nodes, use a shared working directory.

What is checked. To audit the global finite assertions, a reader checks `verify_database.py`, `k11lib.py` and their arithmetic and enumeration dependencies against the rules proved here. The scan needs no separate justification, since it is exact; its transcript lets a reader recheck any part of it without the whole run, with `<dir>` the folder of the data set and `<out>` the results folder of the pack:

```
$ python3 programs/exact_census.py check --data <dir> \
        --transcript <out>/result9_transcript.json --random 50
```

recomputes 50 random blocks and the root. The verifier reads the data set; it selects candidate survivors by the determinant test (3) (Section 3) and checks that the survivors are exactly the keys of the database (same number, same keys, same Gram matrices and the same scale s); for every survivor it runs the check of its row in exact arithmetic; and it prints the counts by kind, the rows of `hand_proof`, the rows that failed (if any) and the verdict.

7.2 Structure

The scan. A module reads each file in chunks of 10^6 records, unpacks the 45 entries (the lower triangle, row by row) into G, computes $\det G$ of every record exactly by Bareiss elimination, decides (3) in integers and feeds the transcript (Section 3); the minimum of a survivor is computed by LLL and Fincke–Pohst enumeration in integers.

The check of one row. The function `verify_row(kind, G, s, cert)` returns `(True, '')` or `(False, reason)`. A `trace` row is checked by `verify_trace`, about thirty lines of Python that need nothing but the interpreter (exact determinant by Bareiss elimination, Sylvester's criterion, the integer test ge_{T_1}). Every other kind needs the library `k11lib.py` (`numpy` and `fpylll`, the latter for exact LLL and enumeration): `exact_minimum`

first checks $\min G = s$; then `verify_certificate2` (`domain`), `verify_glue_certificate` (`glue`), `verify_tree_certificate` or `verify_box_certificate` (`tree`; the two families are told apart by the key `"box_basis"` in the head of the certificate, and the file is read line by line so that a tree with very many leaves is verified without holding all its leaves in memory), `real_chain_check` together with the two checks of `hand_proof` and `VIRTUAL_KEYS` (`virtual`). An `open` row is valid only if its blob is empty.

The whole database. The rows are cut into ranges of ids, small around the rows that need the library and larger elsewhere, and the ranges are checked by a pool of processes (one per processor, one thread each), with progress lines every 30 seconds. The counts of valid rows by kind are compared with `info.counts`, and the verdict is positive only if no row failed and the counts agree. The largest tree (Section 7.4) can be checked subtree by subtree over all processors.

7.3 Dependencies, sizes and timing

Python 3; `numpy`; `fpylll` (with `cysignals`); the NetCDF reader for the data set; all installed by the phase **env** of the pack. The rows of kind `trace`, all but 1 374, need Python alone. The database is the file of Section 6 (1 918 717 952 bytes). Section 7.1 gives the full-run timings. In the verification run, a `trace` row takes 0.38 ms on one processor (all of them: 28 min of processor time); the six other trees with more than 10^4 leaves take from 3 min (19 506 leaves) to 19 min (102 822 leaves) each on one processor, and the tree of `0060:012815567` alone takes 3 h 19 min on one processor and dominates the wall time of the phases **scrub**, **verify** (phase C) and **stats**; the other 63 trees take less than ten seconds each.

7.4 Statistics of the certificates

The phase **stats** of the pack reads the database and prints what follows (Figure 7).

Sizes. The column `cert` holds 1 195 MB in all. A `trace` certificate has from 83 to 257 bytes (median 110; 545 MB in all); all have the denominator $D = 10^8$, and 2 619 885 of them carry a single vector, the mean number of vectors being 2.7 and the maximum 25. A `domain` certificate has from 333 to 1 080 bytes (median 514) and from 1 to 96 vectors (median 7). A `glue` certificate has from 2 677 to 7 057 bytes (median 4 564), from 88 to 137 vectors (median 116) and from 315 to 1 015 triangles (median 556). A `virtual` row has from 79 to 134 bytes. The 70 `tree` certificates hold 648.5 MB compressed (2 662 MB of JSON lines): 2 281 bytes for the smallest, 331 220 848 bytes for the tree of `0060:012815567`, median 9 169 bytes.

Trees. The 70 trees have 1 134 134 leaves in all, every count equal to the one recorded in the head of the certificate, and the SHA-256 of every tree equal to the one listed in the manifest. The 40 trees of cases have 935 leaves in all (from 1 to 310, median 4); every leaf is a certificate $\{H, D, w, \nu, \mu^{-}\}$ of Lemma 12 (kind `case` in the statistics), and no leaf is an empty region. The 30 trees of boxes have 1 133 199 leaves: 21 of them have a single `pspec` leaf on the root box, two have 1 669 and 2 395 leaves (`pattern`

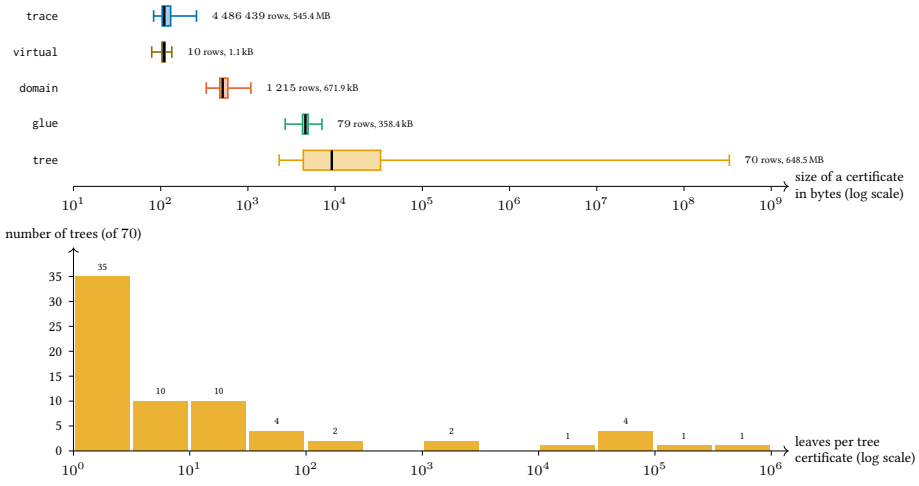

Fig. 7. The certificates of the database, from the phase **stats** of the verification run (`statistics/sizes.csv` and `statistics/trees.csv`). Top: the size in bytes of a certificate, by kind: the line runs from the smallest to the largest, the box from the first to the third quartile, the black mark is the median. Bottom: the 70 tree certificates by number of leaves, two bins per decade; they have 1 134 134 leaves in all, from 1 to 763 594.

Table 4. The seven trees of boxes with more than 10^4 leaves: leaves by kind, size of the pool of dual vectors, and size of the compressed certificate in MB. The first tree carries symmetry data.

form	leaves	uspec	outside	spec	pspec	box	pattern	pool	MB
`0060:012815567`	763 594	392 145	332 452	–	37 258	1 739	–	101	331.2
`0032:026805553`	102 822	–	–	51 473	43 357	7 062	930	122	93.6
`0046:021552255`	80 783	–	–	53 405	25 190	2 073	115	99	71.2
`0014:002912669`	58 602	–	–	28 052	22 640	5 469	2 441	115	51.1
`0011:011658070`	54 766	–	–	28 672	23 913	2 181	–	93	49.3
`0005:013978373`	49 041	–	–	19 720	20 969	7 240	1 112	93	32.6
`0023:005241687`	19 506	–	–	9 939	6 022	2 437	1 108	117	14.8

and box), and seven have more than 10^4 leaves (Table 4). By kind, the leaves of the trees of boxes are: uspec 392 145, outside 332 452, spec 191 261, pspec 179 370, box 28 677, pattern 9 294. One tree carries symmetry data, that of `0060:012815567`, and *no tree has a leaf of kind* three: every tree certificate of the database proves $d \geq d_{\text{cut}}$ (Theorem 20); the leaves of the third level, implemented and verified (Section 5.9), were not needed. The weakest leaf of the largest tree clears d_{cut} by a relative margin of $2.22 \cdot 10^{-8}$: its least value is $1113.0488306\ldots$ against $d_{\text{cut}} = 1113.0488059\ldots$, compared exactly in integers. The program `margin.py` runs the exact check of this tree with the checker of the pack, unchanged, and records the least value over its 823 287 comparisons; it and its result `margin_result.json` are in the verification report `hermite11_verification_report.zip` of the Zenodo record.

8 Assembly

Computational result 19. The database of Section 6 has exactly the $4\,487\,813$ survivor keys of Computational result 5, with their correct Gram matrices and scales. Each nonvirtual row contains a certificate satisfying the exact verification rules of Section 5, including completeness of every covering tree. The counts are those of Table 2; the ten virtual rows are exactly the keys of Table 3 and satisfy the conditions of Section 6.4. There is no open row and no leaf of kind `three` in the 70 trees.

This global finite verification is the run of the reproduction pack described in Section 7.1 (SHA-256 `22a9336ef6677171...`), which ended with `RESULT: EVERYTHING PASSED`. The root paper imports from this paper one statement about the survivors that are not macadamias [2, Section 6.2, "What is imported, precisely"]; we state it in the root paper's form.

Theorem 20 (the exclusion at rank 10). *Assume Hypothesis 2, Theorem 3 and Computational results 5 and 19. Let P be a survivor other than the ten of Table 3, and let M be a lattice of rank* 10 *with* $\min M \geq 4$ *whose section N by a shortest vector of M^* has a Gram matrix admissibly marked by P (Appendix E). Then* $\det M \geq d_{\mathrm{cut}}$.

Proof. Suppose $d = \det M < d_{\mathrm{cut}}$, and let $u = \min M^*$, $e = \det N$, $t = \min N^*$. The pair (N, M) satisfies (Domain) by the marking, (M) because $\min M \geq 4$, (T) and (L2) because N and M are lattices with $\min N^* = t$ and $\min M^* = u$, (u) because $d < d_{\mathrm{cut}}$ and Theorem 3 applies to M^*, and (Symmetry); and $e/t \leq 4d/3 < T_Q$ by (1), which uses only M and N. By Computational result 19 the row of P is of kind `trace`, `domain`, `glue` or `tree`, and it verified. A `trace` or `domain` row gives $e/t \geq T_Q$ (Sections 5.2 and 5.3), a `glue` row gives $d \geq d_{\mathrm{cut}}$ (Section 5.4), and a `tree` row, none of which has a leaf of kind `three` (Computational result 19), gives $d \geq d_{\mathrm{cut}}$ for the first gluing of M over N, whatever L (Section 5.6, Proposition 18): the lemmata of those leaves use (Domain), (T), (L2), (M), (u) and (Symmetry) only. Either conclusion is a contradiction. □

Proof of Theorem 1. Under the stated hypotheses, suppose a lattice L of rank 11 has minimum 4 and determinant below 972. By Theorem 3 and Proposition 4 there is a chain $L \supset M \supset N$ with $\min L = 4$, $\Delta < 972$, $d < d_{\mathrm{cut}}$, and N lies over a perfect form P of rank 9 with $\min P = 4$ and $\det P < e_{\mathrm{cut}}$ (Section 2.3). By Hypothesis 2 and (3), P is equivalent to a survivor, which we take as P; by Computational results 5 and 19 the survivor is a key of the database, and its row verified. If the row is of kind `trace` or `domain`, Sections 5.2 and 5.3 give $e/t \geq T_Q$, contradicting (1). If it is of kind `glue`, Section 5.4 gives $d \geq d_{\mathrm{cut}}$, contradicting Proposition 4. If it is of kind `tree`, Section 5.6 or Proposition 18 gives $d \geq d_{\mathrm{cut}}$ or $\Delta \geq 972$, a contradiction either way. If it is of kind `virtual`, P is one of the ten forms of Table 3: for `0052:005247066`, Theorem 45 gives $\Delta \geq 972$, and for the nine others the companion paper cited in the table proves the same statement (*let $L \supset M \supset N$ be a chain as in Proposition 4 whose rank-*9 *member has a Gram matrix admissibly marked by P; then $\Delta \geq 972$*) for the form printed in its appendix, which is the record of the data set entry by entry (the script `hermite11\_printed\_forms\_check.py` of the Zenodo record, [2, Section 9], checks the

eleven printed forms of the series against the rows of their keys in the certificate database), so that the marking transports; a contradiction. There is no row of kind open. Hence every lattice of rank 11 with minimum 4 has determinant at least 972, that is, $\gamma_{11} \le 4/\sqrt[11]{972}$ by [2, equation (1)]; and K_{11}, with minimum 4 and determinant 972 [9, entry KAPPA11], attains it. □

The hypotheses inherited. Theorem 1 uses the following inputs.

1. Hypothesis 2: the completeness of the classification of [1], used only for the perfect forms of determinant below e_{cut} at minimum 4.
2. Theorem 3 (dimension 10, [2]), which itself rests on Hypothesis 2 and on the computational result of [2] that exactly three records pass the integer filter $4^9 \det G < 814 m^9$, where $m = \min_i G_{ii}$; Proposition 4 and the marking of [2, Proposition 7], proved in [2].
3. Computational result 5: the complete selection of the survivors (the run of the reproduction pack, Section 7.1).
4. Computational result 19: the exact verification of every row and covering tree of the database, by the same run (Section 7.1).
5. Computational result 46: the complete gluing cover for `0052:005247066`, on which Theorem 45 rests.
6. The five companion papers [3,4,5,6,7], each of which proves, for its forms, the statement quoted in the proof above, and states the hypotheses it inherits in turn (the statements of Appendix D among them).

The lemmata of Section 5 are proved here or in [2]; the correctness of the verifier is a matter of reading its code against those lemmata, which are stated in the form the code implements.

Lean correspondence. The Lean statement for the case `0052` is `Hermite11.case0052_of_finite_computational_facts`, in `hermite11_lean_proofs.zip`. Its finite hypotheses, integral-equivalence wrappers and saved reference records are listed in `case_map.json`. The cover itself (Computational result 46) is checked outside Lean.

9 Use of computational tools

Refer to Section 10 of [2].

References

1. Dutour Sikirić, M., van Woerden, W.: The lattice packing problem in dimension 9 by Voronoi's algorithm. arXiv:2508.20719 (August 2025; v2, 2026). Data: https://doi.org/10.5281/zenodo.15707640
2. Géraud-Stewart, R., Naccache, D.: The Hermite constants in dimensions 10, 11 and 12. Posted concurrently to this work (2026)
3. Géraud-Stewart, R., Naccache, D.: γ_{11}: contact geometry. Posted concurrently to this work (2026)
4. Géraud-Stewart, R., Naccache, D.: γ_{11}: reduction by sections. Posted concurrently to this work (2026)
5. Géraud-Stewart, R., Naccache, D.: γ_{11}: a finite spectral relaxation. Posted concurrently to this work (2026)
6. Géraud-Stewart, R., Naccache, D.: γ_{11}: one selected contact, two linked blocks. Posted concurrently to this work (2026)
7. Géraud-Stewart, R., Naccache, D.: γ_{11}: unequal triangles and adapted references. Posted concurrently to this work (2026)
8. Martinet, J.: Perfect Lattices in Euclidean Spaces. Grundlehren der mathematischen Wissenschaften, vol. 327. Springer, Berlin (2003). https://doi.org/10.1007/978-3-662-05167-2
9. Nebe, G., Sloane, N.J.A.: A catalogue of lattices. Entries KAPPA9.2, KAPPA11, K12, http://www.math.rwth-aachen.de/~Gabriele.Nebe/LATTICES/
10. Schrijver, A.: Theory of Linear and Integer Programming. Wiley, Chichester (1986)
11. Voronoï, G.: Nouvelles applications des paramètres continus à la théorie des formes quadratiques. Premier mémoire. Sur quelques propriétés des formes quadratiques positives parfaites. J. Reine Angew. Math. **133**, 97–178 (1908). https://doi.org/10.1515/crll.1908.133.97
12. Horn, R.A., Johnson, C.R.: Matrix Analysis, 2nd edn. Cambridge University Press, Cambridge (2013). https://doi.org/10.1017/CBO9781139020411

A The thresholds and the integer tests

The constants of Section 3.2 and the integer tests that the verifier applies ($e_{\text{cut}}^{55} = 2^{246}3^{197}$, $d_{\text{cut}}^{11} = 4^{11}972^9$). Every test is an inequality between two (large) integers; Python's integers are unbounded, so no overflow can occur.

constant	value	test $x = n/m \geq$ constant
$e_{\text{cut}} = 4\,\sqrt[10]{d_{\text{cut}}^9}/\sqrt[10]{768}$	$1136.0218\ldots$	$n^{55} \geq 2^{246}3^{197}m^{55}$ (the scan tests $<$)
$d_{\text{cut}} = 4\,\sqrt[11]{972^9}$	$1113.0488\ldots$	$n^{11} \geq 4^{11}\,972^9\,m^{11}$
$T_Q = \frac{16}{3}\,\sqrt[11]{972^9} = \frac{4}{3}d_{\text{cut}}$	$1484.0651\ldots$	$(3n)^{11} \geq 16^{11}\,972^9\,m^{11}$
$T_1 = T_Q\,(9/10)^{10}$	$517.4615\ldots$	$n^{11}3^{11}10^{110} \geq m^{11}16^{11}972^9\,9^{110}$
$972 = 2^2 \cdot 3^5$	972	$n \geq 972\,m$
$\det P/d_{\text{cut}}$ (lower end of u)		$(4u_0)^{11}\,972^9 \leq (\det P)^{11}$
$\sqrt[5]{4/3}$ (upper end of u)	$1.0592\ldots$	$3u_1^5 \geq 4$

The survivor test (3) is $(4^9 \det G)^{55} < 2^{246}3^{197}m^{495}$ with m the least diagonal entry of G; it is the test $e_{\text{cut}} > 4^9 \det G/m^9$ with $x = 4^9 \det G/m^9$, both sides raised to the 55th power. The factor $E(s)$ of Lemma 13 is evaluated as the fraction $9^9p^{10}/(q(10p-q)^9)$ with $p = \Sigma$ and $q = 10\min_c H[c]$ (or 1 if $p \leq q$), so that the value of a leaf is a single fraction compared with d_{cut} by the second test.

B The layout of the certificates

Every blob of the column `cert` is either `zlib`-compressed JSON (kinds `trace`, `domain`, `glue`, `virtual`) or the bytes of a gzip file holding one JSON object (kind `tree`). All numbers are integers, or pairs [numerator, denominator] where a rational is meant; vectors are lists of nine (or ten) integers; matrices are lists of rows.

- `trace`: `"U"` (9×9), `"z"` (vectors z_i), `"c"` (integers $c_i > 0$), `"D"` (integer > 0); optional `"x"` (a vector with $G[x] \leq s$).
- `domain`: `"basis_U"`, `"H"` (9×9 symmetric), `"D"`, `"vectors"` (z_i), `"weights"` (c_i).
- `glue`: as `domain`, plus `"triangles"` (triples $[i,j,k]$, $i < j < k$) and `"alpha"` (integers $a_T \geq 0$, one per triangle); some rows also carry `"value_num"`, `"value_den"`, which the checker ignores.
- `tree`, head: `"basis_U"`, `"vectors"` (the pool), `"triangles"`, `"leaves"` (the number of leaves), and, for a tree of boxes, `"box_basis"` (nine pool indices), `"unit"` ($= 4096$), `"box_L"`, `"box_DL"`, optionally `"sym"` $= \{$`"p0"`, `"V"`, `"root"`, `"faces"`$\}$; then `"tree"`.
- inner node: `"v"` (a pool index, or a coordinate j for boxes), `"at"` (the cut), `"le"`, `"ge"` (the two subtrees).
- leaf of a tree of cases: `"H"`, `"D"`, `"w"` (pairs $[i, c_i]$), `"nu"` (pairs $[\text{row}, \nu]$), `"mum"` (pairs $[i, \mu_i^-]$); or `"empty"` (nine pool indices).
- leaf of a tree of boxes: `"H"`, `"D"`, `"w"`, and `"kind"` $\in \{$`pattern`, `spec`, `pspec`, `uspec`, `outside`, `three`$\}$ (absent for `box`), with the data of Table 1: `"x"` (`box`); `"nu"`, `"mum"` (`pattern`, `pspec`); `"vec"`, `"vw"`, `"vd"`, `"gam"`, `"M"`, `"s"`, `"ab"`, `"abd"` (`spec`, `pspec`); `"pieces"` (`uspec`: a list of $\{$`"lo"`, `"hi"`, $\ldots\}$); `"g"` (`outside`); `"v2"`, `"v3"`, `"tri"` (`three`).
- `virtual`: `"tau"` (nine rationals), `"u"` (a rational), `"det"` (a rational), `"name"` (text).

The tree file. The gzip file of a `tree` row is ordinary JSON (`json.load(gzip.open(path))` reads it), laid out so that it can be read without holding all leaves in memory: the first line is the head (the keys above, in this order, ending with `"tree":`), then one line per leaf and one line per inner node.

```
{"basis_U":[...],"vectors":[...],"box_basis":[...],"unit":4096,
 "triangles":[...],"box_L":[...],"box_DL":64,"sym":{...},"leaves":763594,"tree":
{"v":3,"at":1024,"le":
{"H":[[...]],"D":100000000,"w":[[i,c],...],"kind":"spec",...}
,"ge":
...
}
}
```

`k11lib.read_tree_certificate(path)` reads it line by line and hands the leaves to the verifier one at a time.

C Reading the database

The following lines open the database read-only, print its counts, read one row and, for a tree, write the certificate file; `verify_row` then checks it.

```
import sqlite3, struct, zlib, json
DB = 'k11_certificates_v3.sqlite'
con = sqlite3.connect('file:' + DB + '?mode=ro', uri=True)  # read-only

def gram(blob):                                             # the 9x9 matrix G
    v = struct.unpack('<45h', bytes(blob))
    G = [[0] * 9 for _ in range(9)]; k = 0
    for i in range(9):
        for j in range(i, 9): G[i][j] = G[j][i] = v[k]; k += 1
    return G

info = dict(con.execute('SELECT name, value FROM info'))
print(json.loads(info['counts']))
q = 'SELECT kind, step, COUNT(*) FROM form GROUP BY kind, step'
for kind, step, n in con.execute(q): print(kind, step, n)
q = 'SELECT key, statement FROM hand_proof ORDER BY key'
for key, statement in con.execute(q): print(key, statement)

q = 'SELECT key, scale, gram, kind, step, cert FROM form WHERE key = ?'
key, s, g, kind, step, cert = con.execute(q, ('0050:024468269',)).fetchone()
G = gram(g)
if kind in ('trace', 'domain', 'glue', 'virtual'):
    c = json.loads(zlib.decompress(cert))                   # a dict (Appendix B)
elif kind == 'tree':
    path = key.replace(':', '_') + '.tree.json.gz'
    open(path, 'wb').write(cert)                            # the certificate file
    import k11lib; t = k11lib.read_tree_certificate(path)

import verify_database as vd
ok, why = vd.verify_row(kind, G, s, cert)                   # (True, '') or (False, why)
```

The whole database is checked by

```
$ python3 verify_database.py k11_certificates_v3.sqlite [processes]
```

which prints the SHA-256 of the file, checks every row, compares its counts with `info.counts` and ends with the verdict of Section 7; `k11_certificates_v3.sqlite` is the

file shipped in the pack (the scrub writes `v4`). The reproduction pack does not type this command itself: its phase **verify** runs `verifier.py`, which imports `verify_database.py` from the folder of the database and applies the same row check to every row as its phase C, after the scan of phase B, and reports in phase D (Section 7.1). The column `gram` holds the upper triangle of G row by row, as the function `gram` above reads it; the data set holds the lower triangle row by row.

D The common coordinate system and the common inequalities

The local papers and case `0052` use the notation $\Delta = \det L$, $d = \det M$, $e = \det N$, $u = \min M^*$ and $v = \min L^*$. This toolbox contains their shared arguments. Read Sections D.1–D.2 for the admissible chain and its coordinates, then the relevant inequality; Section D.6 handles reference-cell covering arguments, and Section D.7 gives the common exact-verification rules. The stored global certificates use primal gluing coordinates τ, φ as in Section 2.4. For the dual coordinates below, $\beta = -\tau$ and $(\alpha, \vartheta) = -\varphi$; this is a change of sign of the two extension generators.

D.1 Successive shortest dual normals

Let L have rank eleven, minimum four, and determinant $\Delta < 972$. Replacing L by a rescaled dual if necessary, we can arrange $\gamma(L^*) \le \gamma(L)$; this replacement preserves the existence of a counterexample, since if the dual has the larger Hermite invariant, it too exceeds the target. Choose a shortest nonzero dual vector n_{11}, let $v = |n_{11}|^2$, and set $M = L \cap n_{11}^{\perp}$. Choose similarly $n_{10} \in M^*$ shortest, with $|n_{10}|^2 = u$, and let $N = M \cap n_{10}^{\perp}$. Write

$$e = \det N, \qquad d = \det M = \frac{e}{u}, \qquad \Delta = \det L = \frac{e}{uv}. \tag{8}$$

Shortest dual vectors are primitive, and a basis adapted to either primitive hyperplane proves these determinant identities ([2, Fact 4]: the perpendicular height is the reciprocal of the dual normal length). Moreover

$$768 \le d < d_{\mathrm{cut}} := 4\,\sqrt[11]{972^9}, \qquad e < e_{\mathrm{cut}} := \sqrt[10]{\frac{4096}{3}}\ \sqrt[10]{d_{\mathrm{cut}}^9} < 1137. \tag{9}$$

Indeed $v \le 4\Delta^{-2/11}$, so $d = v\Delta < d_{\mathrm{cut}}$; Theorem 3 applied to M gives $d \ge 768$, and applied to the minimum-four rescaling of M^* it gives $u^{10} d \le 4096/3$, hence $e = ud \le \sqrt[10]{4096/3}\, d^{9/10}$. The exact descriptions used in every strict comparison are $d_{\mathrm{cut}}^{11} = 4^{11} 972^9$ and $e_{\mathrm{cut}}^{55} = 2^{246} 3^{197}$; no decimal cutoff enters a proof. This is Proposition 4, with the same cutoffs throughout.

D.2 A common coordinate system

The nested sections $L \supset M \supset N$ form a *flag*. A flag bound combines constraints from the two successive extensions to bound Δ.

Choose an integral basis of N, let Q be its Gram matrix, and let $X = Q^{-1}$. Two gluing vectors $\beta, \alpha \in \mathbb{R}^9$ and a scalar $\vartheta \in \mathbb{R}$ describe the whole chain. The squared dual length at $(z, k, k') \in \mathbb{Z}^9 \times \mathbb{Z}^2$ is

$$X[z] + u\,(\beta^{\mathsf{T}} z + k)^2 + v\,(\alpha^{\mathsf{T}} z + \vartheta k + k')^2. \tag{10}$$

The primal squared length at (x, k, k') is

$$Q[x - k\beta - k'(\alpha - \vartheta\beta)] + \frac{(k - \vartheta k')^2}{u} + \frac{k'^2}{v}. \tag{11}$$

These expressions follow by inverting the triangular coordinate map, or by pairing the displayed primal and dual bases. Their determinant is $e/(uv)$. They keep both successive-normal conditions, as well as minimum four in the primal lattice. Write $\|t\| = \min_{j\in\mathbb{Z}} |t - j|$. Shortness of $n_{10} \in M^*$ gives

$$X[z] + u\,\|\beta^{\mathsf{T}} z\|^2 \geq u \qquad (z \neq 0). \tag{12}$$

Shortness of $n_{11} \in L^*$ gives the analogous inequality for lifts of every nonzero vector of M^*; applied to a lift of n_{10} it yields $v \leq 4u/3$. (These are (L2), (L3) and $v \leq 4u/3$ of Section 2.4.)

A minimum-four form is perfect if the tensors cc^{T} of its minimum vectors span the vector space of symmetric matrices; equivalently its contact equations determine it uniquely. The minimum-four Ryshkov polyhedron is the set of symmetric matrices Y satisfying $Y[z] \geq 4$ for every nonzero $z \in \mathbb{Z}^9$; its positive definite vertices are the perfect forms. Voronoi's reduction [11,8] supplies such a form P with

$$\begin{gathered} X = \sum_{c \in \mathcal{C}(P)} w_c\, cc^{\mathsf{T}}, \qquad w_c \geq 0, \qquad \sum_c w_c \leq \frac{9}{4}, \qquad w_c \leq \frac{1}{4}, \\ \operatorname{tr}(PX) \leq 9, \qquad \det P \leq e. \end{gathered} \tag{13}$$

Here $\mathcal{C}(P)$ contains one vector from each opposite pair of minimum vectors. This is the marking of [2, Proposition 7] and the hypothesis (Domain) of Section 2.4. The existence proof, including compactness and the coefficient bounds, is given in [2, Proposition 7].

Definition 21 (admissible residual chain). *A chain is admissible for P if it satisfies the minimum conditions, the successive shortest-normal conditions, the cutoffs (9), and the marking (13). Excluding a residual case means proving that no such chain can have $\Delta < 972$. The reduction above supplies every condition. The local case theorems assume this chain directly; classification and the global census are used only to show that its marker occurs in the finite list.*

Physical coordinates. When Euclidean coordinates are more useful, choose C_P with $P = C_P^{\mathsf{T}} C_P$ and write

$$Q = C_P^{\mathsf{T}} S C_P, \qquad R = S^{-1}. \tag{14}$$

Thus S is a physical section metric, $\det S = e/\det P$, and $\operatorname{tr} R = \operatorname{tr}(PX) \leq 9$. Integral vectors c, z become $C_P c$, $C_P^{-\mathsf{T}} z$. In the rank-eleven case arguments, Q, X denote matrices in lattice coordinates, S, R physical section metrics, and G a physical rank-ten metric; a case using a different reference scale states that scale before using it.

Block matrices. For $\mathcal{H} = \begin{pmatrix} A & B \\ B^{\mathsf{T}} & C \end{pmatrix}$ with $A \succ 0$, the *Schur complement* of A is $S_C = C - B^{\mathsf{T}}A^{-1}B$. Completing the square gives

$$\mathcal{H}[x, y] = A[x + A^{-1}By] + S_C[y], \qquad \det \mathcal{H} = \det A \, \det S_C.$$

Thus $\mathcal{H} \succ 0$ exactly when $S_C \succ 0$; the lower-right block of $\mathcal{H}^{-1}$ is S_C^{-1}. We write $\mathrm{cof}_{ij} A = (-1)^{i+j} \det A_{\widehat{i},\widehat{j}}$ for a cofactor (delete row i and column j) and $\mathrm{adj}\, A = (\mathrm{cof}_{ji} A)_{ij}$ for the adjugate. Then $A^{-1} = \mathrm{adj}\, A / \det A$ when A is invertible. These identities underlie the determinant and inverse-trace estimates below.

D.3 Additive dual vectors

Lemma 22 (circle triangle). *If $t_0 + t_1 + t_2 = 0$ in $\mathbb{R}/\mathbb{Z}$, then $\sum_i \|t_i\| \le 1$. Consequently, if $y_0 + y_1 + y_2 = 0$ are nonzero vectors of M^* of squared lengths b_i, then the squared length v of the last normal satisfies*

$$\sum_{i=0}^{2} \sqrt{\max\left\{0,\, 1 - \frac{b_i}{v}\right\}} \;\le\; 1. \tag{15}$$

In particular $v \le (9/8)\max_i b_i$.

Proof. Choose representatives $r_i \in [-\frac{1}{2}, \frac{1}{2}]$. Their sum is 0 or ± 1. In the first case $\sum |r_i| = 2\max|r_i| \le 1$. In the second all nonzero terms have the same sign, so $\sum |r_i| = 1$. For the dual vectors, shortness gives $b_i + v\|t_i\|^2 \ge v$. Sum the resulting lower bounds for the three distances. If $v > (9/8)\max_i b_i$, each distance would exceed $1/3$. □

Lemma 23 (one section vector controls both extensions). *For every $0 \ne z \in \mathbb{Z}^9$,*

$$\Delta \ge \frac{e}{2X[z]^2}. \tag{16}$$

If three nonzero section covectors sum to zero and all have squared X-length at most x, then

$$\Delta \ge \frac{16e}{27x^2}. \tag{17}$$

Proof. Let $x = X[z]$ and $t = \|\beta^{\mathsf{T}} z\| \in [0, \frac{1}{2}]$. The two nearest first lifts and their difference have squared lengths $x + ut^2$, $x + u(1-t)^2$, and u. Equation (12) gives $u \le x/(1-t^2)$, and $u \le x + u(1-t)^2$ because $t \le 1/2$. The circle lemma and $v \le 4u/3$ therefore give

$$\frac{\Delta x^2}{e} \ge \max\left\{\frac{3}{4}(1-t^2)^2,\; \frac{4}{9}(1-t)(1+t)^2\right\}.$$

For $t \le 1/3$ the first expression is at least $16/27 > 1/2$. On $[1/3, 1/2]$ the second decreases to $1/2$, proving (16). For a section triangle, one first phase has distance at most $1/3$, so (12) gives $u \le 9x/8$. Together with $v \le 4u/3$, this yields $\Delta \ge 3e/(4u^2) \ge 16e/(27x^2)$, proving (17). □

Lemma 24 (a weighted section triangle). *Let $z_1, z_2, z_3 \in \mathbb{Z}^9 \setminus \{0\}$ satisfy $z_1 + z_2 + z_3 = 0$, and let $q_i = X[z_i]$ and $Q_\triangle = q_1 + q_2 + q_3$. Then*

$$\Delta \geq \frac{841\, e}{162\, Q_\triangle^2}. \tag{18}$$

Proof. Write $p_i = \|\beta^{\mathsf{T}} z_i\| \in [0, \frac{1}{2}]$. The circle lemma gives $\sum_i p_i \leq 1$. The phase-dependent inequalities in the proof of Lemma 23, before taking their uniform minimum, give, for $y_i = \sqrt{2\Delta/e}\, q_i$,

$$y_i^2 \geq \frac{3}{2}(1 - p_i^2)^2, \qquad y_i^2 \geq \frac{8}{9}(1 + p_i)^2(1 - p_i).$$

We prove $\sum_i y_i \geq 29/9$ using rational lower bounds. Set

$$a_* = \frac{153}{125}, \qquad t_* = \frac{11}{27}, \qquad f_0(p) = a_*(1 - p^2), \qquad f_1(p) = \frac{2086 - 422p}{1875}.$$

Since $a_*^2 < 3/2$, we have $y_i \geq f_0(p_i)$. For $t_* \leq p \leq 1/2$, the identity

$$8 \cdot 1875^2(1 + p)^2(1 - p) - 9(2086 - 422p)^2 = (1 - 2p)R(p),$$
$$R(p) = 14062500p^2 + 21895128p - 11037564$$

shows that $y_i \geq f_1(p_i)$ when $p_i \geq t_*$. Indeed R is increasing for $p \geq 0$ and $R(t_*) = 17559040/81 > 0$; both y_i and $f_1(p_i)$ are nonnegative. The two lower bounds agree at t_*.

There are three cases, up to permuting the indices. If all $p_i \leq t_*$, concentration of bounded mass (Lemma 40) gives

$$\sum_i p_i^2 \leq 2t_*^2 + (1 - 2t_*)^2 = \frac{89}{243}, \qquad \sum_i y_i \geq a_* \frac{640}{243} = \frac{2176}{675}.$$

If exactly one phase, denoted p, exceeds t_*, denote the others by q, r. Since $q + r \leq 1 - p$ and $q, r \leq t_*$, the same mass inequality gives $q^2 + r^2 \leq t_*^2 + (1 - p - t_*)^2$. Therefore

$$\sum_i y_i \geq f_1(p) + a_*\big(2 - t_*^2 - (1 - p - t_*)^2\big).$$

This is a concave quadratic in $p \in [t_*, \frac{1}{2}]$, so its minimum is at an endpoint. The two endpoint values are $2176/675$ and $130991/40500$. If two phases p, q exceed t_*, let $v = p + q \in [2t_*, 1]$ (a local variable). The remaining phase satisfies $0 \leq r \leq 1 - v$, and hence

$$\sum_i y_i \geq \frac{4172 - 422v}{1875} + a_*\big(1 - (1 - v)^2\big).$$

Again the expression is a concave quadratic; its endpoint values are $2176/675$ and $403/125$. Three phases exceeding t_* are impossible because $3t_* > 1$. All three displayed endpoint values exceed $29/9$: their respective margins are $1/675$, $491/40500$, and $2/1125$. Thus $\sqrt{2\Delta/e}\, Q_\triangle \geq 29/9$. Squaring proves (18). □

Lemma 25 (a D_4 frame). *Suppose M^* contains a scaled D_4 root system all of whose roots have squared length at most b. Then $v \le 36b/35$ and $\Delta \ge 35d/(36b)$. In a physical metric G on a reference lattice of determinant d_0, if these roots have reference squared length one, then*

$$\Delta \ge \frac{35}{36}\, d_0 \det G\, \lambda_{\min}(G).$$

Proof. A homomorphism from the root lattice to $\mathbb{R}/\mathbb{Z}$ lifts to a real linear functional: choose real representatives on a lattice basis and extend linearly. Write the D_4 roots as $e_i \pm e_j$. Reduce the four coordinate values modulo one, and change their individual signs so that they lie in $[0, \frac{1}{2}]$. Among four ordered points in this interval, one of the three successive gaps is at most $1/6$. Their difference is the phase of one of the original roots. Shortness therefore gives $b + v/36 \ge v$. The metric comparison bounds every root's actual dual squared length by $1/\lambda_{\min}(G)$, proving the last assertion. □

D.4 Determinants and spectra

Lemma 26 (one quadratic interpolation rule). *Let f be three times continuously differentiable on an interval, and let $a \ne b$ belong to it. The quadratic q determined by $q(a) = f(a)$, $q'(a) = f'(a)$, and $q(b) = f(b)$ satisfies*

$$f(x) - q(x) = \frac{f'''(\xi)}{6}(x-a)^2(x-b) \tag{19}$$

for every x in the same interval with $x \ne a, b$, and some ξ between the smallest and largest of a, b, x. Thus $q \le f$ on $x \le b$ if $f''' \le 0$ throughout the interval, and on $x \ge b$ if $f''' \ge 0$ throughout it. Its quadratic coefficient has the sign of f'' whenever that sign is strict throughout the interval.

Proof. Subtract $c(z-a)^2(z-b)$ from $f(z) - q(z)$, choosing c to make the difference vanish at $z = x$. It also vanishes at b and has a double zero at a. Three applications of Rolle's theorem give $c = f'''(\xi)/6$. Equality holds at the interpolation nodes. The quadratic coefficient is $[f(b) - f(a) - f'(a)(b-a)]/(b-a)^2$; strict convexity or concavity gives its sign. □

Lemma 27 (inverse-trace eigenvalue bound). *Let $B \succ 0$ have size $n \ge 2$, $\operatorname{tr} B^{-1} \le n$, and $\det B < \rho$. Define*

$$F_n(t) = t\left(\frac{n-1}{n-\frac{1}{t}}\right)^{n-1} \qquad \left(t > \frac{1}{n}\right).$$

Every eigenvalue λ of B satisfies $F_n(\lambda) < \rho$. In particular, if $H > 1$ and $F_n(H) \ge \rho$, then $B \prec HI$.

Proof. The reciprocals of the other $n-1$ eigenvalues sum to at most $n - 1/\lambda$. AM–GM on those reciprocals gives $\det B \ge F_n(\lambda)$. Also

$$\frac{d}{dt}\log F_n(t) = \frac{n(t-1)}{t(nt-1)}.$$

Thus F_n increases for $t > 1$, proving the final assertion. The decreasing branch below one supplies lower eigenvalue bounds in exactly the same way. □

Lemma 28 (a shared D_n squared-norm bound). *Let E be a symmetric $n \times n$ matrix, $n \geq 4$, with $E_{ii} + E_{jj} \geq 2|E_{ij}|$ for $i \neq j$. Then $\|E\|_F^2 \leq (n+1)(\operatorname{tr} E)^2/2$.*

Proof. Write $x_i = E_{ii}$, $s = \sum_i x_i$. We first prove $\sum_i x_i^2 \leq s^2$. This is immediate if every $x_i \geq 0$. Otherwise exactly one entry can be negative: write $x_k = -u$, $u > 0$. The pair sums give $x_i \geq u$ for $i \neq k$. Set $y_k = 0$, $y_i = x_i - u$ for $i \neq k$, and $Y = \sum_i y_i \geq 0$. Then $s = Y + (n-2)u$ and

$$\sum_i x_i^2 = \sum_i y_i^2 + 2uY + nu^2 \leq Y^2 + 2uY + nu^2.$$

The difference from s^2 is $(n-1)(n-4)u^2 + 2(n-3)uY \geq 0$. Finally $4E_{ij}^2 \leq (x_i + x_j)^2$ also holds for $i = j$. Summing over all ordered pairs gives

$$4\,\|E\|_F^2 \leq 2n \sum_i x_i^2 + 2s^2 \leq 2(n+1)s^2.$$

□

Lemma 29 (shared D_n quadratic bounds). *Let $3 \leq n \leq 9$ and let E be symmetric, with $E_{ii} + E_{jj} \geq 2|E_{ij}|$ for $i \neq j$. Then $-(\operatorname{tr} E)I \preceq E \preceq 2(\operatorname{tr} E)I$.*

Proof. Write $d_i = E_{ii}$. For $x \in \mathbb{R}^n$, let $L_x = \sum_i |x_i|$, $q_x = \sum_i x_i^2$, and $f_i = 2x_i^2 - |x_i|L_x + q_x$. We first check $f_i \geq 0$ and $2f_i \leq \sum_j f_j$. Fix i and write $u = |x_i|$, $A = \sum_{j \neq i} |x_j|$, $W = \sum_{j \neq i} x_j^2$. Cauchy–Schwarz gives $A^2 \leq (n-1)W \leq 8W$, so

$$8f_i = (4u - A)^2 + 8W - A^2 \geq 0, \qquad \sum_j f_j - 2f_i = (n-3)u^2 + nW - A^2 \geq 0.$$

Consequently $\sum_i d_i f_i \geq 0$: if all $d_i \geq 0$ this is immediate; otherwise $d_k = -a < 0$ and the pair sums give $d_i \geq a$ for $i \neq k$, whence $\sum_i d_i f_i \geq a(\sum_i f_i - 2f_k) \geq 0$. Finally the off-diagonal contact bounds give

$$x^{\mathsf{T}} E x \geq \sum_i d_i(2x_i^2 - |x_i|L_x) = \sum_i d_i f_i - (\operatorname{tr} E) q_x \geq -(\operatorname{tr} E) q_x.$$

For the upper bound use $g_i = 2q_x - |x_i|L_x$ instead. The same notation gives

$$4g_i = (2u - A)^2 + 8W - A^2 \geq 0, \qquad \sum_j g_j - 2g_i = (2n-3)u^2 + 2(n-2)W - A^2 \geq 0.$$

The same diagonal argument yields $\sum_i d_i g_i \geq 0$, while

$$x^{\mathsf{T}} E x \leq \sum_i d_i |x_i| L_x = 2(\operatorname{tr} E) q_x - \sum_i d_i g_i \leq 2(\operatorname{tr} E) q_x.$$

□

Lemma 30 (directional bound for the D_n contact inequalities). *Let $n \geq 3$ and let E be symmetric with $E_{ii} + E_{jj} \geq 2|E_{ij}|$ for $i \neq j$. For $p \in \mathbb{R}^n$ put $T_E = \operatorname{tr} E$, $a_p = \max_i |p_i|$, $b_p = \min_i |p_i|$ and $S_p = \sum_i |p_i|$. Then*

$$p^{\mathsf{T}} E p \leq T_E S_p \max\Big(a_p, \frac{S_p - 2b_p}{n-2}\Big).$$

Proof. Put $d_i = E_{ii}$ and $M_p = \max(a_p, (S_p - 2b_p)/(n-2))$. The numbers $f_i = M_p - |p_i|$ are nonnegative and satisfy $2f_i \leq \sum_j f_j$, since $S_p - 2|p_i| \leq (n-2)M_p$. The diagonal criterion in the proof of Lemma 29 gives $\sum_i d_i f_i \geq 0$, hence $\sum_i d_i |p_i| \leq T_E M_p$. Using the pair inequalities on the off-diagonal terms gives

$$p^{\mathsf{T}} E p \leq \sum_i d_i |p_i|^2 + \sum_{i<j} (d_i + d_j)|p_i||p_j| = S_p \sum_i d_i |p_i| \leq T_E S_p M_p.$$

The diagonal criterion uses only the pair sums $d_i + d_j \geq 0$, so applies here for every $n \geq 3$. □

Lemma 31 (equal-diagonal determinant comparison). *Let B be a symmetric $r \times r$ matrix, $r \geq 1$, with $B_{ii} = d$ and $|B_{ij}| \leq c$ for $i \neq j$, where $c \geq 0$ and $d > (r-1)c$. Then*

$$B \succ 0, \qquad \det B \geq (d+c)^{r-1}\big(d - (r-1)c\big).$$

Proof. For every x, Cauchy–Schwarz gives

$$x^{\mathsf{T}} B x \geq (d+c)|x|^2 - c\Big(\sum_i |x_i|\Big)^2 \geq \big(d - (r-1)c\big)|x|^2.$$

This proves positivity. The determinant assertion is immediate for $r = 1$. For the induction step write $B = \begin{pmatrix} K & g \\ g^{\mathsf{T}} & d \end{pmatrix}$, let $a = d - (r-2)c > 0$, and set $h = d - g^{\mathsf{T}} K^{-1} g > 0$. The same quadratic bound gives $K \succeq aI$, while $|g|^2 \leq (r-1)c^2$. Hence

$$ah \geq ad - (r-1)c^2 = (d+c)\big(d - (r-1)c\big).$$

By induction $\det K \geq (d+c)^{r-2} a$. Multiplication by h and the Schur determinant identity finish the proof. □

Lemma 32 (a shared D_n determinant bound). *Let E be symmetric of size $n \geq 7$, $E_{ii} + E_{jj} \geq 2|E_{ij}|$ for $i \neq j$, and $0 \leq s = \operatorname{tr} E \leq 1$. If $1 + s - (n-1)s^2/4 > 0$, then*

$$I + E \succ 0, \qquad \det(I+E) \geq 1 + s - \frac{n-1}{4} s^2.$$

In particular this applies for $n = 7, 8$ with $s \leq 1$, and for $n = 10$ with $s \leq 3/10$.

Proof. At $s = 0$ the contact inequalities force $E = 0$. Assume $s > 0$. If all diagonal entries are nonnegative, their sum-s vector is a convex combination of se_i. If one entry, say i, equals $-c < 0$, every other entry is at least c, and $s \geq (n-2)c$. Subtract the

vector with entry $-c$ at i and c elsewhere. The remaining diagonal is nonnegative. Thus the entire diagonal is a convex combination of se_i and $(s/(n-2))(\mathbf{1}-2e_i)$. Keep each ratio $2E_{ij}/(E_{ii}+E_{jj}) \in [-1,1]$ fixed during this decomposition, setting it to zero when its denominator is zero. It decomposes the full matrix into matrices with the same contact inequalities and the stated extreme diagonals.
At se_i the matrix is an arrow. Its Schur complement is $1+s-\sum_{j\neq i}E_{ij}^2 \geq 1+s-(n-1)s^2/4 > 0$, which proves positivity and the determinant bound. At the other diagonal let $m = n-2$ and $c = s/m$. The negative coordinate is isolated. The other block has size $n-1$, diagonal $1+c$ and off-diagonal magnitudes at most c. Since $(n-3)c < 1$, Lemma 31 proves its positivity and determinant bound. Thus the full vertex matrix is positive definite, and

$$\det(I+E) \geq (1-c)\big(1-(n-3)c\big)(1+2c)^{n-2}$$

at this diagonal. Only the first three binomial terms are needed: $(1+2s/m)^m \geq 1+2s+2(m-1)s^2/m$. Let $P = (1-s/m)(1-(m-1)s/m) > 0$ and $k = m-5 \geq 0$. The following identity makes the comparison explicit:

$$\begin{aligned} &P\Big(1+2s+\frac{2(m-1)s^2}{m}\Big) - \Big(1+s-\frac{m+1}{4}s^2\Big) \\ &= \frac{s^2}{4m^3}\Big[k^4+13k^3+65k^2+147k+118+8(m-1)^2(1-s)(m-1-s)\Big] \geq 0. \end{aligned}$$

Every term in the bracket is nonnegative. Thus both diagonal types satisfy the same determinant bound in every dimension considered.
For completeness, the transfer to their convex combinations needs only $\log x \leq x-1$. Write $B = \sum_a w_a B_a$, where the vertex matrices B_a are positive definite, $w_a \geq 0$, and $\sum_a w_a = 1$. Then $B \succ 0$. Apply the scalar inequality to the eigenvalues of $B^{-1/2}B_aB^{-1/2}$ to obtain

$$\log\det B_a \leq \log\det B + \operatorname{tr}(B^{-1}B_a) - n.$$

Multiplication by w_a and summation cancel the trace terms, giving $\sum_a w_a \log\det B_a \leq \log\det B$. The common positive determinant lower bound therefore holds for B. □

Lemma 33 (joint determinant and inverse averages). *Fix vectors z_j, weights $w_j \geq 0$ and $b \geq 0$, with either $b > 0$ or some $w_j > 0$, $z_j \neq 0$. For $A \succ 0$ let*

$$F(A) = b + \sum_j w_j z_j^{\mathsf{T}} A^{-1} z_j.$$

If $H = \sum_a \mu_a A_a$, where $A_a \succ 0$, $\mu_a \geq 0$ and $\sum_a \mu_a = 1$, then

$$\log F(H) \leq \sum_a \mu_a \log F(A_a).$$

Consequently, for $q \geq 0$,

$$\log\det H - q\log F(H) \geq \sum_a \mu_a\big(\log\det A_a - q\log F(A_a)\big).$$

In particular, a common lower bound on $\det A_a/F(A_a)^q$ holds also for $\det H/F(H)^q$.

Proof. All the values $F(A)$ are positive. Fix $H \succ 0$, and define

$$E_H(A) = b + \sum_j w_j (H^{-1} z_j)^{\mathsf{T}} A (H^{-1} z_j).$$

For every real t, expansion of nonnegative squares gives

$$0 \le b(1-t)^2 + \sum_j w_j (H^{-1} z_j - t A^{-1} z_j)^{\mathsf{T}} A (H^{-1} z_j - t A^{-1} z_j)$$
$$= E_H(A) - 2tF(H) + t^2 F(A).$$

Taking $t = F(H)/F(A)$ proves $F(H)^2 \le F(A) E_H(A)$ and hence $E_H(A) > 0$. Taking logarithms and applying $\log x \le x - 1$ to $E_H(A)/F(H)$ yields

$$\log F(H) \le \log F(A) + \frac{E_H(A)}{F(H)} - 1.$$

The energy is affine in A, and $E_H(H) = F(H)$. Multiplying the last inequality by μ_a and summing therefore cancels its final two terms. This proves the first assertion. Combine it with the log-determinant averaging inequality proved in Lemma 32 and $q \ge 0$; exponentiation gives the ratio assertion. □

The choices $z_j = e_j$ give weighted inverse diagonals, including $F(A) = b + C \operatorname{tr} A^{-1}$. Thus the same diagonal decomposition used in Lemma 32 also transfers joint determinant and inverse bounds. For the low-excess `0030` argument [6], the needed power is $q = 2$; each vertex comparison must bound its determinant and inverse quantities together.

Lemma 34 (determinant from trace and inverse trace). *Let $n \ge 3$, $B \succ 0$, $\operatorname{tr} B = \sigma$, and $\operatorname{tr} B^{-1} = U$. Then $\sigma U \ge n^2$. If equality holds, $B = (\sigma/n) I$. Otherwise define*

$$t = \frac{U\sigma - n(n-2) + \sqrt{(U\sigma - n^2)(U\sigma - (n-2)^2)}}{2U}, \qquad \ell = \frac{\sigma - t}{n-1}. \tag{20}$$

Then $\det B \ge t \ell^{\,n-1}$. This lower bound increases with σ at fixed U, and decreases with U at fixed σ.

Proof. Cauchy–Schwarz gives $\sigma U \ge n^2$ and the equality case. Assume strict inequality. For every eigenvalue x, applying Cauchy–Schwarz to the other $n-1$ eigenvalues gives

$$\frac{1}{x} + \frac{(n-1)^2}{\sigma - x} \le U.$$

On $(0, \sigma)$ the left side has minimum n^2/σ at $x = \sigma/n$ and increases thereafter to infinity. Its larger solution therefore lies in $(\sigma/n, \sigma)$. Solving the quadratic gives that solution as t in (20), so every eigenvalue satisfies $x \le t$. The defining equality gives $1/t + (n-1)/\ell = U$ and $0 < \ell < t$. Apply Lemma 26 to $f(x) = x \log x$, tangent at ℓ

and interpolating at t. Since $f'''(x) = -1/x^2 < 0$, its quadratic $q(x) = q_2x^2 + q_1x + q_0$ satisfies $q(x) \le x \log x$ for $0 < x \le t$. Divide by x and sum:

$$\log\det B \ge q_2\sigma + nq_1 + q_0U = \log t + (n-1)\log \ell.$$

The equality follows because the comparison list $(t, \ell, \dots, \ell)$ has the same trace and inverse trace, and $q(x)/x = \log x$ at both its entries. Finally differentiating its two defining constraints gives

$$d\log(t\ell^{\,n-1}) = \frac{d\sigma - t\ell\, dU}{t + \ell},$$

which proves both monotonicities. Continuity handles the scalar boundary. □

For interval use with $\sigma \ge \sigma_0$ and $U \le U_1$, replace σ_0 by $\max(\sigma_0, n^2/U_1)$ and apply the lemma at (σ_0, U_1). A rational upper enclosure for the square root gives an upper enclosure for t. At fixed σ, $t[(\sigma - t)/(n-1)]^{n-1}$ decreases for $t \ge \sigma/n$, so this gives a rational *lower* determinant bound. The auxiliary t parametrises the extremal comparison spectrum; its range is the one determined by (σ, U) in the lemma.

D.5 Contact identities and radial barriers

Definition 35 (contact cone). *For a reference lattice of minimum four with contact vectors $\mathcal{C}$ in physical coordinates, its contact cone consists of symmetric matrices E satisfying $E[c] \ge 0$ for every $c \in \mathcal{C}$. Every minimum-four metric $I + E$ lies in this cone. Each value $E[c]$ is a* contact slack*: it is the increase in squared length from the reference value four.*

A contact family is *isotropic* if it has nonnegative weights a_c with $\sum_c a_c cc^{\mathsf{T}} = \kappa I$, $\kappa > 0$. Taking the trace against E gives $\kappa \operatorname{tr} E = \sum_c a_c E[c] \ge 0$.
Positive identities such as

$$K(\operatorname{tr} E)^2 - \operatorname{tr}(E^2) = \sum_{c,c'} a_{cc'} E[c]E[c'], \qquad a_{cc'} \ge 0, \tag{21}$$

or their cubic analogues prove norm bounds for *every* contact-cone matrix. They are checked by comparing polynomial coefficients. The electronic coefficient lists specify the finite sums, and their complete algebraic verification is the exact expansion of both sides (Appendix D.7). The cubic variant also covers trace zero whenever the contact family is isotropic. Indeed, isotropy and nonnegative contact slacks give $\operatorname{tr} E \ge 0$. For $\varepsilon > 0$, the matrix $E + \varepsilon I$ still has nonnegative contact slacks and has positive trace. Divide the cubic identity by its positive trace factor to obtain $\operatorname{tr}((E+\varepsilon I)^2) \le K(\operatorname{tr}(E + \varepsilon I))^2$. Letting $\varepsilon \downarrow 0$ gives the same bound for E. In particular, trace zero forces $E = 0$.

Lemma 36 (marked radial barrier). *Let $B = I + E \succ 0$ have size n, E belong to a contact cone, and $\operatorname{tr} B^{-1} \le n$. Along $B_s = I + sE$, $0 \le s \le 1$, both the contact inequalities and marking $\operatorname{tr} B_s^{-1} \le n$ persist, and $\log\det B_s$ is nondecreasing. If a*

cone estimate shows $\log\det B_s > \log\rho$ *at a prescribed positive trace or norm, while* $\det B < \rho$*, the actual metric cannot reach that trace or norm. With only the weaker hypothesis* $\operatorname{tr} B^{-1} \le n + \epsilon$*,* $\epsilon \ge 0$*, one still has*

$$\log\det B_s \le \log\det B + (1-s)\epsilon. \tag{22}$$

Proof. Positivity holds on the segment. The contacts are linear in s. The function $f(s) = \log\det(I+sE)$ is concave and $f'(1) = \operatorname{tr}(E(I+E)^{-1}) = n - \operatorname{tr} B^{-1} \ge 0$. Its derivative is therefore nonnegative everywhere on the segment. For $s > 0$, $n - \operatorname{tr} B_s^{-1} = sf'(s) \ge 0$, proving the intermediate marking. Trace excess and Frobenius norm scale linearly with s, so the stated intermediate point exists whenever the endpoint reaches the prescribed threshold. Under the weaker hypothesis, the tangent bound $f(s) \le f(1) + (s-1)f'(1)$ and $f'(1) \ge -\epsilon$ give (22). □

Lemma 37 (a quadratic minorant for the logarithm). *Suppose* E *has size* n*,* $s = \operatorname{tr} E > 0$*,* $\operatorname{tr} E^2 \le Ks^2$*, and* $E \succeq -asI$*, with* $as < 1$*. Let*

$$b = \frac{K+a}{1+na}, \qquad A = \frac{nb-1}{a+b}, \qquad B = \frac{na+1}{a+b}.$$

If $a > 0$ *and* $K \ge 1/n$*, then*

$$\log\det(I+E) \ge A\log(1-as) + B\log(1+bs). \tag{23}$$

Proof. Apply Lemma 26 to $f(x) = \log(1+x)$, tangent at bs and interpolating at $-as$. Its third derivative is positive, so $f \ge q$ on $x \ge -as$; strict concavity makes the quadratic coefficient negative. Summing q over the eigenvalues and substituting $\sum\lambda_i(E)^2 \le Ks^2$ therefore gives a lower bound. Since $A + B = n$, $-aA + bB = 1$, and $a^2A + b^2B = K$, that bound equals $Af(-as) + Bf(bs)$. □

Lemma 38 (a shared trace–inverse logarithm bound). *Let* $0 < \ell \le r$*,* $H > 0$*, and let* $a_{\log} = 1/(\ell+r)$*,* $b_{\log} = \ell r/(\ell+r)$*. If*

$$q_{\log} \le \min\left\{\log\ell - a_{\log}\ell + \frac{b_{\log}}{\ell},\ \log H - a_{\log}H + \frac{b_{\log}}{H}\right\},$$

then $\log x \ge a_{\log}x - b_{\log}/x + q_{\log}$ *for* $0 < x \le H$*. In particular,*

$$x - 1 \le 3\log x + 2\left(\frac{1}{x} - 1\right) \qquad \left(0 < x \le \frac{14}{5}\right), \tag{24}$$

$$\log(1+x) \ge \frac{17}{40}x + \frac{23}{40}\,\frac{x}{1+x} \qquad \left(-1 < x \le \frac{9}{16}\right). \tag{25}$$

Proof. For $f(x) = \log x - a_{\log}x + b_{\log}/x$,

$$f'(x) = -\frac{a_{\log}(x-\ell)(x-r)}{x^2}.$$

Since $f(x) \to +\infty$ as $x \downarrow 0$, its minimum on $(0, H]$ occurs at ℓ, if present, or at H. Use $(\ell, r, H, q_{\log}) = (1, 2, 14/5, 1/3)$ for (24), and $(1, 23/17, 25/16, 3/20)$ for (25),

replacing x by $1+x$ in the latter. The check at $\ell = 1$ is equality. At H, the required logarithm lower bounds are respectively $36/35$ and $7137/16000$. Four positive terms of (28) suffice:

$$2\sum_{j=0}^{3} \frac{\left(\frac{9}{19}\right)^{2j+1}}{2j+1} > \frac{36}{35}, \qquad 2\sum_{j=0}^{3} \frac{\left(\frac{9}{41}\right)^{2j+1}}{2j+1} > \frac{7137}{16000}.$$

□

Lemma 39 (automatic marking at small trace). *Let $a \geq 0$, $K > 0$, and $B = I + E \succ 0$ have size n. If $s = \operatorname{tr} E \geq 0$, $\operatorname{tr} E^2 \leq Ks^2$, $E \succeq -asI$, and $as < 1$, then*

$$\operatorname{tr} B^{-1} - n \leq -s + \frac{Ks^2}{1-as}.$$

In particular $s \leq 1/(K+a)$ ensures both $as < 1$ and $\operatorname{tr} B^{-1} \leq n$.

Proof. The identity $(I+E)^{-1} = I - E + E^2(I+E)^{-1}$ and $(I+E)^{-1} \preceq (1-as)^{-1}I$ give the estimate. The stated range makes its right side nonpositive. □

Lemma 40 (concentrating bounded mass). *Let $0 \leq x_i \leq r$, $\sum_i x_i \leq m$, and $r > 0$. If f is convex and nondecreasing on $[0, r]$, with $f(0) = 0$, then*

$$\sum_i f(x_i) \leq jf(r) + f(m - jr), \qquad j = \lfloor \frac{m}{r} \rfloor.$$

In particular, define $\mathcal{C}_r(m) = jr^2 + (m-jr)^2$; then $\sum_i x_i^2 \leq \mathcal{C}_r(m)$. For zero capacity use $\mathcal{C}_0(m) = 0$.

Proof. For $0 \leq x \leq y < r$, transferring mass from x to y increases $f(x) + f(y)$ by convexity. Repeat until at most one entry lies strictly between zero and r. Increase the total mass to m if needed, appending zero entries first. The resulting entries are j copies of r and one remainder. □

D.6 Primitive extensions and fixed reference cells

The *covering radius* is $\rho(M) = \sup_x \min_{a \in M} |x - a|$, with $x \in \operatorname{span} M$.

Lemma 41 (a primitive extension). *Let Λ have rank $n \geq 2$ and minimum at least $\mu > 0$, and let $M \subset \Lambda$ be primitive of rank $n-1$. Then*

$$\det \Lambda \geq \det M \left(\mu - \rho^2(M)\right),$$

where $\rho(M)$ is the Euclidean covering radius of M in its span.

Proof. Primitivity gives $\Lambda = M + \mathbb{Z}(\xi + g)$ with $\xi \in \operatorname{span} M$ and $g \perp M$. For a nearest $m \in M$, the nonzero vector $\xi + g - m$ has squared length at least μ. Thus $|g|^2 \geq \mu - |\xi - m|^2 \geq \mu - \rho^2(M)$, and $\det \Lambda = \det M\, |g|^2$. No shortest-normal hypothesis is needed. □

Lemma 42 (averaging in a cell). *Let a_i be finitely many points and let $\pi_i \ge 0$ satisfy $\sum_i \pi_i = 1$ and $\sum_i \pi_i a_i = x$. For every positive definite metric G,*

$$\min_i G[a_i - x] \le \sum_i \pi_i G[a_i] - G[x].$$

Proof. Expansion gives $\sum_i \pi_i G[a_i - x] = \sum_i \pi_i G[a_i] - G[x]$. A minimum is at most a weighted average. □

A full-dimensional *Delaunay cell* is the convex hull of lattice points on a sphere whose interior contains no lattice point. The cells tile space [8]; expressing a point as a convex combination of its cell vertices supplies the weights above. Here $\mathrm{conv}\{a_i\} = \{\sum_i \pi_i a_i : \pi_i \ge 0,\ \sum_i \pi_i = 1\}$ denotes the convex hull. For every metric G, the reference cells serve as the same fixed partition. Together, the preceding lemmata turn finite bounds on reference-cell errors into bounds for every primitive extension.

Lemma 43 (the D_{10}^+ trace criterion). *Write $D_{10} = \{z \in \mathbb{Z}^{10} : \sum_i z_i \in 2\mathbb{Z}\}$ and $D_{10}^+ = D_{10} \cup (\frac{1}{2}\mathbf{1} + D_{10})$. Let G be a minimum-four metric on $\sqrt{2}D_{10}^+$, with $\det G < 557/512$. Assume the following reference-cell bound whenever $0 \le s_G := \mathrm{tr}\, G - 10 \le 1/8$:*

$$\rho_G^2 \le \max\left(\frac{9}{4} + \frac{9s_G}{2},\ \frac{5}{2} + \frac{5s_G}{2}\right).$$

If $\mathrm{tr}\, G \le 103/10$ or $\mathrm{tr}\, G^{-1} \le 151/15$, every minimum-four primitive extension has determinant at least 1216.

Proof. The D_{10} contacts give $s_G \ge 0$. For $0 \le s_G \le 3/10$, Lemma 32 gives $\det G \ge 1 + s_G - 9s_G^2/4$. This concave quadratic exceeds $557/512$ at the two endpoints of $[1/8, 3/10]$ by $1/512$ and $123/12800$. Thus $\mathrm{tr}\, G \le 103/10$ forces $s_G < 1/8$ and $\det G \ge 1$. The assumed cell bound is then at most $45/16$. The reference lattice has determinant 1024, so Lemma 41 gives $1024 \det G\,(4 - 45/16) \ge 1216$.

For the inverse-trace alternative, suppose $\mathrm{tr}\, G \ge 103/10$. Put $t = 16/9$ and $\ell = 767/810$. Then $0 < \ell < t$, $t + 9\ell = 103/10$ and

$$\frac{1}{t} + \frac{9}{\ell} - \frac{151}{15} = \frac{73}{184080} > 0.$$

Lemma 34 therefore gives

$$\det G \ge \frac{16}{9}\left(\frac{767}{810}\right)^9 = \frac{557}{512} + \frac{28882021405184793938632 7}{135085171767299208900000000 0},$$

a contradiction. □

The cell hypothesis has the same finite meaning in both applications (`0030` and `0050`). For every error a from a reference-cell centre to a vertex, its certificate gives either $|a|^2 \le 9/4$, $C(a) \le 9/2$, or $|a|^2 \le 5/2$, $C(a) \le 5/2$, where

$$C(a) = \|a\|_1 \max\bigl(\|a\|_\infty, \frac{\|a\|_1 - 2\min_i |a_i|}{8}\bigr).$$

Lemma 30 gives $G[a] \le |a|^2 + C(a)s_G$. Lemma 42, with the centre as origin, extends the bound to every point of the cell. A complete reference partition and its finite error checks are the only computational input to this transfer.

D.7 One exact rule for all finite covers

Lemma 44 (rational linear certificates). *Suppose a vector z satisfies $Az \le b$ and coordinate bounds $\ell \le z \le h$, all rational. For any rational $\lambda \ge 0$, let $a = A^{\mathsf{T}}\lambda$. If*

$$\sum_j \min(a_j l_j, a_j h_j) > \lambda^{\mathsf{T}} b, \tag{26}$$

there is no such z. More generally, for a linear objective $q^{\mathsf{T}} z$ and $r = q - A^{\mathsf{T}}\lambda$,

$$q^{\mathsf{T}} z \le \lambda^{\mathsf{T}} b + \sum_j \max(r_j l_j, r_j h_j). \tag{27}$$

Proof. Multiply the necessary inequalities by λ and sum. Bound each remaining coordinate term by its appropriate endpoint. This proves both statements, including when the proposed multipliers have a nonzero residual. □

The three obligations of a finite cover. Every finite cover has three obligations: the root contains every counterexample, each terminal witness excludes its whole region, and the regions exhaust the root. A contraction uses a necessary bound; a split covers its parent by two closed children. Induction proves exclusion when no pending region remains; a resumed forest is checked in the same way, region by region. For the trees of Section 5.5 these are the conditions `a`–`c` after Lemma 11.

Products, squares, logarithms and Bernstein's rule. For a bilinear term xy with $x \in [\ell_x, h_x]$, $y \in [\ell_y, h_y]$, the four products $(x-\ell_x)(y-\ell_y)$, $(h_x-x)(h_y-y)$, $(x-\ell_x)(h_y-y)$, and $(h_x-x)(y-\ell_y)$ are nonnegative. Expanding them gives the four usual linear bounds on a variable representing xy. Likewise, nonnegative products of valid affine inequalities and nonnegative quadratic squares give exact polynomial certificates. No independence of the actual variables is assumed: enlarging their possible set makes an exclusion harder, but cannot discard a counterexample.
For $r > 0$ rational, logarithms are enclosed using

$$\log r = 2\sum_{j=0}^{m-1} \frac{z^{2j+1}}{2j+1} + \mathcal{R}_m, \qquad z = \frac{r-1}{r+1}, \qquad |\mathcal{R}_m| \le \frac{2|z|^{2m+1}}{(2m+1)(1-z^2)}. \tag{28}$$

This follows by integrating the geometric series for $2/(1-z^2)$. Square-root enclosures are verified by squaring rational endpoints. A polynomial on $[0,1]$ is nonnegative if all its Bernstein coefficients are nonnegative, because the basis functions $\binom{n}{k}x^k(1-x)^{n-k}$ are nonnegative. Interval subdivision applies the same fact on arbitrary rational intervals. These facts justify the scalar arithmetic used throughout the certificates (see also [2, Appendix C]).

E A direct certificate for every gluing: the form `0052:005247066`

The tenth macadamia of Table 3 is settled here. The argument, in the notation of Appendix D, uses a general determinant certificate that needs neither of the cutoffs

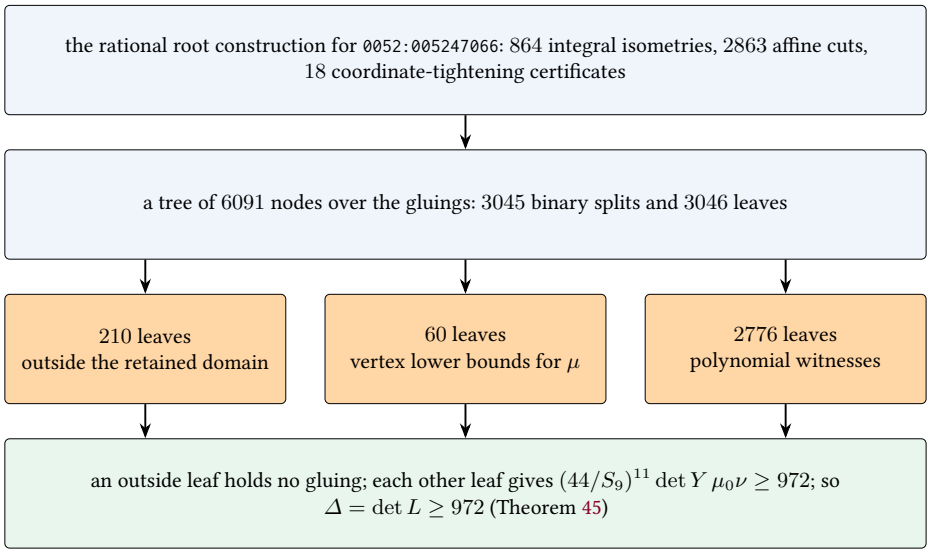

Fig. 8. The certificate for the tenth macadamia, `0052:005247066` (Theorem 45 and Computational result 46). The checker `verify_common_gluing_cover.py` must print `PASS tree replay; complete True nodes 6091 remaining 0`: 6 091 checked nodes and no remaining region.

$d < d_{\mathrm{cut}}$ and $e < e_{\mathrm{cut}}$, so that its lemma (Lemma 47) is stated independently of the case. In the form of the statements that the root paper imports ([2, Section 6.2]), the result is the following; a Gram matrix Q is *admissibly marked* by P when $\min Q \geq 4$ and $Q^{-1} = \sum_c w_c\, cc^{\mathsf{T}}$ with $w_c \geq 0$, $\sum_c w_c \leq 9/4$, $w_c \leq 1/4$, that is, when (M) and (Domain) of Section 2.4 hold.

Theorem 45 (the form `0052:005247066`). *Assume Computational result 46. Let $L \supset M \supset N$ be a chain as in Proposition 4 whose rank-9 member N has a Gram matrix admissibly marked by the survivor $P =$ `0052:005247066` (Appendix E.5). Then $\Delta = \det L \geq 972$.*

Computational result 46 (the complete gluing cover for `0052`). The rational root construction below, its 864 integral isometries, 2863 affine cuts and 18 coordinate-tightening certificates are valid for the printed marker. The 6091-node tree covers that root: 210 leaves are outside the retained domain; 60 give vertex lower bounds for μ; and 2776 give the polynomial witnesses below. Each nonempty leaf has $Y \succ 0$, legal integral lifts and additive triples, nonnegative multipliers, $\mu_0, \nu > 0$, and $(44/S_9)^{11} \det Y\, \mu_0\nu \geq 972$. Coverage and every exact coefficient are checked by the program that replays the record (see below; Figure 8 shows the structure).

The certificate archive `hermite11_local_certificates.zip` contains the complete saved database `shared_certificates_2026-10-12/cover_0052_tight_complete_snapshot1.sqlite` (69 365 760 bytes) and its replay record `cover_0052_tight_complete_snapshot1.verified.json`. These paths, and those below, are relative to `certificates/_research_`

`hermite11_2026-10-10/`. The checker is `verify_common_gluing_cover.py`, in the same directory as the database. The sizes and SHA-256 hashes of all these files are in `certificate_manifest.json`.

With the driver of the archive. From the top directory of the extracted archive, with the Python packages pinned in its `README.txt`, the command

```
$ python3 verify_cases.py --case 0052 --root .
...
PASS_LOCAL_CHECKING_SCHEDULE: 0052
```

first checks the SHA-256 of every input against `certificate_manifest.json`, then runs the two steps of the case: the domain check `verify_common_domain.py` on `domain_0052_005247066_tight.json`, and the replay of the tree, with exact FLINT rationals in place of Python's `Fraction`. It ends with `PASS_LOCAL_CHECKING_SCHEDULE: 0052`.

By hand. In a writable copy of the directory `shared_certificates_2026-10-12/`, give the database the file name the checker reads, then run the checker:

```
$ ln -s cover_0052_tight_complete_snapshot1.sqlite \
       cover_0052_005247066_tight.sqlite
$ python3 verify_common_gluing_cover.py --suffix _tight \
       --snapshot referee_0052.sqlite
...
PASS tree replay; complete True nodes 6091 remaining 0
```

Here `referee_0052.sqlite` is a new file: the checker first copies the database into it (by SQLite's backup) and then reads that copy, so the saved database is never written. With Python's `Fraction` the replay is much slower than through the driver.
Either way, the replay must print `PASS tree replay; complete True nodes 6091 remaining 0`: the tree of 6 091 nodes is complete and no region remains, with the leaf counts of Computational result 46. The argument below proves why verification of the saved tree controls both gluings.

E.1 The certificate

Choose finitely many integral first lifts $(z_i, k_i) \in \mathbb{Z}^9 \times \mathbb{Z}$ and nonnegative weights a_i, b_i. The a_i multiply first-normal inequalities and the b_i multiply second-normal inequalities. A first-normal term must have $z_i \neq 0$; a second-normal term must be a nonzero vector of M^*. Let

$$W = \sum_i (a_i + b_i)\, z_i z_i^{\mathsf{T}}, \qquad \mu(\beta) = \sum_i a_i - \sum_i (a_i + b_i)(\beta^{\mathsf{T}} z_i + k_i)^2.$$

For the first normal itself one may take $z_i = 0$, $k_i = 1$ in a second-normal term. Choose a rational positive definite matrix Y. For every contact c, define its score $s_c = c^{\mathsf{T}}(Y + W)c \geq 0$, and let S_9 be the sum of the nine largest scores. The marking coefficient bounds give

$$\operatorname{tr}((Y + W)X) = \sum_c w_c s_c \leq \frac{S_9}{4}. \tag{29}$$

This follows directly by filling the available total mass $9/4$ into entries of capacity $1/4$, largest score first (it is (4)). Let t_i be the circle distance of the second-gluing phase on (z_i, k_i), that is $t_i = \|\alpha^{\mathsf{T}} z_i + \vartheta k_i\|$. Adding the weighted normal inequalities and using (29) gives

$$\operatorname{tr}(YX) + u\,\mu(\beta) + v\sum_i b_i(1 - t_i^2) \le \frac{S_9}{4}. \tag{30}$$

To bound the last sum uniformly, choose verified additive triples T of these lifts and nonnegative rational multipliers $\sigma_i, \tau_T, \omega_{T,j}$ satisfying

$$b_i \le \sigma_i + \sum_{T \ni i}\Big(\tau_T + \omega_{T,i} - \sum_{j \in T\setminus\{i\}} \omega_{T,j}\Big). \tag{31}$$

Lemma 47 (both gluings). *In this setting let*

$$\nu = \sum_i b_i - \frac{1}{4}\sum_i \sigma_i - \frac{1}{2}\sum_T \tau_T.$$

If $\nu > 0$ and $\mu(\beta) > 0$, then

$$\Delta \;\ge\; \Big(\frac{44}{S_9}\Big)^{11} \det(Y)\,\mu(\beta)\,\nu. \tag{32}$$

Proof. The circle lemma (Lemma 22) gives $\sum_{i\in T} t_i \le 1$; the circle triangle inequality gives $t_i \le \sum_{j\in T\setminus\{i\}} t_j$. Multiplication of (31) by t_i and summation yield $\sum_i b_i t_i \le \frac{1}{2}\sum_i \sigma_i + \sum_T \tau_T$.
Since $t_i^2 \le t_i/2$, a uniform lower bound is $\sum_i b_i(1 - t_i^2) \ge \nu$. AM–GM on the nine eigenvalues of $Y^{1/2} X Y^{1/2}$ and the two positive scalars $u\mu(\beta)$, $v\nu$, whose sum is at most $S_9/4$ by (30) and whose product is $\det Y\,\mu(\beta)\,\nu/\Delta$ by (8) (as in Lemma 16), proves (32). □

Every second gluing has been handled in this inequality. The concave quadratic μ is evaluated exactly; no unknown second-gluing parameter remains. Lemma 47 is Lemma 16 with $a_i = w_i$, $b_i = \omega_j$ and $\nu = m_v$, the multipliers $\omega_{T,j}$ on the rows $t_i \le \sum_{j\ne i} t_j$ being added to Lemma 17; it uses the marking (29), the two normal inequalities and nothing else: neither $d < d_{\mathrm{cut}}$ nor $e < e_{\mathrm{cut}}$.

E.2 A finite domain for the first gluing

Integer translations and integral P-isometries act on β and preserve the chain conditions. Fix a rational center p_0. An orbit representative minimizing $P[\beta - p_0]$ exists because the isometry group is finite and translations are discrete. It satisfies

$$P[\beta - p_0] - P[A\beta + n - p_0] \le 0$$

for every checked isometry A and translation n. Each expression is affine because $A^{\mathsf{T}} P A = P$. A rational Gram–Schmidt basis C has $C^{\mathsf{T}} P C = \operatorname{diag}(d_i)$. Backward rounding in the associated unimodular integral basis gives a covering bound $R_0 =$

$\sum_i d_i/4$. Thus the chosen representative, written $\beta = p_0 + Cy$, has $|y_i| \le \sqrt{R_0/d_i}$. Rational outer bounds define the root box. (This is the fundamental domain of Proposition 15, with the metric P in place of G': the cuts are its half-spaces $f_g \le 0$.)

For `0052`, the certificate retains 2863 affine cuts from 864 individually verified isometries and eighteen rational certificates tightening the signed coordinate bounds. These cuts need not generate the full isometry group or the full Dirichlet domain: the retained intersection still contains every chosen representative. Every transformation, Gram–Schmidt identity and root bound is checked exactly.

E.3 Checking the quadratic leaves

On an affine box, a concave quadratic has its minimum at a vertex, so one option is to evaluate μ at all $2^9 = 512$ vertices. To exploit the domain cuts, normalize box coordinates to $x_i \in [-1, 1]$, and let $\ell_j(x) \ge 0$ be the box and retained domain inequalities. A stronger witness consists of rational $q_{ij} \ge 0$ and a rational positive semidefinite matrix H such that

$$R(x) = \mu(x) - \sum_{i,j} q_{ij}\, \ell_i(x)\ell_j(x) - (1, x)^{\mathsf{T}} H (1, x)$$

has $R_0 - \sum_{\alpha \ne 0} |R_\alpha| \ge \mu_0 > 0$, where R_α are the coefficients of R in the monomial basis and R_0 its constant term. Every nonconstant monomial of degree at most two has absolute value at most one, so $\mu \ge \mu_0$ on the required intersection. Exact expansion and an LDL^{T} factorization of H check the assertion. Substitution in (32) proves the leaf whenever the resulting rational lower bound is at least 972.

E.4 The cover, and the proof of Theorem 45

The complete binary tree has 6091 nodes and 3046 terminal regions: 210 are outside the retained domain by Lemma 44, 60 use vertex minima, and 2776 use nonnegative products and squares. Its topology and every witness were exactly replayed, with no pending region. The smallest certified determinant lower bound is greater than 972.0047 (the certificate retains the exact fraction). Thus every first-gluing orbit has a representative in a terminal region and every possible second gluing is excluded there. This proves `0052`.

Proof of Theorem 45. Let the chain be given, with Q admissibly marked by P and the gluings β, (α, ϑ) of Appendix D. By (Symmetry) and Appendix E.2, replacing β by the representative of its orbit nearest to p_0 changes neither Δ nor the marking, and the representative lies in the root box and satisfies the 2863 cuts and the 18 coordinate bounds. By Computational result 46 it lies in one of the 3046 terminal regions, and not in one of the 210 regions that Lemma 44 shows to contain no point of the retained domain. On every other region the leaf gives $\mu(\beta) \ge \mu_0 > 0$ (at the vertices, or by the witness of Appendix E.3) and $\nu > 0$, so Lemma 47 gives $\Delta \ge (44/S_9)^{11} \det Y\, \mu_0 \nu \ge 972$. □

E.5 The Gram matrix of the form

The survivor `0052:005247066`, in the basis used by the certificate of Computational result 46, is the matrix P below. It is symmetric and positive definite (its leading principal minors are 4, 12, 36, 108, 216, 324, 540, 756, 972), has minimum 4, determinant 972 and 82 pairs of minimal vectors, as Table 3 and the paragraph after it say (these four facts were recomputed exactly). It is, entry by entry, the matrix G of the record `0052:005247066` of the data set (row $5\,247\,066$ of `perfect_0052.nc`, lower triangle row by row), whose least diagonal entry is $m = 4 = \min G$: thus $P = (4/m)G = G$ and the equivalence of the printed matrix with the record is realised by $U = I_9$ (compared exactly against the record as read from the data set; the isometry finder of `result9.py`, run on the pair (P, G), returns a unimodular U with $U^{\mathsf{T}} P U = G$, an automorphism of P).

$$P = \begin{pmatrix} 4 & 2 & 2 & 2 & 2 & 2 & -2 & -2 & -2 \\ 2 & 4 & 1 & 1 & 2 & 2 & -1 & 0 & -1 \\ 2 & 1 & 4 & 1 & 2 & 2 & 0 & -1 & 0 \\ 2 & 1 & 1 & 4 & 2 & 2 & -2 & -2 & -2 \\ 2 & 2 & 2 & 2 & 4 & 1 & -1 & 0 & -2 \\ 2 & 2 & 2 & 2 & 1 & 4 & 0 & -1 & -1 \\ -2 & -1 & 0 & -2 & -1 & 0 & 4 & 1 & 2 \\ -2 & 0 & -1 & -2 & 0 & -1 & 1 & 4 & 0 \\ -2 & -1 & 0 & -2 & -2 & -1 & 2 & 0 & 4 \end{pmatrix}.$$

The lattice M of rank 10 recorded in the virtual row of this form (Table 3) has $\det M = 7776/7$ and $\min M^* = 7/8$, so that $\det P = \min M^* \cdot \det M = 972$.