hexagon:2611.00952v1

Completing the Kim–Kim–Oh Classification of Minimal-Rank n-Universal Lattices for $2 \le n \le 8$

Scott Duke Kominers

Abstract. A positive-definite integral lattice is *n-universal* if it represents every positive-definite integral lattice of rank n. We complete the classification of minimal-rank n-universal lattices for $2 \le n \le 8$ by resolving the three cases left open by Kim, Kim, and Oh. We show that $I_3 \perp A_1 \perp A_2$ and $I_3 \perp A_2 \perp \langle 3 \rangle$ are 3-universal, whereas $I_6 \perp A_2$ is *not* 5-universal.

1. Introduction

A *lattice* is a free $\mathbb{Z}$-module of finite rank with a positive-definite symmetric bilinear form $(\ ,\ )$ taking values in $\mathbb{Z}$. In a basis $e_1, \dots, e_n$ of Λ, the *Gram matrix* is $G = ((e_i, e_j))$ and the *determinant* is $\det \Lambda = \det G$. Write $Q_F(z) = z^{\mathsf{T}} F z$ for any symmetric matrix F. The *norm* $Q(u) = (u, u)$ equals $Q_G(z)$ for the coordinate column z of u.

We say that a lattice L *represents* a lattice Λ if there exists an isometric embedding $\Lambda \hookrightarrow L$ (not necessarily primitive). We identify a lattice in a chosen basis with its Gram matrix. Thus L represents G precisely when L contains vectors with Gram matrix G. A lattice is *n-universal* if it represents every lattice of rank n; it then represents every lattice of rank $r < n$ because adjoining $n - r$ orthogonal vectors of norm 1 gives a lattice of rank n.

We write $\langle a_1, \dots, a_n \rangle$ for the lattice with diagonal Gram matrix $\operatorname{diag}(a_1, \dots, a_n)$ and $\perp$ for orthogonal sum. Thus $I_n = \langle 1, \dots, 1 \rangle$ is $\mathbb{Z}^n$ with the usual dot product. We use the *root lattices* A_n, E_6, E_7, and E_8, normalized so that their roots have norm 2 (see [1]). In particular, the lattice A_n is the sublattice of I_{n+1} comprising the vectors whose coordinates sum to 0.

Kim, Kim, and Oh [7, Theorem 3] recorded the least rank $u_{\mathbb{Z}}(n)$ of an n-universal lattice for $n \le 10$. Synthesizing and building upon earlier work [12, 10, 3, 8, 6, 15] (see also [17, 18]), they classified, up to isometry, all possible minimal-rank n-universal lattices for $2 \le n \le 8$. The question of n-universality remained open for just three candidates, indicated by stars in the following theorem.

2020 *Mathematics Subject Classification.* Primary 11E12, 11E25; Secondary 11E08, 11E20.

Key words and phrases. integral quadratic forms, universal lattices, representations of lattices.

I thank Aaron Tievsky, who introduced me to quadratic forms and the work of Kim, Kim, and Oh [7] more than twenty years ago. I appreciate comments at that time from Ellen Dickstein Kominers, Paul Kominers, William Kominers, Chris Mihelich, Antoni Rangachev, John Rickert, Jenny Sendova, Chris Skinner, Larry Washington, Susan Schwartz Wildstrom, and many others; and more recently from Glenn Bruda, Noam D. Elkies, Ben Golub, Vita Kala, Steven J. Miller, Joachim Neu, Byeong-Kweon Oh, Ken Ono, Igor Rapinchuk, Tim Roughgarden, and Jesse Shapiro. This work was conducted while I was visiting the Technological Innovation, Entrepreneurship, and Strategic Management (TIES) Group at the MIT Sloan School of Management; I greatly appreciate their hospitality. My earliest thinking about this problem was supported by a Research Science Institute summer scholarship.

THEOREM 1.1 (Kim–Kim–Oh [7, Theorem 1 and Proposition 3]).

(1) There are exactly eleven 2-universal $\mathbb{Z}$-lattices of rank $u_{\mathbb{Z}}(2) = 5$ up to isometry. They are:

$$\langle 1,1,1,1,1\rangle,\quad \langle 1,1,1,1,2\rangle,\quad \langle 1,1,1,1,3\rangle,\quad \langle 1,1,1,2,2\rangle,\quad \langle 1,1,1,2,3\rangle,$$
$$\langle 1,1,1\rangle \perp [2,1,2],\quad \langle 1,1,1\rangle \perp [2,1,3],\quad \langle 1,1,2\rangle \perp [2,1,2],\quad \langle 1,1,3\rangle \perp [2,1,2],$$
$$\langle 1,1\rangle \perp [2,1,2,1,2],\quad \langle 1,1\rangle \perp [2,1,2,1,3],$$

where $[a,b,c]$ is shorthand for $\left(\begin{smallmatrix} a & b \\ b & c \end{smallmatrix}\right)$ and $[a,b,c,d,e]$ is shorthand for $\left(\begin{smallmatrix} a & b & 0 \\ b & c & d \\ 0 & d & e \end{smallmatrix}\right)$.

(2) There are nine 3-universal $\mathbb{Z}$-lattices of rank $u_{\mathbb{Z}}(3) = 6$ found so far, and there can be at most two more [indicated by stars]. They are:

$$I_6,\quad I_5 \perp A_1,\quad I_5 \perp \langle 3\rangle,\quad I_4 \perp A_1 \perp A_1,\quad I_4 \perp A_2,\quad I_4 \perp A_1\, 10\left[1\ \tfrac{1}{2}\right],$$
$$I_3 \perp A_3,\quad I_3 \perp A_2\, 21\left[1\ \tfrac{1}{3}\right],\quad I_4 \perp A_1 \perp \langle 3\rangle,\quad I_3 \perp A_1 \perp A_2,^{\star}\quad I_3 \perp A_2 \perp \langle 3\rangle,^{\star}$$

where the brackets in this list indicate glue-vector parameters (see [1]).

(3) There are exactly three 4-universal $\mathbb{Z}$-lattices of rank $u_{\mathbb{Z}}(4) = 7$. They are:

$$I_7,\quad I_6 \perp A_1,\quad I_5 \perp A_2.$$

(4) There are two 5-universal $\mathbb{Z}$-lattices of rank $u_{\mathbb{Z}}(5) = 8$ found so far, and there can be at most one more [indicated by a star]. They are:

$$I_8,\quad I_7 \perp A_1,\quad I_6 \perp A_2.^{\star}$$

(5) There are exactly two 6-universal $\mathbb{Z}$-lattices of rank $u_{\mathbb{Z}}(6) = 13$. They are:

$$I_6 \perp E_7,\quad I_7 \perp E_6.$$

(6) There are exactly three 7-universal $\mathbb{Z}$-lattices of rank $u_{\mathbb{Z}}(7) = 15$. They are:

$$I_7 \perp E_8,\quad I_8 \perp E_7,\quad I_7 \perp E_7\, 6\left[1\ \tfrac{1}{2}\right].$$

(7) $I_8 \perp E_8$ is the only 8-universal $\mathbb{Z}$-lattice of rank $u_{\mathbb{Z}}(8) = 16$.

Each of the starred candidates is *locally n-universal* [7], meaning that it represents all nonsingular integral lattices of rank n over $\mathbb{Z}_p$ for every prime p. But the genus of each candidate comprises multiple isometry classes, so global universality does not immediately follow from local universality.

Main result. We resolve the three remaining cases in Theorem 1.1.

THEOREM 1.2.

(i) $I_3 \perp A_1 \perp A_2$ *is 3-universal.*
(ii) $I_3 \perp A_2 \perp \langle 3\rangle$ *is 3-universal.*
(iii) $I_6 \perp A_2$ *is not 5-universal.*

Theorems 1.1 and 1.2 together imply that there are exactly eleven 3-universal lattices of rank 6 and two 5-universal lattices of rank 8, up to isometry.

Strategy of the proof. Let $L_6 = I_3 \perp A_1 \perp A_2$ and $L_9 = I_3 \perp A_2 \perp \langle 3 \rangle$. Kim, Kim, and Oh prove 2-universality by prescribing one coordinate of an embedding and representing the remaining binary form by a quaternary lattice of class number 1 [7, §4]. We use $L_6 = K_3 \perp \langle 2 \rangle$ and $L_9 = K_9 \perp \langle 1 \rangle$, where the quinary lattice K_j has determinant j and class number 1. In either case write $L = K_j \perp \mathbb{Z}v$ and put $s = Q(v)$.

Every ternary lattice lies in a maximal integral overlattice, and an embedding of the latter restricts to the original lattice. A ternary lattice containing a vector of norm 1 splits as $\langle 1 \rangle \perp M$ with M binary—and in L the orthogonal complement of a coordinate vector of I_3 is 2-universal by Theorem 1.1(1). It therefore suffices to treat maximal ternary lattices of minimum at least 2.

Let G be the Gram matrix of such a lattice. We choose the coefficients $\lambda = (x, y, k)^{\mathsf{T}}$ along v and seek vectors in K_j with Gram matrix $C = G - s\lambda\lambda^{\mathsf{T}}$. It suffices to make C positive definite and represented by K_j over every $\mathbb{Z}_p$.

For $p = 2, 3$, we certify local representation of C using three vectors in $K_j \otimes \mathbb{Z}_p$ that are linearly independent modulo p and whose Gram matrix F satisfies $Q_F \equiv Q_C$ coefficientwise modulo 8 at 2 or modulo 9 at 3. We use classes of (x, y, k) modulo p for which every integral lift admits three such vectors. Certificate 4.1 chooses x and prescribes, at each prime, a congruence for y and, once y is fixed, a congruence for k. Each congruence has modulus p or 1; the Chinese remainder theorem then combines the congruences at 2 and 3 into an arithmetic progression $y_0 + h\mathbb{Z}$ for y and, for each such y, an arithmetic progression $k_0(y) + m\mathbb{Z}$ for k, with $h, m \mid 6$.

In a basis reduced as in Section 3, positive definiteness of C restricts y to a real interval and, once y is chosen, k to another. Taking $y \in y_0 + h\mathbb{Z}$ and $k \in k_0(y) + m\mathbb{Z}$ ensures that K_j represents C over $\mathbb{Z}_2$ and $\mathbb{Z}_3$. If the intervals are sufficiently long, then we can choose terms of these two arithmetic progressions for which $K_j \otimes \mathbb{Z}_p$ also represents C at every prime $p \ge 5$. For any such maximal lattice that could still fail to embed in L over $\mathbb{Z}$, Certificate 4.2 bounds the first diagonal entry and the determinant of the leading 2×2 block of the Gram matrix G in a reduced basis; these bounds leave finitely many blocks to consider.

Certificate 4.3 treats the remaining blocks. For most blocks it gives a pair (x, y) such that, for every maximal ternary lattice having that block in a reduced basis, some k makes C positive definite and represented by K_j over every $\mathbb{Z}_p$. For the other blocks, bounds on $\det G$ in each congruence class of the last column leave finitely many matrices G. For each, the certificate records a λ for which $C_G(\lambda) = G - s\lambda\lambda^{\mathsf{T}}$ is positive definite and represented by K_j over every $\mathbb{Z}_p$.

Thus for each remaining reduced G a single λ gives a matrix C represented by K_j over $\mathbb{R}$ and every $\mathbb{Z}_p$. Since K_j has class number 1, it represents C over $\mathbb{Z}$ as well, say by vectors u_1, u_2, u_3. The vectors $u_i + \lambda_i v$ in L then have Gram matrix G, as desired. Together with the norm-1 case and restriction to sublattices, this proves Theorem 1.2(i) and (ii).

Section 5 proves Theorem 1.2(iii) by exhibiting a quinary lattice of determinant 117 that does not embed in $I_6 \perp A_2$. In a putative embedding, the prescribed pairings force the first three basis images to occupy four coordinates of I_6. The projections of the last two images onto the remaining I_2 would then have nonsquare Gram determinant—contradicting the identity $\det(X^{\mathsf{T}}X) = (\det X)^2$ for their 2×2 integer coordinate matrix X.

Computational supplement and formalization. The Python supplement provides search programs and a separate exact-arithmetic checker for Certificates 4.1–4.3 (Appendix A). The Lean 4 formalization proves all three assertions of Theorem 1.2, including verifying the arithmetic inputs and finite computations in the 3-universality proofs (Appendix B).

2. The local embedding tests

Throughout Sections 2–4, we fix $L \in \{L_6, L_9\}$ and let Λ denote the ternary lattice we seek to embed in L. Write $L = K_j \perp \mathbb{Z}v$ with $s = Q(v)$. The index j is the determinant of the quinary

summand K_j, and js is the determinant of L. Explicitly,

$$\begin{aligned} L_6 &= K_3 \perp \langle 2\rangle, & K_3 &= I_3 \perp A_2, \\ L_9 &= K_9 \perp \langle 1\rangle, & K_9 &= I_2 \perp A_2 \perp \langle 3\rangle. \end{aligned} \tag{1}$$

For any lattice N, put $N_p = N \otimes_{\mathbb{Z}} \mathbb{Z}_p$. In particular $K_{j,p} = (K_j)_p$. Write $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. For p-adic entries, congruence modulo p^e means equality in $\mathbb{Z}_p/p^e\mathbb{Z}_p$.

An *integral overlattice* of Λ is a lattice in $\Lambda \otimes \mathbb{Q}$ containing Λ with finite index and having integral pairings. A lattice is *maximal* if it has no proper integral overlattice. An overlattice of index d has determinant $\det \Lambda/d^2$, so every ternary lattice Λ lies in a maximal integral overlattice, and an embedding of the latter restricts to Λ.

Let Λ be an arbitrary maximal ternary lattice. Fix a basis e_1, e_2, e_3 of Λ and let G be its Gram matrix in this basis. For a proposed embedding $\Lambda \hookrightarrow L$, the coefficient along v is a linear form $\Lambda \to \mathbb{Z}$. Let $\lambda = (x, y, k)^{\mathsf{T}}$ be the column of its values on the basis. The proposed images $e_i \mapsto u_i + \lambda_i v$ have Gram matrix G precisely when their components $u_i \in K_j$ have Gram matrix

$$C = C_G(\lambda) := G - s\lambda\lambda^{\mathsf{T}}. \tag{2}$$

The following lemma gives a sufficient condition for L to represent G in terms of $C = C_G(\lambda)$ for a single $\lambda \in \mathbb{Z}^3$. Part (a) is the local–global step; it uses that K_j has class number 1. Part (b) makes the local condition at primes $p \geq 5$ checkable over $\mathbb{F}_p$: there $K_{j,p}$ is unimodular, and it suffices for the reduction of Q_C to represent j. The primes $p = 2, 3$ are handled by Lemma 2.2 below.

LEMMA 2.1. *Let $\lambda \in \mathbb{Z}^3$ and $C = C_G(\lambda)$ as in (2).*
(a) *If C is positive definite and $K_{j,p}$ represents C for every prime p, then L represents G.*
(b) *Let $p \geq 5$. If $C \bmod p$ has rank at least 2, then $Q_C \bmod p$ represents j over $\mathbb{F}_p$. Whenever $Q_C \bmod p$ represents j, the lattice $K_{j,p}$ represents C.*

PROOF. (a) The *genus* of K_j consists of the lattices N with $N \otimes \mathbb{R} \cong K_j \otimes \mathbb{R}$ and $N_p \cong K_{j,p}$ for every prime p; its *class number* is the number of isometry classes in the genus. In Nipp's tables of positive-definite quinary forms the discriminant is 16 times the lattice determinant. The genera of K_3 and K_9 appear as genus 8 of discriminant 48 and genus 21 of discriminant 144, respectively; each contains only one isometry class [14] (see also [11, Appendix A.7]).

Since C is positive definite, $K_j \otimes \mathbb{R}$ represents C, and by hypothesis $K_{j,p}$ represents C for every prime p. Hence some lattice in the genus of K_j represents C over $\mathbb{Z}$ [16, Example 102:5] (see also [19, Theorem 6.15 and Corollary 6.16]). As the class number is 1, that lattice is isometric to K_j, so there are $u_1, u_2, u_3 \in K_j$ with Gram matrix C. Since $L = K_j \perp \mathbb{Z}v$ and $Q(v) = s$, the vectors $u_i + \lambda_i v \in L$ have Gram matrix $C + s\lambda\lambda^{\mathsf{T}} = G$.

(b) Since $p \geq 5$ and $j \in \{3, 9\}$, j is a unit in $\mathbb{Z}_p$, so $K_{j,p}$ is *unimodular*, i.e., its determinant is a unit. Let H be the hyperbolic plane, with Gram matrix $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. It represents every $d \in \mathbb{Z}_p$, since $(1, d/2)$ has norm d.

Structure of $K_{j,p}$. For odd p, a unimodular $\mathbb{Z}_p$-lattice of rank at least 3 splits off a copy of H [19, Theorem 5.26]. Applying this twice to the rank-5 lattice $K_{j,p}$ gives $K_{j,p} \cong H \perp H \perp \langle \varepsilon \rangle$. Comparing determinants, with $\det H = -1$, gives $\varepsilon = ju^2$ for some $u \in \mathbb{Z}_p^\times$, so $\langle \varepsilon \rangle$ contains a vector of norm j.

Structure of C. Choose $z \in \mathbb{Z}_p^3$ with $Q_C(z) \equiv j \pmod p$. Then $Q_C(z)/j \in 1 + p\mathbb{Z}_p$ is a square in $\mathbb{Z}_p^\times$, and rescaling z gives $Q_C(z) = j$. Because j is a unit, the projection $w \mapsto w - \frac{w^{\mathsf{T}}Cz}{j} z$ is integral, so $M = (\mathbb{Z}_p^3, C)$ splits as $\mathbb{Z}_p z \perp M'$ with M' binary. As p is odd, M' has an orthogonal basis f_1, f_2, of norms d_1, d_2, say.

The embedding. Send z to a vector of norm j in $\langle\varepsilon\rangle$, and send f_i to $(1, d_i/2)$ in the i-th copy of H. The images are pairwise orthogonal of norms j, d_1, d_2, so this is an isometric embedding of M into $K_{j,p}$.

Finally, if C mod p has rank at least 2, then Q_C mod p contains a nonsingular binary subform, which represents every nonzero element of $\mathbb{F}_p$ [19, Corollary 2.8] (also [9, §1.3]); in particular it represents $j \not\equiv 0 \pmod p$. □

Call Λ *maximal at* p if Λ_p has no proper integral $\mathbb{Z}_p$-overlattice. To check maximality over $\mathbb{Z}$, it suffices to exclude overlattices of prime index. Over $\mathbb{Z}$ or $\mathbb{Z}_p$, an overlattice of index p is generated by adjoining z/p in basis coordinates, where $z \not\equiv 0 \pmod p$. The pairings with the basis vectors and the norm of z/p are integral precisely when

$$Gz \equiv 0 \pmod p, \qquad Q_G(z) \equiv 0 \pmod{p^2}. \tag{3}$$

Once the first congruence holds, the second depends only on $z \bmod p$. An integer representative of a nonzero p-adic solution modulo p therefore satisfies both congruences. Thus maximality over $\mathbb{Z}$ is equivalent to maximality at every p. For odd p, maximality implies $G \not\equiv 0 \pmod p$. Otherwise $(G/p) \bmod p$ has a nonzero vector of norm 0. If the form is singular, take a nonzero vector in its radical. In a nonsingular diagonal form, the leading binary form represents the negative of the third diagonal entry over $\mathbb{F}_p$. In either case an integral lift satisfies (3).

At 2, an integral overlattice of index 2 implies $4 \mid \det G$. Conversely, suppose $4 \mid \det G$. On $\ker(G \bmod 2)$, the map $z \mapsto Q_G(z)/2 \bmod 2$ is independent of the lift by (3) and linear, since $z^{\mathsf{T}}Gw$ is even there. If the kernel of G mod 2 has dimension at least 2, this linear form vanishes on a nonzero vector. If it has dimension 1, lift a generator to z and take it last in a $\mathbb{Z}_2$-basis. Modulo 2 the first two vectors span a complement to the radical, so their Gram determinant is odd. Their pairings with z are even. The full determinant is therefore congruent modulo 4 to that odd determinant times $Q_G(z)$, giving $4 \mid Q_G(z)$. In both cases a nonzero class satisfies (3). This proves that maximality over $\mathbb{Z}_2$ is equivalent to $4 \nmid \det G$.

Table 1 gives diagonal Gram matrices for $K_{j,p}$ at $p = 2, 3$. Let α_1, α_2 be simple roots of A_2, with $(\alpha_1, \alpha_2) = -1$. The orthogonal vectors $\alpha_1, \alpha_1 + 2\alpha_2$ have norms $2, 6$ and span a sublattice of index 2. They form a basis over $\mathbb{Z}_3$. If e has norm 1 and is orthogonal to A_2, $e+\alpha_1, e+\alpha_2, e-\alpha_1-\alpha_2$ are orthogonal of norm 3. They span a sublattice of index 3 in $\mathbb{Z}e \perp A_2$, hence form a basis over $\mathbb{Z}_2$.

TABLE 1. Diagonal Gram matrices of $K_{3,p}$ and $K_{9,p}$ for $p = 2, 3$

p	$K_{3,p}$	$K_{9,p}$
2	$\operatorname{diag}(1,1,3,3,3)$	$\operatorname{diag}(1,3,3,3,3)$
3	$\operatorname{diag}(1,1,1,2,6)$	$\operatorname{diag}(1,1,2,3,6)$

For $p = 2, 3$ and a symmetric 3×3 matrix F over $\mathbb{Z}_p$, let $[F]_p$ denote its congruence class in the given basis. At 2 we reduce the diagonal entries modulo 8 and the off-diagonal entries modulo 4. At 3 we reduce every entry modulo 9. Thus equality of two such classes means coefficientwise equality of the quadratic forms modulo 8 or 9, respectively. Since (3) depends only on $[G]_p$, the class $[G]_p$ determines whether the lattice is maximal at p.

We say that N *primitively represents* M if there exists an isometric embedding $\iota : M \hookrightarrow N$ for which $N/\iota(M)$ is torsion-free.

LEMMA 2.2. *Let $p = 2$ or 3, and let J be the Gram matrix of $K_{j,p}$ in Table 1. If X is a 5×3 matrix over $\mathbb{Z}_p$ of rank 3 modulo p and $[X^{\mathsf{T}}JX]_p = [C]_p$, then $K_{j,p}$ primitively represents C.*

PROOF. Extend the columns of X to a basis of $\mathbb{Z}_p^5$ and replace the leading Gram block $X^{\mathsf{T}}JX$ in this basis by C. In the original basis write the modified Gram matrix as $J + E$, so

that $X^{\mathsf{T}}(J+E)X = C$. In the extended basis the coefficients of the change in the quadratic form belong to $8\mathbb{Z}_2$ or $9\mathbb{Z}_3$, respectively. This divisibility is preserved on returning to the original basis. Thus at 2 the diagonal entries of E belong to $8\mathbb{Z}_2$ and the off-diagonal entries to $4\mathbb{Z}_2$. At 3 all entries of E belong to $9\mathbb{Z}_3$.

Starting with $M = J + E$ in the original basis, we orthogonalize in the diagonal order of J. At step i, keep the original indices on the remaining block M, put $d = M_{ii}$, and subtract $M_{i\ell}/d$ times basis vector i from each vector $\ell > i$. This changes $M_{k\ell}$ for $k, \ell > i$ by $-M_{ki}M_{i\ell}/d$. At 2, d is odd and this correction belongs to $16\mathbb{Z}_2$. At 3, $d \equiv J_{ii} \pmod 9$ has valuation at most 1 and the correction belongs to $27\mathbb{Z}_3$. In each case the basis change is integral and preserves the congruences on the remaining block.

The ratio of the i-th diagonal entry to J_{ii} lies in $1 + 8\mathbb{Z}_2$ or $1 + 3\mathbb{Z}_3$, respectively, so it equals u_i^2 for some $u_i \in \mathbb{Z}_p^\times$. Multiplying the i-th orthogonal basis vector by u_i^{-1} gives a basis with Gram matrix J. Thus the combined change of basis $P \in \mathrm{GL}_5(\mathbb{Z}_p)$ satisfies $P^{\mathsf{T}}(J+E)P = J$.

In the basis with Gram matrix J, the original three columns have coordinates $Y = P^{-1}X$. Hence $Y^{\mathsf{T}}JY = X^{\mathsf{T}}(J+E)X = C$. Moreover, P^{-1} takes a $\mathbb{Z}_p$-basis extending the columns of X to one extending the columns of Y. Thus Y gives a primitive embedding of the lattice with Gram matrix C into $K_{j,p}$. □

Let $\mathcal{R}_{j,p}$ consist of the classes $[X^{\mathsf{T}}JX]_p$ as X ranges over 5×3 matrices over $\mathbb{Z}_p$ of rank 3 modulo p. By Lemma 2.2, $[C]_p \in \mathcal{R}_{j,p}$ certifies that $K_{j,p}$ primitively represents C. We compute $\mathcal{R}_{j,p}$ in Python by enumerating the possible residues of each row of X in turn, as described in Appendix A.1.

3. Reduced bases and primes dividing the binary determinant

We take a Hermite–Korkine–Zolotarev reduced basis e_1, e_2, e_3 of Λ [13, Definition 16] and write its Gram matrix as

$$G = \begin{pmatrix} a & b & r_1 \\ b & c & r_2 \\ r_1 & r_2 & f \end{pmatrix} = \begin{pmatrix} B & r \\ r^{\mathsf{T}} & f \end{pmatrix}, \qquad \delta = \det B = ac - b^2, \quad D = \det G.$$

The Gram–Schmidt vectors of this basis have squared lengths a, $\beta = \delta/a$, and $\gamma = D/\delta$, respectively. By size reduction and a choice of signs for e_2, e_3,

$$0 \le 2b \le a, \qquad 0 \le 2r_1 \le a, \qquad 2|ar_2 - br_1| \le \delta.$$

Since e_1 is shortest, $a \le \min(c, f)$ and $\beta = c - b^2/a \ge c - a/4 \ge 3c/4$. In the lattice projected onto $e_1^\perp$, the projection of e_2 is shortest among nonzero vectors. Comparing it with the projection of e_3 gives

$$\beta \le f - r_1^2/a = \gamma + \beta\left(\frac{ar_2 - br_1}{\delta}\right)^2 \le \gamma + \beta/4.$$

Thus we have

$$a \le c \le 4\beta/3, \qquad \gamma \ge 3\beta/4. \tag{4}$$

Write $\lambda = (x, y, k)^{\mathsf{T}}$ for the coefficients of the linear form in this basis and put $\alpha = (x, y)^{\mathsf{T}}$ and $\mu = \alpha^{\mathsf{T}}B^{-1}r$. Positive definiteness of $C = G - s\lambda\lambda^{\mathsf{T}}$ is equivalent to $s\lambda^{\mathsf{T}}G^{-1}\lambda < 1$. Completing squares gives

$$s\lambda^{\mathsf{T}}G^{-1}\lambda = s\left(\frac{x^2}{a} + \frac{(y - bx/a)^2}{\beta} + \frac{(k-\mu)^2}{\gamma}\right). \tag{5}$$

For fixed x, y, the leading block $B' = B - s\alpha\alpha^{\mathsf{T}}$ has determinant $\Delta = \delta(1 - s\alpha^{\mathsf{T}}B^{-1}\alpha)$. Thus B' is positive definite (written $B' > 0$) precisely when $\Delta > 0$. The determinant of the full matrix is

$$\det C = \frac{D\Delta}{\delta} - s\delta\big(k - \mu\big)^2.$$

By Sylvester's criterion [5, Theorem 7.2.5(b)], C is positive definite precisely when $B' > 0$ and $\det C > 0$. When $\Delta > 0$, the formula for $\det C$ shows that $\det C > 0$ precisely when k lies in the open interval

$$I(\alpha) = (\mu - \theta,\ \mu + \theta), \qquad \theta = \sqrt{\frac{D\Delta}{s\delta^2}} = \sqrt{\frac{\gamma\Delta}{s\delta}}.$$

This yields an upper bound on D when L fails to represent Λ. Fix α with $\Delta > 0$ and an arithmetic progression $k_0 + m\mathbb{Z}$ with $k_0 \in \mathbb{Z}$ and $m \in \mathbb{Z}_{>0}$, and suppose there is an integer $g \ge 1$ such that any g consecutive terms of the progression include a k for which $K_{j,p}$ represents $C_G((x, y, k)^{\mathsf{T}})$ at every prime p. If $\theta > mg/2$, then $I(\alpha)$ contains a closed interval of length mg, hence g consecutive terms of $k_0 + m\mathbb{Z}$, hence such a k. For this k the matrix C is positive definite, and Lemma 2.1(a) shows that L represents G. Consequently, if L fails to represent Λ, then $\theta \le mg/2$, that is, $\gamma \le s\delta(mg)^2/(4\Delta)$. Since $D = \delta\gamma$, we have

$$D \le \frac{s\delta^2(mg)^2}{4\Delta} \tag{6}$$

for every such choice of α, $k_0 + m\mathbb{Z}$, and g.

LEMMA 3.1. *Fix $p \ge 5$ with $G \not\equiv 0 \pmod p$, and fix $\alpha = (x, y)^{\mathsf{T}}$. If $p \nmid \Delta$, then C has rank at least 2 modulo p for every k. If $p \mid \Delta$ and $(B, \alpha) \ne (0, 0) \bmod p$, the integers k for which $C \bmod p$ has rank at most 1 lie in at most two residue classes modulo p. At most one such class occurs if, in addition, $p \nmid \delta$, $B \equiv 0 \bmod p$, or $B' \equiv 0 \bmod p$.*

PROOF. We work over $\mathbb{F}_p$. If B' is nonsingular, then it already gives rank at least 2. Now suppose B' is singular and $(B, \alpha) \ne (0, 0)$. For $z \in \mathbb{F}_p^2$ put $\alpha(z) = \alpha^{\mathsf{T}}z$ and $r(z) = r^{\mathsf{T}}z$. If C has rank at most 1, then the Gram determinant of $(z_1, z_2, 0)^{\mathsf{T}}$ and $(0, 0, 1)^{\mathsf{T}}$ for the form $C \bmod p$ vanishes. Thus

$$(Q_B(z) - s\alpha(z)^2)(f - sk^2) - (r(z) - sk\alpha(z))^2 = 0.$$

For $B \ne 0$ choose z with $Q_B(z) \ne 0$. The coefficient of k^2 is $-sQ_B(z) \ne 0$, giving at most two roots. For $B = 0$ we have $\alpha \ne 0$. If $r \ne 0$, choose z outside the union of $\ker\alpha$ and $\ker r$, which has at most $2p - 1 < p^2$ elements. The equation is then linear with nonzero coefficient $2s\alpha(z)r(z)$. If $r = 0$, then $f \ne 0$ and any z with $\alpha(z) \ne 0$ makes the left side nonzero.

Finally, for $z \in \ker B'$ the equation reduces to $r(z) = sk\alpha(z)$. If B is nonsingular, every nonzero $z \in \ker B'$ has $\alpha(z) \ne 0$ because $B = B' + s\alpha\alpha^{\mathsf{T}}$. If $B' = 0$, then $\alpha \ne 0$ and we may again choose z with $\alpha(z) \ne 0$. In either case the equation determines k uniquely in $\mathbb{F}_p$ whenever $C \bmod p$ has rank at most 1. □

4. Proof of 3-universality

4.1. A uniform bound for the leading binary block. Since every ternary lattice lies in a maximal integral overlattice (Section 2), it suffices to show that L represents every maximal ternary lattice Λ. If Λ contains a vector e of norm 1, then $\Lambda = \mathbb{Z}e \perp M$ for a binary lattice M. The orthogonal complement of a coordinate vector of I_3 is $\langle 1, 1, 2\rangle \perp A_2$ in L_6 and $\langle 1, 1, 3\rangle \perp A_2$ in L_9. Both complements represent every binary lattice by Theorem 1.1(1), since $[2, 1, 2] \simeq A_2$. Sending e to the coordinate vector and embedding M in its complement shows that L represents Λ. Thus any maximal ternary lattice that L fails to represent has *minimum* (least nonzero norm) at least 2. We call such a non-represented lattice an *exception* for L.

We may therefore take Λ to have minimum $a \geq 2$. In a Hermite–Korkine–Zolotarev reduced basis with the signs chosen as in Section 3, its Gram matrix G has $G_{11} = a$. Prescribing $\lambda = (x, y, k)^\mathsf{T}$ fixes the coefficients of the three basis images along v. Their components in K_j must then have Gram matrix $C_G(\lambda) = G - s\lambda\lambda^\mathsf{T}$.

For $p = 2, 3$, we check whether $[C_G(\lambda)]_p \in \mathcal{R}_{j,p}$. Membership means that three vectors of $K_{j,p}$, linearly independent modulo p, have a Gram matrix F satisfying the following congruences:

- At 2, the diagonal entries of F and $C_G(\lambda)$ agree modulo 8 and the off-diagonal entries agree modulo 4.
- At 3, all corresponding entries agree modulo 9.

These are the coefficientwise congruences of the norm polynomials modulo 8 and 9, respectively, since each mixed coefficient is twice the corresponding Gram entry. Lemma 2.2 then gives a primitive representation of $C_G(\lambda)$ over $\mathbb{Z}_p$ by $K_{j,p}$.

Different integral lifts of a coefficient class $\bar{\lambda} \in \mathbb{F}_p^3$ can give different Gram classes $[C_G(\lambda)]_p$. To ensure primitive representation for every lift, we use the following set for $\sigma = [G]_p$.

$$\mathcal{U}_{j,p}(\sigma) = \left\{ \bar{\lambda} \in \mathbb{F}_p^3 : [C_G(\lambda)]_p \in \mathcal{R}_{j,p} \text{ for every integral lift } \lambda \text{ of } \bar{\lambda} \right\}.$$

For example, take $L = L_9$, $G = \operatorname{diag}(2, 3, 5)$ and $x = 1$. Then $(1, y, k)^\mathsf{T} \bmod 2$ belongs to $\mathcal{U}_{9,2}([G]_2)$ exactly when $k \equiv 1 - y \pmod 2$, and $(1, y, k)^\mathsf{T} \bmod 3$ belongs to $\mathcal{U}_{9,3}([G]_3)$ for every y, k. We may therefore take any $y \in \mathbb{Z}$ and then any $k \in 1 - y + 2\mathbb{Z}$. The arithmetic progressions for y and k have common differences 1 and 2, respectively.

For $p = 2, 3$, let σ_p range over the classes $[G]_p$ of maximal ternary $\mathbb{Z}_p$-lattices. Fix (σ_2, σ_3) and $x \in \{0, 1, 2, 3, 6\}$. At each prime p, we use $\mathcal{U}_{j,p}(\sigma_p)$ to compute congruences for y and, once y is fixed, for k (Appendix A.2). Their moduli h_p and m_p each belong to $\{1, p\}$. The Chinese remainder theorem combines the congruences at 2 and 3, giving $h = h_2 h_3$ and $m = m_2 m_3$. For each resulting triple (x, h, m) there is an arithmetic progression $y_0 + h\mathbb{Z}$ for y and, for each y in it, an arithmetic progression $k_0(y) + m\mathbb{Z}$ for k such that

$$(x, y, k)^\mathsf{T} \bmod p \in \mathcal{U}_{j,p}(\sigma_p) \qquad (p = 2, 3) \tag{7}$$

for every $k \in k_0(y) + m\mathbb{Z}$.

We impose two further restrictions on the triples (x, h, m). First, we require $sx^2 < a$, so the entry $a - sx^2$ of C is positive, which is necessary for C to be positive definite. Second, suppose $x = 0$, so that $\alpha = (0, y)^\mathsf{T}$. The argument below needs $\alpha \not\equiv 0 \pmod p$ for every prime $p \geq 5$, and it is convenient to have $|y| \leq 6$. We therefore take y to be a *signed divisor of* 6, i.e., $y \in \{\pm 1, \pm 2, \pm 3, \pm 6\}$. At primes $p \geq 5$ dividing a but not c, we need to control the entry $c - sy^2$ of B'. The certificate must choose h uniformly in the second diagonal entry c. We say that h *satisfies the signed-divisor condition (for L and a)* if, for every integer c_* and every $y_0 \in \mathbb{Z}$, there is a signed divisor y of 6 with $y \equiv y_0 \pmod h$ such that, for every prime $p \geq 5$ with $p \mid a$ and $p \nmid c_*$,

$$c_* - sy^2 \equiv 0 \pmod p \qquad \text{or} \qquad c_* - sy^2 \bmod p \in j(\mathbb{F}_p^\times)^2.$$

Here $j(\mathbb{F}_p^\times)^2$ is the *square class* of j in $\mathbb{F}_p^\times$. The condition depends on c_* only modulo the product of the primes $p \geq 5$ dividing a, so it is a finite check. When $x = 0$, we require that h satisfy this condition and that $a \leq 72$. For $a \geq 73$, only $x > 0$ is allowed, and $sx^2 \leq 72 < a$ for every such choice. Thus for $a \geq 73$ the eligible pairs (σ_2, σ_3) and the triples available to each pair depend on a only through $a \bmod 12$ (Appendix A.2).

We state the outcomes of the finite computations as *certificates*. Appendix A describes how the accompanying Python programs check them, and Appendix B describes their verification in Lean.

CERTIFICATE 4.1 (Local choices). *Fix $L \in \{L_6, L_9\}$ and an integer $a \ge 2$, the prescribed first diagonal entry $G_{11} = Q(e_1)$ in the reduced basis of Section 3. For $p = 2, 3$, let σ_p be the Gram class of a maximal ternary $\mathbb{Z}_p$-lattice. Assume that the first diagonal entries of σ_2 and σ_3 are congruent to a modulo 4 and 3, respectively. For each such pair (σ_2, σ_3) there are $x \in \{0, 1, 2, 3, 6\}$ and positive divisors h, m of 6 with the following property:*

> *There is an arithmetic progression $y_0 + h\mathbb{Z}$ such that, for each y in it, (7) holds for every k in an arithmetic progression $k_0(y) + m\mathbb{Z}$.*

Moreover, $sx^2 < a$ and, if $x = 0$, then $a \le 72$ and h satisfies the signed-divisor condition.

For every maximal ternary lattice with Gram matrix G and $G_{11} = a$, the pair $([G]_2, [G]_3)$ satisfies these congruences. Other pairs may satisfy them as well.

Choosing y. Fix a triple (x, h, m) for $([G]_2, [G]_3)$ from Certificate 4.1. We seek $y \in y_0 + h\mathbb{Z}$ near bx/a to keep the second term of (5) small enough for the leading block B' to be positive definite. The choice of y must also ensure that, at each prime $p \ge 5$ dividing $\det B'$, the form $C \bmod p$ represents j for all k outside at most one residue class modulo p.

Let $q_1 < q_2 < \cdots$ be the primes at least 5, put $P_t = q_1 \cdots q_t$ with $P_0 = 1$, and choose t by $P_t \le \delta < P_{t+1}$. Every positive integer at most δ has at most t distinct prime divisors at least 5. The *gap bound* g_t of Appendix A.2 applies to both arithmetic progressions $y_0 + h\mathbb{Z}$ and $k_0(y) + m\mathbb{Z}$. Given one forbidden residue class modulo each of at most t primes $p \ge 5$, any g_t consecutive terms of either arithmetic progression contain a term avoiding all the forbidden classes, since $h, m \mid 6$.

To see when a prime $p \ge 5$ dividing $\delta = \det B$ can also divide $\Delta = \det B'$, use the identity

$$a\Delta = (a - sx^2)\delta - s(ay - bx)^2. \tag{8}$$

For $x > 0$ and each $p \ge 5$ dividing δ but not a, exclude $y \equiv bxa^{-1} \pmod p$. This makes $p \nmid \Delta$. Since $h \mid 6$, one of the g_t terms of $y_0 + h\mathbb{Z}$ nearest bx/a avoids all these classes. For $x = 0$ apply the signed-divisor condition with $c_* = c$ to choose y in $y_0 + h\mathbb{Z}$. Thus $|y - bx/a| \le w/2$, where $w = hg_t$ for $x > 0$ and $w = 12$ for $x = 0$.

Choosing k. With x, y fixed, every $k \in k_0(y) + m\mathbb{Z}$ gives a matrix C primitively represented by $K_{j,2}$ and $K_{j,3}$, by (7) and Lemma 2.2. We seek a k in this progression for which C is positive definite and $C \bmod p$ represents j at every prime $p \ge 5$. Once $B' > 0$, positive definiteness restricts k to the interval $I(\alpha)$ of Section 3, centered at μ. Such a k exists whenever

$$\beta > \frac{s}{1 - sx^2/a}\left(\frac{w^2}{4} + \frac{m^2 g_t^2}{3}\right). \tag{9}$$

Since $|y - bx/a| \le w/2$, the first two terms in parentheses in (5) sum to less than $1/s$. Hence $B' > 0$ and $0 < \Delta \le \delta$. For $p \ge 5$ with $p \nmid \Delta$, the nonsingular block $B' \bmod p$ already represents j. For each $p \ge 5$ dividing Δ, we shall exclude at most one residue class modulo p from the choice of k; for every integer k outside that class, if any, $C \bmod p$ represents j over $\mathbb{F}_p$.

One of x, y is a signed divisor of 6, so $\alpha \not\equiv 0 \pmod p$. If $p \nmid \delta$, Lemma 3.1 shows that $C \bmod p$ has rank at least 2 outside at most one residue class modulo p, and Lemma 2.1(b) gives representation of j.

If p divides both δ and Δ, then (8) gives $ay \equiv bx \pmod p$. For $x > 0$ the choice of y forces $p \mid a$. For $x = 0$ the same follows since $p \nmid y$. Then $p \mid b$ and $\Delta \equiv -sx^2 c \pmod p$. For $x > 0$ this forces $p \mid c$. Whenever $p \mid c$, we have $B \equiv 0 \pmod p$, so Lemma 3.1 gives rank at least 2 for $C \bmod p$ except possibly when k lies in a single residue class modulo p.

It remains to consider $x = 0$ and $p \nmid c$. Here $B' \equiv \operatorname{diag}(0, c - sy^2) \pmod p$. Since $p \mid a$ and $p \nmid c$, the signed-divisor condition with $c_* = c$ gives two possibilities for $c - sy^2$ modulo p. If $c - sy^2 \equiv 0 \pmod p$, then $B' \equiv 0 \pmod p$ and Lemma 3.1 gives $\operatorname{rank}(C \bmod p) \ge 2$ for all k

outside at most one residue class modulo p. Otherwise $c - sy^2 = ju^2$ in $\mathbb{F}_p$ for some $u \in \mathbb{F}_p^\times$. For every k, the vector $(0, u^{-1}, 0)^\mathsf{T}$ then has norm j for C mod p, so no residue class is excluded.

Since $0 < \Delta \le \delta$, at most t primes $p \ge 5$ divide Δ. Among the g_t terms of $k_0(y) + m\mathbb{Z}$ nearest μ, the gap bound gives a k outside every excluded class. Thus C mod p represents j at every $p \ge 5$. Moreover, $|k - \mu| \le mg_t/2$. Using $\gamma \ge 3\beta/4$, we obtain $s(k-\mu)^2/\gamma \le sm^2 g_t^2/(3\beta)$. Together with $|y - bx/a| \le w/2$, inequality (9) now gives $s\lambda^\mathsf{T} G^{-1}\lambda < 1$ in (5). Thus C is positive definite. Lemma 2.1(b) gives representation of C by $K_{j,p}$ at every $p \ge 5$, and (7) gives it at 2 and 3. Lemma 2.1(a) now gives an embedding $\Lambda \hookrightarrow L$.

Fix L, a, and t. For each pair (σ_2, σ_3) in Certificate 4.1, minimize the right-hand side of (9) over its valid triples. The certificate supplies at least one, so the minimum is finite. Let $H_j(a,t)$ be the largest of these minima. An exception satisfies $3a/4 \le \beta = \delta/a \le H_j(a,t)$ by (4). Hence $H_j(a,t)^2 \ge 3\delta/4 \ge 3P_t/4$. The estimate in Appendix A.2 rules this out for $t \ge 27$. For $t < 27$ we compute the endpoints of the determinant intervals in the following certificate.

Certificate 4.2 (Determinant ranges). *For $a \ge 2$ and $0 \le t < 27$, the interval*

$$\max(P_t, 3a^2/4) \le \delta \le \min(P_{t+1} - 1, aH_j(a,t))$$

contains an integer for 536 pairs (a,t) for L_6 and 1,136 for L_9. The largest a values in the respective lists of pairs are 494 and 855.

4.2. The remaining binary blocks. For the fixed L, write

$$\mathcal{B}_j = \bigcup_{(a,t)} \mathcal{B}_j(a,t),$$

where (a,t) ranges over the pairs in Certificate 4.2 and $\mathcal{B}_j(a,t)$ comprises the integral matrices $B = \left(\begin{smallmatrix} a & b \\ b & c \end{smallmatrix}\right)$ with

$$0 \le 2b \le a, \qquad c \ge a, \qquad \delta = ac - b^2 \text{ in the corresponding determinant interval.}$$

To enumerate $\mathcal{B}_j(a,t)$, we take each integer δ in the interval and each b with $0 \le 2b \le a$, and keep $c = (\delta + b^2)/a$ when it is an integer with $c \ge a$.

Every exception has its leading block in $\mathcal{B}_j$: in the reduced basis of Section 3 we have $0 \le 2b \le a \le c$, and Section 4.1 places δ in the determinant interval for $a = G_{11}$ and the t with $P_t \le \delta < P_{t+1}$.

Fix $B \in \mathcal{B}_j$ and let t be the unique index with $P_t \le \det B < P_{t+1}$. Write

$$[B]_2 = (a \bmod 8, b \bmod 4, c \bmod 8), \qquad [B]_3 = B \bmod 9.$$

In the maximum defining $H_j(a,t)$, we restrict to pairs of maximal Gram classes (σ_2, σ_3) with leading blocks $[B]_2, [B]_3$, respectively. If there is no such pair, then B cannot occur in a maximal ternary lattice. Otherwise let $H_j(B,t)$ be the restricted maximum, so $H_j(B,t) \le H_j(a,t)$. We define $\mathcal{B}_j^\circ \subseteq \mathcal{B}_j$ to include B precisely when $H_j(B,t)$ is defined and $\det B \le aH_j(B,t)$. Every exception has its leading block in $\mathcal{B}_j^\circ$ by the argument in Section 4.1, since its pair $([G]_2, [G]_3)$ is among those in the restricted maximum. Enumerating $\mathcal{B}_j$ and retaining the blocks in $\mathcal{B}_j^\circ$ gives 534,827 blocks for L_6 and 8,521,181 for L_9 (Appendix A.3, Table 4, first row).

Representing every maximal completion with one pair. Fix $B = \left(\begin{smallmatrix} a & b \\ b & c \end{smallmatrix}\right) \in \mathcal{B}_j^\circ$ and write $\delta = \det B = ac - b^2$. A *completion* of B is a ternary Gram matrix G with leading block B. It is determined by its last column $(r_1, r_2, f)^\mathsf{T}$. We seek one pair (x,y) such that, for every maximal ternary lattice with a reduced Gram matrix G completing B, some integer k makes $C_G(\lambda)$ positive definite and represented by $K_{j,p}$ at every prime, where $\lambda = (x, y, k)^\mathsf{T}$. By Lemma 2.1(a) such a pair rules out B as the leading block of any exception.

Take $\alpha = (x,y)^\mathsf{T}$ up to sign with $0 \le x \le 6$, $|y| \le 6$ and $\alpha \not\equiv 0 \pmod p$ for every $p \ge 5$. Require $\Delta = \delta - s(cx^2 - 2bxy + ay^2) > 0$. For $p = 2, 3$ and each maximal Gram class $\sigma_p = [G]_p$

with leading block $[B]_p$, we seek an arithmetic progression for k on which $K_{j,p}$ primitively represents $C_G(\lambda)$. For this purpose we use the following sufficient *local representation conditions*, at 2 and 3, respectively,

$$[C_G(\lambda)]_2 \in \mathcal{R}_{j,2}, \qquad \lambda \bmod 3 \in \mathcal{U}_{j,3}(\sigma_3). \tag{10}$$

At 2, the first inclusion asks whether three vectors of $K_{j,2}$ independent modulo 2 have Gram class $[C_G(\lambda)]_2$. For fixed σ_2, x, y this depends only on $k \bmod 4$. At 3, we prescribe k only modulo 3, although $[C_G(\lambda)]_3$ can depend on $k \bmod 9$. The second inclusion therefore requires $[C_G(\lambda')]_3 \in \mathcal{R}_{j,3}$ for every integral column $\lambda' \equiv \lambda \pmod 3$. By Lemma 2.2, each inclusion in (10) gives the claimed primitive representation over the corresponding $\mathbb{Z}_p$.

For each σ_p, take the least positive step of an arithmetic progression all of whose terms satisfy the inclusion at p. Discard α if any σ_p admits no such progression. Otherwise the least steps divide 4 at 2 and 3 at 3, so their maximum m_p at each prime is a multiple of every step there. By the Chinese remainder theorem, for each completion G maximal at both primes there is an arithmetic progression $k_0 + m\mathbb{Z}$, with $m = m_2 m_3$, on which both inclusions in (10) hold. Here k_0 may depend on G.

At $p \ge 5$ dividing Δ, put $\nu_p = 2$ if $p \mid \delta$ and $B \not\equiv 0 \pmod p$, and $\nu_p = 1$ otherwise. Maximality gives $G \not\equiv 0 \pmod p$, so Lemma 3.1 shows that, for each fixed G, the integers k for which $C \bmod p$ has rank at most 1 lie in at most ν_p residue classes modulo p. Thus L represents every maximal ternary lattice with leading block $B = \left(\begin{smallmatrix} a & b \\ b & c \end{smallmatrix}\right)$ in a reduced basis if a positive integer g satisfies

$$\sum_{\substack{p \mid \Delta \\ p \ge 5}} \nu_p \lceil g/p \rceil < g, \qquad sa(mg)^2 < 3\Delta. \tag{11}$$

Indeed, $p \nmid m$, so each excluded class removes at most $\lceil g/p \rceil$ of any g consecutive terms. The first inequality therefore guarantees a k among these terms for which $C \bmod p$ has rank at least 2 at every $p \ge 5$ dividing Δ. At the other primes $p \ge 5$, $B' \bmod p$ is nonsingular. Together with (10), Lemma 2.1(b) and Lemma 2.2 give representation by $K_{j,p}$ at every prime. By (4), $D = \delta\gamma \ge 3\delta\beta/4 = 3\delta^2/(4a)$. Write $D_0 = \lceil 3\delta^2/(4a) \rceil$. The second inequality in (11) puts the upper bound (6) strictly below D_0. Thus no completion of B in a reduced basis can be an exception.

The last-column test. If the computation thus far has not certified representation of every maximal completion of B by one pair (x, y), we group its completions by the class $\rho = (r_1, r_2, f) \bmod 24$, using the reduced bases and signs of Appendix A.3. We allow (x, y) to depend on ρ and bound $D = \det G$ for any exception in that class. A bound below D_0 rules out the class. If the bound is at least D_0, the reduction inequalities leave only finitely many integral last columns to examine.

At 2 the mixed entries r_1, r_2 modulo 4 and f modulo 8 determine $[G]_2$ together with B. At 3 we fix all three entries modulo 3 and consider their lifts modulo 9. Thus it suffices to distinguish r_1, r_2 modulo 12 and f modulo 24. Maximality requires $4 \nmid D$ and $G \not\equiv 0 \bmod 3$, both determined by B and ρ. A class with no maximal lift at 3 contains no exception.

For a fixed ρ, we seek one pair (x, y) and one arithmetic progression $k_0 + m\mathbb{Z}$ for all completions in that class. For every $k \in k_0 + m\mathbb{Z}$ the first inclusion in (10) must hold for the single class $[G]_2$ determined by B and ρ. The second must hold for every maximal class $[G]_3$ with leading block $[B]_3$ and last column congruent to ρ modulo 3. Thus the same pair and progression give local representations for every integral last column in ρ whose completion is maximal at 2 and 3. At primes $p \ge 5$ the residue classes modulo p excluded from the choice of k may still depend on G. We try the integral pairs with $B' > 0$ up to simultaneous sign, since $C_G(-\lambda) = C_G(\lambda)$. For each pair, factor Δ and omit primes $p \ge 5$ dividing Δ at which a diagonal entry of B' lies in $j(\mathbb{F}_p^\times)^2$, since then $C \bmod p$ represents j for every k. Discard the pair if both B and α vanish modulo

any remaining prime. Take the least $g \geq 1$, if it exists, for which the sum in (11) over just the remaining primes is less than g. Equation (6) then bounds D for every exception in this class. For each class take the least bound obtained from these pairs and round it down to an integer. Retain the class if this bound is at least D_0. If any class is retained, let $U(B)$ be the largest of the retained bounds. This argument by last-column class applies directly to every block in $\mathcal{B}_j$, whether or not one first seeks a single pair for the entire block.

Enumeration and witnesses. For each retained last-column class, we use a program to enumerate the integral completions G allowed by $D_0 \leq \det G \leq U(B)$ and the reduction conditions of Appendix A.3. For each such G that is maximal at 3 and has relatively prime entries, we may now choose the covector λ separately.

CERTIFICATE 4.3 (Coverage and representations). *Fix $L \in \{L_6, L_9\}$ with the decomposition given in* (1).

(a) *For all but 836 blocks for L_6 and 5,147 for L_9 in $\mathcal{B}_j^\circ$, there is a recorded pair (x, y) with integers $m, g \geq 1$ satisfying* (11). *For each maximal completion G of such a block there is a k_0 for which the local representation conditions* (10) *hold throughout $k_0 + m\mathbb{Z}$. Hence every maximal ternary lattice with this leading block in a reduced basis embeds in L.*

(b) *For each block without a recorded pair in* (a), *every last-column class ρ compatible with maximality at* 2 *and* 3 *has a finite upper bound* (6) *on the determinant of an exception in that class. Exactly 99 blocks for L_6 and 162 for L_9 have a class whose least bound is at least D_0. For each such block B, the certificate identifies those classes and their common upper bound $U(B)$.*

(c) *In the classes specified in* (b), *exactly 10,905 Gram matrices for L_6 and 7,556 for L_9 satisfy $D_0 \leq D \leq U(B)$, the reduced-basis inequalities and sign conventions of Appendix A.3, maximality at* 3, *and coprimality of the entries. For every such G, the recorded λ gives a positive-definite $C_G(\lambda)$ represented by $K_{j,p}$ at every prime p.*

For $L = L_9$, consider again $G = \mathrm{diag}(2, 3, 5)$ from Section 4.1. Its leading block $B = \mathrm{diag}(2, 3)$ passes to the last-column test in part (b), with $D_0 = 14$ and $U(B) = 81$. This test rules out an exception in the class of the original last column $(0, 0, 5)$ modulo 24. The only completions of B requiring individual witnesses in part (c) have last column $(1, 1, f)$ with $f \in \{4, 5, 8, 9, 12, 13\}$.

At $p = 2, 3$, part (c) requires only an isometric embedding of $M = (\mathbb{Z}_p^3, C)$ into $K_{j,p}$. When $[C]_p \notin \mathcal{R}_{j,p}$, the certificate specifies an integral index-p overlattice M' of M whose Gram matrix F satisfies $[F]_p \in \mathcal{R}_{j,p}$. Lemma 2.2 then gives a primitive embedding of M' into $K_{j,p}$; its restriction to M gives the required local embedding.

The bounds in Section 4.1 and parts (a) and (b) of Certificate 4.3 reduce the proof to the ternary Gram matrices G enumerated in part (c). For each such G, the recorded λ gives a positive-definite $C_G(\lambda)$ represented by $K_{j,p}$ at every prime, so Lemma 2.1(a) shows that L represents G over $\mathbb{Z}$. Thus neither L_6 nor L_9 has an exception. Since every ternary lattice embeds in a maximal integral overlattice (Section 2), both lattices are 3-universal, proving Theorem 1.2(i) and (ii).

5. The quinary counterexample

PROPOSITION 5.1. *The lattice $I_6 \perp A_2$ does not represent the quinary lattice Λ_{117} with Gram matrix*

$$\begin{pmatrix} 2 & -1 & 0 & 1 & 0 \\ -1 & 2 & -1 & 0 & 1 \\ 0 & -1 & 2 & 0 & 0 \\ 1 & 0 & 0 & 6 & -1 \\ 0 & 1 & 0 & -1 & 7 \end{pmatrix}. \tag{12}$$

PROOF. The leading principal minors are $2, 3, 4, 21, 117$, so Λ_{117} is positive definite of determinant 117. Suppose the basis in which (12) is written maps to w_1, w_2, w_3, w_4, w_5 in $I_6 \perp A_2$. For $1 \le i \le 3$, the vector w_i has norm 2. A nonzero A_2 component already has norm at least 2, so w_i lies in one summand. The pairings $(w_1, w_2) = (w_2, w_3) = -1$ put all three vectors in the same summand. They are independent, so this summand is I_6. Each of these three vectors has exactly two nonzero coordinates, both ± 1. The support of w_2 meets each of the other two supports in one coordinate. Since $(w_1, w_3) = 0$, the supports of w_1 and w_3 are disjoint or equal. Equal supports would give $w_1 \equiv w_3 \pmod 2$, contrary to their pairings 1 and 0 with w_4. Thus after permuting the coordinate vectors ε_i of I_6, the support of w_i is $\{i, i+1\}$ for $1 \le i \le 3$. Changing the signs of the coordinate vectors then gives $w_i = \varepsilon_i - \varepsilon_{i+1}$ for $1 \le i \le 3$.

Write $w_4 = (u_0, u)$ and $w_5 = (v_0, v)$ in $I_4 \perp (I_2 \perp A_2)$. The pairings with $w_i = \varepsilon_i - \varepsilon_{i+1}$ give

$$u_0 = (\xi + 1, \xi, \xi, \xi), \qquad v_0 = (\eta + 1, \eta + 1, \eta, \eta).$$

The bounds $Q(u_0) \le 6$ and $Q(v_0) \le 7$ force $\xi, \eta \in \{-1, 0\}$. Both values of η give $Q(v) = 5$. If $\xi = 0$, then $Q(u) = 5$ and $|(u, v)| = |-1 - (u_0, v_0)| \in \{1, 2\}$. If $\xi = -1$, then $Q(u) = 3$ and $|(u, v)| \in \{0, 3\}$.

Now 2 is the only positive norm below 6 in A_2. Indeed, its norm form is $2(h^2 - h\ell + \ell^2)$, and $h^2 - h\ell + \ell^2 \equiv (h + \ell)^2 \pmod 3$ excludes norm 4. Since 3 is not a sum of two squares, a norm-5 vector of $I_2 \perp A_2$ lies in I_2, and a norm-3 vector projects to a vector of norm 1 in I_2. In particular $v \in I_2$. Let u' be the projection of u to I_2. Since $(u', v) = (u, v)$, the Gram determinant of u', v equals $5Q(u') - (u, v)^2$. If X is their coordinate matrix in the basis $\varepsilon_5, \varepsilon_6$, this determinant is $\det(X^{\mathsf{T}} X) = (\det X)^2$. For $\xi = 0$ its possible values are $24, 21$, and for $\xi = -1$ they are $5, -4$. None is an integer square. □

Proposition 5.1 proves Theorem 1.2(iii).

Use of generative AI

I used LLMs to assist with computations, coding, and synthesis in the preparation of this article, including GPT-6.2 Astra, GPT-5.* Pro, Claude Fable 5, Claude Opus 5.5, Claude Opus 4.*, and Gemini 3 Pro (all accessed in part via Poe with the support of Quora, where I am an advisor). Additionally, I used Refine.ink to review the draft for consistency, completeness, and clarity. The choice of problem, the methods, and the final written form are my own. Any errors remain my responsibility.

Appendix A. Finite verification

For each $L \in \{L_6, L_9\}$, our Python search computes the local representation tables at 2 and 3 and uses them to bound the leading binary block B of a possible exception. For each $B \in \mathcal{B}_j^\circ$ it seeks one pair (x, y) that proves L represents every maximal ternary lattice with leading block B in a reduced basis. For the remaining blocks it bounds $\det G$ in each last-column class and enumerates the ternary Gram matrices G still requiring individual verification; for each such G it tries covectors $\lambda \in \{-2, -1, 0, 1, 2\}^3$ until $C_G(\lambda)$ is positive definite and represented by $K_{j,p}$ at every prime.

Table 2 gives the commands to run from `python/` in release v4 of the accompanying repository.[1] Both run on Python 3.10 or later and use only the standard library for exact integer and rational arithmetic. The checker starts from the same primitive representation tables and maximality tests as the search. It reconstructs the local choices and determinant ranges, checks that the block and last-column bounds cover every possible exception, and verifies a witness for each

[1] `https://github.com/scduko/Kim-Kim-Oh-Classification/tree/v4`.

remaining Gram matrix. Below, program paths are relative to `python/`. The five certificate files are in its `certificates/` subdirectory.

TABLE 2. Commands for reproducing the search and checking the certificates

Command	Reference transcript in `expected_output/`
`python3 reproduce_ternary_search.py --workers 4`	`ternary_search.txt`
`python3 verify_ternary_certificates.py --workers 4`	`certificate_verification.txt`

A.1. Local representation tables. The local tables identify which Gram classes admit a primitive representation by $K_{j,p}$ at $p = 2, 3$. In the `verification/` directory, `local_representation.py` constructs $\mathcal{R}_{j,p}$ and counts the classes $[G]_p$ of maximal ternary $\mathbb{Z}_p$-lattices in Table 3. The module `residue_census.py` then determines the coefficient classes $\mathcal{U}_{j,p}([G]_p)$ used in Section 4.1.

Fix $p \in \{2, 3\}$ and let $J = \operatorname{diag}(d_1, \dots, d_5)$ be the Gram matrix of $K_{j,p}$ in Table 1. Writing z_i^{T} for row i of X gives $X^{\mathsf{T}} J X = \sum_i d_i z_i z_i^{\mathsf{T}}$. To construct $\mathcal{R}_{j,p}$, suppose the first $i-1$ rows contribute the matrix M to this sum and their reductions span $V \subseteq \mathbb{F}_p^3$. Appending row z^{T} in position i gives the update

$$([M]_p, V) \longmapsto \big([M + d_i z z^{\mathsf{T}}]_p,\ V + \mathbb{F}_p(z \bmod p)\big).$$

Start with $M = 0$ and $V = \{0\}$. Enumerate z modulo 4 at 2 and modulo 9 at 3 (modulo 3 suffices if $3 \mid d_i$). These residues determine both entries on the right. After five rows, $[M]_p \in \mathcal{R}_{j,p}$ precisely when the pair $([M]_p, \mathbb{F}_p^3)$ occurs. The maximal classes in Table 3 are determined by $4 \nmid \det G$ at 2 and (3) at 3. The last two columns count primitively represented classes among all Gram residues, including those of nonmaximal lattices.

TABLE 3. Counts of ternary Gram matrix classes at $p = 2, 3$

p	All Gram residues	Classes of maximal lattices	$\lvert\mathcal{R}_{3,p}\rvert$	$\lvert\mathcal{R}_{9,p}\rvert$
2	32,768	21,504	28,420	22,624
3	531,441	459,108	451,386	355,485

To construct $\mathcal{U}_{j,p}([G]_p)$, we test the lifts of each $\bar{\lambda} \in \mathbb{F}_p^3$ for membership of $[C_G(\lambda)]_p$ in $\mathcal{R}_{j,p}$. The class $[s\lambda\lambda^{\mathsf{T}}]_p$ depends only on $\lambda \bmod 2$ for $(p, s) = (2, 2)$, on $\lambda \bmod 4$ for $(2, 1)$, and on $\lambda \bmod 9$ at 3.

A.2. Arithmetic progressions and the uniform bound. For each triple (x, h, m) in Certificate 4.1, h is the common difference of the arithmetic progression $y_0 + h\mathbb{Z}$. Once y is chosen, m is the common difference of $k_0(y) + m\mathbb{Z}$. These common differences enter the bound $H_j(a, t)$ that gives the determinant intervals in Certificate 4.2; the module `verification/scalar_sieve.py` computes these intervals. With `-verify-tables`, `audit/verify_steps_and_ranges.py` reconstructs the pairs (h, m) and checks the interval endpoints.

Local choices. For fixed σ and $x \bmod p$, list the pairs $(y, k) \bmod p$ with $(x, y, k)^{\mathsf{T}} \bmod p \in \mathcal{U}_{j,p}(\sigma)$. In the pair of local moduli (h_p, m_p), a modulus of 1 allows all residues modulo p, and a modulus of p selects one residue. The residue selected for k may depend on y. Thus $(1, 1)$ is available if all pairs occur, $(1, p)$ if every $y \bmod p$ admits some $k \bmod p$, $(p, 1)$ if some $y \bmod p$ admits every $k \bmod p$, and (p, p) if at least one pair occurs. If one pair divides another in both coordinates, keep the smaller pair, whose contribution to (9) is no larger. When $x = 0$, the signed-divisor condition also holds for each divisor h' of h, since every residue class modulo h' contains a residue class modulo h. The 176 records in `local_progression_steps.tsv` group maximal Gram matrix classes by K_j, p, the retained lists for each $x \bmod p$, and the first diagonal

entry (modulo 8 at 2 or 9 at 3). The checker reconstructs each list and the number of classes in each group.

For fixed a take the groups whose first entries agree with a modulo 4 at 2 and modulo 3 at 3. For each x, the Chinese remainder theorem combines a choice of (h_2, m_2) and (h_3, m_3) into the triple (x, h_2h_3, m_2m_3). For $x = 0$ test every y_0 mod h and every c_* mod $\prod_{p|a,\ p\ge 5} p$ as in Section 4.1.

For $2 \le a \le 84$ the checker verifies that at least one triple remains for each pair after imposing the restrictions on x. For $a \ge 73$ only $x > 0$ is used, and then $sx^2 \le 72 < a$. Hence the available triples depend only on a mod 12, so the checks for $73 \le a \le 84$ complete Certificate 4.1.

The gap bound. For $0 \le t < 27$, let g_t be the least $g \ge 1$ satisfying $\sum_{i=1}^{t} \lceil g/q_i \rceil < g$. In either arithmetic progression $y_0 + h\mathbb{Z}$ or $k_0(y) + m\mathbb{Z}$ of Section 4.1, a forbidden class modulo $p \ge 5$ excludes at most $\lceil g/p \rceil$ of any g consecutive terms, since p divides neither step. The sum bounds all exclusions, since the i-th smallest prime used is at least q_i. Such a g exists since $\sum_{i=1}^{26} 1/q_i < 1$.

For $t \ge 27$, index the terms of either arithmetic progression by consecutive integers. Its step is coprime to the chosen primes, so each forbidden class excludes one class of indices. For any subset of these primes, the Chinese remainder theorem gives one class of indices modulo their product satisfying all the forbidden congruences in that subset. Its count among g consecutive indices differs from g divided by that product by less than 1. Inclusion–exclusion therefore counts the surviving indices with error less than 2^t from g times their density. This density is at least $\prod_{i=1}^{t}(1 - 1/q_i) \ge 4/(t + 4)$, since $q_i \ge i + 4$. Thus $g_t = (t + 4)2^{t-2}$ guarantees a surviving index.

In this range $w \le 6g_t$ and $(1 - sx^2/a)^{-1} \le 73$, since $sx^2 < a$ and $sx^2 \le 72$. Hence (9) has right-hand side at most $2 \cdot 73(36/4 + 36/3)g_t^2 = 3066g_t^2$. At $t = 27$ direct integer comparison gives $3P_t > 4(3066g_t^2)^2$. As t increases, $\sqrt{P_t}$ grows by $\sqrt{q_{t+1}}$, while g_t^2 grows by $4((t + 5)/(t + 4))^2$. The former factor exceeds the latter at $t = 27$ and the inequality persists by monotonicity. This rules out $\sqrt{3P_t/4} \le H_j(a, t)$ for all $t \ge 27$.

Determinant ranges. For $t < 27$ evaluate $H_j(a, t)$ in rational arithmetic. Test $2 \le a \le 72$ individually. For $a \ge 73$ choose $a_0 \in [73, 84]$ with $a_0 \equiv a \pmod{12}$. The same triples are available for a and a_0, though their bounds in (9) use the actual first entry. For each triple the bound decreases as a increases. Thus $H_j(a, t) \le H_j(a_0, t)$. If $3P_t > 4H_j(a_0, t)^2$, discard the class. Otherwise $3a/4 \le \beta \le H_j(a, t)$ gives $a \le 4H_j(a_0, t)/3$. Within these limits the checker computes the integer endpoints in Certificate 4.2 and compares them with the intervals used to enumerate the blocks.

A.3. Enumeration of bounded matrices. Certificate 4.3 reduces the candidate binary blocks to a finite list of ternary Gram matrices and gives a representation for each. The programs `audit/verify_block_coverage.py` and `audit/verify_representation_witnesses.py` verify the completeness of this list and the representations, respectively.

The checker enumerates the blocks of $\mathcal{B}_j(a, t)$ (Section 4.2) in (b, c) order for each pair (a, t) of Certificate 4.2. For each b it takes the integers $c \ge a$ for which $ac - b^2$ lies in the corresponding determinant interval. It retains B in $\mathcal{B}_j^\circ$ when $H_j(B, t)$ is defined and $ac - b^2 \le aH_j(B, t)$.

Pairs recorded for entire blocks. The file `binary_block_pairs.json.gz` either gives one pair (x, y) for B or records that D must be bounded separately for each last-column class. To check a recorded pair at p, range over the classes $\sigma = [G]_p$ of maximal $\mathbb{Z}_p$-lattices with leading block $[B]_p$. At 2, keep the k mod 4 for which $[C]_2 \in \mathcal{R}_{j,2}$. At 3, keep the k mod 3 with $(x, y, k)^{\mathsf{T}}$ mod $3 \in \mathcal{U}_{j,3}(\sigma)$. An empty set rules out the pair. Otherwise the least step is 1 for the full set, 2 at $p = 2$ if the proper set contains an entire parity class, and the modulus (4 or 3) in the other cases. Take the largest step over these matrix classes at each prime. With their product m the checker verifies (11) for the recorded pair. The search uses the following sufficient estimate for the sum in (11).

LEMMA A.1. *Let d be the product of the primes from 5 through 47 dividing $\Delta > 0$. Let ℓ, ℓ_2 be the largest nonnegative integers with $53^\ell \le \Delta/d$ and $53^{\ell_2} \le \gcd(\Delta, \delta)$, respectively. The first inequality in (11) holds if*

$$\sum_{p \mid d} \nu_p \lceil g/p \rceil + (\ell + \ell_2)\lceil g/53 \rceil < g.$$

If $d < 35$ and $\gcd(\Delta, \delta) < 5$, take $g = 1 + \ell$ for $d = 1$ or $g = 2 + \ell$ for $d > 1$, provided $g \le 5$.

PROOF. The distinct primes $p \ge 53$ dividing Δ have product dividing Δ/d, so there are at most ℓ. Those with weight 2 also divide $\gcd(\Delta, \delta)$, so at most ℓ_2 contribute twice. In the last case all weights are 1, at most one prime divides d, and $\lceil g/p \rceil = 1$ for every $p \ge 5$. □

Last-column classes. For each remaining block take $\rho = (r_1, r_2, f) \bmod 24$ with $4 \nmid D$ and $G \not\equiv 0 \bmod 3$. For each ρ try the pairs (x, y) with $B' > 0$ up to simultaneous sign. They lie in the finite box $sx^2 < a$, $sy^2 < c$. At 2, the block and ρ determine $[G]_2$. Keep each k modulo 2 if $s = 2$, or modulo 4 if $s = 1$, for which $[C_G((x, y, k)^\mathsf{T})]_2 \in \mathcal{R}_{j,2}$. At 3, consider the classes $\sigma = [G]_3$ of maximal $\mathbb{Z}_3$-lattices with leading block $B \bmod 9$ and last column congruent to $\rho \bmod 3$. Keep $k \bmod 3$ if $(x, y, k)^\mathsf{T} \bmod 3 \in \mathcal{U}_{j,3}(\sigma)$ for every such σ. If there is no such σ, then ρ has no maximal lift at 3. The Python checker includes these ρ in its initial count and verifies that none contributes a matrix to the enumeration. For nonempty sets at both primes, the least permissible local steps have product m. The checker reconstructs the surviving classes and $U(B)$ by Section 4.2 and compares them with `last_column_bounds.json.gz`. The record uses one bit per ($r_1 \bmod 12, r_2 \bmod 12, f \bmod 24$), so four nominal classes modulo 24 share each bit.

Integral lifts. Write $R_B(r) = cr_1^2 - 2br_1r_2 + ar_2^2$, so $D = \delta f - R_B(r)$. Combining $D_0 \le D \le U(B)$ with the bounds on the reduced Gram entries from Section 3 gives

$$0 \le 2r_1 \le a, \qquad 2|ar_2 - br_1| \le \delta,$$

$$\max\left(a, \left\lceil \frac{\delta + r_1^2}{a} \right\rceil, \left\lceil \frac{D_0 + R_B(r)}{\delta} \right\rceil\right) \le f \le \left\lfloor \frac{U(B) + R_B(r)}{\delta} \right\rfloor.$$

The enumeration uses two further choices of signs. If $r_1 = 0$, negating e_3 if necessary gives $r_2 \ge 0$. If $b = 0$ or $2b = a$, we may also take $ar_2 - br_1 \ge 0$. Indeed, replacing e_2 by $-e_2$ or $e_1 - e_2$, respectively, preserves B and r_1 and negates $ar_2 - br_1$. Both substitutions preserve the reduction bounds, and when $r_1 = 0$ the two sign conditions agree. The fourth row of Table 4 counts the lifts satisfying these bounds and sign conditions. The last row counts those that are maximal at 3 and have relatively prime entries. Maximality excludes an odd prime dividing all entries, and all entries even would give $8 \mid D$. These necessary conditions can include Gram matrices in nonreduced bases and lattices nonmaximal at larger primes. The checker compares the list of Gram matrices entry by entry with `bounded_gram_matrices.txt.gz`.

TABLE 4. Counts of binary blocks and ternary completions for L_6 and L_9

	L_6	L_9
Binary blocks in $\mathcal{B}_j^\circ$ of Section 4.2	534,827	8,521,181
Blocks with D bounded by last-column class	836	5,147
Blocks with a last-column class of bound $\ge D_0$	99	162
Bounded integral lifts in the surviving classes	29,831	10,407
Gram matrices tested	10,905	7,556

Checking the representations. For each G, `representation_witnesses.jsonl.gz` gives λ and two 5×3 matrices X_2, X_3. Check positivity of the leading principal minors of $C = C_G(\lambda)$. At $p = 2, 3$, take $F = C$ unless the record gives a column z defining an index-p overlattice.

Its first nonzero entry is 1. Replace the corresponding basis vector by z/p and check that the resulting Gram matrix F has entries in $\mathbb{Z}_p$. For J as in Table 1, verify $[X_p^{\mathsf{T}} J X_p]_p = [F]_p$ and $\operatorname{rank}(X_p \bmod p) = 3$. Lemma 2.2 gives an exact local embedding, which in the overlattice case restricts to the lattice with Gram matrix C.

At each $p \ge 5$ dividing the gcd of the 2×2 minors of C, check that a diagonal entry modulo p lies in $j(\mathbb{F}_p^{\times})^2$. At all other $p \ge 5$ the rank is at least 2, so Lemma 2.1(b) gives local representation in both cases. All recorded λ for L_6 lie in $\{-1, 0, 1\}^3$. For L_9 the search first succeeds outside this box for 56 matrices, each with $\max(|x|, |y|, |k|) = 2$.

Appendix B. Formal verification in Lean

We have formalized the argument, including the certificate verification, in Lean 4 [2] with Mathlib [20]. The declaration `KimKimOh.mainTheorem` proves the three assertions of Theorem 1.2 without hypotheses. Within the repository's `lean/` directory, `KimKimOh/Statement.lean` gives the statement and `KimKimOh/Main.lean` assembles its proof. The counts of isometry classes following Theorem 1.2 combine these three assertions with the candidate lists in Theorem 1.1.

For the norm-1 reduction, the formalization proves the 2-universality of $\langle 1, 1, 2\rangle \perp A_2$ and $\langle 1, 1, 3\rangle \perp A_2$. For Lemma 2.1(a), it uses Jonathan Hanke's `QuadFormsKB` [4] to show that if K_j represents C locally everywhere, then some lattice in its genus represents C over $\mathbb{Z}$. The mass formula from the same library, together with the orders of the automorphism groups, gives class number 1 for both K_3 and K_9. In Lean, local representation at p means solvability of the Gram matrix equation modulo p^e for every $e \ge 1$. Compactness gives the equivalent formulation over $\mathbb{Z}_p$. For the quinary case, `KimKimOh/Quinary.lean` proves that the lattice of determinant 117 in Proposition 5.1 does not embed in $I_6 \perp A_2$.

Lean evaluates the finite tests on the certificate data in its kernel (`decide +kernel`). For Certificate 4.1, it checks witnesses for the local representation tables at 2 and 3 and the residue choices giving the steps h, m. For Certificate 4.2, it verifies that the lists of pairs (a, t) cover every possible exception. For Certificate 4.3, it verifies that every block in $\mathcal{B}_j^{\circ}$ either satisfies the whole-block inequality or occurs on the list for the last-column test. For each listed block it checks the bounds and enumerates the remaining integral lifts. The proof requires these lists to cover every remaining case. The enumeration in Appendix A.3 gives the exact counts in Table 4.

For each remaining G, both verifications use the recorded λ and check positive definiteness of $C_G(\lambda)$ and local representation at every prime. At 2 and 3 the Python checker verifies the supplied matrices X_p directly. Lean checks the Gram class of $C_G(\lambda)$, or of its specified index-p overlattice, against its verified local table.

To build the proof with the pinned Lean 4.36.0 toolchain, run `lake exe cache get` and then `lake build` from `lean/`. The axiom audit (`lake env lean scripts/CheckAxiomsMain.lean`) follows the dependencies of the main theorem, including the proofs imported from `QuadFormsKB`, and finds only `propext`, `Classical.choice` and `Quot.sound`. For the Lean declarations corresponding to each step, see `docs/PAPER_CORRESPONDENCE.md`. The verification record in `docs/STATUS.md` reports the full build, the axiom audits, and a second kernel check of all project modules, one module at a time.

References

[1] J. H. Conway and N. J. A. Sloane. *Sphere Packings, Lattices and Groups*, volume 290 of *Grundlehren der mathematischen Wissenschaften*. Springer-Verlag, New York, third edition, 1999. 10.1007/978-1-4757-6568-7.

[2] Leonardo de Moura and Sebastian Ullrich. The Lean 4 theorem prover and programming language. In André Platzer and Geoff Sutcliffe, editors, *Automated Deduction – CADE 28*, volume 12699 of *Lecture Notes in Computer Science*, pages 625–635, Cham, 2021. Springer. 10.1007/978-3-030-79876-5_37.

[3] A. G. Earnest. The representation of binary quadratic forms by positive definite quaternary quadratic forms. *Transactions of the American Mathematical Society*, 345(2):853–863, 1994.

[4] Jonathan Hanke. Quadratic forms over number fields in Lean 4 (QuadFormsKB). Software, version 0.6.1, 2026. URL https://doi.org/10.5281/zenodo.23509792.

[5] Roger A. Horn and Charles R. Johnson. *Matrix Analysis*. Cambridge University Press, Cambridge, second edition, 2013. 10.1017/CBO9781139020411.

[6] B. M. Kim, M.-H. Kim, and S. Raghavan. 2-universal positive definite integral quinary diagonal quadratic forms. *The Ramanujan Journal*, 1(4):333–337, 1997. 10.1023/A:1009797524602.

[7] Byeong Moon Kim, Myung-Hwan Kim, and Byeong-Kweon Oh. 2-universal positive definite integral quinary quadratic forms. In Myung-Hwan Kim, John S. Hsia, Yoshiyuki Kitaoka, and Rainer Schulze-Pillot, editors, *Integral Quadratic Forms and Lattices*, volume 249 of *Contemporary Mathematics*, pages 51–62. American Mathematical Society, Providence, RI, 1999. 10.1090/conm/249/03747.

[8] Myung-Hwan Kim and Byeong-Kweon Oh. Representations of positive definite senary integral quadratic forms by a sum of squares. *Journal of Number Theory*, 63(1):89–100, 1997. 10.1006/jnth.1997.2069.

[9] Yoshiyuki Kitaoka. *Arithmetic of Quadratic Forms*, volume 106 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 1993. 10.1017/CBO9780511666155.

[10] Chao Ko. On the representation of a quadratic form as a sum of squares of linear forms. *Quarterly Journal of Mathematics*, os-8(1):81–98, 1937. 10.1093/qmath/os-8.1.81.

[11] David Lorch and Markus Kirschmer. Single-class genera of positive integral lattices. *LMS Journal of Computation and Mathematics*, 16:172–186, 2013. 10.1112/S1461157013000107.

[12] L. J. Mordell. A new Waring's problem with squares of linear forms. *Quarterly Journal of Mathematics*, os-1 (1):276–288, 1930. 10.1093/qmath/os-1.1.276.

[13] Phong Q. Nguyen. Hermite's constant and lattice algorithms. In Phong Q. Nguyen and Brigitte Vallée, editors, *The LLL Algorithm: Survey and Applications*, Information Security and Cryptography, pages 19–69. Springer, Berlin, Heidelberg, 2009. 10.1007/978-3-642-02295-1_2.

[14] Gordon L. Nipp. Tables of quinary quadratic forms. In *A Catalogue of Lattices*, maintained by Gabriele Nebe and Neil Sloane, accessed November 2026. URL https://www.math.rwth-aachen.de/~Gabriele.Nebe/LATTICES/nipp5.html.

[15] Byeong-Kweon Oh. Universal $\mathbb{Z}$-lattices of minimal rank. *Proceedings of the American Mathematical Society*, 128(3):683–689, 2000. 10.1090/S0002-9939-99-05254-5.

[16] O. Timothy O'Meara. *Introduction to Quadratic Forms*. Classics in Mathematics. Springer-Verlag, Berlin, Heidelberg, 2000. 10.1007/978-3-642-62031-7. Reprint of the 1973 edition.

[17] A. Schinzel. A positive definite binary quadratic form as a sum of five squares of linear forms (completion of Mordell's proof). *Bulletin of the Polish Academy of Sciences. Mathematics*, 61(1):23–26, 2013. 10.4064/ba61-1-3.

[18] A. Schinzel. Note to the paper "A positive definite binary quadratic form as a sum of five squares of linear forms (completion of Mordell's proof)" (Bull. Polish Acad. Sci. Math. 61 (2013), 23–26). *Bulletin of the Polish Academy of Sciences. Mathematics*, 61(2):107, 2013. 10.4064/ba61-2-2.

[19] Rainer Schulze-Pillot. Lecture notes on quadratic forms and their arithmetic. arXiv:2008.12847v2 [math.NT], 2021. URL https://arxiv.org/abs/2008.12847v2.

[20] The mathlib Community. The Lean mathematical library. In Jasmin Blanchette and Cătălin Hriţcu, editors, *Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs*, CPP '20, pages 367–381, New York, NY, USA, 2020. Association for Computing Machinery. 10.1145/3372885.3373824.

Harvard Business School; Department of Economics and Center of Mathematical Sciences and Applications, Harvard University; and a16z Frontier Research

Email address: kominers@fas.harvard.edu