Polynomial parametrizations for two classes of Diophantine equations

Bogdan Grechuk

27 November 2026

Abstract

We prove that the integer solution sets of two classes of Diophantine equations are finite unions of polynomial families with integer coefficients and unrestricted integer parameters. In the first class, each monomial, with at most one exception, contains a variable occurring to the first power and in no other monomial. The second class consists of equations $M = f(t)$, where M is a monomial independent of t with a variable occurring to the first power, and $f \in \mathbb{Z}[t]$ splits completely over a number field of degree at most two. There is no restriction on the degree of f, the multiplicities of its factors, and arbitrarily many irreducible quadratic factors are allowed if they have the same splitting field. In particular, we give polynomial parametrizations for seven equations left open in the monograph *Polynomial Diophantine Equations: A Systematic Approach* (2024).

2020 Mathematics Subject Classification. Primary 11D72; Secondary 11D85, 11E39, 11R11, 11R37, 20H05.

Keywords. Diophantine equations; integer solutions; polynomial parametrization; quadratic fields.

hexagon:2610.00569v2

1 Introduction

For a polynomial Diophantine equation

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

a natural goal is to describe all integer solutions by finitely many explicit formulas. Polynomial parametrizations provide a particularly useful form of such a description: every parameter choice produces a solution, and every solution is attained.

We use the terminology of [1] and [5, Chapter 1].

Definition 1.1. A *polynomial family* in $\mathbb{Z}^n$ is the image of a map $\Phi \in \mathbb{Z}[t_1, \dots, t_\nu]^n$ evaluated at all of $\mathbb{Z}^\nu$, where $\nu \geq 0$. The map Φ is a *polynomial parametrization* of its image. A set $S \subseteq \mathbb{Z}^n$ is a *finite union of polynomial families* if $S = \bigcup_{j=1}^{h} \Phi_j(\mathbb{Z}^{\nu_j})$ for finitely many such maps. We allow $h = 0$, representing the empty set, and $\nu_j = 0$, representing a single point. The families need not be disjoint.

We ask when the integer solution set of (1.1) is a finite union of polynomial families. The coefficients in Definition 1.1 are integers, and the parameters are independent and unrestricted. Rational functions with variable denominators, or formulas with unresolved coprimality conditions, do not by themselves exhibit the solution set as a finite union of polynomial families.

This question can be difficult even for simple equations. The existence of a polynomial parametrization of

$$x_1 x_2 - x_3 x_4 = 1$$

was a longstanding open problem, resolved by Vaserstein [1, Theorem 1]. Chapter 2 of the monograph [5] uses this theorem to represent the solution sets of many other equations as finite unions of polynomial families. Several small examples were left open there and appear in [6, Table 1], including

$$x^2y + zt + 1 = 0, \qquad x_1x_2x_3 + x_4x_5 + 1 = 0, \tag{1.2}$$

$$x^2y + z^2 \pm 1 = 0, \qquad xyz + t^2 - 1 = 0, \tag{1.3}$$

$$x^3 + yz + 1 = 0, \qquad xyz + t^2 + 1 = 0. \tag{1.4}$$

The present paper develops two general constructions that apply to all seven equations and gives parametrizations with coverage proofs in Section 11. The formulas for the first five equations have explicit parameter bounds. For the two equations in (1.4), the formulas are explicit in terms of the covers of Theorems 8.6 and 9.4; these covers are constructed in the proofs, without expanded coordinate polynomials or parameter counts. Together with Grechuk and Ratcliffe's results for $x^2 + y^2 + zt \pm 1 = 0$ [8], our results settle all nine equations in the original table [6, Table 1].

Our main results are the following two theorems. A monic monomial is $x^e = \prod_j x_j^{e_j}$ with nonnegative integer exponents; the constant monomial 1 is allowed.

Theorem A. *Let $M_0, \dots, M_s$ be monic monomials in $x = (x_1, \dots, x_n)$, with $s \geq 1$, and fix integers $\alpha_1, \dots, \alpha_s \neq 0$ and c. Let $y_1, \dots, y_s$ be distinct variables absent from every M_j; the monomial supports may overlap arbitrarily. Then the integer solutions of*

$$\sum_{i=1}^{s} \alpha_i M_i(x) y_i = cM_0(x) \tag{1.5}$$

form a finite union of polynomial families.

Theorem B. *Fix $\kappa \in \mathbb{Z}\setminus\{0\}$, $f \in \mathbb{Z}[t]$, a nonnegative integer r, and positive integers $e_1, \dots, e_r$. Let $z, x_1, \dots, x_r, t$ be distinct variables. Assume that either $f = 0$, or every irreducible factor of f over $\mathbb{Q}$ has degree at most two and all its irreducible quadratic factors have the same splitting field. Equivalently, for nonzero f the hypothesis says that f splits completely over some number field of degree at most two. Nonzero constants are included. Then all integer solutions of*

$$\kappa z \prod_{i=1}^{r} x_i^{e_i} = f(t) \tag{1.6}$$

form a finite union of polynomial families. If $r = 0$, the conclusion holds for every $f \in \mathbb{Z}[t]$.

The first class in the abstract follows from Theorem A: in each non-exceptional monomial choose a variable that occurs to the first power and in no other monomial, call it y_i, and collect all remaining variables in x. Move the exceptional monomial to the right-hand side, or take $c = 0$ if there is none. Equations with at most one nonzero monomial are immediate: their solution sets are unions of coordinate hyperplanes, the empty set, or the whole space.

The equations in (1.2) are covered by Theorem A, and those in (1.3) and (1.4) by Theorem B. Theorem B also answers the parametrization question for $x_1 \cdots x_h = t^2 - d$ for every fixed $h \geq 1$ and $d \in \mathbb{Z}$. For $h = 2$ and $d \neq 0$, Vaserstein [1, Example 7] treats $x_1x_2 = t^2 + D$ with $D = -d \neq 0$ using binary quadratic forms of fixed determinant; the case $d = 0$ is elementary. Theorem B allows arbitrary degree and multiplicities, provided the quadratic factors have a common splitting field. For example, it applies to

$$xy + z^3 + 1 = 0, \qquad xy + z^3 + z = 0, \qquad xy^2 + z^3 + 1 = 0, \tag{1.7}$$

$$xyz + t^3 + 1 = 0, \qquad xy + z^4 - 1 = 0. \tag{1.8}$$

Indeed, $t^3+1=(t+1)(t^2-t+1)$, $t^3+t=t(t^2+1)$, and $t^4-1=(t-1)(t+1)(t^2+1)$. Arbitrary powers of the linear and quadratic factors are allowed, as are several distinct quadratic factors in one field. For instance, the theorem applies to

$$xy^2z^3=(t-1)^5(t^2+1)^3(t^2+4)^2(t^2+9).$$

The hypothesis of Theorem B is sufficient; no converse is asserted. Two extensions left unresolved by the present argument are distinct quadratic splitting fields, as in $xy=(t^2+1)(t^2+2)$, and irreducible factors of degree at least three, as in

$$xy=t^3-2.$$

The common-field hypothesis is used in Step 1 of Theorem 9.4: the auxiliary elements for every quadratic block must lie in the same ring as the first block, so that residues can be prescribed at an ideal and its conjugate. Higher-degree factors also fall outside the quadratic-norm and binary Hermitian constructions developed here. These limitations of the method do not give obstructions to polynomial parametrization of those equations.

The proofs use Vaserstein's parametrization of $\mathrm{SL}_2(\mathbb{Z})$ [1, Theorem 1] and his factorization of congruence subgroups [1, Proposition 5.9 and Corollary 5.11]. We use polynomial families with fixed denominators as in [2, Lemmas 2–3] (see also [5, Chapter 1]), and Gordan's lemma [4, Proposition 2.1.1(a)]. Related work of Frisch and Lettl [3, Theorem 1] concerns integer-valued parametrizations of affine cones over rational projective plane curves, with specified exceptions for singular points.

When f splits over $\mathbb{Q}$, the proof of Theorem B uses only the integer-polynomial tools in Sections 2–4 and the allocation, Hilbert-basis and linear-factor Chinese remainder arguments in Section 10. Thus the completely split case can be read independently of the quadratic arithmetic.

For quadratic factors we use the method of Larsen and Nguyen [9], based on Vaserstein's polynomial matrix identities and the Carter–Keller exponent lemma [10, Lemma 4]. We adapt this method to orders of varying conductor. A direct single-cancellation argument replaces their Hilbert-reciprocity step and works in both real and imaginary quadratic fields. The precise uniformity needed for varying conductors is stated in Section 6. For numerical surjectivity we use ideal arithmetic and Chebotarev's theorem in composita of ray class fields and radical extensions. The principal new step is to parametrize several blocks of quadratic integers with primitive products, allowing fixed norm scale factors, so that the scaled norms of different blocks are pairwise coprime. This is stronger than independent covers of the individual blocks. Two auxiliary prime elements for each subsequent quadratic factor let us prescribe residues at a primitive ideal and its conjugate separately. Polynomial determinant-one shears join these residues. Resultants separate the prime allocations among the distinct irreducible factors, Gordan's lemma encodes arbitrary fixed exponents and multiplicities, and a polynomial Chinese remainder construction then produces a common value of t. The resulting expressions have at most fixed denominators, which are removed by finite residue subdivisions.

Sections 2–4 establish the common polynomial tools, including a congruence matrix with variable level and a parametrization of pairwise coprime block products. Section 5 proves Theorem A. Section 6 obtains uniform congruence matrices over quadratic fields. These yield the relative Hermitian parametrizations and norm-coprime insertions of Section 7, from which the primitive-product theorem of Section 8 follows by induction. Section 9 constructs the joint cover of quadratic and scalar blocks, and Section 10 proves Theorem B. Section 11 gives worked examples.

2 Polynomial operations and algebraic inputs

We take empty products to be 1. Gcds are nonnegative, with $\gcd(0,n) = |n|$; a tuple is primitive (or unimodular) if its coordinates have gcd 1. For $a \neq 0$, $v_p(a)$ is the exponent of p in $|a|$. For a quadratic number field K, its ring of integers is $\mathcal{O}_K$, conjugation is $\alpha \mapsto \bar{\alpha}$, and $\mathrm{N}(\alpha) = \alpha\bar{\alpha}$. Ideal norms extend multiplicatively from $\mathrm{N}(\mathfrak{a}) = [\mathcal{O}_K : \mathfrak{a}]$, so $\mathrm{N}((\alpha)) = |\,\mathrm{N}(\alpha)|$.

For $P \in \mathbb{Q}[t_1, \ldots, t_\nu]^n$, the set $P(\mathbb{Z}^\nu) \cap \mathbb{Z}^n$ is a *rational polynomial family* [5, Chapter 1].

Lemma 2.1 (Fixed denominators and congruences)**.** *Let $\mathbf{t} = (t_1, \ldots, t_\nu)$ and $P \in D^{-1}\mathbb{Z}[\mathbf{t}]^n$, with $D \geq 1$ fixed. The integral values of P on $\mathbb{Z}^\nu$ satisfying finitely many fixed coordinate congruences form a finite union of polynomial families. The same holds for fixed congruences on integer-polynomial expressions in the retained coordinates and parameters.*

Proof. This is the residue-class argument of [2, Lemmas 2–3]; the case without congruences is also [5, Chapter 1]. Let $m_0 > 0$ be a common multiple of the congruence moduli. For every $a \in \mathbb{Z}^\nu$, expansion gives

$$P(a + Dm_0\mathbf{u}) - P(a) \in m_0\mathbb{Z}[\mathbf{u}]^n.$$

Thus integrality and the required residues depend only on a mod Dm_0. On each admissible class, $P(a + Dm_0\mathbf{u})$ has integer coefficients. The finitely many admissible classes give exactly the desired values. For auxiliary expressions, append them as extra coordinates, enlarge D if necessary, apply the same argument, and project to the desired coordinates. □

Remark 2.2 (Polynomial quotients). Polynomial identities persist under every residue substitution above. There are two different reasons why a displayed quotient may be polynomial. A quotient by a variable polynomial, such as $(A - a)/P$, denotes a quotient proved to lie in the integer polynomial ring, *before* parameter specialization. For example, if a construction gives $A - a = P^2H$, we define $(A - a)/P = PH$. It then has value zero when $P = 0$. All parameter substitutions are allowed, including those at which a displayed polynomial denominator vanishes. Congruences between polynomials mean ideal divisibility in their polynomial ring. In contrast, division by a fixed nonzero integer is handled by Lemma 2.1: after retaining the admissible residue classes the resulting expression has integer coefficients. We specify this second mechanism when dividing by fixed scale factors. A varying modulus is always a polynomial output: a congruence modulo it is established algebraically and is never imposed by a fixed residue filter. Rational auxiliary coordinates need not be made integral when only their final polynomial combinations are required as outputs.

2.1 Bézout identities

For $A, B \in \mathcal{R} = \mathbb{Z}[\boldsymbol{u}]$, we use Bézout coefficients $R, S \in \mathcal{R}$ satisfying $AR + BS = 1$ as a polynomial identity. For a tuple $(A_1, \ldots, A_s)$, the corresponding identity is $\sum_i A_i R_i = 1$ with $R_i \in \mathcal{R}$. These identities mean that the polynomials generate the unit ideal; having no common nonunit factor alone would not suffice. The following elementary identities will be used repeatedly. From $AR + BS = 1$ and $A' = A + BH$ one obtains

$$A'R + B(S - RH) = 1. \tag{2.1}$$

From $AR + BS = 1$ and $AU + CV = 1$ one obtains

$$A(R + U - ARU) + BCSV = 1. \tag{2.2}$$

The second identity follows by expanding $(1-AR)(1-AU) = BCSV$. It combines the identities for (A, B) and (A, C) into one for (A, BC); swapping the two roles gives the analogous operation for a product in the first slot. If $A = A_1A_2$, a Bézout identity for (A, B) gives one for (A_1, B) by replacing R with A_2R.

Lemma 2.3 (Raising prescribed powers)**.** *If $X = \prod_i x_i$, $Y = \prod_j y_j$ and $XR + YS = 1$ polynomially, then $A = \prod_i x_i^{e_i}$ and $B = \prod_j y_j^{f_j}$ have polynomial Bézout identities for any fixed positive exponents.*

Proof. For nonempty products put $E = \max_i e_i$, $F = \max_j f_j$. Expand $1 = (XR+YS)^{E+F-1}$: every term is divisible by A or by B, so grouping terms gives the Bézout identities. An empty product equals 1. □

Lemma 2.4 (Automatic polynomial witnesses)**.** *Let $f_1, \dots, f_l \in \mathbb{Z}[v_1, \dots, v_N]$ have gcd one at every integer input. There is a fixed positive integer M, depending only on the f_j, such that on each branch $v = b + Mu$, with $b \in \{0, \dots, M-1\}^N$, there are $g_j \in \mathbb{Z}[u]$ satisfying $\sum_j f_j(b + Mu)g_j(u) = 1$ as a polynomial identity.*

Proof. If their ideal over $\mathbb{Q}$ were proper, there would be a common algebraic zero, by the weak Nullstellensatz. Express its coordinates in a primitive integral element α of a number field, with fixed rational denominators. After clearing denominators the vanishing identities hold modulo the minimal polynomial of α. By Schur's theorem on prime divisors of polynomial values [16], that minimal polynomial has a root modulo some prime avoiding all the finitely many denominators. Reduction gives a common zero modulo that prime, contradicting the hypothesis on integer representatives. Hence there is an integer-polynomial identity $\sum f_j h_j = M$ with a fixed positive integer M. On each branch $v = b + Mu$, choose constants c_j with $\sum c_j f_j(b) \equiv 1 \pmod M$. Then $\sum c_j f_j(b + Mu) = 1 + MR(u)$. Subtract R times the identity for M. This gives the desired witness. The case of a rational zero is included by taking a linear minimal polynomial. □

The witnesses are computable. A Gröbner-basis calculation over $\mathbb{Q}$, with ideal-membership coefficients, gives $\sum f_j h_j = M$ after clearing denominators. Extended Euclidean calculations on the finitely many residue classes then give the c_j and the displayed construction of the g_j.

Definition 2.5 (Polynomial continuation)**.** Let $P \in \mathbb{Z}[\mathbf{u}]^a$, where $\mathbf{u}$ has d coordinates. A *polynomial continuation* of P is a finite collection of maps

$$(\mathbf{v}, \mathbf{w}) \longmapsto (\mathbf{b} + M\mathbf{v}, P(\mathbf{b} + M\mathbf{v}), Q(\mathbf{v}, \mathbf{w})), \qquad (\mathbf{v}, \mathbf{w}) \in \mathbb{Z}^d \times \mathbb{Z}^e,$$

where $M \geq 1$ and $\mathbf{b} \in \mathbb{Z}^d$ are fixed on each branch and $Q \in \mathbb{Z}[\mathbf{v}, \mathbf{w}]^c$ has a fixed number c of specified output coordinates. The number of new parameters may differ between branches. Additional auxiliary outputs may be retained and later projected away. Thus the original parameters and outputs are retained; only fixed residue classes of the original parameters are used.

Let $\mathcal{T}(\mathbf{u}) \subseteq \mathcal{S}(\mathbf{u}) \subseteq \mathbb{Z}^c$ be, respectively, the *required targets* and the *permissible outputs*. The continuation *covers every fibre of $\mathcal{T}$ inside $\mathcal{S}$* if

(i) every branch satisfies $Q(\mathbf{v}, \mathbf{w}) \in \mathcal{S}(\mathbf{b} + M\mathbf{v})$ at every integer parameter value;

(ii) for every $\mathbf{u}_0$ and $y \in \mathcal{T}(\mathbf{u}_0)$, some branch and integer parameters satisfy $\mathbf{b} + M\mathbf{v} = \mathbf{u}_0$ and $Q(\mathbf{v}, \mathbf{w}) = y$.

The old specialization is recovered exactly after any residue subdivision. When $\mathcal{S} = \mathcal{T}$, we simply say that the continuation *covers every fibre of $\mathcal{T}$*. The distinction allows harmless extra outputs, such as zero scalar coordinates, when coverage is required only for nonzero targets. It also allows a target set to be empty outside the numerical domain on which coverage is asserted, while preserving sound outputs there.

Lemma 2.6 (Composition and fixed filters)**.** *Polynomial continuations compose. More precisely, suppose the first continuation covers $\mathcal{T}_1(\mathbf{u})$ inside $\mathcal{S}_1(\mathbf{u})$. Suppose that, over* every *parameter specialization of every branch of the first continuation, the second covers $\mathcal{T}_2(\mathbf{u}, y)$ inside $\mathcal{S}_2(\mathbf{u}, y)$, where y is the first output. Then the composite covers*

$$\{(y, z) : y \in \mathcal{T}_1(\mathbf{u}), \quad z \in \mathcal{T}_2(\mathbf{u}, y)\}$$

inside the analogous set formed with $\mathcal{S}_1, \mathcal{S}_2$. Retained auxiliary outputs may be included in the intermediate tuple y. To prove coverage after projecting away y, it suffices, for each prescribed final target, to choose an attainable augmented intermediate target for which the prescribed final target belongs to $\mathcal{T}_2(\mathbf{u}, y)$.

Fixed congruence filters and divisions by fixed integers are incorporated by Lemma 2.1. Filtering replaces the permissible and required sets by their subsets satisfying the retained fixed conditions. Coverage of these restricted fibres holds over every surviving old specialization. Projecting the resulting finite collection to its specified integer output coordinates gives a finite union of polynomial families.

Proof. Substitute the polynomial expressions from the first continuation into the second. A fixed residue subdivision of the first branch parameters $\mathbf{v}, \mathbf{w}$ is again a fixed residue subdivision of the original parameters, with some new parameters restricted to fixed residue classes. Replacing every restricted parameter by its residue plus a fixed multiple of a new free integer gives the form in Definition 2.5. Only finitely many branches occur, and the two soundness assertions give the stated permissible set.

For a target (y, z), choose parameters in the first continuation attaining y. The second coverage assertion holds over that precise parameter specialization, so it attains z while retaining the old outputs. This proves the claim, also with retained auxiliary data. Lemma 2.1 supplies the fixed filters and integer coefficients; coordinate projection proves the last assertion. □

Throughout the relative arguments, all input data are polynomial outputs in a fixed old parameter tuple. Pointwise coprimality of integer polynomial outputs is converted into a polynomial Bézout identity by Lemma 2.4, after a further fixed residue subdivision if needed. When a construction replaces a current factor, its previous value is retained as an auxiliary coordinate until the final projection. The quotient conventions are those of Remark 2.2.

2.2 A congruence-compatible matrix completion

Lemma 2.7 (Lifting a primitive column)**.** *Let $m_0 > 0$ and $H_0 \in \mathrm{SL}_2(\mathbb{Z})$. If the primitive column $(a, c)^T$ is congruent modulo m_0 to the first column of H_0, it has a completion $H_1 \in \mathrm{SL}_2(\mathbb{Z})$ satisfying $H_1 \equiv H_0 \pmod{m_0}$.*

Proof. Choose any determinant-one completion H of $(a, c)^T$. Modulo m_0 the matrix $H^{-1}H_0$ has first column $(1, 0)^T$ and determinant 1, so it has form $\left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right)$. Choose an integer representative of h and set $H_1 = H \left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right)$. This preserves the first column and gives the required congruence. For $m_0 = 1$ the condition is vacuous and the proof still applies. □

In particular, if two primitive integer columns agree modulo a nonzero integer q, a matrix congruent to I_2 modulo $|q|$ in $\mathrm{SL}_2(\mathbb{Z})$ carries one to the other. This follows by completing the first column and applying Lemma 2.7 to the second.

Lemma 2.8 (Polynomial matrix Chinese remainder operation)**.** *If $A, B \in \mathrm{SL}_2(\mathbb{Z}[v])$ and integer polynomials m, n have gcd one at every integer input, after finite fixed residue substitutions there is $C \in \mathrm{SL}_2(\mathbb{Z}[v])$ satisfying $C \equiv A \pmod{m}$ and $C \equiv B \pmod{n}$ as polynomial congruences.*

Proof. After applying Lemma 2.4, obtain a polynomial e congruent to one modulo m and zero modulo n. Put $G = AB^{-1}$. There is a polynomial path G_λ of determinant one from I_2 to G: use $G(\lambda v)G(0)^{-1}E(\lambda)$, where $G(\lambda v)$ means substituting λv_i for every parameter v_i, and $E(\lambda)$ interpolates from I_2 to $G(0) \in \mathrm{SL}_2(\mathbb{Z})$ by a fixed elementary decomposition, scaling each elementary parameter by λ. Since $G_\lambda - G_1$ is polynomially divisible by $\lambda - 1$ and $G_\lambda - I_2$ by λ, we have $G_e \equiv G \pmod m$ and $G_e \equiv I_2 \pmod n$. Thus $C = G_e B$ has the required congruences. If m, n already generate the unit ideal as polynomials, their Bézout identity gives e directly and no subdivision is needed. □

Lemma 2.9 (Gordan's lemma [4, Proposition 2.1.1(a)])**.** *For a rational polyhedral cone $C \subseteq \mathbb{R}^n_{\geq 0}$, the additive monoid $C \cap \mathbb{Z}^n$ has finitely many generators.*

Lemma 2.10 (Solutions of a linear equation)**.** *Let $s \geq 1$, let $\mathbf{t} = (t_1, \ldots, t_\nu)$, and suppose $A_i, R_i, H \in \mathbb{Z}[\mathbf{t}]$ satisfy $\sum_{i=1}^s A_i R_i = \Lambda$, where $\Lambda > 0$ is fixed. The set*

$$\left\{ (\mathbf{t}, \mathbf{y}) \in \mathbb{Z}^\nu \times \mathbb{Z}^s : \sum_{i=1}^s A_i(\mathbf{t}) y_i = H(\mathbf{t}) \right\}$$

is a finite union of polynomial families. More explicitly, it consists of the integral values of the map $(\mathbf{t}, \mathbf{v}) \mapsto (\mathbf{t}, \mathbf{y})$ defined by

$$y_i = \frac{HR_i}{\Lambda} + v_i - \frac{R_i}{\Lambda} \sum_{j=1}^s A_j v_j, \qquad \mathbf{v} = (v_1, \ldots, v_s) \in \mathbb{Z}^s, \tag{2.3}$$

with $\mathbf{t} \in \mathbb{Z}^\nu$.

Proof. Summing verifies the equation. For any prescribed solution take $v_i = y_i$; the formula returns the target. Lemma 2.1 retains integral outputs and removes the fixed denominator Λ. □

3 A polynomial congruence map with variable level

Vaserstein's Theorem 13 parametrizes each fixed principal congruence subgroup. We need polynomial dependence on the level as well. We prove this from his fixed factorization in [1, Proposition 5.9].

3.1 Polynomial matrices

Put

$$U(v) = \begin{pmatrix} 1 & v \\ 0 & 1 \end{pmatrix}, \qquad L(v) = \begin{pmatrix} 1 & 0 \\ v & 1 \end{pmatrix}, \qquad J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Let $D_j(v_1, \ldots, v_j)$ be the alternating product of j elementary matrices beginning with $U(v_1)$, and let C_j begin with $L(v_1)$. Vaserstein's Δ_j equals D_j, while $\Gamma_j(\mathbf{v}) = J\Delta_j(\mathbf{v})J^{-1} = C_j(-\mathbf{v})$: conjugation changes $U(v)$ to $L(-v)$ and $L(v)$ to $U(-v)$. Thus their images agree with those of D_j, C_j, respectively; see [1, Section 1, definitions after Corollary 1.3]. For the matrices defined before [1, Lemma 1.1], we use the following explicit variants:

$$F(a, c) = \begin{pmatrix} 1 - ac & a^2 \\ -c^2 & 1 + ac \end{pmatrix}, \qquad \Phi_4(a, b, c, d) = F(b, d)F(a, c)F(b, d)J^{-1}. \tag{3.1}$$

Every factor has determinant 1, and $\Phi_4(1, 0, 0, 1) = I_2$. If $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ has determinant 1, conjugating $L(-1)U(1)L(-1) = J$ by α gives

$$\Phi_4(a, b, c, d) = \alpha\alpha^T. \tag{3.2}$$

For five free arguments define

$$W = \Phi_4(1+ae, be, ce, 1+de), \qquad \Phi_5(a,b,c,d,e) = \begin{pmatrix} W_{11} & eW_{12} \\ W_{21}/e & W_{22} \end{pmatrix}. \tag{3.3}$$

Here $W|_{e=0} = I_2$, so W_{21}/e is an integer polynomial, defined also at $e = 0$. The determinant identity for W gives $\det \Phi_5 = 1$ as a polynomial identity.

With q an indeterminate and all v_i free, set

$$\begin{aligned} D_j(q;\mathbf{v}) &= D_j(qv_1,\dots,qv_j), & C_j(q;\mathbf{v}) &= C_j(qv_1,\dots,qv_j), \\ \widehat{X}_4(q;\mathbf{v}) &= \Phi_4(1+q^2v_1, qv_2, qv_3, 1+q^2v_4), & & \\ \widehat{X}_5(q;\mathbf{v}) &= \Phi_5(q^2v_1, qv_2, qv_3, q^2v_4, v_5), & \widehat{Y}_5(q;\mathbf{v}) &= \widehat{X}_5(q;\mathbf{v})^T. \end{aligned} \tag{3.4}$$

All entries belong to $\mathbb{Z}[q,\mathbf{v}]$. To check their congruences, expand (3.1) modulo q^2:

$$\widehat{X}_4 \equiv \begin{pmatrix} 1 & q(v_2+v_3) \\ q(v_2+v_3) & 1 \end{pmatrix}, \qquad \widehat{X}_5 \equiv \begin{pmatrix} 1 & qv_5^2(v_2+v_3) \\ q(v_2+v_3) & 1 \end{pmatrix} \pmod{q^2}.$$

For the lower-left entry of the second matrix, the remainder before division is divisible by both q^2 and v_5, hence by q^2v_5. The elementary products have the same diagonal and off-diagonal divisibilities, since these are preserved under multiplication. Consequently every matrix takes values in

$$G(q) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : q \mid b, c, \quad q^2 \mid a-1, d-1 \right\} \quad (q \geq 2),$$

and every matrix is I_2 at $q = 0$.

3.2 Coverage of the fixed factorization

Throughout [1, Section 5], including Proposition 5.9, the level is an integer $q \geq 2$. With $G(q)$ as defined above, the factor sets used there are

$$X_4(q) = \{\alpha\alpha^T : \alpha \in G(q)\}, \qquad Y_5(q) = \{(x^{-1})^T : x \in X_5(q)\},$$

where $X_5(q)$ consists of the products

$$\begin{pmatrix} 1+aq^2e & bqe^2 \\ cq & 1+dq^2e \end{pmatrix} \begin{pmatrix} 1+aq^2e & cqe^2 \\ bq & 1+dq^2e \end{pmatrix}, \qquad a,b,c,d,e \in \mathbb{Z}, \tag{3.5}$$

subject to the first factor having determinant 1.

Remark 3.1 (Corrections to the congruence factorization). The following corrections to [1, pp. 1000, 1006] are used here.

1. In (3.5), the upper-right entry of the second factor is cqe^2. With the printed entry cq^2e^2, its determinant would instead be
$$1 - bcq^2e^2(q-1).$$
2. Corollary 5.7 gives $\alpha = \left(\begin{smallmatrix} a & bq \\ cq & d \end{smallmatrix}\right) \in G(q)$, where $|b|, |c|$ are odd primes prime to q and $\gcd(|b|-1, |c|-1) = 2$. Thus Proposition 5.9 must choose
$$m \in \frac{|b|-1}{2}\mathbb{Z}_{>0}, \qquad n \in \frac{|c|-1}{2}\mathbb{Z}_{>0}, \qquad n - m = 1.$$

The halved integers are coprime, so such positive m, n exist. Fermat's theorem and $a \equiv 1 \pmod{q^2}$ give

$$a^{2m} \equiv 1 \pmod{bq^2}, \qquad a^{2n} \equiv 1 \pmod{cq^2}.$$

Lemma 5.8 applies to every positive exponent. Its application here produces a matrix in $G(q)$ with lower row $(\pm bq, a^{2m})$; the display for σ_1 on p. 1006 omits this factor q. For completeness, write this matrix as $\sigma = \left(\begin{smallmatrix} r & s \\ \varepsilon bq & a^{2m} \end{smallmatrix}\right)$, where $\varepsilon = \pm 1$. Its determinant gives $r \equiv 1 \pmod{b}$, while $\sigma \in G(q)$ gives $r \equiv 1 \pmod{q^2}$. Consequently

$$\sigma = U\left(\frac{r-1}{\varepsilon bq}\right) L(\varepsilon bq) U\left(\frac{a^{2m}-1}{\varepsilon bq}\right) \in D_3(q; \mathbb{Z}^3),$$

since all three arguments lie in $q\mathbb{Z}$. The transposed argument uses the second congruence, and the final step uses $\alpha^{-2m}\alpha^{2n} = \alpha^2$. No subsequent step requires $|b| - 1 \mid m$ or $|c| - 1 \mid n$.

We now check that these factor sets are covered by (3.4). For $X_4(q)$ this follows from (3.2), using the normalized entries of $\alpha \in G(q)$ as the four free arguments. For $e \neq 0$, put $D_e = \operatorname{diag}(e, 1)$ and $\alpha = \left(\begin{smallmatrix} 1+aq^2e & bqe \\ cqe & 1+dq^2e \end{smallmatrix}\right)$. The two factors in (3.5) are $D_e \alpha D_e^{-1}$ and $D_e \alpha^T D_e^{-1}$. Since $\det \alpha = 1$, (3.2)–(3.3) give

$$D_e \alpha \alpha^T D_e^{-1} = \Phi_5(aq^2, bq, cq, dq^2, e) = \widehat{X}_5(q; a, b, c, d, e).$$

At $e = 0$ the product in (3.5) is $L(q(b + c))$. Here the same arguments cannot in general be used, since

$$\widehat{X}_5(q; a, b, c, d, 0) = L(q(b + c) - 2q^2(a + d)).$$

Instead, the preimage $(0, b, c, 0, 0)$ gives $L(q(b + c))$. Thus the set inclusion $X_5(q) \subseteq \Phi_5(q^2\mathbb{Z}, q\mathbb{Z}, q\mathbb{Z}, q^2\mathbb{Z}, \mathbb{Z})$ asserted in [1, p. 1000] remains valid, including $e = 0$; only the direct choice of preimage changes at that specialization. Replacing (a, b, c, d) by $(d, -c, -b, a)$ reverses and inverts the two factors, so $X_5(q)$ is closed under inversion. Hence Vaserstein's $Y_5(q) = (X_5(q)^{-1})^T$ is covered by $\widehat{Y}_5$.

Suppressing the level and the free arguments, form the following polynomial matrix, with independent arguments at each occurrence:

$$\begin{aligned} \mathcal{P}(q; \theta) = {} & C_6 \widehat{X}_5 D_4 \widehat{Y}_5 C_6 \widehat{X}_5 C_6 \widehat{X}_4 \\ & \cdot C_5 \widehat{Y}_5 C_4 \widehat{X}_5 D_6 \widehat{Y}_5 D_6 \widehat{X}_4 \\ & \cdot C_3 \widehat{X}_5 D_2 \widehat{X}_5 U(q) \widehat{Y}_5 C_2. \end{aligned} \tag{3.6}$$

The elementary products use 50 parameters, the nine five-parameter matrices use 45, and the two four-parameter matrices use 8. Thus $\theta \in \mathbb{Z}^{103}$. For each integer $q \geq 2$, [1, Proposition 5.9] expresses every element of $G(q)$ as this word in the original sets. The inclusions just proved supply preimages in our free polynomial matrices. Conversely, every factor in our word belongs to $G(q)$. Hence

$$\mathcal{P}(q; \mathbb{Z}^{103}) = G(q) \qquad (q \geq 2). \tag{3.7}$$

Remark 3.1 verifies the corrections needed in that factorization proof. The primes and exponents chosen in the proof of that proposition determine preimages in its factor sets. The fixed maps (3.4) and word (3.6) give joint polynomial dependence on the level and the parameters. We use the resulting 103-parameter map. Vaserstein obtains smaller counts for fixed levels in [1, Corollaries 5.10–5.11].

3.3 The full congruence subgroup and levels zero and one

Set $\Gamma(0) = \{I_2\}$ and $\Gamma(q) = \{g \in \mathrm{SL}_2(\mathbb{Z}) : g \equiv I_2 \pmod q\}$ for $q > 0$. For a free integer h put

$$T(q,h) = L(1)U(qh)L(-1) = \begin{pmatrix} 1-qh & qh \\ -qh & 1+qh \end{pmatrix}, \qquad Q(q;\theta,h) = \mathcal{P}(q;\theta)T(q,h).$$

Then $Q \in \mathrm{SL}_2(\mathbb{Z}[q,\theta,h])$, $Q - I_2$ is divisible by q, and $Q(q;\mathbb{Z}^{104}) = \Gamma(q)$ for $q \geq 2$. To see surjectivity, write the diagonal of $g \in \Gamma(q)$ as $(1+q\lambda, 1+q\mu)$. Its determinant gives $\lambda + \mu \equiv 0 \pmod q$. Choose $h \equiv -\lambda \pmod q$. The diagonal of $gT(q,h)^{-1}$ is then $(1,1)$ modulo q^2, so this matrix belongs to $G(q)$ and is attained in (3.7). This verifies directly the extra-parameter step underlying [1, Corollary 5.11].

Lemma 3.2 (Uniform congruence parametrization)**.** *There is $K \in \mathrm{SL}_2(\mathbb{Z}[q,\vartheta_1,\dots,\vartheta_{108}])$ such that $K - I_2$ is polynomially divisible by q and $K(q;\mathbb{Z}^{108}) = \Gamma(|q|)$ for every integer q, including zero.*

Proof. With the 104-parameter map Q above and four free integers t, u, v, w, set

$$K(q;\vartheta) = Q(qt;\theta,h)\,U(qu)L(qv)U(qw). \tag{3.8}$$

All four factors are polynomially congruent to I_2 modulo q. For $|q| \geq 2$ take t with $qt = |q|$ and set $u = v = w = 0$. For $q = \pm 1$ take $t = 2q$, so $qt = 2$. The first factor then covers $\Gamma(2)$. The six classes in $\mathrm{SL}_2(\mathbb{F}_2)$ have representatives I_2, U, L, UL, LU, ULU, where $U = U(1)$ and $L = L(1)$. All six occur in the last three factors. Thus the product covers $\mathrm{SL}_2(\mathbb{Z})$. At $q = 0$ the formula is identically I_2. □

4 Pairwise coprime block products

All the Bézout identities in this section hold in the integer polynomial ring, before specialization.

Lemma 4.1 (A primitive column with prescribed residues)**.** *Let $a, w, P, Q \in \mathcal{R} = \mathbb{Z}[s_1,\dots,s_N]$. Suppose each of (a,P), (w,Q) and (P,Q) generates the unit ideal. With 108 new free integer parameters one can construct a polynomial determinant-one matrix whose first column $(A,u)^T$ is congruent to $(a,w)^T$ modulo PQ. At each specialization its first columns range over all primitive integer columns in that residue class. Modulo zero, the condition means equality.*

Proof. Choose polynomial inverses r of a modulo P and s of w modulo Q from the given Bézout identities. Put $x = (w-1)r$ and $y = (a-1)s$. The matrices

$$H_P = \begin{pmatrix} a & -1 \\ 1+ax & -x \end{pmatrix}, \qquad H_Q = \begin{pmatrix} 1+wy & y \\ w & 1 \end{pmatrix}$$

have determinant one. Their first columns are $(a,w)^T$ modulo P and Q, respectively. These two moduli generate the unit ideal by hypothesis. Lemma 2.8 therefore gives a single polynomial matrix H agreeing with both, without subdivision. Its first column has the required residue modulo PQ since comaximal ideals intersect in their product. Take $K(PQ;\vartheta)H$. For $PQ \neq 0$, Lemmas 2.7 and 3.2 give every primitive column with the same residue. For $PQ = 0$ the first column of H equals $(a,w)^T$ and $K(0) = I_2$. □

In particular (A,P) generates the unit ideal by (2.1), and (A,u) does so by the determinant. Equation (2.2) gives a polynomial Bézout identity for (A,Pu). Whenever $\gcd(a,w) = 1$ at a specialization, the original column $(a,w)^T$ itself is attained.

Proposition 4.2 (Pairwise coprime products)**.** *Partition N coordinates into blocks $I_1, \dots, I_h$, and put $X_j(x) = \prod_{\nu \in I_j} x_\nu$. There is an integer-polynomial map Φ on unrestricted integer parameters whose image is exactly*

$$\{x \in \mathbb{Z}^N : \gcd(X_i(x), X_j(x)) = 1 \text{ for } i < j\}.$$

There are polynomial outputs R_{ij}, S_{ij} with $X_i(\Phi)R_{ij} + X_j(\Phi)S_{ij} = 1$ identically for every $i < j$.

Proof. It suffices to maintain a polynomial Bézout identity for each pair of coordinates in different blocks. These identities combine to give the product identities by (2.2). Order the coordinates block by block, starting with the first block free. When a new coordinate a of block k is added as a free integer, every existing coordinate lies in blocks $1, \dots, k$. Retain the identities among the existing coordinates and visit those in blocks $1, 2, \dots, k-1$ in increasing block order, using a fixed order within each block.

At the coordinate w of block j, let P be the product of the coordinates already visited, and Q the product of all coordinates in blocks strictly after j, omitting a itself. The pair (a, P) has a Bézout identity from the preceding visits. Each coordinate in P and also w belongs to a different block from every coordinate in Q. Thus (P, Q) and (w, Q) have identities from the old pairs. Empty products cause no exception. Apply Lemma 4.1 and replace (a, w) by its first column (A, u). This supplies the new identity for the visited pair. The congruences modulo P preserve all previous identities between a and visited coordinates. They also preserve the identities between w and earlier blocks. The congruences modulo Q preserve those between w and later blocks. Every other old pair is unchanged. Polynomial witnesses for each preservation follow from (2.1).

For a prescribed target, attain the old coordinates by induction and start a at its target value. At each visit the target pair is primitive, so the lemma can return both coordinates exactly. This proves coverage, also when some target coordinates vanish. The number of visits is fixed by the block sizes, and each visit uses a single polynomial matrix. Hence the construction gives one polynomial map. □

Remark 4.3. Both entries of the column are allowed to move. In contrast, suppose one tried to cover all coprime pairs by finitely many maps $(W, \mathbf{v}) \mapsto (A(W, \mathbf{v}), W)$, with W retained as an unrestricted free parameter. At $W = 0$, each polynomial $A(0, \mathbf{v})$ takes only the values ± 1 and is therefore constant. Thus each map has $A \equiv 1$ or $-1 \pmod{W}$ and misses the pair $(2, 5)$. The simultaneous column operation avoids this obstruction; its coverage proof can still return any prescribed primitive target pair exactly.

5 Proof of Theorem A: monomial coefficients

Lemma 5.1 (Monomials omitting a block)**.** *Suppose the products $P_1, \dots, P_h$ of disjoint blocks of polynomial coordinates have polynomial pairwise Bézout identities. Let $B_1, \dots, B_s$, with $s \geq 1$, be monomials with coefficients 1 or -1 in these coordinates. Suppose that for each block j at least one $B_{i(j)}$ contains no coordinate of block j. Then $B_1, \dots, B_s$ have polynomial Bézout identities.*

Proof. Choose $E \geq 1$ at least as large as every exponent in the B_i. For every pair of blocks choose a Bézout identity between P_j^E and P_k^E by Lemma 2.3, and multiply all these identities. Each term of the expansion contains P_j^E for all but at most one index j, since the factor for a pair supplies one of its two indices. If the missing index is k, the term is a multiple of $B_{i(k)}$. If none is missing, use any B_i. Grouping terms gives the identity. With one block the omitted monomial is a unit. With no blocks every monomial is a unit. □

Proof of Theorem A. Write e_i for the exponent vector of M_i, including $i = 0$. First consider targets with all $x_k \neq 0$. For $1 \leq i \leq s$ put

$$E_i = \{v \in \mathbb{R}^n_{\geq 0} : e_i \cdot v \leq e_j \cdot v \text{ for } 1 \leq j \leq s\}.$$

We first separate the fixed factors coming from c. For $c \neq 0$ take the Hilbert basis, given by Gordan's lemma, of each cone

$$\{(v, t) : v \in E_i,\ t \geq 0,\ (e_i - e_0) \cdot v \leq t\}.$$

Write $(g, 0)$ for its generators of last coordinate zero. Give each generator (g, t_g) with $t_g > 0$ a positive integer d_{ig}, with the single fixed product $\prod_{i,g:t_g>0} d_{ig}^{t_g} = |c|$. There are finitely many choices. Generators with $g = 0$ (in particular $(0, 1)$) are retained: they may absorb prime factors of c but do not alter the coordinates. Set $h_k = \prod_{i,g:t_g>0} d_{ig}^{g_k}$. When $c = 0$, take $h_k = 1$ and use $(g, 0)$ for the generators of E_i itself, with a zero appended.

Here is why these choices suffice. At a prime p, let $v = (v_p(x_1), \ldots, v_p(x_n))$ and select an i minimizing $e_i \cdot v$. If $c \neq 0$, the equation implies $e_i \cdot v \leq e_0 \cdot v + v_p(c)$, since every term on the left is divisible by $p^{e_i \cdot v}$. Decompose $(v, v_p(c))$ in the chosen cone. For $c = 0$ just decompose v in E_i. Multiplying the assigned prime powers for each generator gives the stated constants d_{ig} and positive integers u_{ig} for the generators $(g, 0)$. The products of the u_{ig} in different blocks i are coprime, because each prime was assigned to only one block. Only the primes in $c \prod_k x_k$ need be considered when $c \neq 0$, and only the primes in $\prod_k x_k$ when $c = 0$.

Apply Proposition 4.2 with blocks indexed by $i = 1, \ldots, s$: block i consists of the coordinates u_{ig} for the generators $(g, 0)$ of its cone. Empty blocks are allowed and have product 1, as required also in Lemma 5.1. Now allow these polynomial outputs u_{ig} to vary and fix signs $\varepsilon_k = \pm 1$. Write $\varepsilon^e = \prod_k \varepsilon_k^{e_k}$ and set

$$X_k = \varepsilon_k \prod_{i,g} u_{ig}^{g_k}, \qquad G = \prod_{i,g} u_{ig}^{e_i \cdot g},$$
$$B_j = \varepsilon^{e_j} \prod_{i,g} u_{ig}^{(e_j - e_i) \cdot g} \qquad (1 \leq j \leq s).$$

Then $x_k = h_k X_k$ and $M_j(X) = GB_j$. If $c \neq 0$, define $D = \varepsilon^{e_0} \prod_{i,g} u_{ig}^{(e_0 - e_i) \cdot g}$, so $M_0(X) = GD$. All these exponents are nonnegative by the cone inequalities. For $c = 0$ put $D = 0$. The monomial B_i omits block i. Lemma 5.1 therefore gives polynomial coefficients W_j with $\sum_j B_j W_j = 1$. Apply Lemma 2.10 with $\Lambda = 1$ to

$$\sum_j B_j Y_j = cM_0(h)D.$$

Retain the fixed divisibilities $\alpha_j M_j(h) \mid Y_j$ and output $y_j = Y_j/(\alpha_j M_j(h))$ by Lemma 2.1. Multiplying the displayed equation by G proves the required identity, including specializations with $G = 0$. At a target the valuation construction has $G \neq 0$. Hence its $Y_j = \alpha_j M_j(h) y_j$ satisfy the displayed equation and are all attained by the linear formula.

Finally fix the zero coordinates of a target. Delete the coefficient monomials they annihilate and leave the corresponding y_j free. If M_0 vanishes, take zero right-hand side. Apply the preceding argument to the surviving equation. If no coefficient survives, all y_j are free when the right-hand side vanishes, and otherwise there are no targets in this pattern. Fixing the chosen zeros makes each deletion a polynomial identity, so further zeros in the resulting families are harmless. There are finitely many patterns. □

6 Uniform matrix parametrizations over quadratic orders

Throughout Sections 6–10, F is a fixed quadratic field, $\mathcal{O} = \mathbb{Z}[\omega]$ is its full ring of integers, D_F is its discriminant, and $\bar{a}$ denotes conjugation. Write $\omega^2 = \tau\omega + \rho$ with $\tau, \rho \in \mathbb{Z}$. The element $a = a_0 + a_1\omega$ is called *coordinate-primitive* if $\gcd(a_0, a_1) = 1$, and we write $\mathrm{col}(a) = (a_0, a_1)^T$. We identify polynomial maps with values in $\mathcal{O}$ with their two integer coordinate polynomials. Comaximality of elements refers to their generated ideals in $\mathcal{O}$, not to their coordinate columns. For the standard arithmetic of quadratic fields we refer to [13]; for ray class fields (with real places when prescribed) and Chebotarev's density theorem we refer to [14, 15].

Set $R_n = \mathbb{Z} + n\mathcal{O}$, and let $\mu \in \{2, 4, 6\}$ be the number of roots of unity in F. In this section n ranges over the positive integers prime to μ. A row (a, b) over R_n is *unimodular* if $aR_n + bR_n = R_n$; a completion is a matrix in $\mathrm{SL}_2(R_n)$ with first row (a, b).

Definition 6.1 (Uniform boundedness)**.** A family $S_n \subseteq \mathrm{SL}_2(R_n)$ is *uniformly bounded* if there are finitely many fixed matrices $\Phi_k \in \mathrm{SL}_2(\mathbb{Z}[v_1, \dots, v_N])$ such that

$$S_n \subseteq \bigcup_k \Phi_k(R_n^N) \qquad \text{for every admissible } n.$$

The matrices and the number of parameters are independent of n. A family of pairs $(M, M') \in \mathrm{SL}_2(R_n)^2$ is uniformly bounded if there are uniformly bounded families of left and right multipliers such that each pair satisfies $M' = XMY$ for some multipliers X, Y in those families. For families of unimodular rows we write $(a, b) \sim (c, d)$ if the family of all pairs of their determinant-one completions is uniformly bounded in this sense. For polynomial row expressions, the notation also asserts that the two rows are unimodular simultaneously at every specialization.

Lemma 6.2 (Uniform boundedness operations)**.** *Uniform boundedness has the following properties.*

1. *Subfamilies, finite unions, products of a fixed number of factors, inverses and transposes preserve uniform boundedness.*

2. *The relation on pairs is reflexive, symmetric and transitive. A family uniformly related to a uniformly bounded family is itself uniformly bounded.*

3. *Changing a completion of a fixed first row is uniformly bounded. The elementary row operations*

$$(a, b) \sim (a + bc, b), \qquad (a, b) \sim (a, b + ac)$$

   are uniform, as are multiplication by fixed integer determinant-one matrices and the relation between M^{-1} and M^T.

4. *All completions of rows having a unit entry are uniformly bounded.*

Proof. Products, inverses and transposes of universal determinant-one polynomial matrices are again such matrices. The rules for pairs follow by multiplying and inverting the left and right multipliers. Two completions of the same first row differ by one elementary left shear. Right elementary shears give the displayed row operations, and $M^T = JM^{-1}J^{-1}$. Finally a row with a unit entry reduces by shears and, if needed, a fixed interchange to $(u, 0)$ with u a unit. The identity

$$\mathrm{diag}(u, u^{-1}) = U(u)L(-u^{-1})U(u)J^{-1}$$

provides a fixed elementary word for its completions. All parameters, including inverses of units when chosen numerically, lie in R_n; the polynomial words and their lengths do not vary with n. These are the uniform forms of the operations in [9, Lemmas 1.1–1.2]. □

The relation $\sim$ records the existence of values of these fixed polynomial maps. The auxiliary entries selected in its proof need not themselves be polynomial functions of the original row.

Lemma 6.3 (Primes with ray-class and splitting prescriptions)**.** *Let E be a number field, $\mathfrak{m}$ a modulus, with any prescribed real places included, and $E_{\mathfrak{m}}$ its ray class field. Let L/E be a finite Galois extension linearly disjoint from $E_{\mathfrak{m}}$ over E. Every ray class modulo $\mathfrak{m}$ contains infinitely many prime ideals of absolute residue degree one (their residue fields have prime order) that split completely in L. They may be required to avoid any finite set of prime ideals; the resulting set has positive Dirichlet density.*

In particular, given a unit residue modulo the finite part of $\mathfrak{m}$ and prescribed signs at its real places, there are prime elements with that residue and those signs, whose principal ideals have residue degree one. The same auxiliary splitting condition is permitted under the stated disjointness hypothesis.

Proof. The ray-class Artin isomorphism and the existence of its class field are given in [14, Chapter V, Theorems 3.5–3.6]. Disjointness identifies the Galois group of $LE_{\mathfrak{m}}/E$ with the product of the two Galois groups. Prescribe the ray-class Frobenius in the first factor and the identity in the second. Chebotarev's theorem [14, Chapter V, Theorem 3.23] gives positive density. Prime ideals of residue degree greater than one have density zero, and deleting finitely many primes does not change the conclusion. For the last assertion, choose an integral representative α of the desired residue and signs by approximation, and use the ray class of (α). A prime ideal in this class has a generator $\alpha\gamma$, where $\gamma \equiv 1$ at the finite part of the modulus and is positive at its prescribed real places. This generator is integral and has the required residue and signs. □

Lemma 6.4 (Prime selection in the orders)**.** *Let (a, b) be unimodular in R_n with $b \neq 0$. There are elements $p \in R_n$ that are prime elements of $\mathcal{O}$, of residue degree one, such that $p \equiv a \pmod{bR_n}$ and $(p, n\mathcal{O}) = \mathcal{O}$. One may exclude finitely many rational primes, prescribe real signs, and prescribe a unit residue modulo a further ideal coprime to $bn\mathcal{O}$. One may also require (p) to split completely in a finite Galois extension of F linearly disjoint from the ray class field whose finite modulus is $bn\mathcal{O}$ times the extra ideal and whose infinite part consists of the prescribed real places.*

If $c \in R_n$ is coprime to $n\mathcal{O}$, the natural map $R_n/cR_n \longrightarrow \mathcal{O}/c\mathcal{O}$ is an isomorphism.

Proof. Choose $h \in \mathbb{Z}$ such that $a + bh$ is a unit modulo $n\mathcal{O}$. At each rational prime dividing n, the residues of a, b are scalars and are not both zero, so at most one residue for h is forbidden. Also $a + bh$ is a unit modulo $b\mathcal{O}$. Apply Lemma 6.3 to its residue modulo $bn\mathcal{O}$, the additional residue and the desired signs. The resulting prime element satisfies $p = a + b(h + nu)$ for some $u \in \mathcal{O}$, proving the congruence in R_n.

For the quotient map, n is invertible modulo $c\mathcal{O}$ and $n\mathcal{O} \subset R_n$, giving surjectivity. If $cy \in R_n$ and $y \in \mathcal{O}$, then modulo $n\mathcal{O}$ the scalar c is a unit whose inverse is scalar. Hence y is scalar modulo $n\mathcal{O}$ and lies in R_n, proving injectivity. □

Lemma 6.5 (Uniform single cancellation and powers)**.** *For all these orders the relations*

$$(1 + ab, b^2c) \sim (1 + ab, c), \qquad (1 + ab, bc) \sim (1 + ab, c)$$

are uniform. Moreover, if $M \in \mathrm{SL}_2(R_n)$ has first row (a, b) and M^j has first row (a_j, b_j), then $(a_j, b_j) \sim (a^j, b)$ uniformly even as the positive integer j varies.

Proof. Both rows in each claimed cancellation are unimodular simultaneously, since b is invertible modulo $1 + ab$. For the first relation use the universal matrix Φ_5 in (3.3), as in [9,

Proposition 1.3]. If $(1+ab, b^2c)$ is unimodular, choose $d, f \in R_n$ with $(1+ab)d - bcf = -a$. Then $X = I_2 + b\left(\begin{smallmatrix} a & c \\ f & d \end{smallmatrix}\right)$ has determinant one. For $b \neq 0$, equations (3.2)–(3.3) give

$$\Phi_5(a,c,f,d,b) = \begin{pmatrix} 1+ab & b^2c \\ f & 1+bd \end{pmatrix} \begin{pmatrix} 1+ab & b^2f \\ c & 1+bd \end{pmatrix}.$$

The first factor is therefore related by bounded multipliers to the inverse of the second, and the latter inverse is related to its transpose by fixed determinant-one matrices. This proves the relation; when $b = 0$ the first entries are 1 and both rows are bounded.

For single cancellation write $x = 1 + ab$. A unit first entry gives bounded completions; if $x = 0$, primitivity makes the second entries units. The zero cases for a, b, c are immediate as well. Each replacement below is made on both rows by the corresponding elementary shear; the two shear parameters need not be equal. Since shears and their inverses are uniformly bounded, proving the relation after a replacement proves it before that replacement. Replace c by $c_1 = c + x(1-c)$, a shear on each row. Since (x, c_1) is unimodular and x is a nonunit, $c_1 \neq 0$. Also $c_1 \equiv 1 \pmod{aR_n}$. Hence Lemma 6.4 supplies a prime $q \equiv a \pmod{c_1 R_n}$ avoiding $2n$. Changing a to q is again a shear on both rows. Put $x' = 1 + qb$ and handle a zero or unit x' as above. The quadratic extension $F(\sqrt{-q})/F$ is ramified at (q) by Eisenstein's criterion. The ray class field of $x'n\mathcal{O}$ is unramified there, since (q) divides neither x' nor n. The two fields are therefore disjoint. By Lemma 6.4 choose a prime $p \equiv c_1 \pmod{x'R_n}$ splitting in $F(\sqrt{-q})$, away from $2nq$. Then $q \equiv -r^2 \pmod{pR_n}$ for some $r \in R_n$, using the quotient isomorphism of the lemma. Changing c_1 to p is a shear, and

$$(1+qb, bp) \sim (1 - r^2 b, bp) \sim (1 - r^2 b, r^2 b^2 p) \sim (1 - r^2 b, p) \sim (1 + qb, p).$$

The third equivalence is square cancellation with factor rb. The other steps are shears. This proves single cancellation in a fixed number of bounded operations, as required.

For the power relation use Cayley–Hamilton. With $u_0 = 0$, $u_1 = 1$, $u_{j+1} = tu_j - u_{j-1}$, one has $M^j = u_j(\operatorname{tr} M)M - u_{j-1}(\operatorname{tr} M)I_2$, where tr denotes matrix trace. For $j \geq 2$, the identity $u_j u_{j-2} = u_{j-1}^2 - 1$ in $\mathbb{Z}[t]$ permits a factorization $u_j = v_j w_j$ with $v_j \mid u_{j-1} - 1$ and $w_j \mid u_{j-1} + 1$, by unique factorization in $\mathbb{Z}[t]$; for $j = 2$ take $v_j = u_j, w_j = 1$. After evaluating at the trace, $b_j = bv_j w_j$, $a_j \equiv -1 \pmod{v_j}$ and $a_j \equiv 1 \pmod{w_j}$. To make the first cancellation explicit, write $u_{j-1} + 1 = w_j z_j$. Then

$$a_j = 1 + w_j k_j, \qquad k_j = v_j a - z_j.$$

Single cancellation with $(a, b, c) = (k_j, w_j, bv_j)$ removes w_j. If both factors are nonzero, we can then change both signs and cancel v_j:

$$(a_j, bv_j w_j) \sim (a_j, bv_j) \sim (-a_j, -bv_j) \sim (-a_j, -b) \sim (a_j, b).$$

The second cancellation applies because $-a_j \equiv 1 \pmod{v_j}$. Otherwise $u_j(\operatorname{tr} M) = 0$ and M^j is a scalar determinant-one matrix, so $a_j = \pm 1$ and $b_j = 0$. In this case $a^j \equiv a_j \pmod{b}$ gives $(a^j, b) \sim (a_j, b)$ directly by a shear, and both rows have uniformly bounded completions. In all cases $a_j \equiv a^j \pmod{b}$. The number of bounded operations does not depend on j, even though the numerical factor values do. The case $j = 1$ is immediate. This adapts [9, Proposition 1.5], using the uniform cancellation just proved for these orders. □

Lemma 6.6 (Uniform power-row boundedness)**.** *The completions of all unimodular rows (a^μ, b) in the R_n are uniformly bounded.*

Proof. Assume nonzero nonunit entries, the remaining cases being bounded immediately. Replace b modulo $a^\mu R_n$ by a degree-one prime element coprime to $n\mu\mathcal{O}$ by Lemma 6.4 applied

to (b, a^μ). Continue to denote the new prime element by b, and fix a completion M of this new row (a, b) in $\mathrm{SL}_2(R_n)$. We use the Carter–Keller lemma exactly in the general-ideal form of [9, Lemma 1.6 and Remark 1.7]: for a prime element b of residue characteristic prime to μ, an ideal $\mathfrak{a}$ coprime to (b), and a unit u, one can choose nonzero c with $bc \equiv u \pmod{\mathfrak{a}}$ such that $\gcd(\epsilon(b), \epsilon(c)) = \mu\gamma$, where $\epsilon(c)$ is the exponent of $(\mathcal{O}/c\mathcal{O})^\times$, all rational prime divisors of γ divide D_F, and γ can be chosen to avoid any one prescribed rational prime ramifying in F. Apply this with $\mathfrak{a} = an\mathcal{O}$ and $u = -1$. For each distinct rational prime $\ell \mid D_F$, choose c_ℓ with γ_ℓ avoiding ℓ. Then $bc_\ell \equiv -1 \pmod{an\mathcal{O}}$. This stronger congruence ensures c_ℓ is a scalar unit modulo $n\mathcal{O}$ (since b is), so $c_\ell \in R_n$, and

$$d_\ell = (1 + bc_\ell)/a \in n\mathcal{O} \subset R_n.$$

In particular the matrix $M_\ell = \left(\begin{smallmatrix} a & b \\ c_\ell & d_\ell \end{smallmatrix}\right)$ lies in $\mathrm{SL}_2(R_n)$. Both b and c_ℓ are prime to $n\mathcal{O}$; for c_ℓ this follows from $bc_\ell \equiv -1 \pmod{n\mathcal{O}}$. The quotient isomorphism in Lemma 6.4 therefore identifies the exponents used in the Carter–Keller lemma with those of the corresponding quotient rings of R_n.

Let $E_\ell = \mu\gamma_\ell$. For any positive multiple j of E_ℓ we can find positive integers t, v such that $t - v = j$, $\epsilon(b) \mid t$, $\epsilon(c_\ell) \mid v$, by the gcd condition. The power relation of Lemma 6.5 makes M_ℓ^t uniformly bounded: its row is bounded relative to $(a^t, b) \sim (1, b)$ by the unit-exponent condition. The first row of M_ℓ^T is (a, c_ℓ), and $a^v \equiv 1 \pmod{c_\ell R_n}$. Applying the same relation to this transpose, and then transposing back, gives boundedness of M_ℓ^v. Thus $M_\ell^j = M_\ell^t (M_\ell^v)^{-1}$ is uniformly bounded, independently of j.

To transfer this bound to M^j, choose any determinant-one completion of (a^j, b). Lemma 6.5 relates both M^j and M_ℓ^j uniformly to that same completion. Transitivity of the relation on completion pairs in Lemma 6.2 then relates M^j uniformly to M_ℓ^j. The uniform bound for the latter therefore bounds the former. Inverses give the same for negative multiples of E_ℓ, and the zero exponent is trivial. Since $\gcd_\ell \gamma_\ell = 1$, choose integers h_ℓ with $\sum h_\ell \gamma_\ell = 1$. Then

$$M^\mu = \prod_{\ell \mid D_F} M^{h_\ell E_\ell}$$

is uniformly bounded. The integers h_ℓ may depend on the entries, which causes no difficulty: the preceding bound holds for every multiple of E_ℓ. The number of factors depends only on the fixed field. The power relation once more bounds the completions of (a^μ, b). Crucially, no varying power of a polynomial matrix is used as a parametrization: all high numerical powers are related by the fixed bounded maps of Lemma 6.5. □

Theorem 6.7 (Uniform parametrization of quadratic orders)**.** *There exist an integer N and a fixed polynomial matrix $\mathcal{L}(\mathbf{v}) \in \mathrm{SL}_2(\mathbb{Z}[\mathbf{v}])$, where $\mathbf{v} = (v_1, \ldots, v_N)$, such that $\mathcal{L}(R_n^N) = \mathrm{SL}_2(R_n)$ for every positive integer n with $\gcd(n, \mu) = 1$.*

Proof. We reduce a unimodular row (a, b) to a μth-power row in a fixed number of shears. Zero or unit entries already give bounded completions. First replace b by $b + ta$ so that it is a unit modulo every prime above μ. Such $t \in R_n$ exists by CRT, since n is prime to μ and R_n surjects onto these residue fields jointly. If the resulting b is zero, a is a unit and the row is already bounded.

For each rational prime $\ell \mid \mu$, choose a prime ideal $\mathfrak{l} \mid \ell$ and an element $\pi_\mathfrak{l} \in \mathfrak{l} \setminus \mathfrak{l}^2$. By Lemma 6.4 choose a degree-one prime $a' \equiv a \pmod{bR_n}$ avoiding $n\mu$ and satisfying $a' \equiv 1 + \pi_\mathfrak{l} \pmod{\mathfrak{l}^2}$ for every chosen $\mathfrak{l}$. These extra ideals are coprime to $bn\mathcal{O}$. Let $\mathbb{L} = F(\sqrt[\mu]{a'})$. The polynomial $X^\mu - a'$ is Eisenstein at (a'), and F contains the μth roots of unity. Thus $\mathbb{L}/F$ is cyclic of degree μ. For each $\ell \mid \mu$ its unique degree-ℓ subfield is $F(\sqrt[\ell]{a'})$. This subfield is ramified at the chosen $\mathfrak{l}$, because $(X + 1)^\ell - a'$ is Eisenstein there.

Put $\mathfrak{m} = a'n\mathcal{O}$. The ray class field $F_{\mathfrak{m}}$ is unramified at every chosen $\mathfrak{l}$. Any nontrivial subfield of the cyclic extension $\mathbb{L}/F$ contains a subfield of prime degree, so $\mathbb{L} \cap F_{\mathfrak{m}} = F$. Apply Lemma 6.4 to choose a prime $b' \equiv b \pmod{a'R_n}$, away from $a'n\mu$, splitting completely in $\mathbb{L}$. Reducing $\sqrt[\mu]{a'}$ at a prime above (b') gives a μth root of a' in $\mathcal{O}/b'\mathcal{O}$. The quotient isomorphism lifts this root to $c \in R_n$, so a final shear carries (a', b') to (c^μ, b'). Lemma 6.6 now bounds all completions. The disjointness argument uses only finite primes and applies also to real quadratic fields.

All matrix relations above use a fixed finite collection of universal determinant-one polynomial matrices (coefficients in $\mathbb{Z}$), and a fixed number of multiplications. The conductor and numerical primes only appear in their evaluations. Thus finitely many fixed maps cover all the groups. To combine them into one map, for each map $A(v)$ replace it by $A(v)A(0)^{-1}E(\lambda)$, where $E(0) = I_2$, $E(1) = A(0)$ is a polynomial elementary word over $\mathbb{Z}$ as in Lemma 2.8. The values $\lambda = 1$ and $(v, \lambda) = (0, 0)$ give, respectively, the original image and the identity; these parameter values lie in every R_n. Every value of the new map is still in $\mathrm{SL}_2(R_n)$. Taking a fixed product of these maps with independent parameter tuples covers their union, by setting all but one factor to the identity. Its whole image lies in $\mathrm{SL}_2(R_n)$, so it gives the asserted single $\mathcal{L}$. □

Remark 6.8 (Real quadratic fields). Larsen–Nguyen's square-cancellation identity and boundedness rules hold over every commutative ring, and the Carter–Keller exponent lemma used here holds over every number field. Their single cancellation and subsequent power arguments are stated for imaginary quadratic rings of integers. Their general statement for all rings of integers of number fields combines this argument with earlier results when the unit group is infinite, as explained in their introduction. Lemma 6.5 replaces the former argument and verifies the required uniform power relation in the orders R_n, for either signature. Consequently the preceding proof, including its specialization $n = 1$ in a real quadratic field, does not use bounded elementary generation. For the latter approach over rings with infinitely many units, see Carter–Keller–Paige as presented in [11], and [12].

Corollary 6.9 (Uniform field congruence matrices)**.** *For every nonzero signed integer m prime to μ, the subgroup of $\mathrm{SL}_2(\mathcal{O})$ of matrices congruent to the identity modulo $m\mathcal{O}$ is parametrized by a single fixed polynomial matrix in m and free integer parameters, with coefficients in $\mathcal{O}$ and polynomial congruence to I_2 modulo m.*

Proof. With $\mathcal{L}$ from Theorem 6.7, use

$$\mathcal{K}(m; \mathbf{r}, \mathbf{s}, \theta) = \mathcal{L}(\mathbf{r} + m\omega\mathbf{s})\mathcal{L}(\mathbf{r})^{-1}K(m; \theta).$$

All entries are polynomial and the congruence is an identity. Any target $g \equiv I_2 \pmod{m\mathcal{O}}$ belongs to $\mathrm{SL}_2(R_{|m|})$. Write it as $\mathcal{L}(\mathbf{r} + m\omega\mathbf{s})$, with $\mathbf{r}, \mathbf{s}$ integer tuples. Then $\mathcal{L}(\mathbf{r}) \equiv I_2 \pmod{m\mathcal{O}}$ has integer entries and thus lies in the integer principal congruence subgroup; K supplies it. This proves coverage. The two integral coordinates of each entry are polynomial in the indicated integer parameters. □

7 Relative Hermitian levels

For a matrix G over F, let $G^* = \bar{G}^T$. An integral binary Hermitian matrix is

$$H = \begin{pmatrix} p & w \\ \bar{w} & h \end{pmatrix}, \qquad p, h \in \mathbb{Z}, \quad w \in \mathcal{O}.$$

Write $\mathrm{Herm}_2(\mathcal{O})$ for these matrices, identified with their four integer coordinates. Fix $\eta \in \mathcal{O}$ of nonzero signed norm c and set

$$H_0 = \begin{pmatrix} 1 & \eta \\ \bar{\eta} & 0 \end{pmatrix}.$$

We need uniform parametrizations of the matrices of determinant $-c$ agreeing with H_0 modulo a variable rational integer. First we show that the integral forms of this determinant have finitely many orbits, even when $\mathcal{O}$ is not principal. Then we control those orbits at variable congruence levels.

Lemma 7.1 (Finite integral orbits)**.** *For fixed F and $c = \mathrm{N}(\eta) \neq 0$, there are finitely many integral Hermitian matrices H_j of determinant $-c$ such that every integral H of that determinant is gH_jg^* for some $g \in \mathrm{SL}_2(\mathcal{O})$. Each H_j is $C_jH_0C_j^*$ for a fixed $C_j \in \mathrm{SL}_2(F)$.*

Proof. The form is isotropic over F: when $p \neq 0$ its value on a row (x, y) is

$$p\,\mathrm{N}(x + \bar{w}y/p) - c\,\mathrm{N}(y)/p,$$

which vanishes at $y = p$, $x = \eta - \bar{w}$. When $p = 0$ the first coordinate row is isotropic. Choose a nonzero isotropic row $v = (v_1, v_2)$ and scale it by a field element so that the fractional ideal it generates is a fixed integral representative I of its ideal class. There are finitely many choices of I. Because $v_1I^{-1} + v_2I^{-1} = \mathcal{O}$, there is a row $u \in (I^{-1})^2$ with $\det \left(\begin{smallmatrix} u \\ v \end{smallmatrix}\right) = 1$. Thus $G = (u; v) \in \mathrm{SL}_2(F)$ has top row in $I^{-1} \times I^{-1}$ and bottom row in $I \times I$. Fix one matrix G_I with these properties for each representative I; it exists since every ideal of a Dedekind domain is generated by two elements. For every such G, the matrix $U = G_I^{-1}G$ belongs to $\mathrm{SL}_2(\mathcal{O})$: its entries are sums of products of an element of I and one of I^{-1}. Its determinant is one.

The transformed matrix GHG^* has the form

$$\begin{pmatrix} d & \delta \\ \bar{\delta} & 0 \end{pmatrix}, \qquad d \in (\mathrm{N}\,I)^{-1}\mathbb{Z}, \quad \delta \in I^{-1}\bar{I}, \quad \mathrm{N}(\delta) = c.$$

Here $\mathrm{N}\,I = [\mathcal{O} : I] > 0$, equivalently the positive generator of $I\bar{I} \cap \mathbb{Z}$. The restriction on d follows from $I\bar{I} = (\mathrm{N}\,I)\mathcal{O}$. The possibilities for δ are finite modulo the action $\delta \mapsto (\epsilon/\bar{\epsilon})\delta$ for $\epsilon \in \mathcal{O}^\times$. Indeed multiply the fixed fractional ideal by a fixed integer to make it integral. Elements with a given nonzero norm generate one of finitely many ideals of the corresponding absolute norm; generators of a given ideal and given norm differ by norm-one units. The group of such units modulo the image of $\epsilon \mapsto \epsilon/\bar{\epsilon}$ is finite, since that image contains the squares of the norm-one units, and the unit group is finitely generated. Real as well as imaginary quadratic fields are covered by this argument. The action is realized by multiplying u by ϵ and v by ϵ^{-1}, preserving their ideal memberships and determinant. Choose δ from a fixed finite list in this way.

For fixed I, δ, changing u to $u + \lambda v$ for $\lambda \in I^{-2}$ (the inverse square of the ideal) changes d by $\mathrm{Tr}(\lambda\bar{\delta})$, without changing δ or the determinant. The values of this trace form a nonzero additive subgroup of $(\mathrm{N}\,I)^{-1}\mathbb{Z}$: nonzero follows from nondegeneracy of the trace pairing, since I^{-2} spans F over $\mathbb{Q}$. Hence that subgroup has finite index. We may restrict d to finitely many representatives. All modified matrices G still satisfy $G = G_IU$ with $U \in \mathrm{SL}_2(\mathcal{O})$. Consequently

$$H = U^{-1}H_j(U^{-1})^*, \qquad H_j = G_I^{-1}\begin{pmatrix} d & \delta \\ \bar{\delta} & 0 \end{pmatrix}(G_I^{-1})^*.$$

There are finitely many candidates, and those occurring for an integral H are themselves integral; discard nonintegral candidates. This proves the first assertion.

For the second assertion every displayed isotropic form with determinant $-c$ is determinant-one congruent over F to H_0. Since $\mathrm{N}(\eta/\delta) = 1$, Hilbert 90 gives $\epsilon \in F^\times$ with $\epsilon/\bar{\epsilon} = \eta/\delta$

(explicitly take $\epsilon = 1 + \eta/\delta$ unless $\eta/\delta = -1$, in which case take a nonzero trace-zero element). The diagonal matrix $(\epsilon, \epsilon^{-1})$ changes the off-diagonal entry to η. A row shear and its adjoint can then set the top diagonal entry to 1, since the trace map $\lambda \mapsto \mathrm{Tr}(\lambda\bar{\eta})$ onto $\mathbb{Q}$ is surjective. All these changes have determinant one. Composing with G_I shows the existence of each fixed C_j. □

Lemma 7.2 (Variable-level Hermitian parametrization)**.** *There is a fixed positive integer B_c, depending only on F, η, with the following property. Let $m = m(\mathbf{v})$ be an integer polynomial prime to B_c at every input, and define*

$$\mathcal{T}_{\mathrm{H}}(\mathbf{v}) = \{H \in \mathrm{Herm}_2(\mathcal{O}) : \det H = -c,\ H \equiv H_0 \pmod{m(\mathbf{v})\mathcal{O}}\}.$$

There are polynomial continuations that cover every fibre of $\mathcal{T}_{\mathrm{H}}$ in the sense of Definition 2.5. In particular their outputs satisfy $p \equiv 1$, $w \equiv \eta$ and $h \equiv 0$ at the indicated level. Additional fixed coordinate congruences give the corresponding restricted fibres by Lemma 2.1.

Proof. Choose H_j, C_j from Lemma 7.1. Let $J = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ and choose a fixed $T \in \mathrm{GL}_2(F)$ with $TH_0T^* = \xi J$, where $\xi \in F^\times$ has trace zero. Such a T is obtained by first removing the upper diagonal entry of H_0 by a shear over F and then multiplying the first row by ξ/η, with the corresponding adjoint operations. In particular $\det T = \xi/\eta$; we require T to be invertible, not to have determinant one. The conjugate TgC_jT^{-1} below still has determinant one. We choose a fixed integer B_c divisible by μ, $|D_F|$, the primes in all denominators of $T, T^{-1}, C_j, C_j^{-1}, \xi, \xi^{-1}$ and by the denominators of fixed elementary decompositions of C_j^{-1} over F. We may enlarge it at any later fixed requirement.

For a numerical target $H = gH_jg^* \equiv H_0 \pmod{m\mathcal{O}}$, $g \in \mathrm{SL}_2(\mathcal{O})$, reduce all the fixed rational matrices modulo m using the invertibility of their denominators. The matrix

$$V = TgC_jT^{-1} \pmod{m\mathcal{O}}$$

has determinant one and stabilizes ξJ in the sense $V J \bar{V}^T = J$. A determinant-one matrix over a commutative ring satisfies $VJV^T = J$, so $V = \bar{V}$. The fixed elements of conjugation in $\mathcal{O}/m\mathcal{O}$ are precisely the scalar classes $\mathbb{Z}/m\mathbb{Z}$: in the basis $1, \omega$, the fixed condition is that the second coordinate times $\omega - \bar{\omega}$ vanishes, and this difference is a unit since m is coprime to D_F. Thus V is in $\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$.

Take a positive fixed integer D_{lift} supported on the same primes as B_c and sufficiently divisible that, whenever $W \in \mathrm{SL}_2(\mathbb{Z})$ and $W \equiv I_2 \pmod{D_{\mathrm{lift}}}$, the matrix

$$C_jT^{-1}(W^{-1} - I_2)TC_j^{-1}$$

is integral over $\mathcal{O}$. Indeed $W^{-1} - I_2$ is also entrywise divisible by D_{lift}, and the other denominators are fixed. Lift V to $W \in \mathrm{SL}_2(\mathbb{Z})$ with $W \equiv I_2 \pmod{D_{\mathrm{lift}}}$, by the Chinese remainder theorem and surjectivity of $\mathrm{SL}_2(\mathbb{Z})$ onto $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ for every $N \geq 1$: the latter follows by elementary elimination over each ring $\mathbb{Z}/p^k\mathbb{Z}$, where a unimodular column has a unit entry, followed by CRT and lifting the elementary entries to integers. The two moduli are coprime. Put $h_0 = T^{-1}WT$. This stabilizes H_0 exactly, has determinant one, and agrees with gC_j modulo m. The matrix

$$g' = gC_jh_0^{-1}C_j^{-1}$$

belongs to $\mathrm{SL}_2(\mathcal{O})$ by the choice of D_{lift}. Moreover $H = g'H_j(g')^*$ and $g' \equiv C_j^{-1} \pmod{m\mathcal{O}}$. This also works at $m = \pm 1$, where the congruences are vacuous.

It remains to realize the last residue by a polynomial seed. Fix an elementary decomposition of C_j^{-1} over the field F (elementary elimination over a field gives such a decomposition). Choose a common positive fixed denominator D for the elementary entries, including their coefficients

in the integral basis. For each residue $m \equiv b \pmod{D}$ coprime to D, choose an integer k_b with $k_b b \equiv 1 \pmod{D}$. Replace each elementary entry a/D by $a(1-k_b m)/D$, where $a \in \mathcal{O}$ is fixed. The resulting product S_j is a determinant-one polynomial seed with integral coordinates after fixed residue subdivision, congruent to C_j^{-1} modulo $m\mathcal{O}$ at all inputs. Indeed $(1-k_b m)/D$ is an integer on this branch and represents the inverse of D modulo m. The elementary product remains determinant one independently of the congruences. Now the polynomial map

$$g_1 = \mathcal{K}(m;\cdot)S_j, \qquad H = g_1 H_j g_1^*$$

from Corollary 6.9 has the required determinant, integral coordinates and congruences. It attains each target because $g' S_j^{-1} \equiv I_2 \pmod{m}$ and the field congruence map attains that matrix. This argument applies at every specialization of every retained branch of the original data; no condition on a variable modulus has been imposed by filtering. There are finitely many seeds and fixed residue choices, all depending on fixed data only. This proves fibrewise coverage. □

7.1 Relative insertion of norm-coprime integers

Fix once and for all an odd rational prime ℓ_0 which is the positive norm of a degree-one prime element $\eta_0 \in \mathcal{O}$. Lemma 6.3 supplies such a prime, with a totally positive generator if F is real. The constants $c = 1, \ell_0$ are therefore both norms, and the Hermitian argument applies with $\eta_c = 1, \eta_0$ respectively. Choose a fixed positive integer B_* divisible by μ, $|D_F|$, ℓ_0, and the two integers B_c from Lemma 7.2. A modulus or norm prime to B_* is necessarily nonzero. All further coprimalities with B_* or D_F are fixed residue conditions.

Lemma 7.3 (One relative insertion)**.** *Let $m = m(\mathbf{v})$ and $a = a(\mathbf{v}) \in \mathcal{O}$ be polynomial data satisfying $\gcd(m, B_*) = \gcd(m, \mathrm{N}(a)) = 1$ at every input. For each original specialization define*

$$\mathcal{T}_{\mathrm{ins}}(\mathbf{v}) = \left\{ (b,x) \in \mathcal{O} \times \mathbb{Z} \;\middle|\; \begin{array}{c} b \equiv a(\mathbf{v}) \pmod{m(\mathbf{v})\mathcal{O}}, \\ \gcd(\mathrm{N}(b), B_*) = \gcd(x, B_*) = \gcd(x, \mathrm{N}(b)) = 1 \end{array} \right\}.$$

There are polynomial continuations that cover every fibre of $\mathcal{T}_{\mathrm{ins}}$. Their specified outputs are denoted by (a', x). No coordinate-primitivity condition is imposed on a'.

Proof. Fix an original parameter specialization and a target $(a_*, x_*) \in \mathcal{T}_{\mathrm{ins}}(\mathbf{v})$. Write $d = \mathrm{N}(a_*)$ (possibly negative). It is nonzero and prime to mB_*. The congruence $a_* \equiv a$ ensures coprimality with m. Choose a positive rational prime p with

$$p \equiv x_* \pmod{|d|}, \qquad p \equiv 1 \pmod{|m|}, \qquad p \equiv 1 \pmod{4}, \qquad \left(\frac{\ell_0}{p}\right) = -1,$$

excluding all primes dividing B_*. These requirements are compatible by quadratic reciprocity and the Chinese remainder theorem: prescribe a nonzero nonsquare residue modulo ℓ_0, independent of dm which is prime to $2\ell_0$, and apply Dirichlet's theorem. The condition $p \equiv 1 \pmod{4}$ is used here to identify (ℓ_0/p) with (p/ℓ_0) by quadratic reciprocity. Moreover $p \nmid d$, since $p \equiv x_* \pmod{|d|}$ and $\gcd(x_*, d) = 1$. Thus one of the constants $c = 1, \ell_0$ makes d/c a square in $\mathbb{F}_p^\times$. Choose k_* with $ck_*^2 \equiv d \pmod{p}$ and $k_* \equiv 1 \pmod{m}$. Choose w_* with $w_* \equiv a_* k_*^{-1} \pmod{p\mathcal{O}}$ and $w_* \equiv \eta_c \pmod{m\mathcal{O}}$ by CRT, since $p \nmid m$. Then $h_* = (\mathrm{N}(w_*) - c)/p$ is an integer divisible by m, and (p, w_*, h_*) is a point of the relative Hermitian level of Lemma 7.2.

For the polynomial construction take its two covers, with $c = 1, \ell_0$, giving p_0, w, h and

$$\mathrm{N}(w) - p_0 h = c, \quad p_0 \equiv 1 \pmod{m}, \quad w \equiv \eta_c \pmod{m\mathcal{O}}.$$

Retain $\gcd(p_0, c) = 1$ by fixed residue subdivision (this retains the chosen targets). Put $n = \mathrm{N}(w)$. Then $\gcd(p_0, n) = 1$. Act on the primitive integer column $(p_0, n)^T$ by $K(mn; \theta)$, writing the result as $(P, nk)^T$. The quotient defining k is an integer polynomial, since the difference of the matrix from I_2 is polynomially divisible by mn. It is defined even where $n = 0$. We have pointwise

$$P \equiv 1 \pmod{m}, \qquad k \equiv 1 \pmod{m}, \qquad \gcd(P, nk) = 1.$$

For the target $n = \mathrm{N}(w_*) \neq 0$ since its norm modulo p is nonzero. The columns $(p, n)^T, (p, nk_*)^T$ are primitive and agree modulo mn, so column lifting (Lemma 2.7) and K attain $P = p, k = k_*$. The same map works for either sign of the norm.

Use unrestricted parameters $\lambda \in \mathcal{O}$ and $v \in \mathbb{Z}$ and set

$$a' = wk + P(a - wk + m\lambda), \qquad x = P + \mathrm{N}(a')v.$$

The first congruence is automatic. Also $\mathrm{N}(a') \equiv nk^2 \pmod{P}$, so $\gcd(P, \mathrm{N}(a')) = 1$, even when $P = 0$ (then $nk = \pm 1$). Thus $\gcd(x, \mathrm{N}(a')) = 1$. Keep the fixed conditions of coprimality with B_* by fixed residue subdivision. These filters impose precisely the remaining conditions defining $\mathcal{T}_{\mathrm{ins}}$ and preserve every prescribed target in that set. At the numerical target, $(a_* - w_*k_*)/p$ is integral over $\mathcal{O}$ and congruent to $a - w_*k_*$ modulo m; the choice of p, w_*, k_* permits a choice of λ attaining a_*. Finally $v = (x_* - p)/d$ is integral and gives x_*. Every target survives the fixed residue filters. All steps are polynomial continuations or fixed filters, so their composition is a polynomial continuation by Lemma 2.6. The preimage construction applies to every original specialization and every target in $\mathcal{T}_{\mathrm{ins}}$, proving the required fibrewise coverage. The auxiliary primality is used only to choose preimages, and places no restriction on the free parameters of the polynomial maps. □

Corollary 7.4 (Several relative insertions)**.** *Under the hypotheses of Lemma 7.3, fix $j \geq 1$ and put*

$$\mathcal{T}_j(\mathbf{v}) = \left\{ (b, u_1, \ldots, u_j) \in \mathcal{O} \times \mathbb{Z}^j \;\middle|\; \begin{array}{l} b \equiv a(\mathbf{v}) \pmod{m(\mathbf{v})\mathcal{O}}, \\ \gcd\big(\mathrm{N}(b)\prod_i u_i, B_*\big) = 1, \\ \gcd\big(\mathrm{N}(b), m(\mathbf{v})\prod_i u_i\big) = 1 \end{array} \right\}.$$

There are polynomial continuations that cover every fibre of $\mathcal{T}_j$. Denote their outputs by $(c_0, u_1, \ldots, u_j)$ and write $n = \mathrm{N}(c_0)$.

Proof. Iterate Lemma 7.3, at step i using the current element and protective modulus $mu_1 \cdots u_{i-1}$, while retaining all earlier integer outputs. At every specialization of every preceding branch, this modulus is prime to B_* and to the current norm. The next application therefore covers every fibre over that precise specialization. Its congruence preserves coprimality of the new norm with all the previous u_i, so every output belongs to $\mathcal{T}_j$.

For any prescribed target in $\mathcal{T}_j$, choose its element c_0 at the first insertion and return that same element at every later step, along with the successive target integers. It is an allowed target at each enlarged modulus because it equals the current element at the chosen specialization. Lemma 2.6 then gives joint fibrewise coverage of the displayed set. □

8 Primitive products in arbitrary quadratic fields

An element will be called *unramified primitive* if it is coordinate-primitive and its signed norm is prime to D_F. This is equivalent to the ideal condition $(a, \bar{a}) = \mathcal{O}$. Indeed a common prime divisor of these elements is either inert (so a rational prime divides the coordinates), split (so

both conjugate prime ideals divide a, again giving a rational divisor), or ramified (excluded by the norm condition). Conversely a common rational divisor forces common ideal divisors, and a ramified prime dividing the norm forces a common divisor. For a product $A = \prod_i a_i$, it is equivalent to $(a_i, \bar{a}_j) = \mathcal{O}$ for all i, j. We will construct covers of unramified primitive products without imposing that their norms are prime to B_*: the additional primes of B_* are allowed in final outputs. The only moduli used in the relative Hermitian step will be prime to B_*. In the fibre sets below, $\mathbf{v}$ denotes the retained input parameters, and all given moduli and seeds are evaluated at $\mathbf{v}$. We use the distinction in Definition 2.5 between permissible outputs $\mathcal{S}(\mathbf{v})$ and required targets $\mathcal{T}(\mathbf{v}) \subseteq \mathcal{S}(\mathbf{v})$; an exact fibre cover has $\mathcal{T} = \mathcal{S}$.

Lemma 8.1 (Cyclic quotients)**.** *If $q \in \mathcal{O}$ is coordinate-primitive and $n = \mathrm{N}(q)$, the natural map $\mathbb{Z}/|n|\mathbb{Z} \to \mathcal{O}/q\mathcal{O}$ is an isomorphism. In coordinates modulo n, the image of $q\mathcal{O}$ is generated by* $\mathrm{col}(q)$*. If q, u are comaximal, then* $\det(\mathrm{col}(q), \mathrm{col}(u))$ *is a unit modulo n.*

Proof. Complete $\mathrm{col}(q)$ to a determinant-one integer matrix. In the resulting basis the multiplication matrix of q (whose columns are $\mathrm{col}(q), \mathrm{col}(\omega q)$) has the form $\left(\begin{smallmatrix} 1 & j \\ 0 & n \end{smallmatrix}\right)$. Indeed its determinant is the signed norm n, and the change of codomain basis has determinant one, so the lower-right entry is exactly n, including when $n < 0$. Hence the additive quotient is cyclic of order $|n|$, and modulo n the ideal is generated by the first column. The additive order of 1 is the exponent of the quotient ring, namely $|n|$, proving the ring isomorphism. A unit in this cyclic ring has additive order $|n|$; in the chosen basis this is equivalent to the second coordinate of u, i.e. the indicated determinant, being a unit modulo n. □

Lemma 8.2 (A primitive column operation with bounded overlap)**.** *Let Q be a coordinate-primitive polynomial element of $\mathcal{O}$ with $n = \mathrm{N}(Q)$, and let c be a coordinate-primitive polynomial element comaximal with Q. Let ℓ be an integer-polynomial modulus, possibly zero, and fix an integer $\delta > 0$. Work on the fixed residue branches where $\delta \mid n$ and $\delta \mid \ell$, using Lemma 2.1 to make n/δ and ℓ/δ integer polynomials. Put*

$$\mathcal{S}(\mathbf{v}) = \{c' \in \mathcal{O} : \ c' \text{ is coordinate-primitive}, \ c' \equiv c \pmod{Q\mathcal{O}}, \ c' \equiv c \pmod{\ell\mathcal{O}}\},$$

$$\mathcal{T}(\mathbf{v}) = \begin{cases} \mathcal{S}(\mathbf{v}), & \gcd(n, \ell) = \delta, \\ \varnothing, & \gcd(n, \ell) \neq \delta. \end{cases}$$

There are polynomial continuations covering every fibre of $\mathcal{T}$ inside $\mathcal{S}$. The equality $\gcd(n, \ell) = \delta$ *is a condition for required targets, not a filter on polynomial parameters. Congruence modulo zero means equality.*

Proof. Let $v = \mathrm{col}(Q) = (Q_0, Q_1)^T$, and for an integer parameter h put $S = I_2 + \ell h\, v(-Q_1, Q_0)$. This matrix has determinant one, since the rank-one correction has trace zero and square zero. Use

$$\mathrm{col}(c') = K(\ell n/\delta; \theta) S \,\mathrm{col}(c).$$

The level is an integer polynomial and is polynomially a multiple of both n and ℓ, since n/δ and ℓ/δ are integer polynomials on the chosen branch; $n\mathcal{O} \subset Q\mathcal{O}$, and the shear adds a multiple of Q. Thus both congruences hold and primitivity is preserved.

For a numerical target c_*, the case $\ell = 0$ requires $c_* = c$ and is immediate. Otherwise Lemma 8.1 says that the difference of the two columns modulo n is kv for an integer k. Since the difference is divisible by ℓ, $\delta \mid k$: reduce the congruence modulo δ and use the primitivity of v. The coefficient $\det(v, \mathrm{col}(c))$ is a unit modulo n, by the same lemma. At a specialization with $\gcd(n, \ell) = \delta$, we can therefore choose h so that $\ell h \det(v, \mathrm{col}(c)) \equiv k \pmod{n}$. After the shear the two columns agree modulo n and ℓ, hence modulo $|n\ell|/\delta$. The integer column-lifting and uniform congruence lemmas give the desired column exactly. The construction is sound even on a branch where the actual gcd is larger than δ; the gcd equality is needed only in this numerical coverage argument. □

Corollary 8.3 (Primitive-column coset operation)**.** *Under the hypotheses of Lemma 8.2, suppose* $\gcd(n,\ell)=1$ *at every input. Fix positive integers* $d_1,\dots,d_h$ *and integer-polynomial outputs* $b_1,\dots,b_h$*, with* $h=0$ *allowed. There are polynomial continuations giving an exact fibre cover of*

$$\mathcal{T}(\mathbf{v})=\left\{c'\in\mathcal{O}:\ \begin{array}{l} c' \text{ is coordinate-primitive},\quad c'\equiv c \pmod{Q\mathcal{O}},\quad c'\equiv c \pmod{\ell\mathcal{O}},\\ \mathrm{N}(c')\equiv b_i \pmod{d_i}\quad (1\le i\le h)\end{array}\right\}.$$

Proof. Take $\delta=1$ in Lemma 8.2 and apply Lemma 2.1 to the additional congruences. □

Lemma 8.4 (Repair of a primitive representative)**.** *Let* q,w,s *be polynomial elements of* $\mathcal{O}$*, with* q,s *coordinate-primitive and* w *comaximal with* q *at every input. Write* $n=\mathrm{N}(q)$*, and let* m *be a pointwise nonzero integer-polynomial modulus with* $\gcd(m,n)=1$*. There are polynomial continuations giving an exact fibre cover of*

$$\mathcal{T}(\mathbf{v})=\{u\in\mathcal{O}:\ u \text{ is coordinate-primitive},\ u\equiv w \pmod{q\mathcal{O}},\ u\equiv s \pmod{m\mathcal{O}}\}.$$

Proof. By Lemma 2.4, complete $\mathrm{col}(q)$ to a determinant-one polynomial matrix Q. Write $Q^{-1}\mathrm{col}(w)=(v_1,v_2)^T$. The first column of $Q\left(\begin{smallmatrix}1&0\\v_2&1\end{smallmatrix}\right)$ is primitive and differs from $\mathrm{col}(w)$ by a multiple of $\mathrm{col}(q)$. Apply Lemma 2.8 to this matrix and a completion of $\mathrm{col}(s)$, at the levels n,m. Its first column u_0 has both desired congruences; it is still comaximal with q. Apply Lemma 8.3 to u_0,q,m. It attains every target in both cosets. This proves the assertion, and fixed norm congruences may again be imposed after the operation. □

Lemma 8.5 (Normalization of a primitive product)**.** *Let* $m\neq 0$ *be prime to* B_**, and let* $a_1\cdots a_r$ *be unramified primitive with all factor norms prime to* m*. There is a finite sequence of numerical replacements, first of* a_r *and then of* $a_1,a_2,\dots,a_{r-1}$*, with the following properties. At each replacement a factor* a *is replaced by* a' *satisfying*

$$a'\equiv a \pmod{m\mathcal{O}},\qquad a'\equiv a \pmod{\bar{V}\mathcal{O}},$$

where V *is the product of the other current factors. Every intermediate product is unramified primitive. The resulting last factor* c *has positive prime norm* n *prime to* mB_**, and each other resulting factor is congruent modulo* $n\mathcal{O}$ *to an integer* u_j *prime to* nB_**. All other factor norms are prime to* n*. Each replacement can be undone by Corollary 8.3; the undoing order is* $a_{r-1},a_{r-2},\dots,a_1,a_r$*.*

Proof. Let $A=a_1\cdots a_{r-1}$. The unit residues of a_r modulo $m\mathcal{O}$ and $\bar{A}\mathcal{O}$ are compatible, and these ideals are comaximal. By Lemma 6.3, choose a degree-one prime element c in this ray class, with positive prime norm n avoiding $mB_*\,\mathrm{N}(A)$; in a real field prescribe a totally positive generator. Its product with A is unramified primitive, and $n\mathcal{O}=(c)(\bar{c})$ is a product of distinct prime ideals.

Now visit $a_1,\dots,a_{r-1}$ in that order. For a current factor b, let V be the product of the other current factors. The class of b modulo $\bar{c}\mathcal{O}$ is a scalar unit, by Lemma 8.1. Choose an integer representative u of this class, also prime to B_*, using $\gcd(n,B_*)=1$. The prescriptions

$$b'\equiv u \pmod{n\mathcal{O}},\qquad b'\equiv b \pmod{\bar{V}\mathcal{O}},\qquad b'\equiv b \pmod{m\mathcal{O}}$$

are compatible unit residues. Indeed the gcd ideal of $n\mathcal{O}$ and $\bar{V}\mathcal{O}$ is $(\bar{c})$: every factor of V other than c has norm prime to n. The residues agree on this gcd ideal. Lemma 6.3 gives a degree-one prime element b' in the resulting ray class, excluding all rational primes dividing $mB_*\,\mathrm{N}(V)$. Its prime ideal lies above an unramified split rational prime, since $D_F\mid B_*$. Its norm is prime to m, to B_* and to every other current factor norm, including n. Hence b' is unramified primitive and is comaximal with $\bar{V}$; equivalently, $b'V$ is unramified primitive. The

displayed congruences preserve the two required cosets and give the prescribed scalar residue modulo $n\mathcal{O}$.

At each step $\bar{V}$ is coordinate-primitive, its norm is prime to m, and it is comaximal with both factors involved in the replacement. Corollary 8.3 therefore undoes that change. In reverse order, all other factors have exactly the values they had at the corresponding forward step, so the same two cosets are available. □

Theorem 8.6 (Relative primitive-product covering)**.** *Fix $r \geq 1$. Let m be an integer-polynomial output and $s_1, \ldots, s_r$ polynomial elements of $\mathcal{O}$, with*

$$\gcd(m, B_*) = 1, \qquad \gcd\left(m, \prod_j \mathrm{N}(s_j)\right) = 1$$

at every input, and with each s_j coordinate-primitive. There are polynomial continuations giving an exact fibre cover of

$$\mathcal{T}(\mathbf{v}) = \left\{ (a_1, \ldots, a_r) \in \mathcal{O}^r : \begin{array}{l} a_j \equiv s_j \pmod{m\mathcal{O}} \quad (1 \leq j \leq r), \\ \prod_{j=1}^r a_j \text{ is unramified primitive} \end{array} \right\}.$$

In particular, with $m = 1$ and all seeds equal to 1, the set of r-tuples with unramified primitive product has a finite polynomial cover.

Proof. For $r = 1$, act on $\mathrm{col}(s_1)$ by $K(m;\theta)$ and impose the fixed condition $\gcd(\mathrm{N}(a_1), D_F) = 1$. Lemmas 2.7 and 3.2 give every target. Suppose the assertion holds for $r - 1$.

Normalize a target. Apply Lemma 8.5 to an admissible target. Denote its normalized last factor by c, its positive prime norm by n, and the scalar residues of its first $r - 1$ factors by $u_1, \ldots, u_{r-1}$. All u_j and n are prime to B_*. The normalization preserves the original seed residues modulo $m\mathcal{O}$.

Construct the normalized tuple polynomially. Apply Corollary 7.4 to s_r at level m. It gives $c_0 \equiv s_r \pmod{m\mathcal{O}}$, $n = \mathrm{N}(c_0)$ and integers u_j, with

$$\gcd(n, m\prod_j u_j) = 1, \qquad \gcd(n, B_*) = \gcd(u_j, B_*) = 1,$$

and attains the numerical data just chosen. Complete each primitive column $(u_j, n)^T$ and $\mathrm{col}(s_j)$ to polynomial determinant-one matrices. Lemma 2.8, at levels n and m, gives a primitive seed $\tilde{s}_j$ with

$$\tilde{s}_j \equiv u_j \pmod{n\mathcal{O}}, \qquad \tilde{s}_j \equiv s_j \pmod{m\mathcal{O}}.$$

Its norm is prime to mn at every parameter specialization. Since mn is prime to B_*, the induction hypothesis applies over every specialization of this continuation. At the numerical specialization selected above, the normalized first $r - 1$ factors have residues u_j modulo $n\mathcal{O}$ and s_j modulo $m\mathcal{O}$. They therefore belong to the required fibre for the new seeds at level mn, and the induction attains those factors. For every output their product A is unramified primitive and $\gcd(\mathrm{N}(A), mn) = 1$.

Apply Lemma 8.4 with $q = \bar{A}$, $w = c_0$, $s = s_r$ and modulus m. Its hypotheses hold because $\mathrm{N}(A)$ is prime to both m and $\mathrm{N}(c_0)$. It gives a primitive a_r in the required cosets. Impose the fixed condition $\gcd(\mathrm{N}(a_r), D_F) = 1$. Then Aa_r is unramified primitive, since $a_r \equiv c_0 \pmod{\bar{A}\mathcal{O}}$. At the normalized target the operation can return $a_r = c_0 = c$.

Undo the normalization. Apply Corollary 8.3 to the first $r - 1$ factors in reverse order and then to the last factor, preserving the cosets modulo $m\mathcal{O}$ and the conjugate product of the other current factors. After each operation impose the fixed unramified norm condition. Every output remains admissible. At the target these operations undo the replacements of Lemma 8.5 exactly, and so recover the original tuple. All operations are polynomial continuations and compose by Lemma 2.6. The final norms may include split primes dividing B_*. □

9 Joint covers of coprime blocks

The primitive-product covering theorem controls products within one quadratic ring. We now construct joint covers of several such products with coprime scaled norms, allowing additional blocks of rational integers. The scale factors will account for fixed ideal-class representatives in the proof of Theorem B.

For a coordinate-primitive polynomial element $A = A_0 + A_1\omega$, choose $A_0U + A_1V = 1$ by Lemma 2.4, with fixed subdivisions if necessary. Put

$$E_A = V - \tau U + U\omega, \qquad AE_A = L_A + \omega, \qquad \mathrm{red}_A(b_0 + b_1\omega) = b_0 - L_A b_1. \tag{9.1}$$

Here $\omega^2 = \tau\omega + \rho$, and direct multiplication gives the coefficient of ω in AE_A as 1. By Lemma 8.1, red_A represents reduction modulo $A\mathcal{O}$ in the ring $\mathbb{Z}/|\,\mathrm{N}(A)|\mathbb{Z}$. Thus if b is comaximal with A, then $\gcd(\mathrm{red}_A(b), \mathrm{N}(A)) = 1$. The witnesses and the scalar reductions in (9.1) are polynomial in the free integer parameters.

Lemma 9.1 (Relative scalar blocks)**.** *Let m be a pointwise nonzero integer-polynomial modulus, and let $w_1, \dots, w_N$ be polynomial integer seeds with $\gcd(w_i, m) = 1$ at every input. Fix a partition $I_1, \dots, I_h$ of the coordinates into blocks, and write $H_k(u) = \prod_{i \in I_k} u_i$. There are polynomial continuations giving an exact fibre cover of*

$$\mathcal{T}(\mathbf{v}) = \{u \in \mathbb{Z}^N : \ u_i \equiv w_i \pmod m \ (1 \le i \le N), \ \gcd(H_j(u), H_k(u)) = 1 \ (j < k)\}.$$

Empty blocks have product 1*.*

Proof. Begin each coordinate with $w_i + mv_i$ for a free integer parameter v_i, and follow the visits of Proposition 4.2. At a visit write a, w, P, Q as in that proof. Every coordinate stays prime to m, so m, P, Q are pairwise coprime and $(a, mP), (w, Q), (mP, Q)$ are pointwise coprime pairs. Obtain their polynomial Bézout witnesses by Lemma 2.4. Use Lemma 4.1 with P replaced by mP. Its congruences preserve the residues modulo m as well as all previous coprimalities. Each target pair is retained exactly, even when $PQ = 0$, by the coverage assertion of that lemma. Induction through the fixed sequence of visits proves the claim. □

Lemma 9.2 (Normalization with a bounded common part)**.** *Let C, B be positive integers with $C \mid B$ and $D_F \mid B$. Let $m, H \neq 0$, with $\gcd(m, B) = 1$. Suppose $A = \prod_i a_i$ is an unramified primitive product and, writing $n = \mathrm{N}(A)$,*

$$C \mid n, \qquad \gcd(n/C, H) = 1, \qquad \gcd(n, m) = 1.$$

One can replace the factors successively, in their given order, so that every product stays unramified primitive and each replacement preserves the factor modulo $mH\mathcal{O}$ and modulo the conjugate product of the other current factors. The final norm has the form dq_0, where d is a positive divisor of C and q_0 is a signed integer with $\gcd(q_0, BmH) = 1$. The final norm need not be divisible by C.

Proof. For every rational prime $p \mid H$ we have $v_p(|n|) = v_p(C)$. At a current factor a, let V be the product of the other factors. Retain in (a) all prime-ideal powers above rational primes dividing H, calling their product $\mathfrak{d}$, and put $I = (a)/\mathfrak{d}$. The ideal I is prime to $\mathfrak{m} = (mH)\mathcal{O} \cdot (\bar{V})$: the primes above H have been removed, m is prime to $\mathrm{N}(a)$, and a is comaximal with $\bar{V}$. By Lemma 6.3, choose a degree-one prime ideal $\mathfrak{p}$ in the ray class of I modulo $\mathfrak{m}$, avoiding the rational primes dividing $BmH\,\mathrm{N}(V)$ and all earlier and original factor norms. Write $\mathfrak{p} = (\alpha)I$ with $\alpha \equiv 1$ at this ray modulus. No real places are included in $\mathfrak{m}$, so the sign of $\mathrm{N}(\alpha)$ is not prescribed; this is why q_0 is allowed either sign. Then $a' = a\alpha$ is

integral, since $(a') = \mathfrak{d}\mathfrak{p}$. The local congruences for α imply the required global congruences for the integral difference $a' - a$.

The retained prime ideals have their previous orientations, and the new split prime is absent from the other factor norms. Thus the product remains unramified primitive. The norm of each retained ideal above a prime dividing H is unchanged throughout the pass. Their total norm is

$$d = \prod_{p \mid H} p^{v_p(C)},$$

which divides C. All other prime factors in the final norm are the new split primes, which avoid BmH. This gives the claimed form dq_0. All prime choices in this lemma are numerical; no restriction to prime values will be placed on polynomial parameters. □

Lemma 9.3 (Joining residue seeds)**.** *Let A be an unramified primitive polynomial element, put $n = \mathrm{N}(A)$, and let m be an integer-polynomial output with $\gcd(m, n) = 1$ at every input. Let $d > 0$ be fixed, with $d \mid n$, and work on the fixed subdivisions where $q_0 = n/d$ is an integer polynomial.*

Let c, e be polynomial elements of $\mathcal{O}$, with c coordinate-primitive and comaximal with A, and e comaximal with $\bar{A}$. There are polynomial continuations giving an exact fibre cover of

$$\mathcal{T}_{\mathrm{quad}}(\mathbf{v}) = \left\{ s' \in \mathcal{O} : \begin{array}{l} s' \text{ is coordinate-primitive}, \quad s' \equiv c \pmod{m\mathcal{O}}, \\ s' \equiv c \pmod{A\mathcal{O}}, \quad s' \equiv e \pmod{\bar{A}\mathcal{O}} \end{array} \right\}.$$

Every element of this fibre has norm prime to n; if $\gcd(\mathrm{N}(c), m) = 1$, its norm is prime to mq_0. If c and e both represent an element b in their respective residue rings, every element of the fibre is congruent to b modulo $n\mathcal{O}$.

For integer-polynomial outputs r, w with $\gcd(r, n) = \gcd(w, m) = 1$, there are polynomial continuations giving an exact fibre cover of

$$\mathcal{T}_{\mathrm{scal}}(\mathbf{v}) = \{ s' \in \mathbb{Z} : \ s' \equiv r \pmod{q_0}, \ s' \equiv w \pmod{m} \}.$$

Every element of this fibre is prime to mq_0.

Proof. Write $v = \mathrm{col}(A)$ and $\Delta = \det(v, \mathrm{col}(c))$. Both Δ and $\mathrm{red}_{\bar{A}}(A)$ are units modulo n, by Lemma 8.1. Choose a polynomial witness J with $Jm\Delta \,\mathrm{red}_{\bar{A}}(A) \equiv 1 \pmod{n}$ and put

$$h = J \,\mathrm{red}_{\bar{A}}(e - c), \qquad s_0 = c + mh\Delta A.$$

On coordinates this is the determinant-one shear $I_2 + mh\, v(-A_1, A_0)$, so s_0 is coordinate-primitive. The first two congruences are immediate, and scalar reduction modulo $\bar{A}\mathcal{O}$ gives the third. The ideals (A) and $(\bar{A})$ are comaximal and have product $n\mathcal{O}$. Thus the two unit residues show that s_0, and every element of $\mathcal{T}_{\mathrm{quad}}(\mathbf{v})$, has norm prime to n. The additional assertions follow from the residue modulo $m\mathcal{O}$ and from the same ideal Chinese remainder theorem.

For full coverage, set

$$\mathrm{col}(s') = K(mn; \vartheta)\, \mathrm{col}(s_0).$$

These outputs are primitive and preserve all three congruences. Conversely, at a fixed old specialization, every element of $\mathcal{T}_{\mathrm{quad}}(\mathbf{v})$ is congruent to s_0 modulo both $m\mathcal{O}$ and $n\mathcal{O}$, hence modulo $mn\mathcal{O}$ since $\gcd(m, n) = 1$. Lemmas 2.7 and 3.2 therefore attain it. If $m = 0$, then $|n| = 1$ and this fibre consists only of $c = s_0$; the formula still works because $K(0; \vartheta) = I_2$.

For the scalar fibre choose a polynomial witness J_0 with $q_0 J_0 \equiv 1 \pmod{m}$ and use the free integer parameter z in

$$s' = r + q_0 J_0 (w - r) + mq_0 z.$$

Its two residues give the asserted coprimality. Since $\gcd(m, q_0) = 1$, the ordinary Chinese remainder theorem shows that the affine parameter covers the whole scalar fibre. If $m = 0$, then $q_0 = \pm 1$, the witness identity is $q_0 J_0 = 1$, and the fibre and formula both reduce to $s' = w$. Every witness here is supplied by Lemma 2.4; no inverse is a variable denominator. □

Theorem 9.4 (Coprime blocks in one quadratic field)**.** *Fix finitely many quadratic blocks of elements $a_{ji} \in \mathcal{O}$, with positive scale constants C_j, and finitely many scalar blocks of integers u_{ki}. Write*

$$A_j = \prod_i a_{ji}, \qquad n_j = \mathrm{N}(A_j), \qquad H_k = \prod_i u_{ki}.$$

There is a fixed positive integer B with the following property. Let m be an integer-polynomial output prime to B at every input. Let the polynomial seeds $s_{ji} \in \mathcal{O}$ be coordinate-primitive with norms prime to m, and let the polynomial integer seeds w_{ki} be prime to m. Define the permissible fibre

$$\mathcal{S}(\mathbf{v}) = \left\{ ((a_{ji}), (u_{ki})) : \begin{array}{l} a_{ji} \equiv s_{ji} \pmod{m\mathcal{O}}, \quad u_{ki} \equiv w_{ki} \pmod{m}, \\ A_j \text{ is unramified primitive and } C_j \mid n_j \text{ for every } j, \\ \text{the integers } n_j/C_j \text{ and } H_k \text{ are pairwise coprime} \end{array} \right\}, \tag{9.2}$$

and the required fibre

$$\mathcal{T}(\mathbf{v}) = \{((a_{ji}), (u_{ki})) \in \mathcal{S}(\mathbf{v}) : \ u_{ki} \neq 0 \text{ for every scalar coordinate}\}.$$

There are polynomial continuations covering every fibre of $\mathcal{T}$ inside $\mathcal{S}$. Pairwise coprimality includes quadratic–quadratic, scalar–scalar and quadratic–scalar pairs. Zero scalar coordinates are permitted outputs, and the norms may have either sign.

Proof. An empty quadratic block has norm 1: discard it if its scale is 1, and otherwise both fibres are empty. Thus assume each quadratic block is nonempty. Choose B divisible by B_* and by every scale C_j. The same B will work for every subset of the blocks. We induct on the number of quadratic blocks. With no quadratic blocks, use Lemma 9.1.

Step 1: normalize the first target block and choose auxiliary data. Fix an admissible target with nonzero scalar entries. Let A be the first quadratic-block product, C its scale, and $n = \mathrm{N}(A)$. Let H be the product of the scaled norm quotients and scalar block products for all other blocks. Then $H \neq 0$, $\gcd(n/C, H) = \gcd(n, m) = 1$. Apply Lemma 9.2, in the given order of the first-block factors. Write the normalized norm as $n = dq_0$, where $d \mid C$ and $\gcd(q_0, BmH) = 1$. Only the finitely many divisors d of C will index polynomial branches. The other blocks are unchanged.

For each target factor b in a later quadratic block, its full norm is prime to q_0: its scaled block quotient divides H, and its scale divides B. Since $\gcd(d, q_0) = 1$, choose

$$\tilde{b} \equiv b \pmod{q_0\mathcal{O}}, \qquad \tilde{b} \equiv 1 \pmod{d\mathcal{O}}.$$

It is a unit modulo $n\mathcal{O}$. If s_b is the original seed, choose auxiliary degree-one prime elements with the unit residues

$$\begin{aligned} c_b &\equiv \tilde{b} \pmod{A\mathcal{O}}, \quad c_b \equiv s_b \pmod{m\mathcal{O}}, \\ e_b &\equiv \tilde{b} \pmod{\bar{A}\mathcal{O}}, \quad e_b \equiv 1 \pmod{m\mathcal{O}}. \end{aligned}$$

For each target scalar u, similarly choose an integer $\tilde{u} \equiv u \pmod{q}_0$, $\tilde{u} \equiv 1 \pmod{d}$, and a prime element c_u with

$$c_u \equiv \tilde{u} \pmod{A\mathcal{O}}, \qquad c_u \equiv 1 \pmod{m\mathcal{O}}.$$

The Chinese remainder theorem and Lemma 6.3 give these choices. Choose their positive prime norms mutually distinct and away from nmB and all earlier choices; prescribe totally positive generators in a real field. Then

$$A\prod_b(\bar{c}_b e_b)\prod_u \bar{c}_u$$

is unramified primitive. All these elements and both conjugate residue ideals lie in the same quadratic ring; this is where the common-field hypothesis is used.

Step 2: construct the auxiliary data and join their seeds. Apply Theorem 8.6 at level m to the first-block factors and the auxiliary factors displayed above. Use the original first-block seeds, the seed $\bar{s}_b$ for $\bar{c}_b$, and seed 1 for every other auxiliary factor. The hypotheses hold, and the theorem attains the numerical choices from Step 1. Every output has unramified primitive product.

Retain $d \mid n$ by fixed subdivision, form the integer polynomial $q_0 = n/d$, and retain $\gcd(q_0, B) = 1$ by a filter modulo the fixed integer B. Every normalized target from Step 1 survives these filters. On every retained parameter specialization, not just on the chosen target, mq_0 is prime to B. The product construction ensures that c_b is coordinate-primitive and comaximal with A, e_b is comaximal with $\bar{A}$, and c_u is comaximal with A. Also $\gcd(m, n) = 1$. Lemma 9.3 gives primitive quadratic seeds s'_b whose norms are prime to mq_0, with the old residue modulo $m\mathcal{O}$. At the chosen target they are congruent to $\tilde{b}$, hence to b, modulo $q_0\mathcal{O}$.

For a scalar factor with original seed w_u, put $r_u = \mathrm{red}_A(c_u)$. The auxiliary prime element c_u was introduced precisely to make r_u a polynomial output automatically prime to n: the primitive-product construction makes c_u comaximal with A, and Lemma 8.1 gives this coprimality. The scalar part of Lemma 9.3 gives a seed s'_u prime to mq_0 with residues r_u modulo q_0 and w_u modulo m. At the target, $r_u \equiv \tilde{u} \equiv u \pmod{q}_0$. Thus all the other target blocks have the required new seed residues modulo mq_0.

Step 3: construct the other blocks and reverse the normalization. The retained branches satisfy the induction hypotheses at level mq_0 at every specialization: that level is prime to B, the quadratic seeds are primitive with norms prime to mq_0, and the scalar seeds are prime to mq_0. Apply the induction to the remaining blocks. At the chosen numerical specialization the original other blocks are required targets, since their scalar entries are nonzero and they have the new seed residues. The resulting scaled block products are pairwise coprime, and their full factor norms and scalar entries are prime to mq_0. Write H' for the polynomial product of their scaled block products. Then $\gcd(H', mq_0) = 1$. Initially the first-block norm is dq_0, so

$$\gcd(mH', \mathrm{N}(A_{\mathrm{current}})) \mid d. \tag{9.3}$$

Visit the first-block factors in the reverse of their order in Step 1. For a current factor a, let V be the product of the other current factors of that block. Apply Lemma 8.2 with $Q = \bar{V}$, $c = a$, and $\ell = mH'$. Enumerate the fixed divisors $\delta \mid d$ and retain the fixed divisibilities $\delta \mid \mathrm{N}(Q)$ and $\delta \mid \ell$. Impose also the fixed output condition $\gcd(\mathrm{N}(a'), D_F) = 1$. The operation preserves the cosets modulo $mH'\mathcal{O}$ and $\bar{V}\mathcal{O}$, so the new block product remains unramified primitive. Its norm is unchanged modulo mH', which preserves (9.3). Since $\mathrm{N}(Q)$ divides the current full norm, we also have

$$\gcd(mH', \mathrm{N}(Q)) \mid d$$

at every stage.

For coverage choose the induction parameters giving the original other blocks, so $H' = H$. Write the original first-block tuple as $(a_1, \ldots, a_r)$ and its normalized tuple as $(a'_1, \ldots, a'_r)$. After undoing factors $r, r-1, \ldots, k+1$, the current tuple is

$$(a'_1, \ldots, a'_k, a_{k+1}, \ldots, a_r),$$

exactly the tuple after the kth forward replacement. Thus the other factors and both preserved cosets agree with those at that replacement. Choose $\delta = \gcd(mH, \mathrm{N}(\bar{V}))$ at the current specialization; it divides d, so its branch is present. The original factor a_k belongs to the required fibre of Lemma 8.2, and that lemma restores it exactly. This proves the reversal by descending induction. The actual-gcd condition is used only to select a branch for a target; soundness and (9.3) hold at every output. If an output has $H' = 0$, the coset operation is the identity and the same soundness argument applies. No zero scalar target was required.

Step 4: restore the scale and finish the coprimality filters. Retain $C \mid n_{\mathrm{final}}$ and form n_{final}/C, using fixed subdivision. Every rational prime common to this quotient and H' divides d, by (9.3). For each of the finitely many primes dividing d, exclude the residue classes in which it divides both integers. The new scaled quotient is then prime to every other block product, and all old seed residues modulo m are intact. The original target survives every filter because its quotient is prime to H. The finite divisor choices, residue filters and polynomial continuations compose by Lemma 2.6. This completes the induction. □

10 Proof of Theorem B: a common splitting field

We apply the joint covering theorem to the distinct irreducible factors of f. A fixed scale in each quadratic block allows us to pass from ideals of prescribed norm to principal ideals without introducing an incompatible conjugate prime. We first record the relevant choice of ideal-class representatives.

Lemma 10.1 (Oriented ideal representatives)**.** *There is a finite collection of systems of integral ideal-class representatives for $\mathcal{O}$ with this property: for every coordinate-primitive $\beta \in \mathcal{O}$, some system consists entirely of products of unramified split prime ideals, using at most one orientation above each rational prime, and every prime used above a rational prime dividing $\mathrm{N}(\beta)$ is the same orientation as the one dividing (β).*

Proof. Select finitely many prime ideals whose classes generate the class group, all of degree one and above distinct unramified split rational primes. This is Lemma 6.3 for the trivial modulus, with finitely many exclusions. For each of the finitely many choices of orientations (choose one prime above each of the selected rational primes), the classes still generate the group, because replacing a prime by its conjugate replaces its class by its inverse. Since the class group is finite, nonnegative powers of those classes also generate it. For each orientation choice, choose once and for all a product with nonnegative exponents in the selected primes representing each class. This is the claimed finite collection. At a coordinate-primitive β, no unramified split rational prime can occur in both orientations in (β), since their product is the rational ideal. Choose the matching orientation at the selected primes dividing (β) and either orientation at the others. All the representatives in that system have the desired property. □

Proof of Theorem B. For $r = 0$ simply take $z = f(t)/\kappa$ and use fixed residue subdivision. For $f = 0$ use the union of the hyperplanes on which one left factor vanishes. For nonzero constant f all left factors are nonzero and each divides f, so there are finitely many possibilities, with t free. We may henceforth assume $r \geq 1$ and f nonconstant.

Let λ be the leading coefficient of f, and d_f its degree. The polynomial $g(v) = \lambda^{d_f - 1} f(v/\lambda)$ is monic with integer coefficients. Its roots are λ times the roots of f; hence its irreducible factors have the same degrees and splitting fields as those of f, and the hypothesis of the theorem passes to g. Apply the monic case with coefficient $\lambda^{d_f - 1}\kappa$ and impose the fixed congruence $v \equiv 0 \pmod{\lambda}$ to recover $t = v/\lambda$. This substitution works in both directions.

Thus assume f monic, and factor it as

$$f(t) = \prod_{j=1}^{h} F_j(t)^{m_j},$$

where the F_j are distinct monic irreducible polynomials in $\mathbb{Z}[t]$, of degree one or two, and $m_j > 0$. We treat the all-linear case first; when quadratic factors occur, F denotes their common splitting field. If $f(t) = 0$, fix t to one of its finitely many integer roots and one of $z, x_1, \ldots, x_r$ to zero, leaving the other coordinates free. These families handle all zero targets. For the rest of the proof fix a target with $f(t) \neq 0$.

Separate irreducible factors by bounded scales. For each distinct pair of F_j, F_k, their coprimality over $\mathbb{Q}[t]$ gives integer polynomials with a linear combination equal to a fixed nonzero integer R_{jk} (for example their resultant). Let $R = \prod_{j<k} |R_{jk}|$, with empty product 1, let $m_{\mathrm{tot}} = \sum_j m_j$, and set $B_0 = R^{m_{\mathrm{tot}}}$. Take $h_i = \gcd(|x_i|, B_0)$, $X_i = x_i/h_i$ and $C_x = \prod_i h_i^{e_i}$. The h_i have finitely many choices. We allocate prime powers of X_i to columns P_{ij} so that

$$X_i = \prod_j P_{ij}, \qquad \prod_i P_{ij}^{e_i} \mid F_j(t)^{m_j}, \qquad \gcd\left(\prod_i P_{ij}, \prod_i P_{ik}\right) = 1 \ (j \neq k). \tag{10.1}$$

To prove this, for a prime p put $\nu_p = v_p(R)$. At most one $v_p(F_j(t))$ exceeds ν_p, by the fixed polynomial identities for the pairs. Allocate every residual p-power in all X_i to a column of maximal valuation. For $p \nmid R$ at most one column has positive valuation. For $p \mid R$, if any residual valuation is positive, some h_i removed $m_{\mathrm{tot}}\nu_p$ powers of p. Its contribution to the weighted removed valuation is $e_i m_{\mathrm{tot}}\nu_p \geq m_{\mathrm{tot}}\nu_p$. The weighted residual valuation is then at most

$$m_j v_p(F_j(t)) + \sum_{k \neq j} m_k \nu_p - m_{\mathrm{tot}}\nu_p \ \leq \ m_j v_p(F_j(t)).$$

Here we also used $\kappa z \prod_i x_i^{e_i} = f(t)$, since the valuations of κ, z are nonnegative. This proves the allocations and the cross-column coprimalities. Choose signs to recover the X_i.

Encode the exponents. Set $Z_j = F_j(t)^{m_j} / \prod_i P_{ij}^{e_i}$. The valuations in the equation $Z_j \prod_i P_{ij}^{e_i} = F_j(t)^{m_j}$ lie in the nonnegative integral monoid

$$\{(z, p_1, \ldots, p_r, k) \in \mathbb{Z}_{\geq 0}^{r+2} : z + \sum_i e_i p_i = m_j k\}.$$

By Lemma 2.9, its Hilbert basis is finite. Its only indecomposable element with every $p_i = 0$ is $(m_j, 0, \ldots, 0, 1)$; call the other basis elements $g \in \mathcal{G}_j$, with coordinates (g_z, g_{p_i}, g_k). For each choose a positive integer base v_{jg} at the target, using the prime valuation decomposition in the basis. Define

$$P_{ij} = \varepsilon_{ij} \prod_{g \in \mathcal{G}_j} v_{jg}^{g_{p_i}}, \qquad L_j = \prod_{g \in \mathcal{G}_j} v_{jg}^{g_k}, \tag{10.2}$$

$$F_j(t) = L_j U_j, \qquad Z_j = \left(\prod_i \varepsilon_{ij}^{e_i}\right) U_j^{m_j} \prod_{g \in \mathcal{G}_j} v_{jg}^{g_z}.$$

The signs $\varepsilon_{ij} \in \{1, -1\}$ and the signed quotient U_j recover the target. These are identities whenever $F_j(t) = L_j U_j$. Every $g \in \mathcal{G}_j$ has positive g_k and at least one positive g_{p_i}. Consequently any prime dividing v_{jg} at the target occurs in some P_{ij}, and the products of these bases for distinct columns are pairwise coprime by (10.1).

The completely split case. Suppose every $F_j(t) = t - r_j$ is linear. Apply Proposition 4.2 to the scalar blocks $(v_{jg})_{g \in \mathcal{G}_j}$. Since all g_k are positive, the resulting L_j are pairwise coprime. Put

$B_j = \prod_{k\neq j} L_k$, and choose polynomial witnesses $L_jV_j + B_jW_j = 1$ using Lemma 2.4. With a free integer v, set

$$t = \sum_j r_j B_j W_j + \Big(\prod_j L_j\Big)v, \qquad U_j = -r_jV_j + \sum_{k\neq j} r_k\Big(\prod_{i\neq j,k} L_i\Big)W_k + B_jv.$$

Then $t - r_j = L_jU_j$ identically, including specializations with a zero modulus. Use (10.2) and output

$$x_i = h_i \prod_j P_{ij}, \qquad z = \frac{\prod_j Z_j}{\kappa C_x}.$$

The exponent identities prove the equation. Only the fixed denominator κC_x remains, and Lemma 2.1 handles it. At each nonzero target the chosen L_j are nonzero and pairwise coprime; the Chinese remainder theorem therefore supplies v giving its exact value of t, after which all other coordinates are recovered. Together with the zero families already separated, this proves the completely split case without quadratic-field input.

Assume henceforth that at least one quadratic factor occurs, and fix its common splitting field F.

Norm realization of the quadratic columns. For a linear column keep the v_{jg} as a scalar block. For a quadratic column write $F_j(t) = t^2 + b_jt + c_j$ and $\sqrt{b_j^2 - 4c_j} = u_j + w_j\omega$ with fixed integers u_j, w_j and $w_j \neq 0$. This is possible because the square root is integral in F. Put

$$\beta_j = 2t + b_j + u_j + w_j\omega, \qquad \mathrm{N}(\beta_j) = 4F_j(t).$$

In this paragraph the elements are numerical targets. Let $g_0 = \gcd(2t + b_j + u_j, w_j) > 0$ and $\beta'_j = \beta_j/g_0$, which is coordinate-primitive. Define the fixed integer $K_j = w_j^2 \prod_{p|D_F} p$. Remove fixed parts $d_{jg} = \gcd(v_{jg}, K_j)$ and write $v'_{jg} = v_{jg}/d_{jg}$. Then

$$\prod_g (v'_{jg})^{g_k} \mid |\mathrm{N}(\beta'_j)|, \qquad \gcd(v'_{jg}, D_F) = 1. \tag{10.3}$$

Indeed $L_j \mid F_j(t)$, hence $L_j \mid |\mathrm{N}(\beta_j)|$. For a ramified rational prime the valuation of the norm of a primitive element is at most one, so the original weighted valuation is at most $2v_p(w_j) + 1 = v_p(K_j)$ and every base loses its entire power. For an unramified p dividing w_j, if some base has positive residual valuation, its removed weighted valuation is at least $2v_p(w_j)$, which pays for the division by g_0^2. Other primes require no removal. This proves (10.3).

A primitive quadratic integer has no inert prime ideal factor and uses at most one of the two orientations over a split rational prime. By (10.3), allocate to each base an integral ideal $\mathfrak{a}_{jg}$ of norm v'_{jg} with $\prod_g \mathfrak{a}_{jg}^{g_k} \mid (\beta'_j)$, using these orientations. All these ideals use only unramified split primes. By the oriented ideal representative lemma (Lemma 10.1), choose for each $\mathfrak{a}_{jg}$ a representative I_{jg} of its inverse class from a fixed finite list, using compatible orientations with β'_j and with each other within this column. Different quadratic columns may use different systems of representatives. Choose generators a_{jg} of $\mathfrak{a}_{jg}I_{jg}$. Their product is unramified primitive, and $|\mathrm{N}(a_{jg})| = v'_{jg}\,\mathrm{N}\,I_{jg}$. Define the fixed scale $C_j^* = \prod_g \mathrm{N}\,I_{jg}$. The unweighted norm product divided by this scale, namely $\mathrm{N}(\prod_g a_{jg})/C_j^*$, has absolute value $\prod_g v'_{jg}$, hence is coprime to the analogous products in all other columns and to the scalar block products. The signs of the norms cause no change to these coprimalities.

There are finitely many choices of the ideals I_{jg}, hence finitely many tuples of scales C_j^*. Carry out the following construction separately for each such choice. Apply Theorem 9.4 with level 1, seeds 1, these quadratic blocks with their now fixed scales C_j^*, and the linear scalar blocks. Its fixed integer B may depend on this scale choice; the level 1 is admissible for every choice. The scalar target bases are positive, so the theorem attains all the selected data in its

required fibre. Retain the fixed divisibilities $\mathrm{N}\, I_{jg} \mid \mathrm{N}(a_{jg})$ and choose independent fixed signs σ_{jg}. Use the integer-polynomial outputs (after subdivision)

$$v_{jg} = \frac{\sigma_{jg} d_{jg}\, \mathrm{N}(a_{jg})}{\mathrm{N}\, I_{jg}}$$

for the quadratic bases. At the target take the signs to give the original positive bases. For each quadratic column define

$$\widehat{A}_j = \prod_g a_{jg}^{g_k}, \quad \widehat{n}_j = \mathrm{N}(\widehat{A}_j), \quad C_j^{**} = \prod_g (\mathrm{N}\, I_{jg})^{g_k}, \quad q_j = \widehat{n}_j / C_j^{**}.$$

The q_j are integer polynomials after the fixed subdivisions, and their prime supports equal those of the corresponding unweighted norm quotients: both are products of the integers $\mathrm{N}(a_{jg})/\mathrm{N}\, I_{jg}$ with fixed positive exponents. Hence the q_j and the L_j for linear columns are pairwise coprime by Theorem 9.4. For each quadratic column $L_j = \gamma_j \widehat{n}_j$ with a fixed nonzero rational constant $\gamma_j = \prod_g (\sigma_{jg} d_{jg}/\mathrm{N}\, I_{jg})^{g_k}$.

At the numerical target the ideal $(\widehat{A}_j)$ divides $(C_j^{**}\beta_j)$, since the allocated ideals divide (β_j') and every I_{jg} divides its rational norm ideal. The primitive product $\widehat{A}_j$ has the completion (9.1). Reducing $C_j^{**}\beta_j$ modulo $\widehat{A}_j\mathcal{O}$ and using the cyclic quotient lemma therefore gives

$$2t + b_j + u_j \equiv w_j L_{\widehat{A}_j} \pmod{q_j}. \tag{10.4}$$

Indeed $\widehat{n}_j \mid C_j^{**}(2t + b_j + u_j - w_j L_{\widehat{A}_j})$ and $C_j^{**} \mid \widehat{n}_j$. This congruence is used only to check the residue at a numerical target.

Simultaneous completion. Use the common variable $T = 2t$. For a linear factor $F_j(t) = t - r_j$ we seek $T \equiv 2r_j \pmod{L_j}$. For a quadratic factor seek $T \equiv w_j L_{\widehat{A}_j} - b_j - u_j \pmod{q_j}$. Each required residue is an integer polynomial in the parameters already chosen. The moduli are pairwise coprime, as just shown. Write them as M_j and the residues as R_j, let $B_j = \prod_{k \neq j} M_k$, and choose polynomial witnesses $M_j V_j + B_j W_j = 1$. With an unrestricted integer parameter v, set

$$T = \sum_j R_j B_j W_j + \left(\prod_j M_j \right) v,$$

$$W_j' = -R_j V_j + \sum_{k \neq j} R_k \left(\prod_{i \neq j,k} M_i \right) W_k + B_j v.$$

Direct expansion gives $T - R_j = M_j W_j'$ as a polynomial identity. This is the Chinese remainder construction with explicit quotients, valid even when a scalar modulus is zero at a specialization. For a linear column take $U_j = W_j'/2$, so $F_j(T/2) = L_j U_j$. For a quadratic column use its primitive completion from (9.1) and define

$$d_j' = w_j E_{\widehat{A}_j} + \frac{W_j'}{C_j^{**}} \overline{\widehat{A}_j}.$$

Then $\widehat{A}_j d_j' = T + b_j + u_j + w_j \omega$ identically, because $\mathrm{N}(\widehat{A}_j) = C_j^{**} q_j$. Taking norms gives $4F_j(T/2) = \widehat{n}_j\, \mathrm{N}(d_j')$. Thus

$$U_j = \mathrm{N}(d_j')/(4\gamma_j)$$

is a rational polynomial with fixed denominators and satisfies $F_j(T/2) = L_j U_j$. The auxiliary element d_j' need not be integral; only the final output coordinates need be integral. This fixed rational completion avoids a division by a variable norm.

Finally use (10.2) and output

$$t = T/2, \qquad x_i = h_i \prod_j P_{ij}, \qquad z = \frac{\prod_j Z_j}{\kappa C_x}.$$

The Hilbert basis identities give (1.6) identically, because $\prod_j Z_j \prod_{i,j} P_{ij}^{e_i} = \prod_j F_j(t)^{m_j}$. All expressions have only fixed denominators; apply Lemma 2.1 to the final coordinates. There are only finitely many choices of the scales, signs and ideal representatives. Every target survives: the norm and scalar block construction attains its chosen bases and ideals; (10.4) and the linear divisibilities show that its $T = 2t$ has all the required residues. The target moduli are nonzero, so the single CRT parameter v attains that T exactly. The resulting $U_j = F_j(t)/L_j$ then recover the target Z_j, all left variables, and z. This proves the full finite polynomial cover. □

11 Worked examples

We give parametrizations and completeness proofs for seven equations listed as open in [5] and [6]. The first two are instances of Theorem A; the remaining five are instances of Theorem B. The first five formulas use the polynomial maps specified below and have explicit parameter bounds. The last two are explicit in terms of the covers constructed in Theorems 8.6 and 9.4; their coordinate polynomials and parameter counts are not expanded here. For each formula we prove that every parameter choice gives an integer solution and that every integer solution is attained. The last two proofs include the exceptional primes 2 and 3. In the first five formulas, n is an unrestricted integer parameter. Every Bézout coefficient below is a polynomial output of the cited construction.

11.1 Two polynomial parametrizations

The formulas use the following polynomial parametrizations.

(a) Let $(a, b, c, d) = \mathcal{S}(\theta)$ be Vaserstein's 46-parameter polynomial map whose image is exactly the quadruples with $ad - bc = 1$ [1, Theorem 1]. Fixed congruences on its entries are handled by Lemma 2.1.

(b) Write

$$(a_1, \dots, a_p\,;\, b_1, \dots, b_q\,;\, R, S) = \mathcal{B}_{p,q}(\theta), \qquad \Big(\prod_i a_i\Big)R + \Big(\prod_j b_j\Big)S = 1,$$

for the polynomial map of Proposition 4.2, together with its polynomial Bézout coefficients. Its projection to the a_i, b_j coordinates covers exactly the tuples with coprime block products. All entries, including R, S, are polynomial outputs on unrestricted integer parameters θ.

Composing the first five formulas with these parametrizations and applying Lemma 2.1 gives integer polynomials on unrestricted parameters. Their displayed denominators are the fixed integers 1 or 2, and their displayed congruences are resolved by finite residue subdivision. The proofs include zero coordinates. Using these two parametrizations keeps the displayed formulas short. Each visit in Proposition 4.2 adds the 108 parameters of Lemma 3.2. Filling the first block freely and then the second uses at most $p + q + 108pq$ parameters for $\mathcal{B}_{p,q}$. Thus (11.2) and (11.5) use at most 220 and 437 parameters per residue branch, respectively. The other three of these five formulas use at most 47. These upper bounds come directly from the construction.

11.2 The equation $x^2y + zt + 1 = 0$

For $ad - bc = 1$, all solutions are

$$\boxed{(x, y, z, t) = (a,\ -d^2 + bn,\ b,\ c(2 + bc) - a^2n).} \tag{11.1}$$

Indeed, $a^2d^2 - bc(2 + bc) = (ad - bc)(ad + bc) - 2bc = 1$. Conversely, every solution has $\gcd(x, z) = 1$, so choose a determinant-one completion with $(a, b) = (x, z)$. The displayed particular solution and the kernel vector $(b, -a^2)$ give every pair (y, t). This remains valid when $a = 0$ or $b = 0$.

11.3 The equation $x_1x_2x_3 + x_4x_5 + 1 = 0$

Take $(a, b\,;\, c\,;\, R, S) = \mathcal{B}_{2,1}(\theta)$. Then all solutions are

$$\boxed{(x_1, x_2, x_3, x_4, x_5) = (a, b, -R + cn, c, -S - abn).} \tag{11.2}$$

The identity follows from $abR + cS = 1$. Conversely, the equation forces $\gcd(x_1x_2, x_4) = 1$, so the map $\mathcal{B}_{2,1}$ attains $(a, b, c) = (x_1, x_2, x_4)$. For any supplied Bézout coefficients R, S, the kernel vector $(c, -ab)$ gives every pair (x_3, x_5), including all zero cases.

11.4 The equation $x^2y + z^2 - 1 = 0$

For $ad - bc = 1$, put

$$R = d^2(ad - 3bc), \qquad S = c^2(3ad - bc).$$

For either $\eta = 1$ or $\eta = 2$, all the following triples are solutions, and together the two formulas cover every solution:

$$\boxed{\begin{aligned} x &= \eta ab, \\ y &= \big((2/\eta)R + b^2n\big)\big((2/\eta)S - a^2n\big), \\ z &= a^2R - b^2S + \eta a^2b^2n. \end{aligned}} \tag{11.3}$$

Here $2/\eta$ is the fixed integer 2 or 1. The polynomial identity $a^2R + b^2S = (ad - bc)^3$, followed by $ad - bc = 1$, gives $a^2R + b^2S = 1$. Thus the factors of $1 - z^2$ are

$$z + 1 = a^2(2R + \eta b^2n), \qquad 1 - z = b^2(2S - \eta a^2n),$$

which prove the equation.

For completeness, if x is odd, allocate its prime powers between $z + 1$ and $z - 1$, whose gcd divides 2. This gives $x = ab$, $\gcd(a, b) = 1$, $a^2 \mid z + 1$, and $b^2 \mid z - 1$. If $z = \pm 1$, allocate all prime powers to the vanishing factor. Choose c, d completing (a, b); the Chinese remainder theorem gives $z = a^2R - b^2S + a^2b^2n$, the $\eta = 1$ formula. If $x \neq 0$ is even, then z is odd and $(z + 1)/2, (z - 1)/2$ are coprime. Allocating the prime powers of $x/2$ gives $x = 2ab$, $a^2 \mid (z + 1)/2$, and $b^2 \mid (z - 1)/2$. Put $z_0 = a^2R - b^2S$. Since $z_0 + 1 = 2a^2R$ and $1 - z_0 = 2b^2S$, both $2a^2$ and $2b^2$ divide $z - z_0$. Their least common multiple is $2a^2b^2$, giving the $\eta = 2$ formula. In both cases the equation determines y as displayed. Finally, for $x = 0$, the $\eta = 2$ formula with $(a, b) = (0, 1)$ or $(1, 0)$ gives $z = -1$ or 1, respectively, and lets y range over all integers.

11.5 The equation $x^2y + z^2 + 1 = 0$

Take $ad - bc = 1$ with the fixed parity conditions $c \equiv d \equiv 1 \pmod 2$, and set

$$A = a^2 + b^2, \qquad U = ac + bd, \qquad V = c^2 + d^2, \qquad H = UV/2 + An.$$

Together, the choices $\varepsilon = 1$ and $\varepsilon = -1$ cover all solutions:

$$\boxed{(x, y, z) = (\varepsilon A,\ -V^2 - 2Un - H^2,\ U + AH).} \tag{11.4}$$

The denominator 2 is fixed and V is even. Since $AV - U^2 = (ad - bc)^2 = 1$, direct expansion gives

$$(U + AH)^2 + 1 = A^2(V^2 + 2Un + H^2).$$

For completeness, every solution has $x \neq 0$ and $A = |x|$ odd. Unique factorization in $\mathbb{Z}[i]$ supplies a Gaussian divisor $a + bi$ of $z - i$ with norm A and $\gcd(a, b) = 1$: each odd prime $p \mid A$ splits, and its two conjugate Gaussian prime factors cannot both divide $z - i$, whose imaginary part is -1. For the unique factor π dividing $z - i$, $v_\pi(z - i) = v_p(z^2 + 1) \geq 2v_p(A)$. Taking the factor $\pi^{v_p(A)}$ for each $p \mid A$ gives the required divisor. Write

$$z - i = (a + bi)(c_0 - d_0 i).$$

Then $ad_0 - bc_0 = 1$ and $ac_0 + bd_0 = z$. The integers a, b have opposite parity. Replacing (c_0, d_0) by $(c_0 + a\nu, d_0 + b\nu)$ for a suitable integer ν makes both entries odd and preserves the determinant, while making $U \equiv z \pmod{A}$. At $n = 0$, the displayed formula gives a root Z_0 of $Z_0^2 + 1 \equiv 0 \pmod{A^2}$ with $Z_0 \equiv z \pmod{A}$. Since $\gcd(2z, A) = 1$, this root lifts uniquely from modulo A to modulo A^2: from $A^2 \mid (Z_0 - z)(Z_0 + z)$ one obtains $A^2 \mid Z_0 - z$. Varying n changes z by $A^2 n$, so every target z is attained. The sign ε gives the prescribed x, and the original equation then fixes y.

11.6 The equation $xyz + t^2 - 1 = 0$

Take $(a, c\,;\, b, d\,;\, R, S) = \mathcal{B}_{2,2}(\theta)$ and put

$$P = ac, \qquad Q = bd, \qquad U = 2R + Qn, \qquad V = 2S - Pn.$$

For each $(h, k) \in \{(1, 1), (2, 1), (1, 2)\}$, retain the fixed congruence $UV \equiv 0 \pmod{hk}$ and set

$$\boxed{(x, y, z, t) = (hab,\ kcd,\ UV/(hk),\ PR - QS + PQn).} \tag{11.5}$$

Add the six linear families obtained by setting $t = \pm 1$ and one of x, y, z equal to zero, leaving the other two free. Together these families cover all solutions. Indeed, $PR + QS = 1$ gives $t + 1 = PU$ and $1 - t = QV$, so $1 - t^2 = PQ\,UV = xyz$. The denominator hk is the fixed integer 1 or 2.

For completeness when $t \neq \pm 1$, the three coordinates x, y, z are nonzero. All odd prime powers of xy can be allocated wholly to $t + 1$ or $t - 1$. At 2, at most one of $t + 1, t - 1$ has valuation greater than 1. If xy is even, remove one factor 2 from an even coordinate of x, y, choosing $(h, k) = (2, 1)$ or $(1, 2)$; otherwise choose $(1, 1)$. When xy is even, assign the entire remaining 2-part of both x/h and y/k to the same root factor $t + 1$ or $t - 1$, choosing one of larger 2-adic valuation. It has enough powers of 2, since the smaller valuation is 1 and one factor 2 was removed from xy. Thus one can factor $x/h = ab$, $y/k = cd$ with $\gcd(ac, bd) = 1$, $ac \mid t + 1$, and $bd \mid t - 1$. The map $\mathcal{B}_{2,2}$ attains these coordinates. For its supplied Bézout coefficients R, S, the Chinese remainder theorem gives $t = PR - QS + PQn$. The target equation then gives $UV = hkz$, including the required fixed congruence. The six linear families cover $t = \pm 1$.

11.7 The equation $xyz + t^2 + 1 = 0$

Apply Theorem 8.6 to two factors in $\mathbb{Z}[i]$, with level $m = 1$ and both seeds equal to 1. On each branch, write its polynomial outputs as $a + bi$ and $c + di$, and put

$$P = ac - bd, \qquad Q = ad + bc.$$

Their product $P + iQ$ is coordinate-primitive and has odd norm for every parameter value, and the branches attain every pair with these properties. By Lemma 2.4, after a finite residue subdivision there are polynomial outputs U, V satisfying $PU + QV = 1$. For a new unrestricted integer parameter w, put

$$B_0 = V + wP, \qquad B_1 = U - wQ, \qquad T = PB_0 - QB_1.$$

Choose

$$(d_1, d_2) \in \{(1,1), (2,1), (1,2)\}, \qquad \varepsilon_1, \varepsilon_2 \in \{1, -1\}, \qquad d_* = d_1 d_2.$$

Retain the fixed congruence $B_0^2 + B_1^2 \equiv 0 \pmod{d_*}$ by Lemma 2.1. The complete solution set is given by

$$\boxed{\begin{aligned} x &= \varepsilon_1 d_1 (a^2 + b^2), \\ y &= \varepsilon_2 d_2 (c^2 + d^2), \\ z &= -\varepsilon_1 \varepsilon_2 (B_0^2 + B_1^2)/d_*, \\ t &= T. \end{aligned}} \tag{11.6}$$

The only possible denominator is 2. Indeed,

$$(P + iQ)(B_0 + iB_1) = T + i,$$

since $PB_1 + QB_0 = PU + QV = 1$. Taking norms proves $xyz = -(T^2 + 1)$.

For completeness, let (x, y, z, t) be any solution. All three product coordinates are nonzero. In the Gaussian integers, all odd prime factors of $t + i$ lie over split rational primes, and a prime and its conjugate cannot both occur: a common divisor of $t + i$ and $t - i$ divides $2i$. Moreover, $v_2(t^2 + 1)$ is either 0 or 1. Thus at most one of $|x|, |y|, |z|$ is even. Set $d_1 = 2$ if x is even and $d_1 = 1$ otherwise; define d_2 in the same way from y. Unique factorization in $\mathbb{Z}[i]$ lets us allocate the odd prime factors of $t + i$ to factors $a + bi$ and $c + di$ with norms $|x|/d_1$ and $|y|/d_2$, leaving a factor $B_0 + iB_1$ such that

$$(a + bi)(c + di)(B_0 + iB_1) = t + i.$$

The product of the first two factors has odd norm and is coordinate-primitive, so the stated polynomial cover attains them. For the resulting polynomial witnesses U, V, every integral solution of $QB_0 + PB_1 = 1$ has the form $(B_0, B_1) = (V + wP, U - wQ)$ for an integer w, because $\gcd(P, Q) = 1$. Finally, the remaining norm is $d_*|z|$, which satisfies the retained congruence. Taking $\varepsilon_1 = \operatorname{sgn}(x)$ and $\varepsilon_2 = \operatorname{sgn}(y)$ recovers the target, including its third sign. This proves completeness.

Remark 11.1. The same construction gives $x_1 \cdots x_h = t^2 + 1$ for any fixed $h \geq 2$. Take $h - 1$ Gaussian factors a_j with unramified primitive product $P + iQ$. Obtain polynomial witnesses U, V with $PU + QV = 1$ by Lemma 2.4, and use the preceding formulas for B_0, B_1, T with a new free integer w. Choose $d_j \in \{1, 2\}$ with at most one $d_j = 2$, set $d_* = \prod_{j<h} d_j$, and choose signs with $\prod_{j=1}^{h} \varepsilon_j = 1$. The formulas are

$$x_j = \varepsilon_j d_j \, \mathrm{N}(a_j) \ (j < h), \qquad x_h = \varepsilon_h (B_0^2 + B_1^2)/d_*, \qquad t = T,$$

with the fixed integrality filter. The preceding prime allocation and kernel argument prove completeness for any number of factors.

11.8 The equation $x^3 + yz + 1 = 0$

Put $\omega = (1 + \sqrt{-3})/2$, so that $\omega^2 = \omega - 1$ and

$$\mathrm{N}(a + b\omega) = a^2 + ab + b^2.$$

Apply Theorem 9.4 with one quadratic block of one factor in $\mathbb{Z}[\omega]$, one scalar block of one entry, scale 1, and level 1, taking both seeds equal to 1. Write the resulting polynomial outputs as a, b, u. For every parameter value they satisfy

$$\gcd(a, b) = 1, \qquad 3 \nmid N, \qquad \gcd(N, u) = 1, \qquad N = a^2 + ab + b^2.$$

The branches attain every triple with these properties and $u \neq 0$. The parameters of each branch are unrestricted. Lemma 2.4 supplies, after a finite residue subdivision, polynomial outputs $\alpha, \beta, \eta, \zeta$ such that

$$a\alpha + b\beta = 1, \qquad N\eta + u\zeta = 1.$$

With a new unrestricted integer parameter w, define

$$\begin{aligned} \Lambda &= a\beta - (a+b)\alpha, & r &= \eta(\Lambda - 1) + uw, \\ B_0 &= \alpha - \beta + (a+b)r, & B_1 &= -\alpha - br, \\ T &= -\Lambda + Nr, & C &= \zeta(1 - \Lambda) + Nw, \\ \mathcal{N} &= B_0^2 + B_0 B_1 + B_1^2. \end{aligned}$$

For each fixed $\delta \in \{1, 3\}$, retain the congruence $C\mathcal{N} \equiv 0 \pmod{\delta}$ and set

$$\boxed{(x, y, z) = (T,\ \delta uN,\ -C\mathcal{N}/\delta).} \tag{11.7}$$

Add the two linear families $(-1, v, 0)$ and $(-1, 0, v)$, with $v \in \mathbb{Z}$. Lemma 2.1 removes the fixed denominator 3.

To verify the equation, put $A = a + b\omega$ and $E = (\beta - \alpha) + \alpha\omega$. Direct multiplication gives

$$AE = \Lambda + \omega, \qquad B_0 + B_1\omega = -E + r\bar{A}, \qquad A(B_0 + B_1\omega) = T - \omega.$$

Consequently

$$T^2 - T + 1 = N\mathcal{N}, \qquad T + 1 = uC.$$

Multiplying these two identities gives $T^3 + 1 = uCN\mathcal{N} = -yz$. Thus every retained parameter value yields a solution.

For completeness, take a solution with $x \neq -1$, and write $q = x^2 - x + 1$. Then $y, z \neq 0$ and

$$\gcd(|x + 1|, q) = \gcd(|x + 1|, 3).$$

If $3 \mid q$, then $x \equiv -1 \pmod{3}$ and $v_3(q) = 1$. Allocate every prime power of $|y|$ away from 3 to its unique factor among $|x + 1|$ and q. At 3, at most one factor 3 must be taken from q: take $\delta = 3$ precisely when $v_3(y) > v_3(x + 1)$, and otherwise take $\delta = 1$. This gives

$$y = \delta uN, \qquad u \mid x + 1, \qquad N \mid q, \qquad N > 0, \quad 3 \nmid N, \quad \gcd(u, N) = 1.$$

The ring $\mathbb{Z}[\omega]$ is Euclidean for its norm: rounding both coordinates gives a remainder of relative norm at most $3/4$. It therefore has unique factorization. Away from the ramified prime above 3, only one of each pair of conjugate primes can divide $x - \omega$, because a common divisor of $x - \omega$ and $x - \bar{\omega}$ divides $\omega - \bar{\omega}$, whose norm is 3. We may therefore choose a divisor

$A = a + b\omega$ of $x - \omega$ with norm N. It is coordinate-primitive and has norm prime to 3. The joint cover attains this A and the chosen u.

Let B be the remaining factor, so that $AB = x - \omega$. For the polynomial witnesses α, β supplied at this specialization, every such B has the form $-E + r\bar{A}$ with $r \in \mathbb{Z}$: the ω-coordinate equation is $bB_0 + (a+b)B_1 = -1$, and $\gcd(b, a+b) = 1$. Thus $x = -\Lambda + Nr$. Since $u \mid x + 1$ and $N\eta + u\zeta = 1$, we have $r = \eta(\Lambda - 1) + uw$ for some integer w. Formula (11.7) now gives the target x, y; the original equation, with $y \neq 0$, gives its target z and ensures the retained divisibility by δ. The two linear families cover $x = -1$. Hence every integer solution is attained.

11.9 Further applications

Theorem B gives finite polynomial covers for every equation in (1.7) and (1.8). The irreducible quadratic in $t^3 + 1$ splits over $\mathbb{Q}(\sqrt{-3})$; those in $t^3 + t$ and $t^4 - 1$ split over $\mathbb{Q}(i)$. The minus signs on the right-hand sides are absorbed in κ. The result also applies to $2xy + z^3 + 1 = 0$, and to $x^3 + yz + z + 1 = 0$ after the integral translation $y' = y + 1$, since polynomial covers are preserved by inverse integral affine substitutions. All these conclusions include the families at the integral roots of the right-hand polynomials.

Use of AI. OpenAI's ChatGPT and Codex were used extensively in developing proof arguments and parametrizations, checking identities and references, and drafting and revising the manuscript. A review generated by Anthropic's Claude Opus 5.5 also informed the exposition.

References

[1] L. N. Vaserstein, *Polynomial parametrization for the solutions of Diophantine equations and arithmetic groups*, Ann. of Math. (2) **171** (2010), no. 2, 979–1009. https://doi.org/10.4007/annals.2010.171.979.

[2] S. Frisch, *Remarks on polynomial parametrization of sets of integer points*, Comm. Algebra **36** (2008), no. 3, 1110–1114. https://doi.org/10.1080/00927870701776938.

[3] S. Frisch and G. Lettl, *Polynomial parametrization of the solutions of Diophantine equations of genus 0*, Funct. Approx. Comment. Math. **39** (2008), no. 2, 205–209. https://doi.org/10.7169/facm/1229696571.

[4] W. Bruns, J. Gubeladze and N. V. Trung, *Problems and algorithms for affine semigroups*, Semigroup Forum **64** (2002), 180–212. https://doi.org/10.1007/s002330010099.

[5] B. Grechuk, *Polynomial Diophantine Equations: A Systematic Approach*, Springer, Cham, 2024. https://doi.org/10.1007/978-3-031-62949-5.

[6] B. Grechuk, *A systematic approach to Diophantine equations: open problems*, arXiv:2404.08518v1, 12 April 2024. https://arxiv.org/abs/2404.08518v1.

[7] B. Grechuk, *A systematic approach to Diophantine equations: open problems*, arXiv:2404.08518v11 (2026). https://arxiv.org/abs/2404.08518v11.

[8] B. Grechuk and A. Ratcliffe, *Polynomial parametrization of quadratic Diophantine equations: decision and construction*, Hexagon 2610.00652 (2026). https://hexagonmath.org/2610.00652v1.

[9] M. Larsen and D. Q. N. Nguyen, *Polynomial parametrization for* SL_2 *over quadratic number rings*, Int. Math. Res. Not. IMRN **2021**, no. 9, 6993–7003. https://doi.org/10.1093/imrn/rnz046. Preprint: https://arxiv.org/abs/1808.05349.

[10] D. Carter and G. Keller, *Bounded elementary generation of* $\mathrm{SL}_n(\mathcal{O})$, Amer. J. Math. **105** (1983), no. 3, 673–687. https://doi.org/10.2307/2374319.

[11] D. W. Morris, *Bounded generation of* $\mathrm{SL}(n, A)$ *(after D. Carter, G. Keller, and E. Paige)*, New York J. Math. **13** (2007), 383–421. https://nyjm.albany.edu/j/2007/13_383.html.

[12] 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. https://doi.org/10.2140/ant.2018.12.1949.

[13] D. A. Marcus, *Number Fields*, 2nd ed., Universitext, Springer, Cham, 2018.

[14] J. S. Milne, *Class Field Theory*, course notes, 4.03, 6 August 2020. https://www.jmilne.org/math/CourseNotes/CFT.pdf.

[15] J. Neukirch, *Algebraic Number Theory*, Grundlehren der mathematischen Wissenschaften 322, Springer, Berlin, 1999.

[16] I. Schur, *Über die Existenz unendlich vieler Primzahlen in einigen speziellen arithmetischen Progressionen*, Sitzungsber. Berl. Math. Ges. **11** (1912), 40–50.