

Polynomial parametrization of quadratic Diophantine equations: decision and construction

Bogdan Grechuk and Ashleigh Ratcliffe

Abstract

We give an algorithm that, for any polynomial with integer coefficients of degree at most two, decides whether its integer zero set is a finite union of polynomial families with integer coefficients and constructs such families whenever they exist. The main step is a constructive proof that, for every nondegenerate integral quadratic form Q isotropic over $\mathbb{Q}$ and every integer m , the integer solutions of $Q(\mathbf{x}) = m$ form a finite union of polynomial families. This proves the nondegenerate case of a result announced without proof by Vaserstein. For fixed Q , the number of parameters in each family is bounded independently of m . The new descent argument treats forms in at least five variables with rational Witt index one. We also settle the previously open cases $zt - x^2 - y^2 = 1$ and $zt - x^2 - y^2 = -1$ by combining Larsen–Nguyen’s group parametrization with a classical reduction of binary Hermitian forms, obtaining two and three polynomial families, respectively.

2020 Mathematics Subject Classification: 11D09, 11E12, 11E57, 11R11, 20G30.

Keywords: quadratic forms, polynomial parametrization, integral points, arithmetic groups, quadratic fields.

1 Introduction

What does it mean to solve a *polynomial Diophantine equation*? This is an equation

$$P(x_1, \dots, x_n) = 0 \tag{1.1}$$

with integer coefficients, for which we seek all solutions in $\mathbb{Z}^n$. If there are finitely many solutions, a satisfactory answer is a complete list, together with a proof of completeness. If there are infinitely many, the meaning of a complete description is less clear. An algorithm that merely prints every solution eventually is too weak a requirement: one can always enumerate integer tuples in order of increasing maximum absolute coordinate and test the equation. We would like a description that reveals more of the structure of the solution set.

Grunewald and Segal developed algorithms for quadratic equations that give considerably more information than enumeration [18, 19]. If, after a rational linear change of variables, a variable occurs only in a nonzero linear term, the equation is handled by elementary congruences, including those imposed by the change of variables (Section 13). Otherwise, completing squares and omitting free variables reduces a quadratic equation (1.1) to an equation of the form

$$Q(x_1, \dots, x_n) = m,$$

where Q is an integral quadratic form, and $m \in \mathbb{Z}$, with possibly finitely many fixed congruence restrictions on variables. Classical finiteness results, combined with Grunewald–Segal’s algorithms for generators and orbits [17, 18], yield a description by finitely many initial solutions and finitely many transformations that preserve the equation, together with free coordinates or integer scalar multiples where needed. Appendix B gives the effective reduction used here. One then imposes the congruences and returns to the original coordinates. We refer to this kind of description as a *Grunewald–Segal description*.

For example, the equation

$$y + y^2 + z^2 = 3x^2 \quad (1.2)$$

becomes

$$Y^2 + Z^2 = 3X^2 + 1 \quad (1.3)$$

under $X = 2x$, $Y = 2y + 1$ and $Z = 2z$, with the restrictions that Y is odd and X, Z are even. All integer solutions of (1.3) can be obtained from $(0, 1, 0)$ by changing signs, interchanging Y and Z , and applying

$$(X, Y, Z) \mapsto (2X - Y, 3X - 2Y, Z);$$

see [15, Proposition 4.27]. To check completeness, use signs and the interchange to arrange $X \geq 0$ and $Y \geq Z \geq 0$. When $X > 0$, the equation gives $X < Y \leq 2X$, so the displayed transformation replaces X by the smaller nonnegative integer $2X - Y$. Repeating reaches $X = 0$, where $Y^2 + Z^2 = 1$. All operations are reversible. We then retain the required parities and recover $(x, y, z) = (X/2, (Y - 1)/2, Z/2)$.

This is a finite description by generating rules, but such rules can obscure a much simpler answer. Consider, for example, the Pythagorean equation

$$x^2 + y^2 = z^2. \quad (1.4)$$

A nonzero integer tuple is *primitive* if its greatest common divisor is 1. Berggren [1] showed that all positive primitive Pythagorean triples with x odd and y even can be obtained from $(3, 4, 5)$ by the three transformations

$$\begin{aligned} (x, y, z) &\mapsto (x - 2y + 2z, 2x - y + 2z, 2x - 2y + 3z), \\ (x, y, z) &\mapsto (-x + 2y + 2z, -2x + y + 2z, -2x + 2y + 3z), \\ (x, y, z) &\mapsto (x + 2y + 2z, 2x + y + 2z, 2x + 2y + 3z). \end{aligned}$$

Interchanging the two legs, changing signs, taking common multiples, and adjoining the solutions with a zero coordinate gives every integer solution to (1.4). Yet the familiar formulas [10, p. 271] provide a more direct description:

$$\begin{aligned} (x, y, z) &= (2uvw, u(w^2 - v^2), u(w^2 + v^2)) \quad \text{or} \\ &= (u(w^2 - v^2), 2uvw, u(w^2 + v^2)), \quad u, v, w \in \mathbb{Z}. \end{aligned}$$

The three parameters are unrestricted, and these two formulas include all signs and all solutions with a zero coordinate.

These examples suggest a precise goal for solving quadratic equations: seek polynomial formulas in independent integer parameters when they exist, and otherwise retain a description by generating rules. We use the following terminology, as in [34, p. 980].

Definition 1.1. A subset $S \subseteq \mathbb{Z}^n$ is a *polynomial family* if there are an integer $N \geq 0$ and polynomials $P_1, \dots, P_n$ with integer coefficients in N variables such that

$$S = \{(P_1(t_1, \dots, t_N), \dots, P_n(t_1, \dots, t_N)) : (t_1, \dots, t_N) \in \mathbb{Z}^N\}.$$

The map $\Phi = (P_1, \dots, P_n) : \mathbb{Z}^N \rightarrow \mathbb{Z}^n$ is a *polynomial parametrization* of S . Thus every parameter choice is allowed, and every point of S occurs. We allow $N = 0$, with $\mathbb{Z}^0$ consisting of the empty tuple; this means a constant map with a one-point image. The empty set is the union of an empty list of polynomial families. In particular, every finite set is a finite union of polynomial families.

The discussion above motivates the following problem.

Problem 1.2. *Given an integer polynomial P of degree at most two, decide whether its integer zero set is a finite union of polynomial families. If it is, construct a finite list of parametrizations, including their coefficients and numbers of parameters.*

For the first example, (1.2), the answer is negative (Remark 13.5), which implies that the description of the integer solution set by generating rules is justified in this case.

This problem is difficult even for simple equations. For $xy - zt = 1$, the question goes back to Skolem [33, p. 23, Bemerkung 1] in 1938 and was later posed by Beukers [20, p. 390, CNTA 5.15]. Vaserstein proved in 2010 that its full solution set is one polynomial family with 46 parameters [34, Theorem 1]. The number of parameters is a substantive issue: Zannier had proved that finitely many families with only three parameters each cannot cover that solution set [37, Theorem 1, p. 153].

Vaserstein's theorem also gives parametrizations for many other quadratic equations; see [34] and [15, Chapter 2]. Nevertheless, the existence of finite polynomial parametrizations for

$$zt = x^2 + y^2 \pm 1 \tag{1.5}$$

was explicitly asked in [13, Open Question 2.4] and remained listed as open in [14, Table 1]. We settle these cases by combining Larsen–Nguyen's group parametrization with classical reduction; Proposition 1.5 gives the resulting formulas.

To state the result that settles Problem 1.2, we first define the relevant properties of a quadratic form. Its *polar form* is the function

$$B_Q(x, y) = Q(x + y) - Q(x) - Q(y), \quad x, y \in \mathbb{Q}^n.$$

The form Q is *nondegenerate* if the only $x \in \mathbb{Q}^n$ satisfying $B_Q(x, y) = 0$ for every $y \in \mathbb{Q}^n$ is $x = 0$; otherwise it is *degenerate*. It is *isotropic over $\mathbb{Q}$* if $Q(x) = 0$ for some nonzero $x \in \mathbb{Q}^n$, and *anisotropic over $\mathbb{Q}$* otherwise. We write

$$X_m(Q) = \{x \in \mathbb{Z}^n : Q(x) = m\}$$

for its integer *level set* at m .

On p. 982 of [34], Vaserstein states that he will “show elsewhere” that the integer solution set, “for any isotropic quadratic form Q , is a finite union of polynomial families.” The surrounding discussion concerns nonsingular forms. We interpret this assertion in the nondegenerate setting: for degenerate forms, isotropy can come entirely from a direction on which the form vanishes, and the assertion is false in general (Remark 13.4). We know of no published proof in the full nondegenerate case. Our main theorem proves that case constructively.

Theorem 1.3. *Let Q be a nondegenerate integral quadratic form isotropic over $\mathbb{Q}$. For every $m \in \mathbb{Z}$, the set $X_m(Q)$ is a finite union of polynomial families. These families can be computed from Q and m . For fixed Q , their numbers of parameters can be bounded independently of m . The number of families and the coefficients and degrees of their parametrizations may depend on Q and m .*

The new part of the proof concerns forms in at least five variables which, after a rational linear change of variables, have the form $uv + q(z)$ with q anisotropic. Our descent constructs polynomial families on their levels directly, without a parametrization of the whole group of integer matrices preserving the form.

The form $Q(x, y, z, t) = zt - x^2 - y^2$ is nondegenerate and isotropic, since $Q(0, 0, 1, 0) = 0$. Thus Theorem 1.3 applies to both signs in (1.5). In the opposite direction, every polynomial family on a level of an anisotropic form is constant (Lemma 13.1). Combining these facts with an explicit treatment of linear terms and degenerate quadratic parts gives a complete answer to Problem 1.2.

Theorem 1.4 (Decision and construction). *There is an algorithm that, given an integer polynomial of degree at most two in any number of variables, decides whether its integer zero set is a finite union of polynomial families. When the answer is affirmative, the algorithm outputs a finite list of the polynomial maps, including their coefficients and numbers of parameters. For an empty zero set it outputs the empty list.*

Here and throughout, *effective* or *computable* means that a specified procedure terminates after finitely many steps and produces the claimed finite data. We make no assertion about its running time, and the finite lists of families can be very large. Integer solvability of quadratic equations was proved decidable by Siegel [32]; our decision procedure uses the algorithm of Grunewald–Segal [19].

The next proposition gives compact formulas for (1.5). The eight integers appearing in it are intermediate coordinates with two displayed relations. Immediately after the proposition we explain how a fixed polynomial substitution replaces them by unrestricted integer parameters.

Proposition 1.5 (Two explicit parametrizations). *Choose eight integers a_j, b_j, c_j, d_j , $j = 1, 2$, satisfying*

$$\begin{aligned} a_1 d_1 - a_2 d_2 - b_1 c_1 + b_2 c_2 &= 1, \\ a_1 d_2 + a_2 d_1 - b_1 c_2 - b_2 c_1 &= 0. \end{aligned} \tag{1.6}$$

For letters $u, v \in \{a, b, c, d\}$, put

$$N_u = u_1^2 + u_2^2, \quad D_{uv} = u_1 v_1 + u_2 v_2, \quad C_{uv} = u_2 v_1 - u_1 v_2.$$

Then the integer solution sets have the following exact descriptions.

(i) All solutions of $zt - x^2 - y^2 = 1$ are

$$(x, y, z, t) = \sigma(D_{ac} + D_{bd}, C_{ac} + C_{bd}, N_a + N_b, N_c + N_d), \quad \sigma \in \{1, -1\}. \tag{1.7}$$

(ii) All solutions of $zt - x^2 - y^2 = -1$ are

$$\begin{aligned} x &= e(D_{ad} + D_{bc}) + f(C_{bc} - C_{ad}) + \eta D_{bd}, \\ y &= e(C_{ad} + C_{bc}) + f(D_{ad} - D_{bc}) + \eta C_{bd}, \\ z &= 2(eD_{ab} - fC_{ab}) + \eta N_b, \\ t &= 2(eD_{cd} - fC_{cd}) + \eta N_d, \end{aligned} \tag{1.8}$$

where $(e, f, \eta) \in \{(1, 0, 0), (0, 1, 0), (1, 0, 1)\}$.

For each fixed choice of σ or (e, f, η) , the displayed set is a polynomial family in the sense of Definition 1.1. Thus the two solution sets are unions of two and three polynomial families, respectively.

To interpret the constrained formulas, use the Gaussian integers $\mathbb{Z}[i]$ and the group

$$\mathrm{SL}_2(\mathbb{Z}[i]) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z}[i], \ ad - bc = 1 \right\}.$$

Writing $a = a_1 + a_2 i$, and likewise for b, c, d , identifies (1.6) with this set of matrices. Larsen–Nguyen [23, Theorem 1.9] prove that this set admits a single polynomial parametrization over $\mathbb{Z}[i]$: its coordinate polynomials have Gaussian integer coefficients and its parameters range independently over $\mathbb{Z}[i]$. Replacing each Gaussian parameter by its two integer coordinates gives a single integer-coefficient polynomial map onto the eight constrained coordinates. Composing it with each displayed formula proves the polynomial-family assertion. Appendix A makes this substitution effective, and Section 12.C proves that the formulas attain every solution of the two equations.

Related work and organization. The distinction between polynomial formulas with integer coefficients and rational coefficients taking integer values is relevant to earlier parametrizations of Pythagorean triples and analogues in more variables [10, 11]. Frisch [8] showed how fixed residue substitutions relate the two conventions; we give the version with congruence restrictions in Section 3. Frisch–Lettl [9] give further parametrizations for homogeneous quadratic equations in three variables. Vaserstein’s explicit three- and four-variable models [34, Examples 5, 7 and 8], and the determinant-level parametrizations of Gallardo–Vaserstein [12], provide further precedents. For real quadratic fields, the constructions use the bounds on products of elementary matrices of Morgan–Rapinchuk–Sury [27] and Jordan–Zaytman [21]; see Section 12.

The proof separates according to the number of variables. After setting out the notation and the fixed-denominator argument, we treat five or more variables by a uniform construction in Sections 4–10. A rational change of variables puts the form into $uv + q(z)$, where q is a quadratic form in the remaining variables. We first construct polynomial families that contain the points whose u -coordinate is a suitable prime. We then move any primitive point to such a point by a bounded sequence of polynomially parametrized transformations, and invert that sequence. The primes are used only to prove that every target is attained; they are not restrictions on the parameters of the resulting maps. Section 11 follows one point through the construction. Section 12 handles the smaller numbers of variables and a useful special case in higher dimensions. Finally, Section 13 proves the classification and algorithm, while the appendices supply the effective group and representative calculations needed to output the maps. Table 1 records the resulting parameter bounds.

Statement of AI use. The proofs were developed through an extended collaboration between the authors and ChatGPT. After partial results obtained by the authors and earlier models, the final step in the proof of Theorem 1.3 was obtained with ChatGPT 6 Astra. The main text was drafted with ChatGPT 6 Astra under the authors’ guidance; the introduction was written mainly by the authors and received language polishing from AI. Referee-style reports generated by Claude informed the final revisions.

2 Quadratic-form conventions

Vectors are columns. We use the polar form B_Q of the introduction and its Gram matrix $G_Q = (B_Q(e_i, e_j))$, so $Q(x) = \frac{1}{2}x^T G_Q x$. An integral quadratic form has an integral polar matrix with even diagonal. Unless specified otherwise, rank and isotropy are over $\mathbb{Q}$; for a nondegenerate form, the rank equals the number of variables. Write $\text{Rad}(Q) = \ker G_Q$, $\langle a_1, \dots, a_s \rangle = \sum a_i x_i^2$, and $Q_1 \perp Q_2$ for an orthogonal sum. The hyperbolic plane is $H(u, v) = uv$; the *Witt index* is the number of hyperbolic planes in a maximal orthogonal decomposition. A form is *split* if it is a sum of hyperbolic planes. For a commutative ring R , write $\text{GL}_n(R)$ for the invertible $n \times n$ matrices over R , and $\text{SL}_n(R)$ for those of determinant one. For a field k_0 of characteristic different from two, write

$$\text{SO}(Q)(k_0) = \{g \in \text{SL}_n(k_0) : Q(gx) = Q(x) \text{ for all } x \in k_0^n\}.$$

For nondegenerate Q , an isometry with integer matrix automatically has integer inverse. A polynomial family of isometries is a matrix of polynomials whose every parameter value is an isometry.

In a rational quadratic space (V, Q) , a full lattice $L \subset V$ is the $\mathbb{Z}$ -span of a $\mathbb{Q}$ -basis of V . Polynomial maps into L are written in a fixed $\mathbb{Z}$ -basis. The *content* of a nonzero $x \in L$ is the largest integer $c > 0$ with $x \in cL$; equivalently it is the gcd of the coordinates of x . Thus x is primitive exactly when its content is one. We also use level sets $\{x \in L : Q(x) = m\}$ for rational m and arbitrary full lattices.

Lemma 2.1 (Hyperbolic splitting; [30, Chapter IV, §1.3, Proposition 3]). *Over a field of characteristic different from two, a nondegenerate isotropic quadratic form is isometric to $uv + q(z)$ with q nondegenerate. The change of basis is computable from an isotropic vector by linear algebra.*

Proof. Choose $e \neq 0$ with $Q(e) = 0$ and v with $B_Q(e, v) = 1$. Then $f = v - Q(v)e$ satisfies $Q(f) = 0$ and $B_Q(e, f) = 1$. The span of e, f is a hyperbolic plane; adjoining a basis of its orthogonal complement gives the required coordinates. $\square$

3 Polynomial families and fixed denominators

Frisch [8, main theorem and Lemmas 2–3] proved that the integer points in the image of a rational-coefficient polynomial map on integer parameters form a finite union of polynomial families. The same residue substitution also imposes fixed congruences.

Lemma 3.1 (Residue substitutions). *Let $\Phi \in D^{-1}\mathbb{Z}[\mathbf{t}]^n$, where $\mathbf{t} = (t_1, \dots, t_N)$ and $D \geq 1$ is fixed. Fix $M \geq 1$ and $b \in \mathbb{Z}^n$, and let $\mathcal{R} \subseteq (\mathbb{Z}/DM\mathbb{Z})^N$ be the set of residue vectors a with $\Phi(a) \in b + M\mathbb{Z}^n$. Then:*

- (i) *the condition $\Phi(\mathbf{t}) \in b + M\mathbb{Z}^n$ depends only on $\mathbf{t} \bmod DM$;*
- (ii) *for each $a \in \mathcal{R}$, represented by an integer vector, the polynomial map $\mathbf{s} \mapsto \Phi(a + D\mathbf{M}\mathbf{s})$ has its constant term in $b + M\mathbb{Z}^n$ and all its nonconstant coefficients in $M\mathbb{Z}^n$; in particular it has integer coefficients;*
- (iii) *the finitely many maps in (ii) have union of images exactly $\Phi(\mathbb{Z}^N) \cap (b + M\mathbb{Z}^n)$, each uses the same N parameters, and each satisfies every polynomial identity satisfied by Φ .*

There are at most $(DM)^N$ maps. Taking $M = 1$ retains precisely the integer points in the image of Φ . Several fixed congruences can be imposed by using a common modulus and retaining all allowed residue classes.

Proof. Put $f = D\Phi \in \mathbb{Z}[\mathbf{t}]^n$. The condition is $f(\mathbf{t}) \equiv Db \pmod{DM}$. For an allowed residue vector a , expanding each term shows that every nonconstant coefficient of $f(a + D\mathbf{M}\mathbf{s})$ is divisible by DM . Its constant coefficient is $f(a) \equiv Db \pmod{DM}$. Dividing by D proves the coefficient assertions. These substitutions partition the allowed integer parameters and preserve all polynomial identities. $\square$

Lemma 3.2 (Change of lattice). *Let L_0, L be full lattices in a rational quadratic space (V, Q) , with $Q(L_0) \subseteq \mathbb{Z}$. If every integral level on L_0 is a finite union of polynomial families, the same is true of every rational level on L . Uniform bounds on parameters per family are preserved.*

Proof. Choose $D, D' \geq 1$ with $DL \subseteq L_0$ and $D'L_0 \subseteq L$. If $D^2m \notin \mathbb{Z}$, the level on L is empty. Otherwise choose finitely many polynomial maps Φ_j whose images exhaust the level D^2m on L_0 , and divide their values by D . In a basis of L , these maps have coefficient denominators dividing DD' . Lemma 3.1 retains precisely their integral values. Since $Q(\Phi_j/D) = D^{-2}Q(\Phi_j) = m$, the resulting families exhaust the required level, without additional parameters. $\square$

In particular, if $C \in \mathrm{GL}_n(\mathbb{Q})$ and $Q(C \cdot)$ is integral, take $L_0 = C\mathbb{Z}^n$ and $L = \mathbb{Z}^n$ to transfer the polynomial families for its integral levels to Q on $\mathbb{Z}^n$. Scalar multiples cause no further difficulty: for $c \in \mathbb{Q}^\times$, $Q(x) = m$ is equivalent to $cQ(x) = cm$. Thus both the form and its level are scaled together whenever we pass to a similar form.

Lemma 3.3 (Content reduction). *Let Q be integral on a lattice L . Suppose that on every integral level, finitely many polynomial families contained in that level together contain all primitive vectors. Then every integral level is a finite union of polynomial families. Nonzero levels require no additional parameters; the zero level requires at most one.*

Proof. Every nonzero $x \in L$ is cv for a primitive v and an integer $c > 0$. If $Q(x) = m \neq 0$, then $c^2 \mid m$: use the finitely many primitive levels m/c^2 and multiply their outputs by c [34, remark after Corollary 4, p. 982]. At zero, multiply the primitive-level families by a free integer scalar; if there are none, use the constant zero map. $\square$

Vaserstein's theorem [34, Theorem 1] gives a matrix with polynomial entries and determinant identically one,

$$\mathcal{V} \in \mathrm{SL}_2(\mathbb{Z}[t_1, \dots, t_{46}]), \quad \mathcal{V}(\mathbb{Z}^{46}) = \mathrm{SL}_2(\mathbb{Z}). \quad (3.1)$$

An explicit construction is given in [34, Section 1, Proposition 1.5].

4 Elementary isometries and a ternary representation

The high-rank argument concerns

$$F(u, v, z) = uv + q(z), \quad z \in \mathbb{Q}^r, \quad r \geq 3,$$

where q is nondegenerate and integral. Theorem 7.4 constructs polynomial families containing points whose first coordinate is a prime of the prescribed type. Theorem 9.3 moves every primitive point into that subset after a bounded integral rescaling. Inverting this reduction and applying Lemma 3.1 gives the required families; see (10.1).

Put

$$q(z) = \frac{1}{2}z^\top Gz, \quad B(z, t) = z^\top Gt, \quad \Delta = |\det G|.$$

Thus G is integral with even diagonal and $\Delta > 0$. The elementary constructions in this section also apply in any positive rank over a field of characteristic different from two. For a vector t , define the Eichler transformations

$$T_t(u, v, z) = (u - B(z, t) - vq(t), \quad v, \quad z + vt), \quad (4.1)$$

$$S_t(u, v, z) = (u, \quad v - B(z, t) - uq(t), \quad z + ut). \quad (4.2)$$

They preserve F , satisfy $T_s T_t = T_{s+t}$ and $S_s S_t = S_{s+t}$, and have inverses T_{-t}, S_{-t} (see [5, §3] and [16, §3.1, (5)]). For integral t they preserve the lattice and primitivity. We also use $R_\epsilon(u, v, z) = (\epsilon u, \epsilon v, z)$, where $\epsilon = \pm 1$.

Fix w with $k = q(w) \neq 0$. The classical action $X \mapsto gXg^\top$ of SL_2 on symmetric binary matrices, applied to

$$X = \begin{pmatrix} u & B(z, w)/2 \\ B(z, w)/2 & -kv \end{pmatrix},$$

and fixing the component of z orthogonal to w , defines a transformation $\rho_w(g)$. For $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, its coordinates are

$$u' = a^2 u + abB(z, w) - kb^2 v, \quad (4.3)$$

$$v' = d^2 v - \frac{c^2 u + cdB(z, w)}{k}, \quad (4.4)$$

$$z' = z + \left(\frac{acu + bcB(z, w)}{k} - bdv \right) w. \quad (4.5)$$

Lemma 4.1. *Over any field E of characteristic different from two, ρ_w is a representation of $\mathrm{SL}_2(E)$ by isometries of F , fixing $\{(0, 0, z) : B(z, w) = 0\}$ pointwise. For integral q, w , both $\rho_w(g)$ and $\rho_w(g)^{-1}$ have matrix entries in $k^{-1}\mathbb{Z}[a, b, c, d]$.*

Proof. Write $z = \lambda w + z_\perp$, with $\lambda = B(z, w)/(2k)$. Then $\det X = -k(uv + k\lambda^2)$, while $q(z_\perp)$ is fixed. This proves preservation of F and the representation identity. The off-diagonal entry transforms to $acu + (ad + bc)k\lambda - bdkv$; using $ad - bc = 1$ gives (4.5). The displayed formulas prove the denominator bound, also for the inverse after replacing (a, b, c, d) by $(d, -b, -c, a)$. $\square$

Substituting Vaserstein's matrix (3.1) gives polynomial isometry families in 46 unrestricted integer parameters, with denominators dividing k .

Lemma 4.2 (Moving the first coordinate). *Let q be nondegenerate in $r \geq 1$ variables over a finite field $\mathbb{F}$ of odd order. For every nonzero $(u, v, z) \in \mathbb{F}^{r+2}$, some $t \in \mathbb{F}^r$ makes the first coordinate of $T_t(u, v, z)$ nonzero.*

Proof. The polynomial $u - B(z, t) - vq(t)$ is nonzero by nondegeneracy. Its degree in each variable is at most $2 < |\mathbb{F}|$, so it cannot vanish on all of $\mathbb{F}^r$, by the usual root bound applied successively to the variables. $\square$

5 An imaginary quadratic field of prime discriminant

For a number field K , write $\mathcal{O}_K$ for its ring of integers. A prime ideal $\mathfrak{p}$ above p has *residue degree one* when $\mathcal{O}_K/\mathfrak{p} \simeq \mathbb{F}_p$. For quadratic K , a bar denotes conjugation, and $\mathrm{Tr}(\alpha) = \alpha + \bar{\alpha}$, $\mathrm{Nm}(\alpha) = \alpha\bar{\alpha}$. A rational prime p *splits* in K when $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$ with two distinct prime ideals; both then have residue degree one. Write $\mathbb{Q}_\ell$ for the ℓ -adic field. For rational $a \neq 0$, $v_\ell(a)$ is the exponent of ℓ in a , with $v_\ell(0) = \infty$.

Lemma 5.1. *Let q be a nondegenerate rational quadratic form of rank $r \geq 3$. Outside any prescribed finite set of rational primes there is a prime $P \equiv 3 \pmod{8}$ such that q is isotropic over $K = \mathbb{Q}(\sqrt{-P})$, whose discriminant is $-P$. For $r \geq 5$, every imaginary quadratic field makes q isotropic.*

Proof. If $r \geq 5$, q is isotropic over every $\mathbb{Q}_\ell$ [30, Chapter IV, Theorem 6], hence over every finite completion of K . Its complex completions present no obstruction, so Hasse–Minkowski proves the last assertion [35, Theorem 14.6.9].

For $r = 3, 4$, choose a nondegenerate ternary subform $aX^2 + bY^2 + cZ^2$. It is isotropic precisely when the quaternion algebra $\mathcal{A} = (-ab, -ac)_\mathbb{Q}$ splits, that is, becomes $M_2(\mathbb{Q})$ [35, §5.3.23 and Main Theorem 5.4.4]. Here $(s, t)_\mathbb{Q}$ is generated by ι, j with $\iota^2 = s$, $j^2 = t$ and $\iota j = -j\iota$. Let Σ be the finite set of rational primes where $\mathcal{A}$ ramifies, meaning that it is not a matrix algebra over $\mathbb{Q}_\ell$. For each odd $\ell \in \Sigma$, prescribe a nonzero class of $P \bmod \ell$ for which $-P$ is a nonsquare, and impose $P \equiv 3 \pmod{8}$. The Chinese remainder theorem and Dirichlet's theorem provide infinitely many such primes P [30, Chapter VI, §4.1]. No ramified place of $\mathcal{A}$ splits in K : at 2 this uses $-P \equiv 5 \pmod{8}$, and a real place becomes complex. Consequently K splits $\mathcal{A}$ [35, Proposition 14.6.7], proving isotropy. In both cases choose P outside the prescribed set. Since $P \equiv 3 \pmod{4}$, $\mathrm{disc}(K) = -P$. $\square$

The congruence modulo 8 handles possible ramification of $\mathcal{A}$ at 2; the descent itself requires only $P \equiv 3 \pmod{4}$.

6 Polynomial maps for quadratic levels over finite fields

Put

$$\mathcal{U}(t) = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}, \quad \mathcal{L}(t) = \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix}, \quad \mathcal{W}_2(x, y) = \mathcal{U}(x)\mathcal{L}(y) = \begin{pmatrix} 1 + xy & x \\ y & 1 \end{pmatrix}.$$

Lemma 6.1 (Two elementary factors). *Let $\mathbb{F}$ be a finite field of odd order and $d, U \in \mathbb{F}^\times$. Some first row (a, b) of $\mathcal{W}_2(x, y)$ satisfies $a^2 - db^2 = U$.*

Proof. For $U = 1$, take $x = y = 0$. Otherwise the binary quadratic count [25, Lemma 6.24] gives

$$\#\{(a, b) : a^2 - db^2 = U\} = |\mathbb{F}| - \chi(d),$$

where $\chi(0) = 0$ and $\chi(x)$ is 1 or -1 according as $x \neq 0$ is a square or a nonsquare. At most two solutions have $b = 0$, so one has $b \neq 0$ when $|\mathbb{F}| \geq 5$. For $|\mathbb{F}| = 3$, $U \neq 1$ is a nonsquare and every solution has $b \neq 0$. Set $x = b$, $y = (a - 1)/b$. $\square$

Lemma 6.2 (Reduction onto finite-field levels). *Let q be a nondegenerate rational quadratic form in $r \geq 3$ variables, isotropic over a number field K . For every $m \in \mathbb{Z}$ there is a polynomial map $Z_m \in K[\theta]^r$ with $q(Z_m) = m$, using $N = 2r - 2$ parameters if $m \neq 0$ and $N = 2r - 3$ if $m = 0$. There are an integer $D_Z > 0$ and a finite set $\mathcal{B}_0$ of rational primes, both independent of m , with the following properties. Put $\mathcal{B} = \mathcal{B}_0 \cup \{p : p \mid m\}$ for $m \neq 0$ and $\mathcal{B} = \mathcal{B}_0$ for $m = 0$.*

- (i) $D_Z Z_m \in \mathcal{O}_K[\theta]^r$;
- (ii) if $\mathfrak{p}$ has residue degree one above $p \notin \mathcal{B}$, the reductions of $Z_m(\mathbb{Z}^N)$ exhaust $q = m$ over $\mathcal{O}_K/\mathfrak{p}$.

The set $\mathcal{B}_0$ includes 2 and the primes dividing D_Z or the coefficient denominators of q . Only imaginary quadratic K will be used below.

Proof. By Lemma 2.1, fix $C \in \mathrm{GL}_r(K)$ with

$$q(C(U, V, W)) = UV + q_1(W), \quad \mathrm{rank} \, q_1 = r - 2 \geq 1.$$

Choose w_0 with $k_0 = q_1(w_0) \neq 0$. In this proof T, S, ρ_{w_0} refer to this auxiliary form, using (4.1)–(4.5) with q_1 in place of q . Define

$$Z_m = C T_{\mathbf{t}_T} S_{\mathbf{t}_S} \rho_{w_0}(\mathcal{W}_2(a_1, a_2))(1, m, 0), \quad m \neq 0, \quad (6.1)$$

$$Z_0 = C T_{\mathbf{t}_T} S_{\mathbf{t}_S}(a_0, 0, 0), \quad (6.2)$$

where $\mathbf{t}_T, \mathbf{t}_S \in \mathbb{Z}^{r-2}$ and all scalar parameters are integers. The initial vectors have value m under $UV + q_1(W)$, which T, S and ρ_{w_0} preserve; hence $q(Z_m) = m$ identically. The first is polynomial jointly in its parameters and m , so one integer D_Z clears denominators in both formulas for every m .

Choose $\mathcal{B}_0$ so that outside it the coefficients of $C, C^{-1}, q, q_1, w_0, k_0^{-1}$ and the inverse polar determinant of q_1 are integral. Include 2 and the prime divisors of D_Z . Then reduction preserves the splitting, the nondegeneracy of q_1 , and $k_0 \neq 0$.

At a prime in (ii), work over $\mathcal{O}_K/\mathfrak{p} \simeq \mathbb{F}_p$. Apply Lemma 4.2 to $UV + q_1(W)$, whose residual form q_1 has rank $r - 2 \geq 1$, to move a nonzero target to one with first coordinate $U \neq 0$. If $m \neq 0$, every target is nonzero because $p \nmid m$, and Lemma 6.1 gives a first row (a, b) with $a^2 - k_0 m b^2 = U$. Thus $\rho_{w_0}(\mathcal{W}_2)(1, m, 0)$ has first coordinate U . The factor $S_{\mathbf{t}_S}$ gives it any required W -coordinates, and the level equation forces V . The factor $T_{\mathbf{t}_T}$ reverses the initial move. For $m = 0$, start instead from $(U, 0, 0)$; $a_0 = 0$ also attains zero. Residue degree one ensures that all these parameter residues lift to ordinary integers, proving (ii). $\square$

Remark 6.3. The condition $r \geq 3$ is essential here. For a split binary form, $U(\theta)V(\theta) = m \neq 0$ forces both polynomials to be constant. Finitely many such maps cannot exhaust the levels $UV = m$ over residue fields of unbounded size.

7 The trace equation and quadratic descent

Fix a prime $P \equiv 3 \pmod{4}$ and put

$$K = \mathbb{Q}(\sqrt{-P}), \quad \omega = (1 + \sqrt{-P})/2, \quad \mathcal{O}_K = \mathbb{Z}[\omega].$$

Conjugation of polynomials acts on coefficients and fixes parameters. The descent uses a trace-one element $\alpha = A\pi$ to combine Z and $\bar{Z}$. Choosing π in a prime ideal ensures the desired residue; its norm need only be a bounded multiple of p .

Lemma 7.1 (The trace equation). *The coordinate vectors of pairs $\pi, A \in \mathcal{O}_K$ satisfying*

$$\mathrm{Tr}(A\pi) = 1 \tag{7.1}$$

are covered by at most P^{46} integer-coefficient polynomial maps with 46 parameters each, satisfying the equation identically. For $\pi = a_1 + a_2\omega$, such an A exists precisely when $\gcd(a_1, a_2) = 1$ and $P \nmid \mathrm{Nm}(\pi)$.

Proof. Write $A = c_1 + c_2\omega$ and set $X = 2a_1 + a_2$, $Y = a_1 + (1 - P)a_2/2$. Then (7.1) is $c_1X + c_2Y = 1$, so it corresponds to

$$\begin{pmatrix} X & Y \\ -c_2 & c_1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}), \quad X \equiv 2Y \pmod{P},$$

with inverse coordinates

$$a_1 = \frac{(P-1)X/2 + Y}{P}, \quad a_2 = \frac{X - 2Y}{P}.$$

Substitute (3.1) and apply Lemma 3.1 with denominator P and modulus one. For the criterion, A exists exactly when $\gcd(X, Y) = 1$. Away from P , the inverse formulas identify common prime divisors of X, Y with those of a_1, a_2 . At P , use $2Y = X - Pa_2$ and $4\mathrm{Nm}(\pi) = X^2 + Pa_2^2$. $\square$

Lemma 7.2 (Descent identity). *Let q be rational, with polar form B , and let polynomial vectors Z over K and polynomials A, π over $\mathcal{O}_K$, in independent parameter blocks, satisfy $q(Z) = m \in \mathbb{Q}$ and $\mathrm{Tr}(A\pi) = 1$. Writing $\alpha = A\pi$, the rational polynomial coordinates*

$$u = \mathrm{Nm}(\pi), \tag{7.2}$$

$$v = \mathrm{Nm}(A)(2m - B(Z, \bar{Z})), \tag{7.3}$$

$$z' = \bar{\alpha}Z + \alpha\bar{Z} \tag{7.4}$$

satisfy $uv + q(z') = m$ identically.

Proof. Conjugation fixes these coordinates. Since $q(Z) = q(\bar{Z}) = m$,

$$q((1 - \lambda)Z + \lambda\bar{Z}) = m + \lambda(1 - \lambda)(B(Z, \bar{Z}) - 2m).$$

Take $\lambda = \alpha$, using $1 - \alpha = \bar{\alpha}$ and $\alpha\bar{\alpha} = \mathrm{Nm}(A)\mathrm{Nm}(\pi)$. $\square$

Lemma 7.3 (Bounded norm multiples). *If $p \neq P$ splits in K , then either prime $\mathfrak{p}$ above p contains $\pi = a_1 + a_2\omega$ with*

$$\gcd(a_1, a_2) = 1, \quad \mathrm{Nm}(\pi) = cp, \quad 1 \leq c < P.$$

For this π there is $A \in \mathcal{O}_K$ with $\mathrm{Tr}(A\pi) = 1$.

Proof. Put $H_p = \lfloor \sqrt{p} \rfloor$. Among the $(H_p + 1)^2 > p$ elements $a + b\omega$, $0 \leq a, b \leq H_p$, two agree modulo $\mathfrak{p}$. Their difference is a nonzero $\pi_0 = a + b\omega \in \mathfrak{p}$ with $|a|, |b| \leq H_p$. Divide by $g = \gcd(a, b)$; since $g < p$, the resulting primitive π still belongs to $\mathfrak{p}$. Its positive norm is divisible by p , and

$$0 < \text{Nm}(\pi) \leq a^2 + ab + \frac{P+1}{4}b^2 \leq \frac{P+9}{4}H_p^2 \leq PH_p^2 < Pp.$$

Thus $\text{Nm}(\pi) = cp$ with $1 \leq c < P$, so $P \nmid \text{Nm}(\pi)$. Apply Lemma 7.1. This is the pigeonhole argument underlying Thue's lemma [31, Theorem 2.33]. $\square$

Theorem 7.4 (Points with prime first coordinate). *Let $q \in \mathbb{Z}[z_1, \dots, z_r]$ be nondegenerate, $r \geq 3$, and isotropic over $K = \mathbb{Q}(\sqrt{-P})$, where $P \equiv 3 \pmod{4}$ is prime. For each $m \in \mathbb{Z}$, finitely many integer-coefficient polynomial families on $X_m(uv + q)$ contain every point (p, v, z) for which p splits in K and avoids a fixed finite exceptional set $\mathcal{B}_m$. Each family uses $3r + 44$ parameters for $m \neq 0$ and $3r + 43$ for $m = 0$.*

Proof. Take $Z_m, D_Z, \mathcal{B}$ from Lemma 6.2, and set $\mathcal{B}_m = \mathcal{B}$. Combining Z_m with each map of Lemma 7.1 in the descent identity (Lemma 7.2) gives rational polynomial maps (u, v, z') on $F = m$. Their coordinates $u, D_Z z', D_Z^2 v$ have integer coefficients: they are algebraic integers fixed by conjugation.

For each $1 \leq c < P$, compose with $S_{\mathbf{s}/(D_Z c)}$, $\mathbf{s} \in \mathbb{Z}^r$, and the fixed rational isometry

$$\mathcal{N}_c(u, v, z) = (u/c, cv, z).$$

The resulting map is

$$\left(\frac{u}{c}, \quad cv - \frac{B(z', \mathbf{s})}{D_Z} - \frac{uq(\mathbf{s})}{D_Z^2 c}, \quad z' + \frac{u\mathbf{s}}{D_Z c} \right),$$

with coefficient denominator dividing $D_Z^2 c$.

For a target (p, v_0, z_0) , the split prime p differs from the ramified prime P . Choose $\mathfrak{p}$ above p and use Lemma 7.3 to obtain π, A with $\text{Nm}(\pi) = cp$, $\text{Tr}(A\pi) = 1$. Realize them by trace parameters. Since $q(z_0) \equiv m \pmod{\mathfrak{p}}$, choose parameters with $Z_m \equiv z_0 \pmod{\mathfrak{p}}$. Both Z_m and $\bar{Z}_m$ are integral at $\mathfrak{p}$, since $p \nmid D_Z$. Thus $\alpha \equiv 0, \bar{\alpha} \equiv 1$ imply $z' \equiv z_0 \pmod{\mathfrak{p}}$. As $p \nmid D_Z$ and $D_Z z'$ is integral,

$$D_Z(z' - z_0) \in \mathfrak{p}\mathcal{O}_K^r \cap \mathbb{Z}^r = p\mathbb{Z}^r.$$

The integral choice $\mathbf{s} = D_Z(z_0 - z')/p$ therefore corrects the z -coordinates. The level equation forces the corrected point to be $(cp, v_0/c, z_0)$, and $\mathcal{N}_c$ gives the target. Lemma 3.1 retains exactly the integral values, without losing any target or adding parameters. The count is $N + 46 + r$, giving the stated bounds. $\square$

8 Compatible prime representation

The content of an integral binary form is the gcd of its coefficients; the form is primitive when this is one. We use Weber's theorem that every primitive positive definite integral binary quadratic form represents infinitely many primes (see [36] and [4, Theorem 9.12]).

Lemma 8.1. *Let $P \equiv 3 \pmod{4}$ be prime. Every primitive positive definite integral binary form f of discriminant $\mathfrak{D}$ with $P \nmid \mathfrak{D}$ represents infinitely many primes splitting in $\mathbb{Q}(\sqrt{-P})$, avoiding any prescribed finite set.*

Proof. The reduction of f modulo P is nondegenerate and represents 1 [30, Chapter IV, §1.7, Proposition 4]. Rescaling a representing vector gives either $(t, 1)$ or $(1, 0)$ on which f takes a nonzero square value. Lifting t to an integer gives a primitive $v \in \mathbb{Z}^2$; complete it to the first column of $U_0 \in \mathrm{SL}_2(\mathbb{Z})$. Write

$$f\left(U_0 \begin{pmatrix} X \\ Y \end{pmatrix}\right) = a_f X^2 + b_f XY + c_f Y^2.$$

Then $P \nmid a_f$ and a_f is a square modulo P . The form

$$g(X, Y) = a_f X^2 + P b_f XY + P^2 c_f Y^2$$

is positive definite and primitive: a common prime divisor other than P would divide a_f, b_f, c_f , and $P \nmid a_f$. By Weber's theorem it represents infinitely many primes p . For $p \neq 2, P$, its representation gives $p \equiv a_f X^2 \not\equiv 0 \pmod{P}$. Quadratic reciprocity yields $\left(\frac{-P}{p}\right) = \left(\frac{p}{P}\right) = 1$, so p splits in $\mathbb{Q}(\sqrt{-P})$ [4, (1.12) and Proposition 5.16]. It is also represented by f ; discard the prescribed finite set. $\square$

9 Prime-coordinate reduction with the required splitting

Assume that q has positive index of inertia at least two. Rational diagonalization and clearing denominators give fixed $w, h \in \mathbb{Z}^r$ with

$$k = q(w) > 0, \quad q(h) > 0, \quad B(w, h) = 0.$$

Choose P by Lemma 5.1, avoiding the prime divisors of $2kq(h)\Delta$, and put $K = \mathbb{Q}(\sqrt{-P})$.

Lemma 9.1 (Bounded content). *For every primitive (u, v, z) with $u \neq 0$, some $t \in \mathbb{Z}^r$ makes $S_t(u, v, z) = (u, v', z')$ satisfy*

$$\gcd(u, v') = \gcd(u, v, (Gz)_1, \dots, (Gz)_r) \mid \Delta.$$

Proof. For each $\ell \mid u$, let $e = \min\{v_\ell(u), v_\ell(v), v_\ell((Gz)_1), \dots, v_\ell((Gz)_r)\}$. If $e < v_\ell(u)$, the affine polynomial $(v - (Gz) \cdot t)/\ell^e$ is nonzero modulo ℓ ; choose $t \bmod \ell$ where it is nonzero. Since $uq(t)$ vanishes modulo ℓ^{e+1} , this gives the desired valuation of v' . The Chinese remainder theorem gives all choices simultaneously.

Let g denote the displayed gcd before transformation. The identity $\mathrm{adj}(G)Gz = (\det G)z$ shows that g divides $(\det G)z_i$ for every i , as well as u, v . Primitivity then gives $g \mid \det G$. $\square$

Proposition 9.2. *Every primitive integral point x can be moved to $x' = S_{\mathbf{s}}R_{\epsilon}T_{\mathbf{t}}x = (u, v, z)$, with $\mathbf{s}, \mathbf{t} \in \mathbb{Z}^r$, $\epsilon = \pm 1$, such that $u > 0$, $P \nmid u$, and*

$$\beta_{x'}(\xi, \eta) = u\xi^2 + B(z, w)\xi\eta - kv\eta^2$$

is positive definite, has content $\kappa \mid k\Delta$, and has discriminant prime to P .

Proof. Primitivity and $P \nmid \Delta$ allow Lemma 4.2 modulo P ; choose $T_{\mathbf{t}}$ with $P \nmid u$, and R_{ϵ} with $u > 0$. Lemma 9.1 then makes $\gcd(u, v) \mid \Delta$. Apply $S_{u\tau h}$, obtaining

$$z_{\tau} = z + u^2\tau h, \quad v_{\tau} = v - u\tau B(z, h) - u^3\tau^2 q(h).$$

Since $v_{\tau} - v$ is a multiple of u , this preserves $\gcd(u, v)$; it also preserves u and $B(z, w)$. The new discriminant is

$$\mathcal{D}(\tau) = B(z, w)^2 + 4kuv - 4ku^2\tau B(z, h) - 4ku^4\tau^2 q(h).$$

Its leading coefficient is negative and nonzero modulo P . Since $P \geq 3$, some residue class avoids its at most two roots; choose τ there with sufficiently large absolute value. Then $\mathcal{D}(\tau) < 0$ and $P \nmid \mathcal{D}(\tau)$. Moreover, $\kappa = \gcd(u, B(z_\tau, w), kv_\tau) \mid k \gcd(u, v_\tau) \mid k\Delta$. The two S -transformations combine into one. $\square$

Theorem 9.3 (Compatible prime-coordinate reduction). *There are two rational polynomial isometry families $\mathcal{A}_\epsilon(\xi)$ of F , $\epsilon = \pm 1$, each with $46 + 2r$ parameters, such that $k\mathcal{A}_\epsilon$ and $k\mathcal{A}_\epsilon^{-1}$ have integer-coefficient entries. For every primitive integral x and finite set of primes $\mathcal{E}$, some integer parameter choice gives*

$$y = k\mathcal{A}_\epsilon(\xi)x \in \mathbb{Z}^{r+2}, \quad y_1 = \delta_0 p, \quad F(y) = k^2 F(x),$$

where $\delta_0 > 0$ divides $k^2\Delta$ and $p \notin \mathcal{E}$ splits in K . The families depend only on the fixed data above.

Proof. Apply Proposition 9.2. Dividing $\beta_{x'}$ by κ divides its discriminant by κ^2 , so the resulting primitive form still has discriminant prime to P . Lemma 8.1 gives $\beta_{x'}(a, b) = \kappa p$ for a prime of the required type. The pair (a, b) is primitive because its square content divides p . Complete it to the first row of $g \in \mathrm{SL}_2(\mathbb{Z})$. By (4.3), the first coordinate of $\rho_w(g)x'$ is exactly this binary-form value. Multiplying by k clears denominators and gives $\delta_0 = k\kappa \mid k^2\Delta$. Thus take

$$\mathcal{A}_\epsilon = \rho_w(\mathcal{V}(\mathbf{a}))S_{\mathbf{s}}R_{\epsilon}T_{\mathbf{t}}.$$

Lemma 4.1 bounds the denominators of this product and its inverse; its parameter count is $46 + 2r$. $\square$

10 Completion of the proof in rank at least five

Theorem 10.1. *Let q be a nondegenerate integral quadratic form in $r \geq 3$ variables. Every integral level of $uv + q(z)$ is a finite union of integer-coefficient polynomial families.*

Proof. Since $r \geq 3$, q or $-q$ has positive index at least two. Replacing (q, m, u) by $(-q, -m, -u)$ if necessary, assume this for q . Choose w, h, k first, then P, K as in Section 9. At level k^2m , construct the maps Ψ_i and exceptional set $\mathcal{B}_{k^2m}$ of Theorem 7.4. All these choices precede the target.

For a primitive $x \in X_m(F)$, Theorem 9.3 with $\mathcal{E} = \mathcal{B}_{k^2m}$ gives

$$x \xrightarrow{k\mathcal{A}_\epsilon(\xi)} (\delta_0 p, v, z) \xrightarrow{\mathcal{N}_{\delta_0}} (p, \delta_0 v, z) = \Psi_i(\boldsymbol{\eta}).$$

Consequently the finitely many rational polynomial maps

$$\frac{1}{k}\mathcal{A}_\epsilon(\xi)^{-1}\mathcal{N}_{\delta_0}^{-1}\Psi_i(\boldsymbol{\eta}), \quad \epsilon = \pm 1, \quad 0 < \delta_0 \mid k^2\Delta, \quad (10.1)$$

lie on $F = m$ and cover every primitive integral point. More explicitly, writing $\mathcal{D}(Z, \pi, A)$ for the map of Lemma 7.2, each Ψ_i is a residue substitution into

$$\mathcal{N}_c S_{\mathbf{s}/(D_{Zc})} \mathcal{D}(Z_{k^2m}(\boldsymbol{\theta}), \pi_j(\mathbf{a}), A_j(\mathbf{a})),$$

where (π_j, A_j) ranges over the trace maps of Lemma 7.1 and $1 \leq c < P$. Thus the finite choices are ϵ, δ_0, c, j and the residue classes. All these maps have coefficient denominators independent of m . Apply Lemma 3.1 to (10.1), then the common content reduction, Lemma 3.3. $\square$

Proof of Theorem 1.3 in rank $n \geq 5$. Lemma 2.1 over $\mathbb{Q}$, followed by clearing denominators in the complementary basis, gives $Q(C(u, v, z)) = uv + q(z)$ with $C \in \mathrm{GL}_n(\mathbb{Q})$ and q integral, nondegenerate, of rank $n - 2$. Apply Theorem 10.1 on $C\mathbb{Z}^n$ and transfer to $\mathbb{Z}^n$ by Lemma 3.2. $\square$

Remark 10.2 (Parameters and number of families). Here $n \geq 5$ and $r = n - 2$. Theorems 7.4 and 9.3 give $(3r + 44) + (46 + 2r) = 5r + 90 = 5n + 80$ parameters per family for $m \neq 0$. At zero, the prime-coordinate construction saves one parameter and content reduction adds one. Residue substitutions, finite choices and lattice changes add none.

For fixed Q and $m \neq 0$, the number of families is at most

$$C_Q s(|m|), \quad s(a) = \#\{d \in \mathbb{Z}_{>0} : d^2 \mid a\},$$

for a computable constant C_Q . Indeed, Lemma 6.2 chooses D_Z uniformly in m , and all subsequent denominators and finite choices are fixed. Primes dividing m affect only prime avoidance. Thus the primitive construction uses a bounded number of residue substitutions, while content adds $s(|m|)$. A lattice change replaces m by $D^2 m$ and changes only the constant, since $s(D^2 a) \leq s(D^2) s(a)$. In particular the number is bounded uniformly for squarefree m . For every $\varepsilon > 0$ it is at most $C_{Q,\varepsilon} |m|^\varepsilon$: indeed, $s(a) \leq \prod_{\ell \mid a} (v_\ell(a) + 1)$, and $e + 1 \leq \ell^{\varepsilon e}$ for $e \geq 1$ and all sufficiently large primes ℓ ; the finitely many remaining primes contribute a bounded factor. The constant can be enormous: even the trace step permits P^{46} maps, before subsequent residue substitutions.

11 A worked example

Take $q(z) = z_1^2 + z_2^2 + z_3^2$, $m = -1$, $K = \mathbb{Q}(\sqrt{-3})$, and $\omega = (1 + \sqrt{-3})/2$. Choose $w = e_1, h = e_2$, so $k = 1$, $\Delta = 8$ and $P = 3 \nmid 2kq(h)\Delta$. The identity $q(1, \omega, \omega - 1) = 0$ gives the required isotropy. For the primitive point

$$x = (55, -2, -10, -3, 0), \quad \beta_x(X, Y) = 55X^2 - 20XY + 2Y^2,$$

the preparatory transformations can be identities. The binary form is primitive, positive definite, of discriminant -40 , and represents 7 at $(1, 4)$. Thus

$$\rho_{e_1}(\mathcal{U}(4))x = (7, -2, -2, -3, 0).$$

Put $Z = (\omega, \omega - 1, 0)$, $\zeta = (\omega - 1, -\omega, 0)$, and take C with columns $(Z + e_3)/2, (e_3 - Z)/2, \zeta$. Then $q(C(U, V, W)) = UV - W^2$, $\det C = -1/2$ and $C^{-1} \in M_3(\mathcal{O}_K)$. With $w_0 = 1, k_0 = -1$, Lemma 6.2 gives $Z_{-1}(0) = Z$, $D_Z = 2$ and exceptional set $\{2\}$. Choose

$$\pi = 2 + \omega, \quad A = \omega, \quad \alpha = -1 + 3\omega; \quad \text{Nm}(\pi) = 7, \quad \text{Nm}(A) = 1, \quad \text{Tr}(\alpha) = 1.$$

Modulo (π) , $\omega \equiv -2$, so $Z \equiv z_0 = (-2, -3, 0)$. Since $B(Z, \bar{Z}) = 4$, descent gives $(u, v, z') = (7, -6, 5, 4, 0)$. The correcting parameter $\mathbf{s} = D_Z(z_0 - z')/7 = (-2, -2, 0)$ yields

$$S_{\mathbf{s}/2}(7, -6, 5, 4, 0) = (7, -2, -2, -3, 0),$$

and $\rho_{e_1}(\mathcal{U}(-4))$ returns this point to x . Here zero parameters in Z_{-1} already give the required residue; in general its parameters must be chosen to match the target modulo $\mathfrak{p}$.

A norm factor greater than one can be unavoidable. Take $P = 59$, $p = 5$, and $\omega = (1 + \sqrt{-59})/2$. The polynomial $T^2 - T + 15$ splits modulo 5, so 5 splits in K . There is no element of norm 5, since

$$\text{Nm}(a + b\omega) = (a + b/2)^2 + 59b^2/4$$

exceeds 5 for $b \neq 0$ and is a square for $b = 0$. Nevertheless $\pi = \omega \in (5, \omega)$ has norm $15 = 3p$, and $A = 1$ gives $\text{Tr}(A\pi) = 1$. The final rescaling $\mathcal{N}_3$ sends $(15, v_0/3, z_0)$ to $(5, v_0, z_0)$.

12 Orbit constructions

The cases of rank at most four follow from known polynomial matrix families and finiteness of integral orbits. We also record the resulting Gaussian formulas and extend Vaserstein's two-plane construction to rational splittings and arbitrary lattices.

Let Q be a nondegenerate rational quadratic form on V , and let $L \subset V$ be a full lattice. Let $O(Q)$ denote the group of all isometries of Q , and write

$$\Omega_L = \{g \in O(Q)(\mathbb{Q}) : gL = L\}, \quad \Gamma_L = \{g \in SO(Q)(\mathbb{Q}) : gL = L\}.$$

Thus $[\Omega_L : \Gamma_L] \leq 2$; for $L = \mathbb{Z}^n$ we also write $\Gamma_L = SO(Q, \mathbb{Z})$.

Polynomial matrix families. For $SL_2(\mathbb{Z})$ use the 46-parameter map $\mathcal{V}$ in (3.1). For imaginary quadratic E , Larsen–Nguyen [23, Theorem 1.9] give a polynomial parametrization of $SL_2(\mathcal{O}_E)$; Appendix A makes the construction and parameter bounds explicit. For real quadratic E , Morgan–Rapinchuk–Sury give nine elementary factors [27, Theorem 1.1]; the corrected theorem of Jordan–Zaytman [21, Theorem 1.2] gives at most eight elementary factors, starting with a lower triangular factor. Combining consecutive factors of the same type and padding with zero parameters gives the surjective map

$$\mathcal{L}(t_1)\mathcal{U}(t_2)\mathcal{L}(t_3)\mathcal{U}(t_4)\mathcal{L}(t_5)\mathcal{U}(t_6)\mathcal{L}(t_7)\mathcal{U}(t_8), \quad t_j \in \mathcal{O}_E. \quad (12.1)$$

An integral basis converts its eight ring parameters into 16 integer parameters. Here $\mathcal{U}, \mathcal{L}$ are the elementary matrices of Lemma 6.1.

12.A Finiteness and transfer of orbits

Lemma 12.1 (Orbit finiteness). *Let Q be nondegenerate and L a full lattice in its rational quadratic space. Every nonzero rational level on L , and the set of primitive isotropic vectors in L , consists of finitely many Γ_L -orbits. The same holds for every subgroup of finite index in Γ_L .*

Proof. After scaling Q and the prescribed level together, assume Q is integral on L . The effective reduction in Lemma B.1 gives finitely many Gram matrices for lattice bases beginning with a primitive vector of a prescribed value. Equal Gram matrices give vectors in the same Ω_L -orbit. At a nonzero level m , only contents c with $c^2 \mid m$ occur. Finally, passing from Ω_L to Γ_L , or to a subgroup of finite index, splits each orbit into finitely many orbits. For nonzero levels, existence also follows from [2, Theorem 6.9]. $\square$

An arithmetic subgroup is one commensurable with the integral points in a faithful rational matrix representation; commensurability means that the intersection has finite index in both groups. Surjectivity of algebraic groups is understood over an algebraic closure of $\mathbb{Q}$, and need not imply surjectivity on rational points.

Lemma 12.2 (Arithmetic images). *Let $\varphi : \mathcal{G} \rightarrow SO(Q)$ be a surjective homomorphism of algebraic groups over $\mathbb{Q}$. If $\Lambda \subset \mathcal{G}(\mathbb{Q})$ is arithmetic and $\varphi(\Lambda) \subseteq \Gamma_L$, then $\varphi(\Lambda)$ has finite index in Γ_L .*

Proof. The arithmetic-image theorem [29, Theorem 4.1, pp. 174, 204] makes $\varphi(\Lambda)$ arithmetic. It is therefore commensurable with the arithmetic lattice stabilizer Γ_L ; the inclusion gives finite index. $\square$

Lemma 12.3 (From matrix families to level sets). *Suppose Q is integral on L and a subgroup of finite index in Γ_L is a finite union of integer-coefficient matrix families in a basis of L . Then every integral level on L is a finite union of polynomial families.*

Proof. Apply the matrix families to representatives from Lemma 12.1, using primitive representatives at zero. Lemma 3.3 completes the zero level with one additional scalar parameter. $\square$

12.B Ranks at most four

Proposition 12.4. *Theorem 1.3 holds in ranks at most four.*

Proof. A nondegenerate rank-one form is anisotropic. By hyperbolic splitting (Lemma 2.1) and lattice transfer (Lemma 3.2), rationally similar integral models suffice. In rank two the model is UV : nonzero levels give finitely many divisor pairs, and the zero level is the union of the axes.

In rank three the model is $UV - Z^2 = \det \begin{pmatrix} U & Z \\ Z & V \end{pmatrix}$. Its zero level is $(U, V, Z) = (sa^2, sb^2, sab)$ [34, Example 5]. For $m \neq 0$, classical binary reduction [34, Example 7, p. 983] gives representatives $\mathbf{X} = \begin{pmatrix} a & b \\ b & c \end{pmatrix}$ with

$$0 < 3a^2 \leq 4|m|, \quad |b| \leq |a|/2, \quad c = (m + b^2)/a \in \mathbb{Z},$$

or $a = c = 0$ and $b^2 = -m$. When $-m$ is a square, first use a primitive isotropic vector to obtain $\begin{pmatrix} 0 & b \\ b & c \end{pmatrix}$, with $|c| \leq |b|$. If $c \neq 0$, move it to the first diagonal entry and reduce the off-diagonal entry modulo c ; this gives the first case. Thus the list is finite, computable, and covers this case too. The maps $\mathcal{V}(\mathbf{t})\mathbf{X}\mathcal{V}(\mathbf{t})^\top$ therefore exhaust the level, using 46 parameters each.

In split rank four the model is the determinant on $M_2(\mathbb{Z})$. For $m \neq 0$, determinant-one row operations give the finite list

$$H_{d,b} = \begin{pmatrix} d & b \\ 0 & m/d \end{pmatrix}, \quad d \mid |m|, \quad d > 0, \quad 0 \leq b < |m/d|.$$

Hence $\mathcal{V}(\mathbf{t})H_{d,b}$ gives 46 parameters per family, as in the orbit method of [34, Example 8]. At zero, every integer matrix of rank at most one is an outer product $\begin{pmatrix} a \\ b \end{pmatrix} \begin{pmatrix} c & d \end{pmatrix}$, giving four parameters; see also [12].

In rank four of Witt index one, write the rational form as $uv + ax^2 + by^2$. Then $\delta = -ab$ is not a square. Replace Q, m by $-aQ, -am$ and set $U = -au, V = v, X = ax, Y = y$, giving

$$UV - X^2 + \delta Y^2 = \det \begin{pmatrix} U & X + Y\sqrt{\delta} \\ X - Y\sqrt{\delta} & V \end{pmatrix}.$$

Put $E = \mathbb{Q}(\sqrt{\delta})$ and use the Hermitian lattice

$$L_E = \left\{ \begin{pmatrix} U & w \\ \bar{w} & V \end{pmatrix} : U, V \in \mathbb{Z}, w \in \mathcal{O}_E \right\}, \quad q_E(\mathbf{X}) = \det \mathbf{X},$$

where the bar is quadratic conjugation, also for real E . The action $\mathbf{X} \mapsto g\mathbf{X}\bar{g}^\top$ of $\mathrm{SL}_2(\mathcal{O}_E)$ preserves L_E and is polynomial over $\mathbb{Z}$ in an integral basis of $\mathcal{O}_E$. Writing entries over E in a rational basis defines the restriction-of-scalars group $\mathrm{Res}_{E/\mathbb{Q}} \mathrm{SL}_2$, whose rational points are $\mathrm{SL}_2(E)$. The action induces a surjective homomorphism

$$\varphi : \mathrm{Res}_{E/\mathbb{Q}} \mathrm{SL}_2 \longrightarrow \mathrm{SO}(q_E)$$

with kernel $\{I, -I\}$ [22, Chapter 6, Theorem 7, and Chapter 9, pp. 80–81]. Over an algebraic closure it becomes the action $(g, h) : \mathbf{X} \mapsto g\mathbf{X}h^\top$ on M_2 ; its kernel is the diagonal $\{I, -I\}$, and both groups are connected of dimension six, so the action is surjective. Lemma 12.2 shows that $\Gamma'_E = \varphi(\mathrm{SL}_2(\mathcal{O}_E))$ has finite index in Γ_{L_E} . Composing the polynomial group maps above with this action and applying Lemma 12.3 proves the claim on L_E . Lemma 3.2 transfers it to the original lattice. $\square$

Together, Section 10 and Proposition 12.4 prove the existence assertion in Theorem 1.3; Proposition 13.6 supplies computability.

12.C The equations $zt - x^2 - y^2 = \pm 1$

The Hermitian method already appears in Frisch–Vaserstein [11, Proposition 1], which gives a five-parameter family for $zt = x^2 + y^2$. For the two nonzero levels we use the classical Hermitian action [6, Chapter 9] and the following explicit orbit reduction.

Proof of Proposition 1.5. Put $R = \mathbb{Z}[i]$ and $g^* = \bar{g}^\top$. Associate (x, y, z, t) with

$$\mathbf{X} = \begin{pmatrix} z & w \\ \bar{w} & t \end{pmatrix}, \quad w = x + iy, \quad R_{u,\eta} = \begin{pmatrix} 0 & u \\ \bar{u} & \eta \end{pmatrix}.$$

Writing $a = a_1 + ia_2$ and similarly for b, c, d , the constraints (1.6) say that $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(R)$. Direct multiplication identifies (1.7) with $\sigma g g^*$ and (1.8) with $g R_{e+if,\eta} g^*$. Their determinants are 1 and -1 . The actions $\mathbf{X} \mapsto g \mathbf{X} g^*$ and $\mathbf{X} \mapsto g^* \mathbf{X} g$ have the same orbits.

Level 1. The form $v \mapsto v^* \mathbf{X} v$ is definite. In the positive case choose a Gaussian integer vector of least positive value z . Its coordinates have Gaussian gcd 1, so it extends to a determinant-one basis. Subtracting a Gaussian multiple of its first vector from the second makes $|w| \leq z/\sqrt{2}$. Minimality gives $t \geq z$, so $1 = zt - |w|^2 \geq z^2/2$. Thus $z = 1$, $w = 0$, $t = 1$. Changing sign handles the negative case: there are exactly two orbits, represented by I and $-I$.

Level -1 . If $z \neq 0$, the identity

$$z(v^* \mathbf{X} v) = |zv_1 + wv_2|^2 - |v_2|^2$$

makes $(1 - w, z)^\top$ isotropic; if $z = 0$, use $(1, 0)^\top$. Dividing by a Gaussian gcd and completing to a determinant-one basis gives $R_{u,t}$ with $u \in R^\times$. Adding λ times the first basis vector to the second changes t by $2\mathrm{Re}(\bar{\lambda}u)$, an arbitrary even integer. A diagonal unit change changes u by a sign. Thus the representatives are $R_{u,\eta}$ with $u \in \{1, i\}$ and $\eta \in \{0, 1\}$. Since

$$\mathcal{U}(i-1)R_{1,1}\mathcal{U}(i-1)^* = R_{i,1},$$

three suffice. They are inequivalent: $R_{1,1}$ represents 1, whereas $R_{1,0}$ and $R_{i,0}$ represent only even integers; and the upper-right entry of $gR_{1,0}g^*$ satisfies $a\bar{d} + b\bar{c} \equiv ad + bc \equiv 1 \pmod{2R}$, so cannot equal i . This proves both explicit descriptions.

Finally compose these orbit maps with a single polynomial parametrization of $\mathrm{SL}_2(R)$ from [23, Theorem 1.9], expanding each Gaussian parameter in the basis $1, i$. This gives exactly two and three integer-coefficient polynomial families, respectively. $\square$

Two families are necessary at level 1. A polynomial map whose integer values lie on this level satisfies the defining equation identically, hence also over $\mathbb{R}$. Its first diagonal coordinate z never vanishes, since $zt = 1 + x^2 + y^2 > 0$, so its sign is constant on the connected parameter space $\mathbb{R}^N$. One family cannot therefore contain integer points with both signs of z .

For $E = \mathbb{Q}(i)$, the discriminant has one prime divisor, so Corollary A.4 gives 13 440 integer parameters for each of these two or three families. Using instead Proposition A.1 gives a larger finite union with at most 2800 parameters per family. These bounds are not optimized; they are much larger than the five parameters at level zero in [11, Proposition 1].

12.D Two rational hyperbolic planes

The following complement improves the parameter bounds when two hyperbolic planes are available. For the integral shape $x_1x_2 + x_3x_4 + q_0$, the finite-union assertion is already discussed after [34, Corollary 4]. The following argument extends it to forms splitting two planes only over $\mathbb{Q}$ and to arbitrary lattices. A vector $x \in L$ is Q -unimodular if $B_Q(x, L) = \mathbb{Z}$.

Proposition 12.5. *Let Q be a nondegenerate integral quadratic form in n variables of rational Witt index at least two. Every $X_m(Q)$ is a finite union of polynomial families with at most $3n + 80$ parameters each for $m \neq 0$, and $3n + 81$ for $m = 0$. If the Witt index is at least three, the bounds improve to $3n - 6$ and $3n - 5$, respectively.*

Proof. By Lemmas 2.1 and 3.2, use the integral model $Q = x_1x_2 + x_3x_4 + q_0$; when available, split the third plane from q_0 as well. Put $\Gamma = \text{SO}(Q, \mathbb{Z})$ and $y = (1, m, 0, \dots, 0)$. This vector is Q -unimodular. Vaserstein gives a polynomial map Φ onto all Q -unimodular vectors of value m , with $3n + 80$ parameters [34, Corollary 4], or $3n - 6$ with three planes [34, Proposition 3.4, p. 997].

Take finitely many Γ -orbit representatives x_i , using only primitive vectors if $m = 0$. Witt's extension theorem [30, Chapter IV, §1.5, Theorem 3] gives rational isometries $g_ix_i = y$. Choose $M_i \geq 1$ such that M_ig_i and $M_ig_i^{-1}$ are integral, and put $\Gamma_i = \{\gamma \in \Gamma : \gamma \equiv I \pmod{M_i^2}\}$. This subgroup has finite index, and

$$g_i(I + M_i^2 A)g_i^{-1} = I + (M_ig_i)A(M_ig_i^{-1})$$

shows that $g_i\Gamma_i g_i^{-1} \subseteq \Gamma$. Choose left coset representatives γ_{ij} . For $h \in \Gamma_i$, the vector $g_i h x_i = (g_i h g_i^{-1})y$ is integral and Q -unimodular, so it is a value of Φ . Consequently the rational polynomial map $\gamma_{ij}g_i^{-1}\Phi$ contains $\gamma_{ij}\Gamma_i x_i$ in its image and always has value m under Q . Lemma 3.1 extracts its integral values without adding parameters. These maps exhaust the nonzero level; at zero, Lemma 3.3 adds one scalar parameter. Lattice transfer preserves the bounds.

All choices are effective. Take the $\Omega_{\mathbb{Z}^n}$ -representatives from Appendix B and, if necessary, their images under a determinant- -1 generator to obtain the x_i . Generators of the integral isometry groups are computable [18]. Enumeration of rational isometries finds the g_i , and the finite images of Γ modulo M_i^2 give the representatives γ_{ij} . $\square$

For forms of rank at least five and Witt index at least two, Erovenko–Rapinchuk show that the integral special orthogonal groups are products of finitely many cyclic subgroups [7, Main Theorem]; their Witt-index-one case requires an additional finite place. Rational Witt index one occurs in every rank at least two, as $uv + z_1^2 + \dots + z_{n-2}^2$ shows. The descent of Sections 5–10 treats all such forms of rank at least five.

13 Classification and constructive algorithms

The following leading-term obstruction extends the observation in [26, §1] and Vaserstein's Pell-equation example [34, Example 9].

Lemma 13.1 (Anisotropic quadratic parts). *Let q be a rational quadratic form in r variables anisotropic over $\mathbb{Q}$, let ℓ be a rational linear form, and let $d \in \mathbb{Q}$. For $N \geq 0$, every polynomial map $\Phi \in \mathbb{Q}[t_1, \dots, t_N]^r$ satisfying $q(\Phi) + \ell(\Phi) + d = 0$ on $\mathbb{Z}^N$ is constant.*

Proof. The equality is a polynomial identity. If $e = \max_i \deg \Phi_i > 0$, its degree- $2e$ part is $q(H) = 0$, where H is the nonzero degree- e homogeneous part of Φ . Choose an integer tuple t with $H(t) \neq 0$. Then $q(H(t)) = 0$, contradicting anisotropy. $\square$

Lemma 13.2 (Anisotropic indefinite levels in a congruence class). *Let q be an integral quadratic form anisotropic over $\mathbb{Q}$ and indefinite over $\mathbb{R}$. For integers $m_0 \neq 0$, $D_0 \geq 1$ and $\eta \in \mathbb{Z}^r$, the set $\{x \in \mathbb{Z}^r : q(x) = m_0, x \equiv \eta \pmod{D_0}\}$ is empty or infinite.*

Proof. Take a point x_0 in this set. By the real signature of q , the orthogonal complement of x_0 contains a real vector on which q has sign opposite to m_0 . Rational approximation in this

rational subspace, followed by clearing denominators, gives $w \in \mathbb{Z}^r$ with $B_q(x_0, w) = 0$ and $m_0 q(w) < 0$. The positive integer $N_0 = -m_0 q(w)$ is nonsquare, since $N_0 = d^2$ would make $dx_0 + m_0 w$ a nonzero rational zero of q . By the Pell theorem [24, pp. 182–183], choose a unit $\lambda = a + c\sqrt{N_0} > 1$ of norm 1 in $\mathbb{Z}[\sqrt{N_0}]$. Taking a positive power makes $\lambda \equiv 1 \pmod{D_0}$ in this ring, since its reduction is a unit in a finite ring. Write $\lambda^j = a_j + c_j\sqrt{N_0}$. Then

$$x_j = a_j x_0 + m_0 c_j w, \quad q(x_j) = m_0(a_j^2 - N_0 c_j^2) = m_0, \quad x_j \equiv \eta \pmod{D_0}.$$

These vectors are distinct because x_0, w are independent and the positive powers of λ are distinct. $\square$

13.A The classification

Theorem 13.3 (Quadratic polynomials). *Let $f = Q + \ell + c \in \mathbb{Z}[x_1, \dots, x_n]$ have degree at most two, with Q homogeneous quadratic and ℓ linear. If $Q = 0$, its integer zero set is a finite union of polynomial families. Otherwise choose an integer basis whose last s vectors span $\text{Rad}(Q) \cap \mathbb{Z}^n$, and write*

$$f(y, z) = g(y) + a \cdot z, \quad g(y) = q(y) + b \cdot y + c, \quad (y, z) \in \mathbb{Z}^r \times \mathbb{Z}^s, \quad (13.1)$$

where q is nondegenerate, $a \in \mathbb{Z}^s$, $b \in \mathbb{Z}^r$ and $r + s = n$. Put $Y = \{y \in \mathbb{Z}^r : g(y) = 0\}$. Then the integer zero set of f is a finite union of polynomial families if and only if

$$a \neq 0, \quad \text{or} \quad q \text{ is isotropic over } \mathbb{Q}, \quad \text{or} \quad Y \text{ is finite.}$$

The first condition means that ℓ is nonzero on the radical; when it fails, the other two conditions are independent of the adapted basis.

Proof. For $Q = 0$, integer linear algebra gives either the empty set or one affine integer family, including the constant-polynomial cases. For $Q \neq 0$, integer row and column reduction gives the adapted basis in (13.1).

If $a \neq 0$, change the z -basis so that $a \cdot z = g_0 z_1$, with $g_0 > 0$ the gcd of its entries. For each residue vector $\eta \in \{0, \dots, g_0 - 1\}^r$ satisfying $g(\eta) \equiv 0 \pmod{g_0}$, use unrestricted integer parameters t and $\mathbf{s}$ in

$$y = \eta + g_0 t, \quad z_1 = -g(\eta + g_0 t)/g_0, \quad (z_2, \dots, z_s) = \mathbf{s}.$$

These have integer coefficients and exhaust the solutions.

Suppose $a = 0$. Completing the square gives $g(y) = q(y + \zeta) - c_0$, where $\zeta = G_q^{-1}b$ and $c_0 = q(\zeta) - c$. Choose $D_\zeta \geq 1$ with $D_\zeta \zeta \in \mathbb{Z}^r$. Then $u = D_\zeta(y + \zeta)$ identifies Y with

$$\{u \in \mathbb{Z}^r : q(u) = m_0, \quad u \equiv D_\zeta \zeta \pmod{D_\zeta}\}, \quad m_0 = D_\zeta^2 c_0 \in \mathbb{Z}. \quad (13.2)$$

For isotropic q , apply Theorem 1.3 and Lemma 3.1. The residue substitutions make the coefficients of $u - D_\zeta \zeta$ divisible by D_ζ , so returning to y and adjoining the free z -coordinates gives the required integer-coefficient families. For anisotropic q , Lemma 13.1 makes the y -coordinates of every family constant. Hence a finite union exists exactly when Y is finite; use $\{y_0\} \times \mathbb{Z}^s$ for each $y_0 \in Y$. $\square$

Remark 13.4 (Degenerate forms). Isotropy supplied by the radical is insufficient: $Q(x, y, z) = x^2 - 2y^2$ is isotropic, but $X_1(Q)$ is the product of an infinite Pell level with $\mathbb{Z}$, so Lemma 13.1 excludes a finite polynomial cover. This qualifies the announcement in [34, p. 982] if it is read as including degenerate forms.

Remark 13.5 (The introductory example). The form $y^2 + z^2 - 3x^2$ is anisotropic: a primitive integer zero would satisfy $3 \mid y, z$ by reduction modulo 3, and the equation would then force $3 \mid x$. However,

$$(x, y, 0) \mapsto (7x + 4y + 2, 12x + 7y + 3, 0)$$

preserves (1.2) and, starting at zero, produces infinitely many solutions with strictly increasing first coordinate. Lemma 13.1 therefore rules out a finite polynomial cover of (1.2).

13.B Decision and construction

Decision part of Theorem 1.4. Compute the data of Theorem 13.3. The answer is affirmative if $Q = 0$, $a \neq 0$, or q is isotropic. To decide isotropy, diagonalize over $\mathbb{Q}$ and multiply by a common denominator to obtain a form $\sum_{i=1}^r a_i X_i^2$, with $a_i \in \mathbb{Z} \setminus \{0\}$. Rank one is anisotropic; in rank two test whether $-a_1/a_2$ is a rational square. In ranks three and four, it suffices to test indefiniteness and local isotropy at the finitely many primes $p \mid 2 \prod_i a_i$; the explicit local criteria use only finite arithmetic with valuations and residue classes. In ranks at least five, Meyer's theorem reduces the test to indefiniteness. See [30, Chapter II, §3; Chapter III, §1.2; Chapter IV, Theorems 6 and 8].

It remains to decide finiteness of Y for anisotropic q and $a = 0$. In (13.2), $m_0 = 0$ gives at most the point $y = -\zeta$. A definite form gives a bounded, hence finite, set. Otherwise $m_0 \neq 0$ and q is indefinite. Apply Grunewald–Segal's decision procedure for a single quadratic equation [19] to $g(y) = 0$. An empty set gives an affirmative answer; a nonempty set is infinite by Lemma 13.2, giving a negative answer. $\square$

Proposition 13.6 (Effective construction for isotropic forms). *Given a nondegenerate isotropic integral quadratic form Q and $m \in \mathbb{Z}$, one can compute the polynomial families in Theorem 1.3.*

Proof. Once isotropy is known, enumerating integer vectors finds a rational isotropic vector; Lemma 2.1 then computes a hyperbolic splitting. In rank at least five, make the sign choice in Theorem 10.1, so the complementary form q , in r variables, has positive index at least two, and find the orthogonal integral vectors w, h by rational search. To find the field in Lemma 5.1, at stage B test the first B primes $P \equiv 3 \pmod{8}$ outside its prescribed finite exceptional set and all nonzero vectors $u + v\sqrt{-P}$ with $u, v \in \{-B, \dots, B\}^r$. That lemma guarantees termination. Compute the splitting over $K = \mathbb{Q}(\sqrt{-P})$ by Lemma 2.1. The descent maps now follow by polynomial arithmetic, using [34, §1, Proposition 1.5] and every norm factor $1 \leq c < P$. Formula (10.1), divisor lists and residue substitutions are therefore computable; the varying primes in the coverage proof need not be found.

The rank-two, rank-three and split rank-four constructions are already explicit. In nonsplit rank four, compute an integral basis of $\mathcal{O}_E$ and use (12.1) for real E , or Corollary A.4 or Proposition A.1 for imaginary E . Compose these group maps with the Hermitian action and the finite orbit lists computed in Appendix B. Apply content reduction and lattice transfer (Lemmas 3.3 and 3.2); their residue substitutions are effective. $\square$

Construction part of Theorem 1.4. The affine and radical constructions are explicit, and Proposition 13.6 handles isotropic q . For anisotropic q , only finite Y need be listed. The empty and zero-level cases are immediate. In the definite case, replace (q, m_0) by $(-q, -m_0)$ if needed so that G_q is positive definite. For $m_0 > 0$, Cauchy–Schwarz gives $u_i^2 \leq 2m_0(G_q^{-1})_{ii}$; enumerate this finite box and test (13.2). For $m_0 < 0$ there are no solutions. Return to y , use the affine families $\{y_0\} \times \mathbb{Z}^s$, and undo the integer basis changes. All output coefficients are integers. $\square$

A Effective polynomial parametrizations of groups

Larsen–Nguyen prove polynomial parametrizability of $\mathrm{SL}_2(\mathcal{O}_E)$ for imaginary quadratic E [23, Theorem 1.9]; their Remark 1.10 suggests extracting a parameter bound. We give an explicit recipe and count the moves in their proof. The group map $\mathcal{V}$ in (3.1) is obtained from the explicit construction in [34, §1, Proposition 1.5].

The auxiliary polynomial matrix

With $\mathcal{U}, \mathcal{L}$ as in Lemma 6.1, put

$$J = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \Xi(x, y) = \begin{pmatrix} 1 - xy & x^2 \\ -y^2 & 1 + xy \end{pmatrix}.$$

Set $\mathcal{W}_4(\mathbf{x}) = \Xi(x_2, x_4)\Xi(x_1, x_3)\Xi(x_2, x_4)J$. This is Vaserstein’s Φ_4 [34, p. 989], with $\mathcal{W}_4(1, 0, 0, 1) = I$. Substitute $\mathbf{x} = (1 + z_5 z_1, z_5 z_2, z_5 z_3, 1 + z_5 z_4)$, write the resulting entries as w_{ij} , and set

$$\mathcal{H}(\mathbf{z}) = \begin{pmatrix} w_{11} & z_5 w_{12} \\ w_{21}/z_5 & w_{22} \end{pmatrix}.$$

Since w_{21} vanishes at $z_5 = 0$, the division is exact in $\mathbb{Z}[\mathbf{z}]$. Thus $\mathcal{H} \in \mathrm{SL}_2(\mathbb{Z}[\mathbf{z}])$ and $\mathcal{H}(0) = I$.

Proposition A.1. *Given an integral basis of $R = \mathcal{O}_E$ for an imaginary quadratic field E , one can compute finitely many polynomial maps whose images exhaust $\mathrm{SL}_2(R)$ in integer basis coordinates. Each map uses at most $10(216\nu + 64)$ integer parameters, where ν is the number of distinct prime divisors of $\mathrm{disc}(E)$.*

A row $(a, b) \in R^2$ is primitive if $aR + bR = R$. Write $\mu = |R^\times|$ and, for $x \neq 0$, let $e(x)$ be the exponent of $(R/xR)^\times$, with $e(x) = 1$ for a unit. We use the following precise arithmetic inputs.

Lemma A.2 (Carter–Keller). *Suppose aR, bR are nonzero coprime prime ideals and the residue characteristic of bR does not divide μ . For each rational prime p_0 ramified in E , there are $c \neq 0$ and $\gamma \geq 1$ such that*

$$bc \equiv -1 \pmod{aR}, \quad \gcd(e(b), e(c)) = \mu\gamma,$$

every prime divisor of γ ramifies in E , and $p_0 \nmid \gamma$.

Proof. This is [23, Lemma 1.6], with ideal aR and unit -1 . The prime-ideal hypothesis also matches the printed statement of [3, Lemma 4]; the extension discussed in [23, Remark 1.7] is unnecessary here. $\square$

For the initial prime-power step, we use the following specialization of Morgan–Rapinchuk–Sury in place of [3, Lemma 3], the input used in the proof of [23, Theorem 1.9].

Lemma A.3 (Morgan–Rapinchuk–Sury). *If $(s, t) \in R^2$ is primitive, $s \neq 0$, and $sR + \mu R = R$, then at most three elementary operations take it to (a', π^μ) , where $a' \neq 0$ and πR is prime.*

Proof. In [27, Lemma 4.4], take S to consist of the archimedean places, write $s = \alpha r^\mu$ with $\alpha = s, r = 1$, and choose the exponent $m = 1$. The condition on the primes dividing α is $sR + \mu R = R$; the required congruence $m \equiv 1 \pmod{|(R/a'R)^\times|}$ is automatic. That lemma does not require infinitely many units. Primitivity and the nonunit π^μ imply $a' \neq 0$. $\square$

Proof of Proposition A.1. Use words in the nine polynomial matrix types

$$\mathcal{A} = \{\mathcal{U}(t), \mathcal{L}(t), J, J^{-1}, -I, \mathcal{H}(\mathbf{z}), \mathcal{H}(\mathbf{z})^{-1}, \mathcal{H}(\mathbf{z})^\top, \mathcal{H}(\mathbf{z})^{-\top}\},$$

with independent variables at each occurrence. This alphabet is closed under inverse and transpose, up to parameter changes. Compare matrices at cost c if $N = XMY$ with $|X| + |Y| \leq c$, where $|X|$ denotes word length. For primitive rows, the comparison is required for every pair of determinant-one completions. Completions of the same row differ by one left $\mathcal{L}$ factor. Thus each elementary operation, simultaneous sign change, or move $(a, b) \mapsto (b, -a)$ costs at most two. Costs add, and comparison with a word of length d gives a word of length at most $c + d$.

The polynomial moves of [23, Propositions 1.3–1.5] have the following costs in this alphabet:

Comparison of primitive rows	Cost	Source
$(1 + ab, b^2c) \longleftrightarrow (1 + ab, c)$	5	Proposition 1.3
$(1 + ab, bc) \longleftrightarrow (1 + ab, c)$	23	Proposition 1.4
$\text{row}_1(A^n) \longleftrightarrow (a^n, b)$	52	Proposition 1.5

In the last row, $A \in \text{SL}_2(R)$ has first row (a, b) and $n \geq 0$. We justify the numerical costs and the explicit witnesses.

For the square-factor move choose d, e with $(1 + ab)e - bcd = -a$ and put

$$A_0 = \begin{pmatrix} 1 + ab & b^2c \\ d & 1 + be \end{pmatrix}, \quad B_0 = \begin{pmatrix} 1 + ab & c \\ b^2d & 1 + be \end{pmatrix}.$$

Both have determinant one, and direct multiplication gives $A_0 B_0^\top = \mathcal{H}(a, c, d, e, b)$ and $B_0 = \mathcal{H}(a, c, d, e, b)^\top J A_0 J^{-1}$. These identities hold also for $b = 0$. Three letters and the two completion changes give cost five.

For the factor move

$$(1 + ab, bc) \longleftrightarrow (1 + ab, c), \tag{A.1}$$

use the prime choices and reciprocity argument of [23, Proposition 1.4]. Its replacements $c \mapsto c + (1 + ab)d$, $a \mapsto a + ce$, $c \mapsto c + (1 + ab)f$ use one elementary operation on each row, six in total, and arrange $a \equiv -r^2 \pmod{c}$. The final chain is

$$\begin{aligned} (1 + ab, bc) &\longleftrightarrow (1 - r^2b, bc) \longleftrightarrow (1 - r^2b, r^2b^2c) \\ &\longleftrightarrow (1 - r^2b, c) \longleftrightarrow (1 + ab, c). \end{aligned}$$

It uses three elementary operations and the square-factor move with parameters $(-r, rb, c)$, for total cost $9 \cdot 2 + 5 = 23$. If $abc(1 + ab) = 0$, the rows either coincide or each reaches $(1, 0)$ in at most two elementary operations, so the same bound holds.

For the power move, the proof of [23, Proposition 1.5] uses two factor moves, two sign changes, and one elementary operation, giving $2 \cdot 23 + 2 \cdot 2 + 2 = 52$. To make its factorizations explicit, set $\psi_{-1} = -1$, $\psi_0 = 0$, $\psi_{j+1} = T\psi_j - \psi_{j-1}$. For $n \geq 1$, the following pairs $(r, s) \in \mathbb{Z}[T]^2$ satisfy $\psi_n = rs$, $r \mid \psi_{n-1} - 1$, $s \mid \psi_{n-1} + 1$:

n	r	s
$2j$	$\psi_{j+1} - \psi_{j-1}$	ψ_j
$2j + 1$	$\psi_{j+1} - \psi_j$	$\psi_{j+1} + \psi_j$.

These identities follow from the recurrence before evaluation in R . Since $A^n = \psi_n(\text{tr } A)A - \psi_{n-1}(\text{tr } A)I$, its first row (a_n, b_n) has $b_n = brs$, $a_n \equiv -1 \pmod{r}$, $a_n \equiv 1 \pmod{s}$, after evaluating at $T = \text{tr } A$. Remove s , change sign, remove r , and change sign back; then $a_n \equiv a^n \pmod{b}$ gives the final elementary operation. Vanishing evaluated factors are covered by the degenerate cases of (A.1); no division in R is needed. The case $n = 0$ is immediate.

Arithmetic reduction. We first bound completions of primitive rows (a^μ, b) with aR prime. By [27, Theorem 3.3], a move $b \mapsto b + a^\mu t$ of cost two makes bR prime with residue characteristic prime to μ . Write the ramified rational primes as $p_1, \dots, p_\nu$. Lemma A.2 gives c_i, γ_i with

$$bc_i \equiv -1 \pmod{a}, \quad \gcd(e(b), e(c_i)) = \mu\gamma_i, \quad p_i \nmid \gamma_i.$$

Every prime divisor of γ_i is among the p_j , so $\gcd(\gamma_1, \dots, \gamma_\nu) = 1$. Choose $\sum_i h_i \gamma_i = 1$, a completion M of (a, b) , and put

$$N_i = \begin{pmatrix} a & b \\ c_i & (1 + bc_i)/a \end{pmatrix}.$$

For $h_i \neq 0$, choose positive s_i, t_i with $t_i - s_i = \lambda_i := \mu|h_i|\gamma_i$, $e(c_i) \mid s_i$ and $e(b) \mid t_i$; the gcd condition permits this. The rows (a^{t_i}, b) and (a^{s_i}, c_i) each reach $(1, 0)$ in two elementary operations. The power comparison applied to N_i and $N_i^\top$ makes $N_i^{t_i}$ and $(N_i^\top)^{s_i}$ words of length at most $52 + 4 = 56$. Hence $N_i^{\lambda_i}$ has length at most 112. Two power comparisons, through the common row (a^{λ_i}, b) , transfer this to M^{λ_i} at cost 104. Inversion handles negative h_i . Consequently

$$M^\mu = \prod_{i=1}^{\nu} M^{\mu h_i \gamma_i}$$

has length at most 216ν . One final power comparison and the initial prime-producing move give $216\nu + 54$ for every completion of (a^μ, b) . The same bound holds for $a = 0$ or $a \in R^\times$, where at most two elementary operations reduce the row to $(1, 0)$.

For an arbitrary primitive row with nonzero coordinates, one elementary operation makes its first coordinate nonzero and coprime to μR , by the Chinese remainder theorem. Apply Lemma A.3 and then multiply by J to obtain $(\pi^\mu, -a')$. These four elementary operations and the move by J cost at most ten. Zero-coordinate cases take at most three elementary operations. Thus every matrix in $\mathrm{SL}_2(R)$ is a word of length at most $\ell_E = 216\nu + 64$.

The output algorithm simply enumerates all words of length at most ℓ_E in $\mathcal{A}$, including the empty word, with independent variables. Each letter has at most five ring parameters. Expanding them in the given integral basis gives at most $10\ell_E$ integer parameters and integer coefficients. Surjectivity was proved above; none of its auxiliary arithmetic choices is needed to compute the maps. $\square$

Corollary A.4. *One can compute a single polynomial parametrization of $\mathrm{SL}_2(R)$ with $48(216\nu + 64)$ integer parameters.*

Proof. Use independent parameters in the block

$$\mathcal{P} = \mathcal{U}(t_1)\mathcal{L}(t_2)\mathcal{U}(t_3)\mathcal{L}(t_4)\mathcal{H}(\mathbf{z}_1)\mathcal{H}(\mathbf{z}_2)^{-1}\mathcal{H}(\mathbf{z}_3)^\top\mathcal{H}(\mathbf{z}_4)^{-\top}.$$

Its 24 ring parameters give a polynomial matrix whose image contains I and every letter of $\mathcal{A}$: all factors take the value I , and the first four factors contain

$$\begin{aligned} J &= \mathcal{U}(-1)\mathcal{L}(1)\mathcal{U}(-1), & J^{-1} &= \mathcal{U}(1)\mathcal{L}(-1)\mathcal{U}(1), \\ -I &= \mathcal{U}(1)\mathcal{L}(-2)\mathcal{U}(1)\mathcal{L}(-2). \end{aligned}$$

A product of ℓ_E independent copies of $\mathcal{P}$ contains every word of length at most ℓ_E , so is surjective. Expanding its ring parameters gives $48\ell_E$ integer parameters. $\square$

Table 1: Upper bounds on integer parameters per family; n is the rank. Here $\ell_E = 216\nu + 64$, where ν counts the distinct prime divisors of $\text{disc}(E)$ for the quadratic field E in the four-variable construction. Take the minimum over applicable rows. The bounds are not optimized.

Case	$m \neq 0$	$m = 0$	Construction
Rank 2	0	1	Divisor pairs and axes
Rank 3	46	3	Vaserstein's models
Split rank 4	46	4	Row reduction
Rank 4, real quadratic E	16	17	Eight-factor word [21]
Rank 4, imaginary quadratic E	$10\ell_E$	$10\ell_E + 1$	Appendix A
Rank $n \geq 5$	$5n + 80$	$5n + 80$	Uniform descent
Witt index at least 2	$3n + 80$	$3n + 81$	Proposition 12.5
Witt index at least 3	$3n - 6$	$3n - 5$	Proposition 12.5

B Effective reduction and orbit representatives

We give a short constructive form of classical integral reduction that keeps a prescribed primitive first vector. It supplies the finite candidate list for the orbit algorithm below and applies to definite and indefinite forms alike. Integral congruence means $G \mapsto U^\top G U$ with $U \in \text{GL}_n(\mathbb{Z})$.

Lemma B.1 (Gram matrices with a prescribed first vector). *Given integers $n \geq 1$, $\mathfrak{d} \neq 0$ and a , one can compute a finite set $\mathcal{C}_n(\mathfrak{d}; a)$ of symmetric integer matrices with determinant $\mathfrak{d}$ and $(1, 1)$ -entry a such that, whenever G_0 is symmetric integral with $\det G_0 = \mathfrak{d}$ and a primitive $v \in \mathbb{Z}^n$ satisfies $v^\top G_0 v = a$, some $U \in \text{GL}_n(\mathbb{Z})$ satisfies $Ue_1 = v$ and $U^\top G_0 U \in \mathcal{C}_n(\mathfrak{d}; a)$. Here e_1 is the first coordinate vector.*

Proof. Simultaneously construct a complete finite congruence list $\mathcal{C}_n(\mathfrak{d})$ without a prescribed first entry. Dimensions zero and one are immediate, with the empty matrix having determinant 1. Complete v to an integer basis; subsequent changes fix its first vector.

If $a \neq 0$, write $G = \begin{pmatrix} a & b^\top \\ b & G_1 \end{pmatrix}$ and set $G_* = aG_1 - bb^\top$, whose determinant is $a^{n-2}\mathfrak{d}$. Reduce G_* to $\mathcal{C}_{n-1}(a^{n-2}\mathfrak{d})$ and reduce b modulo $|a|$ by adding multiples of v to the other basis vectors. These additions preserve G_* . Enumerating the residues and retaining the integral matrices with $G_1 = (G_* + bb^\top)/a$ gives the required list.

If $a = 0$, integer column reduction gives

$$\begin{pmatrix} 0 & \delta & 0 \\ \delta & a' & b'^\top \\ 0 & b' & G_1 \end{pmatrix}, \quad \delta > 0, \quad \mathfrak{d} = -\delta^2 \det G_1.$$

Reduce G_1 to $\mathcal{C}_{n-2}(-\mathfrak{d}/\delta^2)$. Adding multiples of v reduces a' modulo 2δ and b' modulo δ , without changing G_1 or the first row. Enumerate these residues and the finitely many $\delta^2 \mid \mathfrak{d}$.

To close the induction, replace the eigenvalues of G_0 by their absolute values, obtaining G_+ with determinant $|\mathfrak{d}|$ and $|x^\top G_0 x| \leq x^\top G_+ x$. Minkowski's theorem [28, Chapter I, Theorem (4.4)], applied to the convex symmetric body $G_+^{-1/2}[-2|\mathfrak{d}|^{1/(2n)}, 2|\mathfrak{d}|^{1/(2n)}]^n$ of volume 4^n , gives, after division by content, a primitive v with $|v^\top G_0 v| \leq 4n|\mathfrak{d}|^{1/n} \leq 4n|\mathfrak{d}|$. Thus

$$\mathcal{C}_n(\mathfrak{d}) = \bigcup_{|a| \leq 4n|\mathfrak{d}|} \mathcal{C}_n(\mathfrak{d}; a).$$

The prescribed lists use only lower-dimensional lists, so this completes the induction and the algorithm. $\square$

The Grunewald–Segal algorithms [18], announced as Algorithms A1–A2 in [17, p. 915], compute generators for the full integer-point group of a rational matrix algebraic group, and

decide orbits in rational linear representations, returning a group element carrying one vector to the other when one exists. Their input includes the defining equations of a rational matrix algebraic group G and a subgroup Γ of its integer-point group $G(\mathbb{Z})$, together with a membership test for Γ and an upper bound for $[G(\mathbb{Z}) : \Gamma]$. In both applications below we use the full group $G(\mathbb{Z})$ itself, namely $\mathrm{GL}_n(\mathbb{Z})$ or Ω_L . Thus the index bound is 1, and membership within $G(\mathbb{Z})$ is automatic.

Lemma B.2. *For a nondegenerate integral quadratic form on a specified lattice L , one can compute finite lists meeting every Ω_L -orbit on each nonzero level and on the primitive zero level.*

Proof. In a basis of L , write $Q(x) = \frac{1}{2}x^\top G_0 x$ and $\mathfrak{d} = \det G_0$. Apply the orbit algorithm to $\mathrm{GL}_n(\mathbb{Z})$ acting on symmetric matrices by $U \cdot S = U^{-\top} S U^{-1}$. For each $G \in \mathcal{C}_n(\mathfrak{d}; 2m)$, this decides whether $U^\top G_0 U = G$ and produces such a U by inverting the returned group element. Retain Ue_1 . Lemma B.1 gives all primitive orbits, including $m = 0$. For $m \neq 0$, include c times the lists at m/c^2 for all positive c with $c^2 \mid m$, as in Lemma 3.3. $\square$

For the Hermitian model, put $\Gamma'_E = \varphi(\mathrm{SL}_2(\mathcal{O}_E))$ as in Section 12. Apply the generator algorithm to the integral isometry group Ω_{L_E} . For $g \in \Omega_{L_E}$, membership in Γ'_E is decidable: exclude determinant -1 , and for determinant 1 solve $\varphi(h) = g$ with $h \in \mathrm{SL}_2(E)$ in rational coordinates relative to an integral basis of $\mathcal{O}_E$. Since $\ker \varphi = \{\pm I_2\}$, this polynomial system has at most two complex solutions. Exact elimination and factorization over $\mathbb{Q}$ compute its rational solutions; integral coordinates decide whether a lift lies in $\mathrm{SL}_2(\mathcal{O}_E)$.

Lemma 12.2 gives finite index in Ω_{L_E} . Enumerate right cosets by multiplying known representatives by the generators and their inverses, using

$$\Gamma'_E \gamma_i = \Gamma'_E \gamma_j \iff \gamma_i \gamma_j^{-1} \in \Gamma'_E.$$

Stop when every retained representative has been processed. Finite index guarantees termination, without a numerical index bound. If γ_i are these representatives and v_j are the vectors from Lemma B.2, then $\gamma_i v_j$ meet all required Γ'_E -orbits.

References

- [1] B. Berggren, *Pytagoreiska trianglar*, Tidskrift för elementär matematik, fysik och kemi **17** (1934), 129–139.
- [2] A. Borel and Harish-Chandra, *Arithmetic subgroups of algebraic groups*, Annals of Mathematics (2) **75** (1962), 485–535. doi:10.2307/1970210.
- [3] D. Carter and G. Keller, *Bounded elementary generation of $\mathrm{SL}_n(\mathcal{O})$* , American Journal of Mathematics **105** (1983), no. 3, 673–687. doi:10.2307/2374319.
- [4] D. A. Cox, *Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication*, second edition, Pure and Applied Mathematics, Wiley, Hoboken, NJ, 2013. doi:10.1002/9781118400722.
- [5] M. Eichler, *Quadratische Formen und orthogonale Gruppen*, Grundlehren der mathematischen Wissenschaften 63, Springer-Verlag, Berlin–Göttingen–Heidelberg, 1952. doi:10.1007/978-3-662-01212-3.
- [6] J. Elstrodt, F. Grunewald and J. Mennicke, *Groups Acting on Hyperbolic Space: Harmonic Analysis and Number Theory*, Springer Monographs in Mathematics, Springer, Berlin, 1998. doi:10.1007/978-3-662-03626-6.
- [7] I. V. Erovenko and A. S. Rapinchuk, *Bounded generation of S -arithmetic subgroups of isotropic orthogonal groups over number fields*, Journal of Number Theory **119** (2006), no. 1, 28–48. <https://arxiv.org/abs/math/0508480>.

- [8] S. Frisch, *Remarks on polynomial parametrization of sets of integer points*, Communications in Algebra **36** (2008), no. 3, 1110–1114. doi:10.1080/00927870701776938.
- [9] S. Frisch and G. Lettl, *Polynomial parametrization of the solutions of Diophantine equations of genus 0*, Functiones et Approximatio Commentarii Mathematici **39** (2008), no. 2, 205–209. doi:10.7169/facm/1229696571.
- [10] S. Frisch and L. Vaserstein, *Parametrization of Pythagorean triples by a single triple of polynomials*, Journal of Pure and Applied Algebra **212** (2008), no. 1, 271–274. doi:10.1016/j.jpaa.2007.05.019.
- [11] S. Frisch and L. Vaserstein, *Polynomial parametrization of Pythagorean quadruples, quintuples and sextuples*, Journal of Pure and Applied Algebra **216** (2012), no. 1, 184–191. doi:10.1016/j.jpaa.2011.06.002.
- [12] L. H. Gallardo and L. N. Vaserstein, *Polynomial parametrization of integer matrices with given determinant*, Journal of Pure and Applied Algebra **218** (2014), no. 2, 321–322. doi:10.1016/j.jpaa.2013.06.003.
- [13] B. Grechuk, *On the smallest open Diophantine equations*, ACM SIGACT News **53** (2022), no. 1, 36–57. doi:10.1145/3532737.3532743. Author’s version: <https://arxiv.org/abs/2204.11624v1> (2022).
- [14] B. Grechuk, *A systematic approach to Diophantine equations: open problems*, arXiv preprint, arXiv:2404.08518v4, 23 January 2026. <https://arxiv.org/abs/2404.08518v4>.
- [15] B. Grechuk, *Polynomial Diophantine Equations: A Systematic Approach*, Springer, Cham, 2024. doi:10.1007/978-3-031-62949-5.
- [16] V. Gritsenko, K. Hulek and G. K. Sankaran, *Abelianisation of orthogonal groups and the fundamental group of modular varieties*, Journal of Algebra **322** (2009), no. 2, 463–478. doi:10.1016/j.jalgebra.2009.01.037.
- [17] F. J. Grunewald and D. Segal, *The solubility of certain decision problems in arithmetic and algebra*, Bulletin of the American Mathematical Society (N.S.) **1** (1979), no. 6, 915–918. doi:10.1090/S0273-0979-1979-14692-5.
- [18] F. Grunewald and D. Segal, *Some general algorithms. I: Arithmetic groups*, Annals of Mathematics (2) **112** (1980), no. 3, 531–583. doi:10.2307/1971091.
- [19] F. J. Grunewald and D. Segal, *How to solve a quadratic equation in integers*, Mathematical Proceedings of the Cambridge Philosophical Society **89** (1981), no. 1, 1–5. doi:10.1017/S030500410005787X.
- [20] R. K. Guy, *Conference problems session conducted by J. L. Selfridge*, in *Number Theory* (Ottawa, 1996), R. Gupta and K. S. Williams (eds.), CRM Proceedings & Lecture Notes **19**, American Mathematical Society, Providence, RI, 1999, 385–390; Beukers’s Problem CNTA 5.15, p. 390.
- [21] B. W. Jordan and Y. Zaytman, *On the bounded generation of arithmetic SL_2* , Proceedings of the National Academy of Sciences of the USA **116** (2019), no. 38, 18880–18882. doi:10.1073/pnas.1907728116. Correction, **118** (2021), no. 32, e2111531118. doi:10.1073/pnas.2111531118. Corrected preprint: <https://arxiv.org/abs/1810.12972v3>.
- [22] M.-A. Knus, *Quadratic Forms, Clifford Algebras and Spinors*, Seminars in Mathematics 1, IMECC–UNICAMP, Campinas, 1988. <https://people.math.ethz.ch/~knus/papers/campinas.pdf>.
- [23] M. Larsen and D. Q. N. Nguyen, *Polynomial parametrization for SL_2 over quadratic number rings*, International Mathematics Research Notices **2021**, no. 9, 6993–7003. doi:10.1093/imrn/rnz046. In <https://arxiv.org/abs/1808.05349>, statements numbered 1. j in the published article are numbered j .
- [24] H. W. Lenstra, Jr., *Solving the Pell equation*, Notices of the American Mathematical Society **49** (2002), no. 2, 182–192. <https://www.ams.org/notices/200202/fea-lenstra.pdf>.
- [25] R. Lidl and H. Niederreiter, *Finite Fields*, 2nd ed., Encyclopedia of Mathematics and its Applications 20, Cambridge University Press, Cambridge, 1997. doi:10.1017/CB09780511525926.

- [26] J. Liu and P. Sarnak, *Integral points on quadrics in three variables whose coordinates have few prime factors*, Israel Journal of Mathematics **178** (2010), 393–426. doi:10.1007/s11856-010-0069-y.
- [27] A. V. Morgan, A. S. Rapinchuk and B. Sury, *Bounded generation of SL_2 over rings of S -integers with infinitely many units*, Algebra & Number Theory **12** (2018), no. 8, 1949–1974. doi:10.2140/ant.2018.12.1949.
- [28] J. Neukirch, *Algebraic Number Theory*, Grundlehren der mathematischen Wissenschaften 322, Springer, Berlin, 1999. doi:10.1007/978-3-662-03983-0.
- [29] V. Platonov and A. Rapinchuk, *Algebraic Groups and Number Theory*, translated by R. Rowen, Pure and Applied Mathematics 139, Academic Press, Boston, 1994.
- [30] J.-P. Serre, *A Course in Arithmetic*, Graduate Texts in Mathematics 7, Springer, New York, 1973. doi:10.1007/978-1-4684-9884-4.
- [31] V. Shoup, *A Computational Introduction to Number Theory and Algebra*, second edition, Cambridge University Press, Cambridge, 2008. Author’s version 2.5: https://www.shoup.net/ntb/ntb-v2_5.pdf.
- [32] C. L. Siegel, *Zur Theorie der quadratischen Formen*, Nachrichten der Akademie der Wissenschaften in Göttingen, Mathematisch-Physikalische Klasse II (1972), no. 3, 21–46.
- [33] Th. Skolem, *Diophantische Gleichungen*, Ergebnisse der Mathematik und ihrer Grenzgebiete 5, no. 4, Springer, Berlin, 1938.
- [34] L. N. Vaserstein, *Polynomial parametrization for the solutions of Diophantine equations and arithmetic groups*, Annals of Mathematics (2) **171** (2010), no. 2, 979–1009. doi:10.4007/annals.2010.171.979.
- [35] J. Voight, *Quaternion Algebras*, Graduate Texts in Mathematics 288, Springer, Cham, 2021. doi:10.1007/978-3-030-56694-4.
- [36] H. Weber, *Beweis des Satzes, dass jede eigentlich primitive quadratische Form unendlich viele Primzahlen darzustellen fähig ist*, Mathematische Annalen **20** (1882), 301–329. doi:10.1007/BF01443599.
- [37] U. Zannier, *Remarks on a question of Skolem about the integer solutions of $x_1x_2 - x_3x_4 = 1$* , Acta Arithmetica **78** (1996), no. 2, 153–164. doi:10.4064/aa-78-2-153-164.