REALIZATION AND RIGIDITY OF FINITE DISCRIMINANT PAIRINGS

ANASS NIFA

ABSTRACT. Let $\mu(A, b)$ be the least cycle rank of a connected loopless multigraph whose Jacobian has a prescribed nonsingular symmetric pairing (A, b). For odd-order groups, $d(A) \le \mu(A, b) \le d(A) + 2$, where $d(A)$ is the minimum number of generators. Exact formulas hold for odd-primary pairings and for mixed-prime pairings with at most two elementary-divisor exponents at each prime. For every finite pairing, adjoining one cyclic pairing of prime order permits planar realization in cycle rank $\max\{1, d(A)\}$. In rank at least two, the graphs subdivide a fixed ladder. The local pairings remain fixed while one path length varies through a primitive arithmetic progression of determinants. Prescribed prime residue and pairing classes are characterized by local determinant and Hasse invariants. Symmetric ladders give hyperelliptic Jacobians with prescribed positive monodromy pairings, up to one prime summand, at finitely many places of odd residue characteristic and in the least possible semistable dimension when $\max_v d(A_v) \ge 2$. The local fields remain unchanged. Finally, a rational homology three-sphere of first homology $\mathbb{Z}/2$ cannot embed locally flatly in a simply connected topological four-manifold with intersection lattice an orthogonal power of the positive Leech lattice.

CONTENTS

1. Introduction 3
1.1. Minimum cycle rank 3
1.2. One prime complement 4
1.3. Monodromy over prescribed local fields 5
1.4. A fixed definite ambient lattice 5
1.5. Positive integral presentations 6
2. Integral lattices and unimodular gluing 6
2.1. Graph lattices 7
3. Local integral presentations 9
3.1. Primary decomposition and local presentations 10
3.2. Local determinant and Hasse data in small rank 13
3.3. Integral lifts of an orthogonal decomposition 13
3.4. Rational existence and integral gluing 16
4. Graphical presentations of ranks two and three 17
4.1. Reduction in dimension three 17
4.2. Local integral presentations 18
4.3. Global existence and proof of the criterion 18
4.4. The criterion with arbitrary two-primary data 18
4.5. A closed formula when the two-primary part is cyclic 20
4.6. The binary realization criterion 20
4.7. Minimum cycle rank for odd cyclic pairings 21
4.8. Even cyclic pairings in ranks at most three 23
5. Exact rank bounds and mixed-prime constructions 24
5.1. Orthogonal sums of binary presentations 24
5.2. Pairing two primary cyclic summands without extra cycles 26
5.3. Primary pairings for $p \not\equiv 7 \pmod 8$ 26
5.4. A composite-order binary construction 27

2020 *Mathematics Subject Classification.* 11E08, 11E12, 05C50, 14H40, 11G20, 57N35.

Key words and phrases. Discriminant pairing, integral lattice, graph Jacobian, monodromy, prime complement, locally flat embedding.

5.5. Primary forms at distinct scales 30
5.6. Minimum cycle rank for odd-primary pairings 30
5.7. Scale multiplicities and minimum rank 32
5.8. Prescribed norm extraction and global cycles 33
5.9. Coprime complements of specified order 35
5.10. Counting the pairing classes at each minimum 35
5.11. Orthogonal sums and graph blocks 36
5.12. Optimal realizations with one nontrivial block 36
5.13. Reduction to generator ranks three, four and five 38
6. Prime stabilization with prescribed arithmetic 39
6.1. Tridiagonal flow matrices on planar ladders 39
6.2. A primitive arithmetic progression of determinants 41
6.3. Prime residue and pairing classes 43
7. Equivariant graphical realization 47
7.1. Unimodular forms with prescribed row sums 47
7.2. Length-preserving involutions on prime-complement graphs 48
8. Prescribed monodromy of hyperelliptic Jacobians 49
8.1. Lifting over the prescribed valuation ring 50
9. Global arithmetic with fixed local pairings 52
9.1. Global approximation and absolute simplicity 52
9.2. The maximal adelic group 54
9.3. Galois representations in coefficient congruence classes 55
9.4. Nonisogenous realizations with independent branch fields 57
9.5. Inertia invariants and the component group 58
10. Fixed ambient lattices and stable nonembedding 58
10.1. Homology of the complementary regions 59
10.2. The integral sign-change obstruction 60
10.3. Orthogonal powers of the Leech lattice 60
11. Further realization questions 61
Appendix A. Quadratic refinements and prime classes 62
A.1. Even presentations and full local stability 62
A.2. The quadratic refinement of a bipartite graph 65
A.3. A local criterion for prime residue classes 66
A.4. The exact cycle rank with a prescribed prime Brown invariant 68
Appendix B. Cyclic two-primary minima 70
Appendix C. The pairing of a complete graph 73
C.1. Divisor generators and their pairings 73
C.2. Hyperbolic reduction at the prime two 73
Appendix D. Explicit integral and arithmetic examples 76
D.1. Pairings with minimum cycle ranks four and five 76
D.2. Two prime-complement pairings 78
D.3. An explicit genus-three coefficient progression 79
D.4. An index-two orthogonal sublattice of E_8 81
D.5. Cyclic pairings of order at most 2048 82
References 88

1. Introduction

Let A be a finite abelian group and let $b : A \times A \to \mathbb{Q}/\mathbb{Z}$ be a nonsingular symmetric bilinear pairing. For a nonsingular integral lattice K, its dual and discriminant pairing are

$$K^\vee = \{x \in K \otimes \mathbb{Q} : (x, K) \subset \mathbb{Z}\}, \qquad \mathcal{D}(K) = \big(K^\vee/K,\ (x,y) \bmod \mathbb{Z}\big).$$

If C is a Gram matrix, the same pairing on $\mathbb{Z}^r/C\mathbb{Z}^r$ is $([x],[y]) \mapsto x^{\mathsf{T}} C^{-1} y \bmod \mathbb{Z}$. Write $\perp$ for orthogonal sum, and put

$$\left\langle \tfrac{a}{n} \right\rangle = \left(\mathbb{Z}/n\mathbb{Z},\ ([x],[y]) \longmapsto \frac{axy}{n} \bmod \mathbb{Z}\right) \qquad (n \geq 1,\ \gcd(a,n) = 1).$$

The pairing with denominator one is trivial. If A_p is the p-primary part of A, then

$$d(A) = \max_p \dim_{\mathbb{F}_p}(A_p/pA_p), \qquad d(0) = 0.$$

All graphs are finite and connected. They are loopless unless stated otherwise; parallel edges are permitted. Each edge has weight one. An edge of integral length denotes its subdivision into that number of unit edges. Biconnectivity means that there are at least three vertices and deletion of any vertex leaves the graph connected. The cycle rank and minimum realization rank are

$$\beta(G) = |E(G)| - |V(G)| + 1, \qquad \mu(A,b) = \min\{\beta(G) : (\mathrm{Jac}(G), b_G) \cong (A,b)\}. \tag{1.1}$$

Here b_G is the pairing of the positive graph Laplacian, and an empty minimum is $+\infty$. The graph on one vertex realizes the trivial pairing. The cut and flow lattices satisfy

$$(\mathrm{Jac}(G), b_G) \cong \mathcal{D}(\mathcal{B}(G)) \cong -\mathcal{D}(\mathcal{F}(G)).$$

These isomorphisms follow from primitive orthogonal complementation in the unimodular edge lattice [3, 32]; the signs and integral maps are given in Section 2. Since $\mathcal{F}(G)$ has rank $\beta(G)$, every realization satisfies $d(A) \leq \beta(G)$.

1.1. Minimum cycle rank.

Minimum graphical rank need not increase under orthogonal addition. For primes $\ell \equiv 7 \pmod 8$,

$$\mu\big(\left\langle \tfrac{1}{8} \right\rangle\big) = 7, \qquad \mu\big(\left\langle \tfrac{1}{8} \right\rangle \perp \left\langle \tfrac{-8}{\ell} \right\rangle\big) = 1. \tag{1.2}$$

The first equality is Theorem B.1. For the second, let z generate the paired Jacobian $\left\langle \frac{-1}{8\ell} \right\rangle$ of the cycle of length 8ℓ. Then

$$b(\ell z, \ell z) = -\ell/8 = 1/8, \qquad b(8z, 8z) = -8/\ell, \qquad b(\ell z, 8z) = 0 \quad \text{in } \mathbb{Q}/\mathbb{Z}.$$

The two cyclic subgroups have coprime orders 8 and ℓ and exhaust the group. A nontrivial Jacobian has positive cycle rank.

Theorem A. *For every nontrivial odd-order pairing,*

$$d(A) \leq \mu(A,b) \leq d(A) + 2.$$

There is a planar realization of cycle rank at most $d(A)+2$ and treewidth at most three. No smaller additive constant holds for all nontrivial odd-order pairings. If A is an odd p-group, $d = d(A) \geq 3$, and

$$(A,b) = \mathop{\perp}_{i=1}^{d} \left\langle \frac{a_i}{p^{s_i}} \right\rangle, \qquad \Delta = \left(\frac{(-1)^d \prod_i a_i}{p}\right),$$

then $\mu(A,b) = d + (1-\Delta)/2$. Each primary minimum has a planar realization.

The uniform bound is Theorem 5.3; $\mu(\langle \frac{1}{7} \rangle) = 3$ makes the additive constant necessary. Theorem 5.12 and Corollary 5.13 include the two exceptional families in generator ranks one and two. The stronger inequality $\mu(A, b) \le d(A) + 1$ for odd-order pairings with $d(A) \ge 2$ remains Conjecture 5.25.

At an odd prime with $d(A_p) = d(A)$, a presentation of rank $d(A)$ has no unimodular summand. Its determinant square class is therefore fixed by the finite pairing. For odd $N = |A|$, put $N_p = N/|A_p|$ and let α_p be the product of the local cyclic unit coefficients modulo squares. If $d = d(A) \ge 3$ and at most two elementary-divisor exponents occur at each prime, Theorem 5.15 gives

$$\mu(A, b) = \begin{cases} d, & \left(\dfrac{(-1)^d N_p \alpha_p}{p}\right) = 1 \text{ for every } p \text{ with } d(A_p) = d, \\ d+1, & \text{otherwise.} \end{cases}$$

Adjoining a coprime odd-order pairing of order m with at most two generators multiplies these characters by $\left(\frac{m}{p}\right)$ (Theorem 5.19).

Orthogonal assembly alone need not attain the minimum. For $p \equiv 7 \pmod 8$ and distinct odd $s_1 < s_2 < s_3$, the pairing $\perp_{i=1}^{3} \left\langle \frac{1}{p^{s_i}} \right\rangle$ has minimum four, whereas every realization with two or more nontrivial blocks has cycle rank at least five (Theorem 5.7 and Proposition 5.22).

Wall's generators and the two-primary relations of Kawauchi–Kojima and Miranda describe the finite pairings [39, 24, 30]. Greene's continued-fraction graph lattices [21, Section 3.3, p. 466], together with the inverse-Laplacian pairing [37], give exact cyclic realization. Orthogonal primary decomposition and vertex sums then give exact realization for every odd-order pairing. Gaudet–Jensen–Ranganathan–Wawrykow–Weisman study the paired graphical realization problem [19]; [20, Theorem 25] includes every cyclic two-primary pairing. The additional condition in Theorem A is the bound on cycle rank and its exact value in the primary case.

1.2. **One prime complement.**

Theorem B. *Let (A, b) be any finite pairing. For infinitely many odd primes $\ell \nmid |A|$, there are simple planar biconnected graphs G_ℓ with*

$$(\mathrm{Jac}(G_\ell), b_{G_\ell}) \cong (A, b) \perp \left\langle \tfrac{\kappa}{\ell} \right\rangle, \qquad \beta(G_\ell) = \max\{1, d(A)\}.$$

The integer $\kappa \neq 0$ is fixed in the family. The primes avoid any prescribed finite set. Every vertex degree belongs to $\{2, 3\}$, the treewidth is at most two, and the girth has any prescribed lower bound. In rank at least two, the graphs are subdivisions of a fixed ladder with one path length varying. In rank one, they are cycles.

The ladder separates the integral rank from the size of the discriminant. Its bounded facial cycles have a tridiagonal Gram matrix (Figure 1). Local integral presentations can be approximated by such matrices while their row sums and adjacent weights are made arbitrarily large. Put $N = |A|$. Proposition 6.3 gives positive integers u, v, F such that

$$\det L_t = N(u + vt), \qquad \gcd(u, v) = 1, \qquad \mathcal{D}(L_t) \cong (A, -b) \perp \left\langle \tfrac{NF}{u+vt} \right\rangle.$$

Here F is the last principal cofactor and only the last diagonal entry varies. The tridiagonal determinant recurrence gives $\gcd(u + vt, NF) = 1$; the class $N[e_r]$ has norm $NF/(u + vt)$ and order $u + vt$. Thus both the order and the pairing of the complementary summand are determined; the graph pairing has $\kappa = -NF$. Dirichlet's theorem supplies infinitely many prime values of $u + vt$, proving Theorem 6.4.

Prescribing the prime residue class and the square class of its pairing introduces a local obstruction. For $m \ge 1$, $(a, m) = 1$ and $\varepsilon \in \{1, -1\}$, infinitely many realizations with $\ell \equiv a \pmod m$ and $\left(\frac{\kappa}{\ell}\right) = \varepsilon$ exist at every rank

$$r \ge \max\{d(A) + 1, d(A_2) + 3\}.$$

This universal bound is sharp. At each individual rank, the necessary and sufficient determinant and Hasse conditions are those of Theorem 6.7.

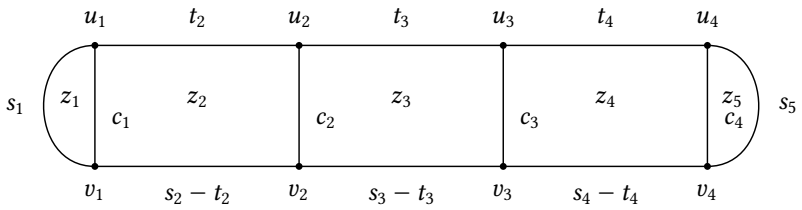


FIGURE 1. The ladder Q_5. Each edge denotes a path of the indicated positive integral length. Put $c_0 = c_5 = 0$ and $b_i = s_i + c_{i-1} + c_i$. Consistently oriented facial cycles z_i have Gram matrix with diagonal b_i, adjacent entries $-c_i$, and all other entries zero. Interchange of the two rails preserves lengths when $t_i = s_i/2$ for $2 \le i \le 4$.

Tridiagonal facial matrices occur in Chen–Mohar's polygon families [6, 7]. The independent length congruences in Proposition 6.3 prescribe the local pairings and the primitive determinant progression simultaneously. For random graphs, Hodges prescribes finitely many primary pairings [23, Corollary 10.5], while Nguyen–Wood obtain a cyclic complement for underlying groups [31, Theorem 1.22]. Theorem B imposes one prime complement at minimum cycle rank in a fixed planar family. Related distributions of paired cokernels are treated in [9, 40, 35].

1.3. **Monodromy over prescribed local fields.** For a split semistable Jacobian, write $\lambda^+ = \mathcal{D}(Q)$ for the positive finite monodromy pairing of its integral length form Q. The graph pairing of the same flow matrix is $-\mathcal{D}(Q)$.

Theorem C. *Let F be a number field and S a finite nonempty set of places of odd residue characteristic. Prescribe (A_v, b_v) at $v \in S$, and let $g \ge \max\{2, \max_v d(A_v)\}$. There are fixed $\kappa_v > 0$ and infinite prime sets $\mathcal{P}_v$ such that every tuple $(\ell_v) \in \prod_v \mathcal{P}_v$ occurs on a genus-g hyperelliptic curve:*

$$(\Phi_{\mathrm{Jac}\,C,v}(\overline{k_v}), \lambda_v^+) \cong (A_v, b_v) \perp \left\langle \tfrac{\kappa_v}{\ell_v} \right\rangle .$$

The reduction is split and totally degenerate over each original local field F_v, with integral symmetric ladder lengths. The geometric endomorphism ring may be $\mathbb{Z}$. When $D = \max_v d(A_v) \ge 2$, one may take $g = D$; this dimension is minimal among semistable Jacobians whose geometric component groups admit A_v as a quotient at every $v \in S$.

The local realization is Lemma 8.2 and the simultaneous realization is Theorem 9.3. The parity conditions of Section 7 make the two rail lengths equal and integral without increasing the rank. Equivariant smoothing over the given valuation ring retains every node thickness. In contrast, ramification of index e replaces Q by eQ and can change its discriminant pairing. Baker–Norine relate hyperelliptic graphs to involutions with tree quotient [4]; Amini–Baker–Brugallé–Rabinoff develop lifting for harmonic morphisms and group actions [1, Section 4]. The specified valuation ring and integral lengths are the additional conditions in Theorem C.

For each fixed tuple (ℓ_v), the local pairings are constant in an integral coefficient congruence class by [13, Theorem 19.1]. Zarhin's and Hall's theorems give the endomorphism and residual-image conclusions [41, 22]. The theorem of Landesman–Swaminathan–Tao–Xu gives maximal admissible adelic image on a relative density-one subset of that class [27, Theorem 1.2]; see also [28] and Corollary 9.8. The density is in integral coefficient vectors in a fixed congruence class. Theorem 9.9 gives infinitely many pairwise geometrically nonisogenous Jacobians with jointly linearly disjoint branch splitting fields.

1.4. **A fixed definite ambient lattice.** The preceding realizations allow the integral lattice to vary. A fixed unimodular ambient lattice can impose a further obstruction. Let Λ_{24} be the positive Leech lattice.

Theorem D. *No closed oriented rational homology three-sphere Y with $H_1(Y;\mathbb{Z}) \cong \mathbb{Z}/2$ embeds locally flatly in a closed simply connected oriented topological four-manifold with intersection lattice $\Lambda_{24}^{\perp n}$, for any $n \ge 1$.*

Such an embedding would give determinant-two side lattices $U \perp V \subset \Lambda_{24}^{\perp n}$ of index two. For $2x = u+v$, the isometry $s = 1_U \perp (-1_V)$ satisfies $s(x) = x - v \in \Lambda_{24}^{\perp n}$. The even lattice V has odd rank, so $\det s = -1$. Conway's classification excludes this involution in every orthogonal power of the Leech lattice [11, Chapter 10, Section 3.7]; see also [36, Theorem 3.3]. Freedman's theorem supplies the corresponding topological four-manifold [18, Theorem 1.5]. Section 10 gives the integral and homological details. The relation with Edmonds's Conjecture 1.3 in the 21 December 2001 preprint [17] is stated in Remark 10.9.

1.5. **Positive integral presentations.** Kneser–Puppe's Satz 3 identifies integral presentations of an odd-order linking pairing up to integral congruence and addition of unimodular rank-one forms of either sign [25, p. 382]. Positivity and fixed graphical rank impose further conditions. Rational quadratic-space existence [33, Theorem 7.35] and reduction in dimensions two and three [34, 10] give the low-rank criteria in Section 4. Edmonds gives rank-two integral presentations without positivity and a positive presentation bound of six [17, Theorem 3.2 and Proposition 6.4]. Zhu determines positive even-lattice ranks for specified finite quadratic modules [42, Theorems 5.8 and 5.9]. Appendix A imposes this additional quadratic refinement. Bosch–Lorenzini's realization by arithmetical graphs permits a nonconstant vertex-multiplicity vector [5, Proposition 5.2].

Recognition of a given cographic form is treated by Chua–Kummer–Sturmfels in dimension four [8, Section 3], and by Mandelshtam through conorms [29]. Prescribing the discriminant and rank instead asks whether a set of integral forms contains a cographic form. For example, Remark B.5 gives a positive integral rank-four presentation of $-\left\langle \frac{1}{8} \right\rangle$, although $\mu(\left\langle \frac{1}{8} \right\rangle) = 7$.

The complete-graph pairings in Appendix C give explicit biconnected hyperbolic examples at higher powers of two. The identity $(\mathrm{Jac}(K_4), b_{K_4}) \cong \mathcal{F}_4$ from [19] and the relation $\mathcal{F}_4 \perp \mathcal{F}_4 \cong \mathcal{E}_4 \perp \mathcal{E}_4$ [30, Table 1.2, relation (IV)] already give $(\mathrm{Jac}(K_4 \vee K_4), b_{K_4 \vee K_4}) \cong \mathcal{E}_4^{\perp 2}$, a counterexample to [20, Conjecture 27].

2. Integral lattices and unimodular gluing

An integral lattice is a finite-rank free abelian group K with a nonsingular symmetric bilinear form $K \times K \to \mathbb{Z}$. Put

$$K^\vee = \{x \in K \otimes \mathbb{Q} : (x, K) \subset \mathbb{Z}\}, \qquad \mathcal{D}(K) = K^\vee / K.$$

The induced scalar product modulo $\mathbb{Z}$ is nonsingular. If C is a Gram matrix, the map $[x] \mapsto [C^{-1}x]$ identifies it with

$$\left(\mathbb{Z}^r / C\mathbb{Z}^r,\ ([x],[y]) \mapsto x^{\mathsf{T}} C^{-1} y \bmod \mathbb{Z}\right).$$

Its order is $|\det C|$. The empty lattice has trivial discriminant pairing. If T is the integral basis matrix of a full-rank inclusion $K \subset L$, then $C_K = T^{\mathsf{T}} C_L T$, $[L : K] = |\det T|$, and hence $\det K = [L : K]^2 \det L$. These identities include the empty matrix, whose determinant is one.

Lemma 2.1. *Let U be integral unimodular and let $K \subset U$ be primitive and nonsingular. Put $T = K_{\mathbb{Q}}^{\perp} \cap U$. The quotient $U/(K \perp T)$ is the graph of an anti-isometry $\mathcal{D}(K) \to \mathcal{D}(T)$. In particular $\mathcal{D}(T) \cong -\mathcal{D}(K)$.*

Proof. The subspace $K_{\mathbb{Q}}^{\perp}$ is defined over $\mathbb{Q}$, so $T \otimes \mathbb{Q} = K_{\mathbb{Q}}^{\perp}$ and $\operatorname{rank} K + \operatorname{rank} T = \operatorname{rank} U$. If $mx \in T$ for $x \in U$ and $m \neq 0$, then $m(x, K) = 0$, whence $x \in T$. Thus T is primitive. The rational projections give an inclusion $U \subset K^\vee \perp T^\vee$. Its image modulo $K \perp T$ is a subgroup $\Gamma \subset \mathcal{D}(K) \oplus \mathcal{D}(T)$. The scalar product of two elements of U is integral; hence Γ is isotropic for the sum pairing. If an element of Γ has zero first coordinate, a representative $x \in U$ has projection in K. Subtracting that element gives $x \in K_{\mathbb{Q}}^{\perp} \cap U = T$, so its second coordinate is zero. If the second coordinate is zero, subtraction of the projection in T leaves an element of $K_{\mathbb{Q}} \cap U = K$, since K is primitive. Thus the second projection is also injective, and $|\Gamma| \leq |\mathcal{D}(K)|$ and $|\Gamma| \leq |\mathcal{D}(T)|$. The index formula and unimodularity give $|\Gamma|^2 = |\mathcal{D}(K)|\,|\mathcal{D}(T)|$. Both inequalities are equalities. The two projections are isomorphisms; isotropy says their composite is an anti-isometry. □

The lemma applies to nonsingular integral lattices of arbitrary signature; see [32].

Lemma 2.2. *Let $K_+ \perp K_- \subset L$ be a full-rank orthogonal inclusion of integral lattices with $2L \subset K_+ \perp K_-$. Then the rational isometry equal to $+1$ on $K_+ \otimes \mathbb{Q}$ and -1 on $K_- \otimes \mathbb{Q}$ preserves L. Its determinant is $(-1)^{\operatorname{rank} K_-}$.*

Proof. For $x \in L$, write $2x = u + v$ with $u \in K_+$ and $v \in K_-$. The sign change sends x to $(u - v)/2 = x - v \in L$. Its square is the identity, so it is an automorphism of L. Its two rational eigenspaces have dimensions $\operatorname{rank} K_+$ and $\operatorname{rank} K_-$. □

2.1. **Graph lattices.** Let G be a finite connected graph, with vertex set V and edge set E. Parallel edges are allowed at this stage. Loops, if present, have zero incidence column. Choose an orientation of the edges and write

$$\partial : \mathbb{Z}^E \longrightarrow \mathbb{Z}^V$$

for the incidence map, with a column having -1 at its initial vertex and $+1$ at its terminal vertex. The edge group $\mathbb{Z}^E$ has the Euclidean scalar product and is a unimodular integral lattice. Put

$$\beta(G) = |E| - |V| + 1, \qquad \mathcal{F}(G) = \ker \partial, \qquad \mathcal{B}(G) = \partial^{\mathsf{T}} \mathbb{Z}^V.$$

These are the integral flow and cut lattices. Reversing an edge orientation changes one edge coordinate by a sign and therefore does not change either lattice up to isometry.

In Gram coordinates,

$$\mathcal{D}(C) = (\mathbb{Z}^r / C\mathbb{Z}^r, C^{-1} \bmod \mathbb{Z}). \tag{2.1}$$

The graph Laplacian is $L_G = \partial\partial^{\mathsf{T}}$. Define

$$\operatorname{Div}^0(G) = \left\{ x \in \mathbb{Z}^V \,:\, \sum_{v \in V} x_v = 0 \right\}, \qquad \operatorname{Jac}(G) = \operatorname{Div}^0(G) / L_G \mathbb{Z}^V.$$

For $x, y \in \operatorname{Div}^0(G)$, choose a rational potential f with $L_G f = x$ and put

$$b_G([x],[y]) = f^{\mathsf{T}} y \pmod{\mathbb{Z}}. \tag{2.2}$$

For every $f \in \mathbb{Q}^V$,

$$f^{\mathsf{T}} L_G f = \sum_{e \in E} (f(e_+) - f(e_-))^2.$$

Connectedness gives $\ker L_G = \mathbb{Q}\mathbf{1}$. Since L_G is symmetric, its rational image is the subspace of coordinate sum zero. The potential therefore exists. Changing f by a constant does not change the expression. Replacing x by $x + L_G g$, with g integral, replaces f by $f + g$ and changes the value by $g^{\mathsf{T}} y \in \mathbb{Z}$. Replacing y by $y + L_G h$ changes it by $f^{\mathsf{T}} L_G h = x^{\mathsf{T}} h \in \mathbb{Z}$. For rational potentials f, h of x, y, symmetry follows from $f^{\mathsf{T}} L_G h = h^{\mathsf{T}} L_G f$. Equivalently, after deleting one row and column of L_G to obtain the positive definite reduced Laplacian Q, this pairing is presented by Q^{-1} on $\mathbb{Z}^{|V|-1}/Q\mathbb{Z}^{|V|-1}$. This is the monodromy pairing of [37].

The following cut–flow correspondence fixes the sign of the inverse-matrix pairing; compare [3].

Lemma 2.3. *The lattices $\mathcal{F}(G)$ and $\mathcal{B}(G)$ are primitive sublattices of $\mathbb{Z}^E$, of ranks $\beta(G)$ and $|V| - 1$. Their rational spans are orthogonal complements. In particular, an integral linear functional on either lattice extends to an integral linear functional on $\mathbb{Z}^E$.*

Proof. Choose a spanning tree T. For every edge $e \notin T$, the edge e and the unique tree path joining its endpoints give an oriented fundamental cycle z_e, with coefficient one on e and zero on all other edges outside T. A loop itself is its fundamental cycle. For an integral flow z, subtract $\sum_{e \notin T} z(e) z_e$, where $z(e)$ is its coefficient on e. The remainder is a flow supported on a tree. At a leaf its incident coefficient is zero by the incidence equation. Deleting that leaf and repeating gives the zero flow. Thus the fundamental cycles form an integral basis of $\mathcal{F}(G)$. Matching the coordinates outside T also gives the direct-sum decomposition

$$\mathbb{Z}^E = \mathcal{F}(G) \oplus \mathbb{Z}^{E(T)},$$

where the second summand consists of vectors supported on tree edges.

Fix a root of T. An integral assignment of signed differences to the tree edges integrates uniquely to an integral vertex potential which is zero at the root. Consequently restriction to tree-edge coordinates gives an isomorphism

$$\mathcal{B}(G) \longrightarrow \mathbb{Z}^{E(T)}.$$

Every integral edge vector has a unique cut vector with the same tree coordinates. Subtracting that cut vector leaves a vector supported outside T, proving that $\mathcal{B}(G)$ is also a direct summand of $\mathbb{Z}^E$.

The ranks are now $|E \setminus E(T)| = \beta(G)$ and $|E(T)| = |V| - 1$. For $z \in \mathcal{F}(G)$ and any potential f,

$$\langle z, \partial^{\mathsf{T}} f \rangle = \langle \partial z, f \rangle = 0.$$

The ranks sum to $|E|$, proving the assertion about rational orthogonal complements. A functional on a direct summand extends by zero on a chosen integral complement. □

Lemma 2.4. *There are isometries of finite pairings*

$$(\mathrm{Jac}(G), b_G) \cong \mathcal{D}(\mathcal{B}(G)) \cong -\mathcal{D}(\mathcal{F}(G)). \tag{2.3}$$

In particular, if C is the Gram matrix of an integral flow basis, then

$$(\mathrm{Jac}(G), b_G) \cong \left(\mathbb{Z}^{\beta(G)}/C\mathbb{Z}^{\beta(G)}, -C^{-1} \pmod{\mathbb{Z}}\right). \tag{2.4}$$

Proof. Lemma 2.3 and Lemma 2.1 identify the two discriminants with opposite signs. The common quotient is

$$\mathbb{Z}^E/(\mathcal{F} + \mathcal{B}). \tag{2.5}$$

The incidence map sends an oriented path to its endpoint difference, hence surjects onto $\mathrm{Div}^0(G)$. It maps $\mathcal{F} + \mathcal{B}$ onto $L_G\mathbb{Z}^V$. If $\partial z = L_G f$ for an integral potential f, then $z - \partial^{\mathsf{T}} f \in \mathcal{F}$; thus the induced map from the common quotient to $\mathrm{Jac}(G)$ is an isomorphism. For a rational f with $L_G f = \partial z$, the cut projection is $\pi_{\mathcal{B}} z = \partial^{\mathsf{T}} f$. For integral z, z', one has

$$(\pi_{\mathcal{B}} z, \pi_{\mathcal{B}} z') = (\partial^{\mathsf{T}} f, z') = f^{\mathsf{T}} \partial z'.$$

Modulo $\mathbb{Z}$ this is the graph pairing. The cut discriminant is therefore the positive graph pairing, and the flow discriminant is its negative. □

Lemma 2.5. *Let H be a connected plane multigraph, and let H^* be its plane dual. The edge correspondence, with compatible orientations, induces an integral isometry*

$$\mathcal{B}(H) \cong \mathcal{F}(H^*).$$

Consequently $(\mathrm{Jac}(H^*), b_{H^*}) \cong -(\mathrm{Jac}(H), b_H)$.

Proof. Orient each dual edge from the face on the right of its primal edge to the face on its left. The signed edge correspondence is an isometry $\mathbb{Z}^{E(H)} \to \mathbb{Z}^{E(H^*)}$. For an integral potential f on $V(H)$, the incidence sum of its edge differences at a dual vertex is the sum of successive differences around the corresponding facial boundary. This sum is zero, including repeated edges in that boundary. Hence the image of $\mathcal{B}(H)$ lies in $\mathcal{F}(H^*)$. The dual graph is connected, and Euler's formula gives

$$\operatorname{rank} \mathcal{F}(H^*) = |E(H)| - |F(H)| + 1 = |V(H)| - 1 = \operatorname{rank} \mathcal{B}(H).$$

The two groups therefore have the same rational span. Since $\mathcal{B}(H)$ is primitive in the edge group by Lemma 2.3, the inclusion is equality. The last assertion follows from Lemma 2.4. □

Lemma 2.6. *A vertex sum of connected graphs has the orthogonal sum of their paired Jacobians and the sum of their cycle ranks. Uniform subdivision by an integer $m \geq 1$ multiplies an integral flow Gram matrix by m and preserves cycle rank. Deleting a loop leaves the paired Jacobian unchanged.*

Proof. Delete the identified vertex in a vertex sum. Its reduced Laplacian is block diagonal, with the reduced Laplacians of the summands as blocks; its inverse has the same block structure. This proves the pairing assertion. The edge and vertex counts give the rank assertion. On a subdivided edge, the incidence equation at every new degree-two vertex forces equal coefficients on the two consecutive segments. Restriction and constant extension are inverse maps of integral flow groups. A path of m edges contributes m times the old scalar product. A loop has zero incidence column, so it does not alter the Laplacian. □

In a loopless graph, a block is a maximal connected subgraph with at least one edge and no cut vertex; a bridge by itself is a block. The graph on one vertex and no edges has no blocks. A block is nontrivial if it contains a cycle.

Lemma 2.7. *The paired Jacobian of a connected loopless graph is the orthogonal sum of those of its blocks, and its cycle rank is their sum. A block consisting of one bridge has trivial Jacobian. Every other block has at least two spanning trees and a nontrivial Jacobian.*

Proof. If a vertex v disconnects the graph, take the subgraphs consisting of v and each component of $G - v$, with all incident edges. They form a vertex sum; Lemma 2.6 applies. Repetition terminates because each proper factor has fewer edges. The remaining factors have no cut vertex, including a single edge and the two-vertex parallel-edge case. A single edge has reduced Laplacian $[1]$. A factor with a cycle has two distinct spanning trees: extend all but one edge of that cycle to a spanning tree, then exchange the missing cycle edge for a different edge of the cycle. Finally, the reduced incidence matrix D_0 satisfies

$$\det(D_0 D_0^{\mathsf{T}}) = \sum_{|T|=|V|-1} \det(D_{0,T})^2.$$

A tree minor has determinant ± 1, by successive leaf deletion. A non-tree minor has dependent columns, either from a cycle or because it does not connect all vertices. The displayed sum counts the spanning trees, so a cyclic block has Jacobian order at least two. □

Lemma 2.8. *Let G be connected and loopless. If $b_G(x, x) = 0$ for every $x \in \mathrm{Jac}(G)$, then G is a tree and its Jacobian is trivial.*

Proof. For an edge $e = vw$, let $D = e_v - e_w$ and choose $L_G f = D$. Put $\rho = f(v) - f(w)$. The energy identity gives

$$0 < \rho = f^{\mathsf{T}} L_G f = \rho^2 + \sum_{e' \neq e} (f(e'_+) - f(e'_-))^2.$$

Thus $0 < \rho \leq 1$. Its residue modulo $\mathbb{Z}$ is $b_G([D], [D])$, so the hypothesis forces $\rho = 1$. Every other edge difference is zero. A path from v to w avoiding e would then have total difference zero, contrary to $\rho = 1$. Every edge is a bridge. A connected graph all of whose edges are bridges is a tree, and the spanning-tree formula in Lemma 2.7 gives Jacobian order one. □

In particular the nonzero alternating pairing on $(\mathbb{Z}/2)^2$ has no exact graph realization, although Theorem 6.4 gives its prime completions.

3. Local integral presentations

For a prime p, the discriminant of an integral $\mathbb{Z}_p$-lattice takes values in $\mathbb{Q}_p/\mathbb{Z}_p$, identified with the p-primary part of $\mathbb{Q}/\mathbb{Z}$. Normalize the valuation by $v_p(p) = 1$. For a diagonal rational quadratic space set

$$h_p(\mathrm{diag}(c_1, \dots, c_r)) = \prod_{i<j} (c_i, c_j)_p.$$

Its orthogonal-sum formula is $h_p(S \perp T) = h_p(S)h_p(T)(\det S, \det T)_p$. For $x = p^a u$ and $y = p^b v$, with units u, v, the Hilbert symbols are

$$(x,y)_p = (-1)^{ab(p-1)/2}\left(\frac{u}{p}\right)^b\left(\frac{v}{p}\right)^a \qquad (p \neq 2),$$
$$(x,y)_2 = (-1)^{\epsilon(u)\epsilon(v)+a\omega(v)+b\omega(u)}, \qquad \epsilon(u) = (u-1)/2 \bmod 2, \quad \omega(u) = (u^2-1)/8 \bmod 2.$$

For a rational nonsingular form C, $\prod_{p\le\infty} h_p(C) = 1$. For a positive definite real form, $h_\infty = 1$. These conventions are those of [33].

3.1. **Primary decomposition and local presentations.**

Lemma 3.1. *Every nondegenerate symmetric bilinear pairing on a finite abelian group of odd order is an orthogonal sum of nondegenerate cyclic pairings.*

Proof. Let n be the exponent of A, and write $n = \prod_p p^{r_p}$. For each prime divisor p choose an integer e_p which is 1 modulo p^{r_p} and 0 modulo each q^{r_q} for $q \neq p$. Such integers exist because the prime powers are pairwise coprime, by Bézout's identity. Modulo n they satisfy $\sum_p e_p = 1$ and $e_p e_q = 0$ for $p \neq q$. Thus

$$A = \bigoplus_p A_p, \qquad A_p = e_p A = \{x \in A : p^{r_p} x = 0\}. \tag{3.1}$$

Indeed, $x = \sum_p e_p x$, and applying e_q to a relation among these summands shows that its q-th summand is zero. Moreover, $p^{r_p} e_p$ is divisible by n, whereas $e_p - 1$ is divisible by p^{r_p}; these two divisibilities give the equality defining A_p in (3.1). For $x \in A_p$ and $y \in A_q$ with $p \neq q$, the value $b(x,y)$ is annihilated by both p^{r_p} and q^{r_q}. Bézout's identity therefore gives $b(x,y) = 0$. Each restricted pairing on A_p is nondegenerate: an element in its radical is orthogonal to every primary summand and hence is zero. It remains to treat a nontrivial p-group, with p odd. Let its exponent be p^r. The orders of its elements are powers of p, so their least common multiple is their maximum. Choose x of order p^r. The character $b(x,-)$ has order p^r, since $p^{r-1}b(x,-) = 0$ would imply $b(p^{r-1}x, A) = 0$ and then $p^{r-1}x = 0$. Consequently some $y \in A$ has $b(x,y)$ of order p^r in $\mathbb{Q}/\mathbb{Z}$; otherwise every value of that character would be annihilated by p^{r-1}. Choose integers u, v, w modulo p^r with

$$b(x,x) = \frac{u}{p^r}, \qquad b(y,y) = \frac{v}{p^r}, \qquad b(x,y) = \frac{w}{p^r}, \qquad p \nmid w, \tag{3.2}$$

where the fractions denote classes modulo $\mathbb{Z}$. If $p \nmid u$, take $z = x$; if $p \nmid v$, take $z = y$. If $p \mid u$ and $p \mid v$, take $z = x + y$. Then $b(z,z) = (u + 2w + v)/p^r$, whose numerator is a unit modulo p because p is odd and $p \nmid w$. In all cases there is z with

$$b(z,z) = \frac{c}{p^r}, \qquad p \nmid c. \tag{3.3}$$

Its order is exactly p^r: its self-pairing has that order, and the exponent of A is p^r. Let $C = \langle z \rangle$. For any $t \in A$, the value $b(t,z)$ belongs to $p^{-r}\mathbb{Z}/\mathbb{Z}$. Multiplication by the unit c is a bijection of $\mathbb{Z}/p^r\mathbb{Z}$, so there is a unique k modulo p^r such that $b(t,z) = kb(z,z)$. Then $t - kz \in C^\perp$. If $kz \in C^\perp$, (3.3) implies $kc \equiv 0 \pmod{p^r}$, hence $kz = 0$. Thus

$$(A,b) = (C, b|_C) \perp (C^\perp, b|_{C^\perp}). \tag{3.4}$$

An element of $C^\perp$ pairing to zero with $C^\perp$ also pairs to zero with C, hence with all of A; it is zero. The complementary pairing is therefore nondegenerate. Its group has smaller order than A, since $|C| = p^r > 1$. Induction on $|A|$ completes the proof for the p-group, and (3.1) completes the general case. □

Lemma 3.2. *Every finite paired group is an orthogonal sum of nondegenerate cyclic pairings and pairings*

$$\left((\mathbb{Z}/N\mathbb{Z})^2, B/N\right), \qquad N = 2^r, \quad r \ge 1, \tag{3.5}$$

where B is symmetric integral with even diagonal and odd determinant.

Proof. Primary subgroups are mutually orthogonal and nondegenerate by the proof of Lemma 3.1; that lemma treats all odd primes. Let A be a nonzero 2-primary paired group of exponent $N = 2^r$. Suppose $b(x,x)$ has order N. Then x has order N and $b(x,x) = a/N$ with a odd. For every $z \in A$, choose k modulo N with $b(z,x) = kb(x,x)$. It follows that $z - kx \in \langle x\rangle^\perp$. If kx belongs to this orthogonal complement, then $ka \equiv 0 \pmod N$, so $kx = 0$. Consequently $A = \langle x\rangle \perp \langle x\rangle^\perp$, and the second summand is nondegenerate. Suppose instead that every self-pairing has order strictly less than N. It then belongs to $2N^{-1}\mathbb{Z}/\mathbb{Z}$. Choose x of order N. If every value of $b(x,-)$ were annihilated by $N/2$, nondegeneracy would give $(N/2)x = 0$, a contradiction. Choose y with $b(x,y) = c/N$, where c is odd. The order of y is N, since it annihilates this value and divides N. Choose the numerator matrix

$$B = \begin{pmatrix} 2a & c \\ c & 2d \end{pmatrix}. \tag{3.6}$$

Its determinant $4ad - c^2$ is odd. If $\alpha x + \beta y = 0$, pairing with x and y gives $B(\alpha,\beta)^{\mathsf T} = 0$ modulo N. Multiplication by $(\det B)^{-1}\operatorname{adj}(B)$ gives $\alpha = \beta = 0$ modulo N. Thus $U = \langle x, y\rangle$ is isomorphic to $(\mathbb{Z}/N\mathbb{Z})^2$, with nondegenerate pairing B/N. For $z \in A$, write $(b(z,x), b(z,y))^{\mathsf T} = v/N$ and solve $B\alpha = v$ modulo N. The element $u = \alpha_1 x + \alpha_2 y$ satisfies $z - u \in U^\perp$. Nondegeneracy on U gives $U \cap U^\perp = 0$, so $A = U \perp U^\perp$. An element of the radical of $b|_{U^\perp}$ annihilates both summands and hence is zero. In either case a nontrivial summand has been removed. Induction on $|A|$ terminates and proves the lemma. For $r = 1$, the second case has zero diagonal modulo two; the same inverse-matrix argument applies. □

Lemma 3.3. *Every even unimodular binary lattice over $\mathbb{Z}_2$ is isometric to exactly one of the forms*

$$H = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad F = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}.$$

Their determinant square classes are respectively -1 and 3.

Proof. Write half the norm as $q(x,y) = ax^2 + uxy + by^2$, where u is odd. The polar matrix modulo two is nonsingular. Suppose first that q has a nonzero zero modulo two. At that vector one partial derivative of q is odd. Successive Hensel corrections produce a primitive $v \in \mathbb{Z}_2^2$ with $(v,v) = 0$. Unimodularity gives w with $(v,w) = 1$. If $(w,w) = 2c$, replace w by $w - cv$. The resulting Gram matrix is H. Its determinant is a unit, so these vectors form a $\mathbb{Z}_2$-basis.

Otherwise q takes value one on each nonzero vector modulo two. Hensel lifting of $q(x,y) - 1$ gives a primitive vector v with $(v,v) = 2$. Choose w with $(v,w) = 1$. Its reduction is independent of that of v, and $(w,w) = 2c$ with c odd. The polynomial

$$f(s) = c - 1 - 3s - 3s^2$$

satisfies $f(0) \in 2\mathbb{Z}_2$ and $f'(0) \in \mathbb{Z}_2^\times$. Choose $s \in \mathbb{Z}_2$ with $f(s) = 0$ and put $w' = (w + sv)/(1 + 2s)$. Then

$$(v, w') = 1, \qquad \frac{(w', w')}{2} = \frac{c + s + s^2}{(1 + 2s)^2} = 1.$$

The change of basis has determinant $(1+2s)^{-1} \in \mathbb{Z}_2^\times$; the resulting Gram matrix is F. Finally, $\det H \equiv 7$ and $\det F \equiv 3 \pmod 8$. A determinant changes under integral congruence by an odd square, which is one modulo eight. The two forms are not isometric. □

Lemma 3.4. *Let (A_p, b_p) be a nonsingular finite p-primary pairing with d_p generators. It has an integral symmetric tridiagonal presentation of rank d_p over $\mathbb{Z}_p$. Appending unimodular lines gives such a presentation at every rank $r \geq d_p$. If p^{e_p} is the exponent of A_p, the presenting matrix satisfies $p^{e_p} C^{-1} \in \operatorname{Mat}_r(\mathbb{Z}_p)$.*

Proof. At an odd prime, the orthogonal cyclic decomposition gives blocks $\langle a/p^k\rangle$, with a a unit. The matrix $[ap^k]$, with generator $[a]$, presents the block. At two, Lemma 3.2 gives cyclic blocks and even

unimodular binary numerator matrices. By Lemma 3.3, each binary numerator is congruent over $\mathbb{Z}_2$ to one of

$$H = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad F = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}.$$

The cyclic blocks again have rank-one presentations. A binary block with numerator $B \in \{H, F\}$ and denominator 2^k is presented over $\mathbb{Z}_2$ by $2^k B$: the map $x \mapsto [Bx]$ gives $(Bx)^{\mathsf{T}}(2^k B)^{-1}(By) = 2^{-k} x^{\mathsf{T}} By$. Both H and F are unimodular over $\mathbb{Z}_2$. The total ranks of these blocks equal the numbers of generators of their groups. Their orthogonal sum is tridiagonal. A unimodular line has trivial local discriminant; adjoining it increases the rank by one and does not change the discriminant pairing. Finally p^{e_p} kills the cokernel precisely when multiplication of the inverse matrix by p^{e_p} is integral. □

Lemma 3.5. *Let C be nonsingular and symmetric over $\mathbb{Z}_p$, and suppose $p^e C^{-1}$ is integral for some integer $e \geq 0$. Let D be symmetric over $\mathbb{Z}_p$. If*

$$D - C \in \begin{cases} p^{e+1} \operatorname{Mat}_r(\mathbb{Z}_p), & p \neq 2, \\ 2^{e+3} \operatorname{Mat}_r(\mathbb{Z}_2), & p = 2, \end{cases}$$

then there is $V \in \mathrm{GL}_r(\mathbb{Z}_p)$ such that

$$D = V^{\mathsf{T}} C V.$$

In particular, D is nonsingular and its discriminant bilinear pairing is isometric to that of C. If p is odd, or if $p = 2$ and C has even diagonal, then $Q_p(D) \cong Q_p(C)$, with Q_p defined in Appendix A; in the latter case D also has even diagonal. No evenness assumption is required for the integral lattice isometry or the bilinear conclusion. The stronger precision p^{2e+3} is sufficient at every prime.

Proof. Put $S = C^{-1}(D - C)$. Then $S \in p \operatorname{Mat}_r(\mathbb{Z}_p)$ when p is odd and $S \in 8 \operatorname{Mat}_r(\mathbb{Z}_2)$ when $p = 2$. Symmetry of C and D gives

$$S^{\mathsf{T}} C = CS.$$

Consider

$$V = \sum_{j \geq 0} \binom{1/2}{j} S^j.$$

For odd p, the coefficients are p-integral. For $j \geq 1$,

$$\binom{1/2}{j} = (-1)^{j-1} \frac{\mathrm{Cat}_{j-1}}{2^{2j-1}}, \qquad \mathrm{Cat}_{j-1} = \frac{1}{j}\binom{2j-2}{j-1} = \binom{2j-2}{j-1} - \binom{2j-2}{j} \in \mathbb{Z}.$$

Thus the series converges p-adically, and $V \in I + p \operatorname{Mat}_r(\mathbb{Z}_p)$. At two, the numerator in

$$\binom{1/2}{j} = \frac{1(1-2)\cdots(1-2(j-1))}{2^j j!}$$

is odd. The valuation of its jth matrix term is at least

$$3j - j - v_2(j!) = 2j - v_2(j!) \geq j + 1 \qquad (j \geq 1).$$

The series therefore converges and belongs to $I + 4 \operatorname{Mat}_r(\mathbb{Z}_2)$. In either case V is invertible. The formal identity for the square root may be evaluated in this convergent series, yielding $V^2 = I + S$. Every partial sum is C-self-adjoint, so passage to the limit gives $V^{\mathsf{T}} C = CV$. Consequently

$$V^{\mathsf{T}} C V = CV^2 = C(I + S) = D.$$

An integral lattice isometry induces an isometry of the discriminant bilinear modules, and of the quadratic modules whenever these are defined. At two, evenness is preserved by integral change of basis. In the displayed cokernel coordinates the map is $[x] \mapsto [V^{-\mathsf{T}} x]$ from the D-cokernel to the C-cokernel, and

$$(V^{-\mathsf{T}} x)^{\mathsf{T}} C^{-1} (V^{-\mathsf{T}} y) = x^{\mathsf{T}} D^{-1} y.$$

When the quadratic discriminants are defined, the same identity with $x = y$, divided by two, proves preservation of the quadratic form. □

3.2. **Local determinant and Hasse data in small rank.** Let (A, b) be a finite nonsingular symmetric pairing, $N = |A|$, and $d_p = d(A_p)$. At every odd $p \mid N$, fix an orthogonal decomposition

$$(A_p, b_p) = \perp_{i=1}^{d_p} \left\langle \frac{a_{p,i}}{p^{s_{p,i}}} \right\rangle, \qquad p \nmid a_{p,i}. \tag{3.7}$$

Define

$$S_p = \operatorname{diag}(-p^{s_{p,1}}/a_{p,1}, \dots, -p^{s_{p,d_p}}/a_{p,d_p}), \quad D_p = \det S_p, \quad w_p = N/D_p, \tag{3.8}$$

and

$$H_{\mathrm{odd}} = \prod_{\substack{p \mid N \\ p \neq 2}} h_p(S_p)(D_p, w_p)_p. \tag{3.9}$$

Every w_p is a p-adic unit. Empty products are one.

At two, fix *one* orthogonal decomposition of $(A_2, -b_2)$ into the finite bilinear blocks [39, 30]

$$C_k(c) = \left\langle \tfrac{c}{2^k} \right\rangle, \qquad \mathcal{E}_{2^k} = \left((\mathbb{Z}/2^k)^2, \frac{H}{2^k} \right), \qquad \mathcal{F}_{2^k} = \left((\mathbb{Z}/2^k)^2, \frac{F}{2^k} \right),$$

where $k \geq 1$, c is odd, and

$$H = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad F = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}.$$

The two blocks $\mathcal{E}_2, \mathcal{F}_2$ are isometric as finite *bilinear* pairings. Both local integral lifts must nevertheless be retained. For odd c put

$$\mathcal{U}_k(c) = \begin{cases} \{1,3,5,7\}, & k = 1, \\ \{u \in \{1,3,5,7\} : u \equiv c \pmod 4\}, & k = 2, \\ \{c \bmod 8\}, & k \geq 3. \end{cases} \tag{3.10}$$

Form a finite list $\mathscr{S}(A_2, -b_2)$ by taking orthogonal sums of the following integral lifts of the chosen blocks:

Finite block	Allowed integral lift	Determinant	Hasse invariant at two
$C_k(c)$	$[2^k u]$, $u \in \mathcal{U}_k(c)$	$2^k u$	1
$\mathcal{E}_2$ or $\mathcal{F}_2$	$2H$ or $2F$	-4 or 12	1
$\mathcal{E}_{2^k}$, $k \geq 2$	$2^k H$	-2^{2k}	1
$\mathcal{F}_{2^k}$, $k \geq 2$	$2^k F$	$3 \cdot 2^{2k}$	$(-1)^{k+1}$

For the trivial primary group the list contains the empty matrix. Each member has rank d_2 and determinant valuation $v_2 N$. Its Hasse invariant is obtained by multiplying the tabulated block invariants and the Hilbert symbols of each pair of block determinants.

For an odd unit v, define the following finite sign sets:

t	$\mathscr{H}_t(v)$
0	$\{1\}$ if $v \equiv 1 \pmod 8$, $\emptyset$ otherwise,
1	$\{1\}$,
2	$\{1\}$ if $v \equiv 7 \pmod 8$, $\{1, -1\}$ otherwise,
3	$\{1, -1\}$.

(3.11)

Congruences of rational odd units are interpreted in $\mathbb{Z}_2$.

3.3. **Integral lifts of an orthogonal decomposition.**

Lemma 3.6. *An integral $\mathbb{Z}_p$-lattice of rank r and discriminant generator rank d_p is an orthogonal sum of a unimodular lattice of rank $r - d_p$ and a lattice whose Gram matrix is divisible by p. The latter has rank d_p and the same discriminant pairing. At an odd prime, unimodular lattices are determined by rank and determinant square class, and their Hasse invariant is one.*

Proof. A vector of unit norm splits off an integral line: subtracting $(x,v)(v,v)^{-1}v$ projects every vector x onto $v^{\perp}$. If p is odd and some Gram entry is a unit, such a vector exists. Indeed, either a diagonal entry is a unit, or the sum of the two basis vectors at a unit mixed entry has unit norm. At two, if every diagonal entry is even but a mixed entry is odd, the corresponding binary principal matrix B has odd determinant. For a Gram matrix

$$\begin{pmatrix} B & X \\ X^{\mathsf{T}} & D \end{pmatrix}, \qquad R = \begin{pmatrix} I & -B^{-1}X \\ 0 & I \end{pmatrix},$$

the matrix R is integral unimodular and

$$R^{\mathsf{T}} \begin{pmatrix} B & X \\ X^{\mathsf{T}} & D \end{pmatrix} R = B \perp (D - X^{\mathsf{T}}B^{-1}X).$$

Thus a unimodular line or binary lattice splits off whenever a Gram entry is a unit. Repetition leaves a matrix divisible by p. Its cokernel modulo p has dimension equal to its rank, while every removed summand has zero cokernel. That rank is therefore d_p.

For odd p, a unimodular lattice diagonalizes into unit lines by successive unit-line splittings. A binary unit form $ax^2 + by^2$ represents one modulo p: the sets $a\{x^2\}$ and $1 - b\{y^2\}$ each have $(p+1)/2$ elements and hence intersect. At a solution one partial derivative is a unit. Hensel lifting gives a vector of norm one over $\mathbb{Z}_p$. Splitting it off and repeating reduces a unimodular form to $\operatorname{diag}(1, \dots, 1, v)$, where v has its determinant square class. Unit norms of the same square class differ by an integral change of basis on the final line. Finally, the Hilbert symbol of two units at an odd prime is one, so every such form has Hasse invariant one. □

Lemma 3.7. *Let S be a nonsingular symmetric integral matrix over $\mathbb{Z}_p$ all of whose entries are divisible by p. Every integral lattice of the same rank and the same discriminant pairing as S is integrally isometric to*

$$T_E = (S^{-1} + E)^{-1}$$

for an integral symmetric matrix E. Conversely every such T_E is integral and has the same discriminant pairing as S. If p is odd, every T_E is integrally isometric to S.

Proof. The discriminant of S has generator rank equal to its matrix size. Thus every presentation of that size is minimal and has all Gram entries divisible by p. Let R be one such presentation. An isometry of the finite discriminant groups lifts to a matrix $Q \in \mathrm{GL}_d(\mathbb{Z}_p)$: both finite groups modulo p have dimension d, so the reduction of any lift is invertible. The pairing identity gives

$$R^{-1} = Q^{\mathsf{T}}S^{-1}Q + E_0$$

with E_0 integral symmetric. Congruence by Q gives

$$(QRQ^{\mathsf{T}})^{-1} = S^{-1} + Q^{-\mathsf{T}}E_0Q^{-1}.$$

Conversely $I + ES$ is integral and invertible, and

$$T_E = S(I + ES)^{-1}.$$

Thus T_E is integral, is divisible by p, and $T_E\mathbb{Z}_p^d = S\mathbb{Z}_p^d$. On this identical finite quotient its inverse pairing differs from the pairing of S by the integral matrix E. For odd p, put $U = S^{-1}T_E = (I + ES)^{-1}$. Then $U - I \in p\,\mathrm{Mat}_d(\mathbb{Z}_p)$ and $U^{\mathsf{T}}S = SU$, since $SU = T_E$ is symmetric. The convergent binomial series of Lemma 3.5 gives a square root $V \in I + p\,\mathrm{Mat}_d(\mathbb{Z}_p)$ of U. Each term is S-self-adjoint, so $V^{\mathsf{T}}SV = SV^2 = SU = T_E$. □

Lemma 3.8. *Suppose $S = S_1 \perp \cdots \perp S_j$ is a minimal integral presentation of a finite pairing over $\mathbb{Z}_p$. Every minimal integral presentation of that pairing is an orthogonal sum of minimal integral presentations of the finite pairings $\mathcal{D}(S_i)$, in the same order.*

Proof. By Lemma 3.7, it suffices to split $S^{-1} + E$. For the first block write

$$S^{-1} + E = \begin{pmatrix} S_1^{-1} + E_{11} & E_{12} \\ E_{21} & S_{\mathrm{rest}}^{-1} + E_{22} \end{pmatrix}.$$

Set $B = S_1^{-1} + E_{11}$ and $D = S_{\mathrm{rest}}^{-1} + E_{22}$. The inverse B^{-1} is integral and divisible by p. Thus

$$T = \begin{pmatrix} I & -B^{-1}E_{12} \\ 0 & I \end{pmatrix} \in \mathrm{GL}_d(\mathbb{Z}_p), \qquad T^{\mathsf{T}} \begin{pmatrix} B & E_{12} \\ E_{21} & D \end{pmatrix} T = B \perp (D - E_{21}B^{-1}E_{12}).$$

This gives

$$B \perp \left(S_{\mathrm{rest}}^{-1} + E_{22} - E_{21}B^{-1}E_{12}\right).$$

The correction in the second block is integral symmetric. Induction splits all the blocks. Inverting the congruence gives the asserted orthogonal decomposition. Lemma 3.7 identifies each finite pairing. □

Lemma 3.9. *The integral lifts listed above contain a representative of every minimal integral presentation of each displayed finite block. Consequently $\mathscr{S}(A_2, -b_2)$ contains every possible determinant square class and Hasse invariant of a minimal integral presentation.*

Proof. For a cyclic block $C_k(c)$ take the minimal presentation $[2^k c]$; the class of c is a generator with norm $c/2^k$. Its inverse perturbations are

$$\left[\frac{2^k c}{1 + 2^k ce}\right], \qquad e \in \mathbb{Z}_2.$$

The possible odd unit square classes of the norm are precisely $\mathcal{U}_k(c)$: for $k = 1$ all four classes occur, for $k = 2$ the two lifts of c mod 4 occur, and for $k \geq 3$ the class modulo eight is fixed. Two rank-one unit norms of the same class modulo eight are integrally isometric by multiplication by a unit square root.

For a binary block take $2^k B$, $B = H$ or F. Every minimal lift is

$$2^k (B^{-1} + 2^k E)^{-1}.$$

The matrix $B^{-1} + 2^k E$ is unimodular with even diagonal. Its inverse is even: the binary adjugate interchanges the diagonal entries and divides them by the odd determinant. Lemma 3.3 gives its isometry to H or F. If $k \geq 2$, the matrix $B^{-1} + 2^k E$ has the same reduction modulo four as B^{-1}. For an even unimodular binary matrix its reduction modulo four determines its determinant modulo eight: write the matrix as $\left(\begin{smallmatrix} 2a & t \\ t & 2b \end{smallmatrix}\right)$ with t odd, whose determinant is $4ab - t^2$. Thus its type is fixed when $k \geq 2$, since the determinant classes of H, F are $7, 3$. At $k = 1$ both types are possible: $\boldsymbol{D}(2H)$ and $\boldsymbol{D}(2F)$ have the same alternating pairing on $(\mathbb{Z}/2)^2$.

The scaled hyperbolic block always has Hasse invariant one. Rational diagonalization of the other block gives

$$2^k F \cong \mathrm{diag}(2^{k+1}, 3 \cdot 2^{k-1}),$$

so its Hasse invariant is $(-1)^{k+1}$. The final assertion follows from Lemma 3.8. □

Lemma 3.10. *The set of Hasse invariants of unimodular integral $\mathbb{Z}_2$-lattices of rank $t \leq 3$ and determinant square class v is exactly $\mathscr{H}_t(v)$.*

Proof. In rank zero the only form has determinant square class one and Hasse invariant one. In rank one the form $[v]$ has determinant square class v and Hasse invariant one, since its defining product is empty. In rank three the matrices $\mathrm{diag}(1, 1, v)$ and $\mathrm{diag}(-1, -1, v)$ have determinant v and opposite Hasse invariants. In rank two $\mathrm{diag}(1, v)$ always gives Hasse invariant one. For $v \equiv 1, 5 \pmod 8$, the matrix $\mathrm{diag}(-1, -v)$ has Hasse invariant -1. For $v \equiv 3 \pmod 8$, the matrix F has determinant square class v and Hasse invariant $(2, 3/2)_2 = -1$. If $v \equiv 7 \pmod 8$, diagonalize a binary space as $[a] \perp [b]$. Then $-ab$ is a square and $(a, b)_2 = (a, -ab)_2 = 1$. Thus no second sign occurs in that class. □

Lemma 3.11. *Let p be odd and let C, C' be nonsingular integral symmetric matrices over $\mathbb{Z}_p$, of size t, with every elementary divisor divisible by p. If $\mathcal{D}(C) \cong \mathcal{D}(C')$, then* $\det C' / \det C$ *is a square in $\mathbb{Z}_p^\times$.*

Proof. An isometry of the finite quotients lifts to a matrix $S \in \mathrm{GL}_t(\mathbb{Z}_p)$: the quotients modulo p both have dimension t, so any lift of the isometry is invertible modulo p. For some integral symmetric matrix E one has

$$C'^{-1} = S^{\mathsf{T}} C^{-1} S + E.$$

The matrix C is divisible by p, and therefore

$$C'^{-1} = S^{\mathsf{T}} C^{-1} S \left(I + S^{-1} C S^{-\mathsf{T}} E\right),$$

where the last factor is congruent to I modulo p. Taking determinants gives $\det C' / \det C \equiv (\det S)^{-2} \pmod{p}$ after cancellation of the common power of p. A unit which is a square modulo an odd prime is a square in $\mathbb{Z}_p^\times$, by Hensel's lemma. □

3.4. **Rational existence and integral gluing.**

Lemma 3.12. *For odd p, the isometry class of a finite nonsingular p-primary pairing is determined by the rank and determinant square class at each occupied exponent. These data are intrinsic and add orthogonally at each exponent.*

Proof. For $s \geq 1$ form the $\mathbb{F}_p$-space

$$J_s(A_p) = A_p[p^s] / \left(A_p[p^{s-1}] + pA_p[p^{s+1}]\right).$$

On representatives define

$$\beta_s(\bar{x}, \bar{y}) = p^s b(x, y) \pmod{p},$$

where $b(x, y)$ is represented in $p^{-s}\mathbb{Z}$. Changing that representative adds a multiple of p^s. A vector in $A_p[p^{s-1}]$ also contributes a multiple of p, as does a vector pz with $z \in A_p[p^{s+1}]$, since $b(z, y) \in p^{-s}\mathbb{Z}/\mathbb{Z}$. The form is therefore well defined. In an orthogonal cyclic decomposition, every exponent other than s gives zero quotient, and the exponent-s block gives its coefficient matrix modulo p. Consequently β_s is nonsingular and records exactly the rank and determinant square class of that block. It is intrinsic and commutes with orthogonal sums.

Conversely, lift each homogeneous coefficient matrix over $\mathbb{Z}/p^s\mathbb{Z}$ to a unimodular symmetric matrix over $\mathbb{Z}_p$. Lemma 3.6 identifies two such lifts of the same rank and determinant square class. Reducing the isometry modulo p^s identifies the homogeneous finite pairings. The orthogonal cyclic decomposition of Lemma 3.1 then proves the assertion. □

Theorem 3.13. *Fix a dimension r, a positive rational determinant square class N, and a real positive definite space of dimension r. Prescribe rational quadratic spaces of dimension r over $\mathbb{Q}_p$ at all finite primes, with determinant square class N and Hasse invariant one at all but finitely many primes. A rational quadratic space with precisely these completions exists if and only if the product of their Hasse invariants, including the real place, is one* [33, Theorem 7.35].

Lemma 3.14. *Let V be a rational quadratic space. Suppose a full integral $\mathbb{Z}_p$-lattice $L_p \subset V \otimes \mathbb{Q}_p$ is given at every prime, and agrees with the completion of one fixed rational lattice at almost all primes. Then there is a full integral lattice $L \subset V$ with $L \otimes \mathbb{Z}_p = L_p$ for every prime.*

Proof. Choose a full reference lattice $L_0 \subset V$ and an integer $c > 0$ such that $cL_{0,p} \subset L_p \subset c^{-1}L_{0,p}$ for every prime p, and $L_p = L_{0,p}$ when $p \nmid c$. Put $Q = c^{-1}L_0 / cL_0$. This finite group is annihilated by c^2 and has the decomposition

$$Q = \bigoplus_{p \mid c} Q_p, \qquad Q_p \cong c^{-1}L_{0,p} / cL_{0,p}.$$

Let M_p be the image of L_p in Q_p, let $M = \bigoplus_{p|c} M_p$, and let L be its inverse image in $c^{-1}L_0$. Then $cL_0 \subset L \subset c^{-1}L_0$, so L is a full free abelian subgroup of V. Tensoring this description with $\mathbb{Z}_p$ identifies $L \otimes \mathbb{Z}_p$ with the inverse image of M_p in $c^{-1}L_{0,p}$, namely L_p. For $p \nmid c$ it gives $L_{0,p}$. For $x, y \in L$, the scalar product $(x, y) \in \mathbb{Q}$ belongs to every $\mathbb{Z}_p$; hence $(x, y) \in \bigcap_p \mathbb{Z}_p \cap \mathbb{Q} = \mathbb{Z}$. □

4. Graphical presentations of ranks two and three

Suppose $N = |A|$ is odd. At each prime $p \mid N$ choose an orthogonal cyclic decomposition

$$(A_p, b_p) \cong \perp_{i=1}^{t_p} \left\langle \frac{a_{p,i}}{p^{s_{p,i}}} \right\rangle, \qquad p \nmid a_{p,i}, \quad s_{p,i} \geq 1, \tag{4.1}$$

where $t_p = d_p(A)$, and put

$$N_p = \frac{N}{|A_p|}, \qquad \alpha_p = \prod_{i=1}^{t_p} a_{p,i}.$$

The conditions below depend only on the square class of α_p mod p.

Theorem 4.1. *Let (A, b) be a finite pairing of odd order N. The following conditions are equivalent.*

(1) There is a connected loopless graph G with $(\mathrm{Jac}(G), b_G) \cong (A, b)$ and $\beta(G) \leq 3$.
(2) There is such a graph which is planar.
(3) A positive definite integral lattice of rank three has discriminant pairing $(A, -b)$.
(4) One has $d(A) \leq 3$ and, for each prime $p \mid N$ with $t_p = 3$,

$$\left(\frac{-N_p \alpha_p}{p} \right) = 1. \tag{4.2}$$

In particular, condition (4.2) *is independent of the cyclic decomposition* (4.1).

Corollary 4.2. *Every finite pairing of odd order with at most two generators is the entire paired Jacobian of a connected planar loopless multigraph of cycle rank at most three.*

Proof. For every prime p, one has $d(A_p) \leq 2$. There is therefore no rank-three local determinant condition in Theorem 4.1. Its sufficient conditions hold. □

The bound $\mu(A, b) \leq 3$ is independent of $|A|$ and $\exp(A)$. The realizing graphs may have parallel edges and cut vertices.

4.1. Reduction in dimension three.

Lemma 4.3. *Every positive definite integral lattice of rank three has an obtuse superbase: vectors v_0, v_1, v_2, v_3 such that any three form an integral basis, $\sum_i v_i = 0$, and $v_i \cdot v_j \leq 0$ for $i \neq j$.*

Proof. Every basis v_1, v_2, v_3, together with $v_0 = -v_1 - v_2 - v_3$, is a superbase. Choose a superbase minimizing the positive integer $\sum_{a=0}^{3} v_a^2$. Suppose $v_i \cdot v_j > 0$, and let k, l be the remaining indices. Set

$$u_i = -v_i, \quad u_j = v_j, \quad u_k = v_k + v_i, \quad u_l = v_l + v_i.$$

Their sum is zero. Relative to the basis v_i, v_j, v_k, the vectors u_i, u_j, u_k have determinant -1; hence they form a basis, and the zero-sum relation implies the same for each other triple. Moreover,

$$\sum_{a=0}^{3} u_a^2 - \sum_{a=0}^{3} v_a^2 = 2v_i \cdot (v_k + v_l) + 2v_i^2 = -2v_i \cdot v_j < 0.$$

This contradicts minimality. Thus $v_i \cdot v_j \leq 0$ for $i \neq j$. □

The reduction is due to Selling [34]; see also [10, Theorem 8] and [26, Lemma A.1].

Lemma 4.4. *If L is a positive definite integral lattice of rank three, then $-\mathcal{D}(L)$ is the entire paired Jacobian of a connected planar loopless multigraph of cycle rank at most three.*

Proof. Take the superbase from Lemma 4.3. On vertices $0, 1, 2, 3$, join i to j by $-v_i \cdot v_j$ edges. The resulting multigraph H has no loops. Since $\sum_j v_j = 0$, its reduced Laplacian at vertex 0 is the Gram matrix of v_1, v_2, v_3. Positive definiteness implies that H is connected. Its underlying simple graph is a subgraph of K_4, so it has a plane embedding. The plane dual H^* has paired Jacobian $-\mathcal{D}(L)$ and $\beta(H^*) = |V(H)| - 1 = 3$. A bridge of H gives a loop of H^*. Delete all such loops. A loop has no effect on the reduced Laplacian, and deletion preserves connectedness while decreasing cycle rank by one. The remaining graph has all the required properties. □

4.2. **Local integral presentations.**

Lemma 4.5. *Fix an odd integer $N > 0$ and a pairing (A_p, b_p) of order p^s, where $p \mid N$ and $v_p(N) = s$. There is an integral ternary $\mathbb{Z}_p$-lattice with discriminant pairing $(A_p, -b_p)$ and determinant square class N if and only if $t_p \le 3$ and, when $t_p = 3$, $\left(\frac{-N_p \alpha_p}{p}\right) = 1$.*

Proof. A ternary discriminant group has at most three generators, so $t_p > 3$ is impossible. Assume $t_p \le 3$. The diagonal lattice

$$C_p^0 = \operatorname{diag}\left(-p^{s_{p,1}} a_{p,1}^{-1}, \dots, -p^{s_{p,t_p}} a_{p,t_p}^{-1}\right)$$

has discriminant pairing $(A_p, -b_p)$. Its determinant has valuation s. If $t_p \le 2$, adjoin $2 - t_p$ unit lines of norm one and the unit line of norm $N/\det C_p^0$. The resulting ternary lattice has determinant exactly N and the desired discriminant pairing.

If $t_p = 3$, the quotient of N by $\det C_p^0$ is a unit of square class $-N_p \alpha_p$. Thus the displayed condition is sufficient. Conversely, a ternary presentation of a group of local generator rank three has all elementary divisors divisible by p. Lemma 3.11 then gives the same determinant square class as C_p^0, proving necessity. □

4.3. **Global existence and proof of the criterion.**

Proof of Theorem 4.1. Every planar graph is a graph, so (2) implies (1). If (1) holds, take the cycle lattice and adjoin enough orthogonal unit lines to obtain rank three. Equation (2.4) proves (3). Condition (3) implies $d(A) \le 3$, and Lemma 4.5 proves (4.2) at each prime of local rank three. Thus (3)⇒(4).

Assume (4). At every odd prime dividing N, choose the ternary lattice of Lemma 4.5. At every odd prime not dividing N, take the unimodular lattice with Gram matrix $\operatorname{diag}(1, 1, N)$. Write ϵ_p for the Hasse invariant of these rational local spaces. At all primes outside the divisors of $2N$ it equals one.

At $p = 2$, both matrices

$$U_+ = \operatorname{diag}(1, 1, N), \qquad U_- = \operatorname{diag}(-1, -1, N) \tag{4.3}$$

are unimodular over $\mathbb{Z}_2$ and have determinant N. Their Hasse invariants are, respectively,

$$\epsilon_2(U_+) = 1, \qquad \epsilon_2(U_-) = (-1, -1)_2 (-1, N)_2^2 = -1.$$

Choose the one whose Hasse invariant is $\prod_{p \text{ odd}} \epsilon_p$. At the real place prescribe a positive definite ternary space, of determinant square class N and Hasse invariant one. The determinant compatibility, the finite-support condition, and the product formula now all hold. Theorem 3.13 supplies a rational space V with these completions. It is positive definite because its real completion is positive definite.

Transfer the chosen local lattices into $V \otimes \mathbb{Q}_p$ by local isometries. The completion of a fixed rational lattice is integral and unimodular outside finitely many primes. At these odd primes, Lemma 3.6 identifies it with the chosen lattice, since their determinant square classes agree. Choose these identifications and apply Lemma 3.14. The determinant of the resulting integral lattice is positive and has p-adic valuation $v_p(N)$ at every prime; hence it is exactly N. Its discriminant pairing has the prescribed primary part at every prime, so it is isometric to $(A, -b)$. This proves (3). Finally, Lemma 4.4 proves (3)⇒(2). □

Remark 4.6. The two unimodular $\mathbb{Z}_2$-lattices in (4.3) have the same determinant square class and opposite Hasse invariants. One therefore satisfies the required product formula. These lattices are not required to be even, and no quadratic refinement is prescribed. An evenness or quadratic-refinement condition requires a separate local existence condition.

4.4. **The criterion with arbitrary two-primary data.**

Theorem 4.7 (Graphical realization in ranks at most three). *Fix $r \in \{2, 3\}$. The following are equivalent:*

(1) (A, b) is the paired Jacobian of a connected loopless graph with cycle rank at most r.

(2) *Such a graph can be chosen planar.*
(3) *A positive definite integral lattice of rank r has discriminant pairing $(A, -b)$.*
(4) *All of the following finite conditions hold:*
   (a) *$d_p \le r$ for every prime p;*
   (b) *if p is odd and $d_p = r$, then w_p is a square unit in $\mathbb{Z}_p$, equivalently $\left(\frac{w_p}{p}\right) = 1$;*
   (c) *for at least one $S \in \mathscr{S}(A_2, -b_2)$, on putting $D = \det S$, $v = N/D$ and $t = r - d_2$, there exists $\eta \in \mathscr{H}_t(v)$ such that*

$$H_{\mathrm{odd}}\, h_2(S)(D, v)_2\, \eta = 1. \tag{4.4}$$

When $d_2 \le r \le 3$, the list has at most $4^{d_2} \le 64$ members. The conditions are independent of all the chosen primary decompositions.

Proof of Theorem 4.7. At an odd prime a minimal presentation of $(A_p, -b_p)$ is S_p. Lemma 3.7 makes every other minimal presentation integrally isometric to S_p. By Lemma 3.6, a rank-r presentation is its orthogonal sum with a unimodular part of rank $r - d_p$. If this rank is zero, its determinant can have square class N precisely when w_p is a square. If it is positive, take the unimodular part $\mathrm{diag}(1, \dots, 1, w_p)$. Lemma 3.6 gives Hasse invariant one and uniqueness at the prescribed rank and determinant class. Thus the required local Hasse invariant is exactly $h_p(S_p)(D_p, w_p)_p$, including the case with no unimodular summand, where w_p is square.

At two, Lemma 3.6 separates a unimodular summand from a minimal part of rank d_2. Lemma 3.9 lists all possible minimal determinant and Hasse data. Lemma 3.10 gives all possible unimodular data. A cyclic block contributes at most four lifts and an even binary block at most two; since their total rank is d_2, the number of sums is at most 4^{d_2}. Their orthogonal sum has Hasse invariant $h_2(S)(D, v)_2\eta$. This proves that the displayed arithmetic conditions are necessary for a positive rank-r lattice, since the Hasse invariant at infinity is one and the total product is one.

Conversely, suppose the conditions hold. Choose the indicated local integral lattices at primes dividing $2N$. At all other odd primes choose a unimodular lattice of determinant square class N; its Hasse invariant is one. Choose the positive definite real space of rank r and determinant square class N. The local determinant classes agree globally and the Hasse product equals one. Theorem 3.13 for rational quadratic spaces [33, Theorem 7.35] gives a positive definite rational space with these localizations. Outside finitely many primes, a fixed reference lattice is unimodular and has the prescribed local isometry class by Lemma 3.6. Thus Lemma 3.14 supplies a positive integral lattice with the chosen local integral lattices. Its determinant has valuation $v_p N$ at every prime and is positive, hence is exactly N. Its discriminant pairing is $(A, -b)$.

For rank three, Lemma 4.4 converts the lattice into a planar loopless graph with pairing $-\boldsymbol{D}(L)$ and cycle rank at most three. For rank two, Lemma 4.12 gives the corresponding assertion. Thus (3) implies (2), which implies (1). Conversely, a graph of cycle rank at most r has a positive integral flow lattice of that rank and discriminant $(A, -b)$ by Lemma 2.4. Adjoining orthogonal unit lines gives rank r without changing the discriminant. This proves (1)⇒(3) and completes the equivalences. □

Remark 4.8 (Treewidth of the realizations). The realizations furnished by Theorem 4.7 can be chosen of treewidth at most three. Indeed, the support of the graph obtained from an obtuse superbase is a connected subgraph of K_4. Choose its embedding by restricting a fixed plane embedding of K_4, and place every parallel edge in the corresponding edge bundle. Deleting a missing support edge contracts its dual edge; increasing an edge multiplicity subdivides its dual edge. The dual is therefore obtained from $K_4^* \cong K_4$ by contractions and subdivisions, with any loops subsequently deleted. These operations do not increase treewidth above three. For a contraction, identify the two endpoints in every bag of a tree decomposition; the bags containing them form a connected subtree since an edge bag contains both. For subdivision of an edge uv by a vertex w, attach the bag $\{u, v, w\}$ to a bag containing u, v. Iteration preserves the bound three, and deletion removes vertices or edge conditions. A bridge of the support only produces a loop in the dual, removed by loop deletion. For rank two

the same argument starts from a triangle and gives treewidth at most two. The supports here are connected because their reduced Laplacians are positive definite.

4.5. **A closed formula when the two-primary part is cyclic.**

Corollary 4.9. *Suppose A_2 is cyclic of order 2^k, $k \geq 1$, with $b_2 = \left\langle \frac{a_2}{2^k} \right\rangle$, and put $N_0 = N/2^k$. Assume $d(A) \leq 3$ and the odd-prime determinant conditions of Theorem 4.7 for $r = 3$. A graph realization of cycle rank at most three exists unless*

$$k \geq 3, \qquad a_2 \equiv N_0 \pmod 8.$$

In this exceptional case, it exists if and only if

$$H_{\mathrm{odd}} = (-1)^{(N_0+1)/2}.$$

Proof. The minimal lift has norm $2^k u$ with $u \in \mathcal{U}_k(-a_2)$; the binary unimodular summand has determinant class $v = N_0/u$. For $k \leq 2$ the allowed unit classes u give at least two distinct classes v mod 8, one of which differs from seven. For that class, Lemma 3.10 supplies either Hasse sign for the binary unimodular summand, hence either sign for the full ternary lattice. For $k \geq 3$ the class $u = -a_2$ mod 8 is fixed. Only $v = 7$ can obstruct realization; this is exactly $a_2 = N_0$ mod 8. In that case the local Hasse invariant is

$$(2^k u, -1)_2 = (-1)^{(u-1)/2} = (-1)^{(N_0+1)/2}.$$

□

4.6. **The binary realization criterion.** Let (A, b) have odd order N. At each $p \mid N$ fix an orthogonal decomposition

$$(A_p, b_p) = \perp_{i=1}^{t_p} \left\langle \frac{a_{p,i}}{p^{s_{p,i}}} \right\rangle, \qquad N_p = N/|A_p|.$$

For $t_p = 1$ define

$$C_p = \mathrm{diag}\left(-p^{s_{p,1}} a_{p,1}^{-1}, -N_p a_{p,1}\right).$$

For $t_p = 2$ define

$$C_p = \mathrm{diag}\left(-p^{s_{p,1}} a_{p,1}^{-1}, -p^{s_{p,2}} a_{p,2}^{-1}\right).$$

All matrices here are over $\mathbb{Z}_p$. Put

$$H(A, b) = \prod_{p|N} h_p(C_p), \qquad h_p(\mathrm{diag}(x, y)) = (x, y)_p.$$

When $t_p = 2$, the following theorem assumes the determinant condition for the indicated C_p.

Theorem 4.10. *A pairing (A, b) of odd order N has an exact graph realization of cycle rank at most two if and only if all the following hold:*

(1) $d(A) \leq 2$;

(2) for every p with $t_p = 2$,

$$\left(\frac{N_p a_{p,1} a_{p,2}}{p}\right) = 1;$$

(3) either $N \not\equiv 7 \pmod 8$ or $H(A, b) = 1$.

The stated conditions are independent of the orthogonal decompositions. Whenever a realization exists, it may be chosen planar.

Proof. Specialize Theorem 4.7 to $r = 2$ and $A_2 = 0$. The odd-prime local presentations can be taken to be the displayed C_p. At primary rank two their determinants have square class N exactly when (2) holds. At two the entire presentation is unimodular, and Lemma 3.10 permits both Hasse signs except when $N \equiv 7 \pmod 8$, where it permits only one. Its unique sign in that case is $+1$. The global Hasse product is therefore equivalent to (3). The full criterion supplies both necessity and planar attainment. □

4.7. **Minimum cycle rank for odd cyclic pairings.** For a finite pairing (A, b), let $\mu(A, b)$ denote the least cycle rank of a connected loopless graph whose entire paired Jacobian is (A, b). The graphs in this definition may have parallel edges. For an integer $n > 1$ and an integer a prime to n, put

$$\mu(n, a) = \mu\left(\mathbb{Z}/n\mathbb{Z}, (x, y) \longmapsto \frac{axy}{n}\right).$$

Write $\left(\frac{a}{n}\right)$ for the Jacobi symbol.

Theorem 4.11 (Minimum cycle rank of odd cyclic pairings). *For every odd $n > 1$ and every a prime to n,*

$$\mu(n, a) = \begin{cases} 1, & \text{if } -a \text{ is a square in } (\mathbb{Z}/n\mathbb{Z})^\times, \\ 3, & \text{if } n \equiv 7 \pmod 8 \text{ and } \left(\frac{a}{n}\right) = 1, \\ 2, & \text{otherwise.} \end{cases}$$

Every realization of minimum cycle rank may be taken planar. The first two cases are disjoint.

Lemma 4.12. *If C is a positive definite integral binary Gram matrix, then $-\mathcal{D}(C)$ is the entire paired Jacobian of a connected planar loopless graph of cycle rank at most two.*

Proof. Let v_1 be a shortest nonzero vector of the lattice. It is primitive and hence extends to a basis v_1, v_2. Subtract an integer multiple of v_1 from v_2 and, if necessary, replace v_2 by $-v_2$ so that

$$-\frac{v_1^2}{2} \le v_1 \cdot v_2 \le 0.$$

Shortestness gives $v_2^2 \ge v_1^2$. Thus $v_0 = -v_1 - v_2$ has nonpositive scalar product with each of v_1, v_2, and v_0, v_1, v_2 form an obtuse superbase. As in the ternary Selling construction, form a graph H on three vertices with $-v_i \cdot v_j$ edges between i and j. Its reduced Laplacian is a Gram matrix of the lattice. It is connected and planar. Its plane dual has pairing $-\mathcal{D}(C)$ and cycle rank two. Delete any loops, which have no effect on the pairing. □

Lemma 4.13. *Let n be an odd positive integer. Among unimodular integral binary $\mathbb{Z}_2$-lattices of determinant square class n, both Hasse invariants occur unless $n \equiv 7 \pmod 8$. In the latter case the Hasse invariant is always one.*

Proof. The matrix $\operatorname{diag}(1, n)$ always has Hasse invariant one. If $n \equiv 1 \pmod 4$, the matrix $\operatorname{diag}(-1, -n)$ has determinant n and Hasse invariant

$$(-1, -n)_2 = -1.$$

If $n \equiv 3 \pmod 8$, the even binary matrix

$$\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$$

has determinant three, which is the same square class as n, and has Hasse invariant

$$(2, 3/2)_2 = -1.$$

This provides both signs in all residue classes except seven.

Now suppose $n \equiv 7 \pmod 8$. An odd unimodular binary lattice diagonalizes as $[u] \perp [v]$ with uv of square class n. Its Hasse invariant is

$$(u, v)_2 = (u, -uv)_2 = (u, -n)_2 = 1,$$

because $-n$ is a square in $\mathbb{Q}_2$. An even unimodular binary lattice also has determinant n, hence determinant minus a square. Its rational quadratic space is hyperbolic and has Hasse invariant one. These exhaust the odd and even possibilities. □

Lemma 4.14. *There is a positive definite integral binary lattice L with*

$$\mathcal{D}(L) \cong \left\langle \frac{-a}{n} \right\rangle$$

if and only if

$$n \not\equiv 7 \pmod 8 \quad \text{or} \quad \left(\frac{a}{n}\right) = -1.$$

Proof. For each odd prime $p \mid n$, write $n = p^s n_p$. The p-primary part of $\langle a/n \rangle$ has coefficient an_p/p^s: a generator is $n_p \bmod n$. Over $\mathbb{Z}_p$, consider the integral matrix

$$C_p = \operatorname{diag}\left(-\frac{p^s}{an_p}, -an_p^2\right).$$

Its determinant is exactly n, its second line is unimodular, and its discriminant pairing is the negative of the prescribed primary pairing. Its Hasse invariant is

$$h_p(C_p) = \left(\frac{-an_p^2}{p}\right)^s = \left(\frac{-a}{p}\right)^s.$$

Conversely, any integral binary local presentation of this cyclic primary pairing has one unimodular line and one line of valuation s. The finite pairing fixes the unit square class on the latter; the determinant square class n then fixes the former. Thus its Hasse invariant is the one just displayed. At every odd $p \nmid n$, take a unimodular binary lattice of determinant n; its Hasse invariant is one. Consequently the product of the Hasse invariants at all odd primes is

$$\prod_{p \text{ odd}} h_p(C_p) = \prod_{p \mid n} \left(\frac{-a}{p}\right)^{v_p n} = \left(\frac{-a}{n}\right). \tag{4.5}$$

At two the required lattice is unimodular, because n is odd. At infinity prescribe a positive definite binary space, whose Hasse invariant is one. By Lemma 4.13, the finite Hasse product can be made one in every case except possibly $n \equiv 7 \pmod 8$. In that case the two-adic invariant is forced to be one, and the product formula requires

$$\left(\frac{-a}{n}\right) = 1.$$

Since $n \equiv 3 \pmod 4$, this is equivalent to $\left(\frac{a}{n}\right) = -1$.

These necessary conditions are sufficient. Choose the two-adic unimodular binary form with the required Hasse invariant. The local spaces have dimension two, determinant square class n, Hasse invariant one at almost all places, and total Hasse product one. Theorem 3.13 for rational quadratic spaces gives a global space with precisely these completions and the prescribed positive real signature. Integral gluing gives an integral lattice with the prescribed local lattices. Its positive determinant has valuation $v_p n$ at every prime and is therefore exactly n. Its discriminant pairing is the required cyclic pairing. □

Proof of Theorem 4.11. A connected loopless graph of cycle rank one consists of one cycle, with trees attached. If its Jacobian order is n, the cycle has length n and its pairing is $\langle -1/n \rangle$. Isometries of cyclic pairings multiply the coefficient by a square unit. Thus cycle rank one is possible exactly when $-a$ is a square modulo n.

A graph of cycle rank at most two yields a positive integral cycle lattice of rank at most two. Adjoining unit lines, if necessary, gives a binary presentation of $\langle -a/n \rangle$. Conversely, Lemma 4.12 converts any positive binary presentation into a graph of cycle rank at most two. Therefore Lemma 4.14 is an exact criterion for cycle rank at most two.

The odd ternary realization theorem supplies cycle rank at most three in every case. Combining these three statements proves the formula. If $n \equiv 7 \pmod 8$ and $-a$ is a square unit, then $\left(\frac{a}{n}\right) = \left(\frac{-1}{n}\right) = -1$; hence the first and second cases do not overlap. All constructions above are planar. □

Example 4.15 (A three-generator obstruction). The pairing $\langle 1/3\rangle^{\perp 3}$ has minimum graph cycle rank four. The ternary criterion excludes rank at most three because $\left(\frac{-1}{3}\right) = -1$. Let B_3 be the two-vertex graph with three parallel edges, and let C_3 be a triangle. The wedge $B_3 \vee C_3 \vee C_3$ has cycle rank four and pairing with diagonal coefficients $(1,-1,-1)/3$. Over $\mathbb{F}_3$, the vectors $(1,1)$ and $(1,-1)$ are an orthogonal basis with norm one for $\mathrm{diag}(-1,-1)$. Thus this wedge realizes the required pairing and proves sharpness.

4.8. **Even cyclic pairings in ranks at most three.** Let $n = 2^k n_0$ with $k \geq 1$ and n_0 odd. Let a be a unit modulo n, and put $J = \left(\frac{a}{n_0}\right)$, where the symbol is Jacobi's and $\left(\frac{a}{1}\right) = 1$.

Theorem 4.16. *For the pairing $\left\langle \frac{a}{n} \right\rangle$, the following statements hold.*

(1) Cycle rank at most one is possible if and only if $-a$ is a square unit modulo n.

(2) Cycle rank at most two is always possible when $k = 1$. When $k \geq 2$, it is possible if and only if

$$J = (-1)^{1+(1+\epsilon(n_0))\epsilon(a)+k\omega(a)}. \tag{4.6}$$

(3) Cycle rank at most three is possible if and only if

$$k \leq 2 \quad \text{or} \quad a \not\equiv 1 \pmod 8 \quad \text{or} \quad J = -1. \tag{4.7}$$

Every permitted realization can be chosen planar. Thus these formulas determine the minimum cycle rank as one, two, three, or at least four for every even cyclic pairing.

Proof. A loopless graph of cycle rank one has a unique cycle of length n, with trees attached, and its pairing is $\left\langle \frac{-1}{n} \right\rangle$. Changing a cyclic generator multiplies the coefficient by a unit square. This proves the first assertion.

At an odd prime $p \mid n$, write $n = p^s n_p$. The local cyclic pairing is $\left\langle \frac{an_p}{p^s} \right\rangle$. For both ranks two and three its negative pairing has minimal presentation $[-p^s/(an_p)]$, with unimodular summand of determinant $-an_p^2$. The local Hasse invariant is

$$\left(-\frac{p^s}{an_p}, -an_p^2\right)_p = \left(\frac{-a}{p}\right)^s.$$

Consequently

$$H_{\mathrm{odd}} = \left(\frac{-a}{n_0}\right) = (-1)^{\epsilon(n_0)} J. \tag{4.8}$$

At two the local coefficient of the negative pairing is $-an_0$. The minimal lattice is $[2^k u]$, where $u \in \mathcal{U}_k(-an_0)$. In rank two the unimodular summand is a line of norm $v = n_0/u$, so its full Hasse invariant is

$$\begin{aligned}(2^k u, v)_2 &= (-1)^{\epsilon(u)\epsilon(v)+k\omega(v)} \\ &= (-1)^{(1+\epsilon(n_0))\epsilon(u)+k(\omega(n_0)+\omega(u))}.\end{aligned} \tag{4.9}$$

When $k = 1$, all four choices of u occur, and the two characters $\epsilon(u)$ and $\omega(u)$ show that both signs occur. When $k \geq 2$, the displayed sign is independent of the choice of lift. Substituting $u = -an_0$ modulo eight gives

$$(2^k u, v)_2 = (-1)^{(1+\epsilon(n_0))(1+\epsilon(a))+k\omega(a)}.$$

For $k = 2$ this substitution depends only on u mod 4, because the term with ω has even coefficient. Comparing with (4.8) proves (4.6).

For rank three, Corollary 4.9 applies with $a_2 = an_0$. Its exceptional condition is precisely $k \geq 3$ and $a = 1$ mod 8. In this case its required Hasse sign is $-(-1)^{\epsilon(n_0)}$, which by (4.8) is equivalent to $J = -1$. The complete criterion proves both existence and necessity. □

Corollary 4.17. *For $k \geq 3$ the minimum cycle rank $\mu(2^k, a)$ obeys*

$a \bmod 8$	1	3	5	7
k even	≥ 4	2	3	1
k odd	≥ 4	3	2	1.

At order four the minimum is three for $a = 1 \bmod 4$ and one for $a = 3 \bmod 4$. At order two the minimum is one.

Proof. Set $n_0 = 1$ and $J = 1$ in Theorem 4.16. For $k \geq 3$, rank one occurs precisely when $a = 7 \pmod 8$. Rank two occurs precisely when $\epsilon(a) + k\omega(a) = 1$. For $a = 1, 3, 5, 7 \pmod 8$, the pairs $(\epsilon(a), \omega(a))$ are respectively $(0, 0), (1, 1), (0, 1), (1, 0)$. Substitution gives the two rows. Rank three is available in every remaining case except $a = 1 \pmod 8$. When $k = 2$, the binary condition requires $a = 3 \pmod 4$, already of cycle type; the other class has rank three. When $k = 1$, the sole pairing is that of the two-edge cycle. □

5. Exact rank bounds and mixed-prime constructions

5.1. **Orthogonal sums of binary presentations.** For an odd-primary cyclic pairing $\langle a/p^s \rangle$, its type is

$$\left(s \bmod 2, \left(\frac{a}{p} \right) \right).$$

There are four types. Two constituents of the same type have a product of orders which is a square and a product of coefficients which is a residue.

Lemma 5.1. *Suppose (X, c) is a nontrivial odd-order pairing such that every nontrivial primary part is an orthogonal sum of two cyclic constituents of the same type. Then (X, c) has an exact planar realization of cycle rank two.*

Proof. Its order M is a square. At every nontrivial primary part, the coefficient product is a residue and $M/|X_p|$ is a square unit. Thus every local determinant condition in Theorem 4.10 is satisfied. Since $M \equiv 1 \pmod 8$, there is no remaining binary Hasse obstruction. The generator lower bound is two. □

Lemma 5.2. *Let (B, b) have odd order and $d(B) \leq 4$. Assume that every primary part of generator rank four admits an orthogonal cyclic decomposition containing exactly one constituent of each of the four types. Then (B, b) has an exact planar realization of cycle rank at most five.*

In particular, every odd-order pairing on at most three generators has an exact planar realization of cycle rank at most five.

Proof. It suffices to construct an orthogonal decomposition

$$(B, b) = (X, c) \perp (Y, d)$$

with $d(Y) \leq 2$ and with (X, c) admitting a binary presentation. Corollary 4.2 then realizes (Y, d) in at most three cycles.

Fix the indicated cyclic primary decompositions, and write t_p for their ranks. If $t_p \leq 2$, assign the whole primary part to Y_p. The remaining choices concern only primes with $t_p = 3$ or 4.

First suppose there is no rank-four primary part. At a rank-three prime, if any constituent has even exponent, assign one such constituent to X_p. If all three exponents are odd, two of the three coefficients have the same Legendre sign; assign that pair to X_p. Assign the remaining constituents to Y_p. The order $M = |X|$ is a square. At every prime where X_p has rank two, its coefficient product is a residue. Hence its local determinant condition holds, and the binary criterion realizes X in at most two cycles. This proves the assertion when every primary rank is at most three.

Now let S_4 be the nonempty set of rank-four primes. Among the rank-three primes, let S_3 consist of those for which all three exponents are odd and all three coefficient Legendre signs agree. Put

$$P = \prod_{p \in S_4 \cup S_3} p.$$

Choose X_p by the following rules.

(1) If $p \in S_3$, assign any one constituent to X_p.
(2) At a rank-three prime with an even exponent, assign one even-exponent constituent to X_p.
(3) At any other rank-three prime, all exponents are odd and both coefficient signs occur. Assign two constituents whose coefficient product has Legendre sign $\left(\frac{P}{p}\right)$. Such a pair exists: a same-sign pair has product sign $+1$, and a mixed-sign pair has product sign -1.
(4) If $p \in S_4$, assign an even-exponent constituent and an odd-exponent constituent whose coefficient product has sign

$$\delta_p = \left(\frac{P/p}{p}\right).$$

Each parity occurs with both coefficient signs, so this is possible.

The order $M = |X|$ has rational square class P: the selected exponent sum is odd exactly at the primes of $S_4 \cup S_3$. At every prime where X_p has rank two, the selected coefficient product has square class $M/|X_p|$. Indeed, in (3) the valuation of M at p is even, giving unit square class P, and in (4) it is odd, giving unit square class P/p. Consequently all the binary local determinant conditions hold.

It remains only to arrange the Hasse product if $M \equiv 7 \pmod 8$. At a fixed $p \in S_4$, there are two choices in (4) with the same prescribed product sign. Denote their exponents by s_e and s_o and their coefficients by a_e and a_o, where s_e is even and s_o is odd. The local presentation is

$$\operatorname{diag}(-p^{s_e}/a_e, -p^{s_o}/a_o),$$

and its Hasse invariant is

$$(-p^{s_e}/a_e, -p^{s_o}/a_o)_p = \left(\frac{-a_e}{p}\right).$$

The two choices have opposite coefficient signs for a_e, so they have opposite Hasse invariants. Both choices retain the same determinant square class and the same parity of the selected exponent sum. Thus they change M only by a rational square. The determinant square classes and Hasse invariants at all other primes are unchanged. Choose between them so that the odd-prime Hasse product is one. The binary criterion now supplies a positive integral binary presentation of $(X, -c)$.

In every case at most two constituents remain in each Y_p, so $d(Y) \le 2$. The binary realization of X and the ternary realization of Y finish the proof. □

Theorem 5.3 (Sharp cycle-rank bound for odd-order pairings). *For every nontrivial finite nonsingular symmetric pairing (A, b) of odd order, with $d = d(A)$, there is a connected planar loopless graph G such that*

$$(\mathrm{Jac}(G), b_G) \cong (A, b), \qquad \boxed{\beta(G) \le d + 2.}$$

The constant two is sharp. The graphs may have parallel edges. They may be chosen to have treewidth at most three. Apart from at most two pieces obtained from subdivisions of K_4 by contraction and deletion, they are vertex sums of graphs of cycle rank at most two. For odd d, at most one K_4 piece is needed.

Proof. Decompose each primary part into $d_p \le d$ cyclic constituents and classify them by the four types. Pair constituents within each type as far as possible. Write L_p for the number of pairs and $r_p = d_p - 2L_p$ for the number of unpaired constituents. Then

$$0 \le r_p \le 4, \qquad r_p \equiv d_p \pmod 2.$$

For any nonnegative integer k, take $\min(k, L_p)$ of these pairs at each prime. Assemble the first selected pair at every prime into one global finite pairing X_1, the second into X_2, and so on. Each nontrivial X_j satisfies Lemma 5.1 and has minimum cycle rank two. Let B be the orthogonal sum of all constituents not selected. Its local generator ranks are

$$t_p = d_p - 2\min(k, L_p).$$

If $L_p < k$, all available pairs of the same type have been removed, so the remaining constituents have distinct types. If $L_p \geq k$, then $t_p = d_p - 2k$.

For $d = 1$, the exact cyclic theorem gives three cycles. For $d = 2$, the odd two-generator theorem gives three cycles. Suppose first that $d \geq 4$ is even, and take $k = (d-4)/2$. Then $t_p \leq 4$ for every p. Grouping the remaining cyclic constituents into two global two-generator pairings realizes B in at most six cycles. The total is

$$2k + 6 = d + 2.$$

If $d \geq 3$ is odd, take $k = (d-3)/2$. At a prime with $L_p \geq k$, one has $t_p \leq 3$. At every other prime, the remaining constituents have distinct types, so $t_p \leq 4$; if equality holds, all four types occur exactly once. Thus Lemma 5.2 realizes B in at most five cycles. The total is

$$2k + 5 = d + 2.$$

Vertex sums preserve planarity and add both the paired Jacobians and the cycle ranks. Finally, the pairing $\langle 1/7 \rangle$ has minimum cycle rank three, proving sharpness of the constant. □

Proof of the geometric refinement. By Remark 4.8, each ternary realization is obtained from a subdivision of K_4 by contraction and loop deletion and has treewidth at most three. Each binary realization has treewidth at most two. For even $d \geq 4$, the residual pairing requires at most two ternary graphs; for odd $d \geq 3$, at most one binary and one ternary graph. The cases $d = 1, 2$ require only one ternary graph. The selected binary components contribute the remaining pieces. Joining tree decompositions at bags containing the identified vertex shows that a vertex sum has treewidth equal to the maximum of those of its summands. □

If no nontrivial binary component occurs, its orthogonal sum is the trivial pairing and is realized by the graph on one vertex, of cycle rank zero.

5.2. **Pairing two primary cyclic summands without extra cycles.**

Lemma 5.4. *Let p be odd, let $s, t \geq 1$, and let a, b be units at p. If*

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right),$$

then the pairing

$$\left\langle \frac{a}{p^s} \right\rangle \perp \left\langle \frac{b}{p^t} \right\rangle$$

has an exact planar graph realization of cycle rank two whenever either $p \not\equiv 7 \pmod 8$ or $s \equiv t \pmod 2$.

Proof. The generator lower bound is two. In the binary criterion the sole local determinant condition is $(ab/p) = 1$, which is the assumption. The order is p^{s+t}. It is not congruent to seven modulo eight under either of the stated alternatives. The binary criterion therefore applies. □

5.3. **Primary pairings for $p \not\equiv 7 \pmod 8$.** Let

$$(A, b) = \perp_{i=1}^{d} \left\langle \frac{a_i}{p^{s_i}} \right\rangle, \qquad s_i \geq 1,$$

be an odd p-primary pairing. Define

$$\Delta(A, b) = \left(\frac{(-1)^d \prod_{i=1}^{d} a_i}{p} \right) \in \{1, -1\}.$$

The invariant Δ is intrinsic by Lemma 3.12. Lemma 3.11 identifies it with the determinant obstruction to a presentation of rank d and determinant $|A|$.

Theorem 5.5. *If $p \not\equiv 7 \pmod 8$, then*

$$\boxed{\mu(A,b) = \begin{cases} d, & \Delta(A,b) = 1, \\ d+1, & \Delta(A,b) = -1. \end{cases}}$$

Every minimum is attained by a planar graph.

Proof. A cyclic summand is of cycle type if $(-a_i/p) = 1$. Such a summand is the pairing of a cycle of length p^{s_i}, and has minimum cycle rank one. All summands not of cycle type have the same coefficient square class. Pair them arbitrarily. Lemma 5.4 realizes each pair in two cycles. If an unpaired summand not of cycle type remains, its order is not seven modulo eight. The exact odd cyclic theorem realizes it in two cycles.

If the number of summands not of cycle type is even, the total cycle rank is d; if odd, it is $d+1$. If there are m such constituents, then $\Delta = (-1)^m$. The generator bound excludes ranks below d. If $\Delta = -1$, the determinant lemma for the minimal local presentation excludes rank d as well. Taking vertex sums of the constructed planar graphs proves the asserted upper bounds and their optimality. □

5.4. **A composite-order binary construction.** The following construction gives reduced Laplacians of planar graphs on five vertices.

Lemma 5.6. *For every odd $x \geq 1$ and unit $a \bmod x$, there is a positive binary integral lattice Q of determinant $2x$ whose negative odd discriminant pairing is $\left\langle \frac{a}{x} \right\rangle$. It has an obtuse basis with*

$$Q = \begin{pmatrix} b+2h & -b \\ -b & b+2r \end{pmatrix}, \quad b > 0 \text{ odd}, \quad h, r \geq 0, \quad x = b(h+r) + 2hr.$$

In particular $h + r$ is odd and $1 \leq h + r \leq x$.

Proof. At each odd $p \mid x$, take a rank-one local presentation of the negative of $(\left\langle \frac{a}{x} \right\rangle)_p$ and adjoin a unit line so that the determinant has square class $2x$. At odd primes outside x, take a unimodular binary form of determinant square class $2x$. At two put

$$Q_u = [2u] \perp [x/u], \qquad u \in \{1,3,5,7\}.$$

These forms have determinant $2x$ and a cyclic discriminant of order two. With $v = x/u$, their Hasse invariant is $(-1)^{\omega(v)+\epsilon(u)\epsilon(v)}$. Its values are

$x \bmod 8 \backslash u$	1	3	5	7
1	+1	+1	−1	−1
3	−1	+1	+1	−1
5	−1	−1	+1	+1
7	+1	−1	−1	+1

Both signs occur in each row. Choose the sign whose product with the prescribed odd-prime Hasse invariants is +1 and prescribe a positive definite real plane. Theorem 3.13 and Lemma 3.14 give a positive integral binary lattice of determinant $2x$ with the required odd discriminant.

Choose an obtuse superbase. If both diagonal norms in a basis were even, the determinant would be either odd, when the mixed product is odd, or divisible by four, when it is even. Since its valuation at two is one, the norm functional modulo two is nonzero. Exactly two of the three superbase vectors have odd norm; choose them as a basis. Write their norms q, B and their mixed product $-b \leq 0$. Since $qB - b^2 = 2x$ and q, B are odd, b is positive and odd. The other two superbase pairings give $q - b \geq 0$ and $B - b \geq 0$. Thus $q = b + 2h$, $B = b + 2r$ with $h, r \geq 0$, and

$$2x = (b+2h)(b+2r) - b^2 = 2b(h+r) + 4hr.$$

Consequently $h + r > 0$, $h + r \equiv x \equiv 1 \pmod 2$, and $x = b(h+r) + 2hr \geq h + r$. □

Theorem 5.7. *Let $1 \le x \le y$, $y \mid z$, with x, y, z odd. Let a, b, c be units at x, y, z, respectively. Suppose*

$$\left(\frac{2bc}{p}\right) = 1 \quad (p \mid y). \tag{5.1}$$

Then $\left\langle \frac{a}{x} \right\rangle \perp \left\langle \frac{b}{y} \right\rangle \perp \left\langle \frac{c}{z} \right\rangle$ has an exact planar loopless graph realization of cycle rank at most four.

Proof. Put $P = z/y$. Apply Lemma 5.6 to the odd pairings $\left\langle \frac{a}{x} \right\rangle$ and $\left\langle \frac{c/2}{P} \right\rangle$, where $c/2$ denotes multiplication by the inverse of two modulo P. Write the resulting two forms as

$$Q_1 = \begin{pmatrix} b_0 + 2h & -b_0 \\ -b_0 & b_0 + 2r \end{pmatrix}, \qquad Q_2 = \begin{pmatrix} c_0 + 2v & -c_0 \\ -c_0 & c_0 + 2u \end{pmatrix}.$$

Thus $x = b_0(h + r) + 2hr$, $P = c_0(u + v) + 2uv$, b_0, c_0 are positive odd integers, and h, r, u, v are nonnegative. Set $w = c_0 + 2v$ and define

$$C = \begin{pmatrix} b_0 + 2h & -b_0 & -h & 0 \\ -b_0 & b_0 + 2r & -r & 0 \\ -h & -r & (wy + h + r)/2 & -yv \\ 0 & 0 & -yv & y(u + v) \end{pmatrix}. \tag{5.2}$$

Since $w, y, h + r$ are odd, its third diagonal entry is integral. Its row sums are

$$h, \quad r, \quad (c_0 y - h - r)/2, \quad yu.$$

These are nonnegative because $h + r \le x \le y$ and $c_0 \ge 1$. On vertices $0, 1, 2, 3, 4$, take the edge multiplicities

ij	01	02	03	04	12	13	23	34
m_{ij}	h	r	$(c_0 y - h - r)/2$	yu	b_0	h	r	yv.

Every other multiplicity is zero. The support embeds in a tetrahedron on $0, 1, 2, 3$ with vertex 4 added along edge 03. Its reduced Laplacian at 0 is C.

Put

$$T = \begin{pmatrix} 1 & 0 & 1/2 & 0 \\ 0 & 1 & 1/2 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, U = \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix}.$$

The vector $(1/2, 1/2)^{\mathsf{T}}$ satisfies $Q_1(1/2, 1/2)^{\mathsf{T}} = (h, r)^{\mathsf{T}}$. Thus the shear T eliminates the mixed column $(-h, -r)^{\mathsf{T}}$ and subtracts $(h + r)/2$ from the third diagonal entry. It follows that $\det T = 1$, $\det U = -1$, and

$$T^{\mathsf{T}} C T = Q_1 \perp \frac{y}{2} U^{\mathsf{T}} Q_2 U, \qquad U^{\mathsf{T}} Q_2 U = \begin{pmatrix} w & -2v \\ -2v & 2(u + v) \end{pmatrix}. \tag{5.3}$$

In particular $C \cong Q_1 \perp (y/2)Q_2$ over $\mathbb{Z}[1/2]$. Both summands on the right are positive definite and

$$\det C = (2x)(y^2/4)(2P) = xyz.$$

The first factor has the required odd pairing $\left\langle \frac{a}{x} \right\rangle$.

The odd discriminant of Q_2, with its sign reversed, is $\left\langle \frac{c/2}{P} \right\rangle$. At an odd prime dividing y, consider the integral binary lattice

$$\operatorname{diag}(-2/b, -2P/c).$$

Its determinant is $4P/(bc)$, whose ratio to $2P$ has square class $2bc$. Condition (5.1) therefore gives the same determinant square class as Q_2. If $p \mid P$, the second line has negative discriminant $\left\langle \frac{c/2}{P} \right\rangle_p$;

uniqueness of minimal odd presentations fixes this line, and the determinant fixes the unimodular line. If $p \nmid P$, both lattices are unimodular and Lemma 3.6 identifies them. Hence, at every $p \mid y$,

$$\frac{y}{2}Q_2 \cong \operatorname{diag}(-y/b, -yP/c).$$

Its negative discriminant is $(\left\langle \frac{b}{y} \right\rangle \perp \left\langle \frac{c}{yP} \right\rangle)_p$. If $p \mid P$ but $p \nmid y$, multiplication of the Gram matrix by the unit $y/2$ multiplies the inverse pairing by $2/y$, giving the same p-part of $\left\langle \frac{c}{yP} \right\rangle$. At all other odd primes this summand is unimodular. Together with Q_1, this proves the prescribed orthogonal decomposition of $-\boldsymbol{D}(C)_p$ at every odd prime. Since $\det C = xyz$ is odd, $\boldsymbol{D}(C)_2 = 0$.

Positive definiteness of C implies that its graph H is connected: a component disjoint from vertex 0 would give a nonzero vector in the kernel of the reduced Laplacian. The full plane dual H^* has flow Gram matrix C, by Lemma 2.5, and cycle rank $|V(H)| - 1 = 4$. Its pairing is $-\boldsymbol{D}(C)$. Deleting its loops preserves this pairing and gives the required loopless graph of cycle rank at most four. □

The congruence (5.3) is defined over $\mathbb{Z}[1/2]$ and therefore over every $\mathbb{Z}_p$ with p odd.

Corollary 5.8. *Suppose $1 < n_0 \mid n_1 \mid n_2 \mid n_3$ are odd, with unit coefficients $a_i \bmod n_i$, and*

$$\left(\frac{2a_0a_1}{p}\right) = 1 \ (p \mid n_0), \qquad \left(\frac{2a_2a_3}{p}\right) = 1 \ (p \mid n_2).$$

Then $\perp_{i=0}^{3} \left\langle \frac{a_i}{n_i} \right\rangle$ has minimum cycle rank four, attained by a planar loopless graph.

Proof. In (5.2), put $x = n_1/n_0$, $y = n_2/n_0$ and $P = n_3/n_2$. Take Q_1 and Q_2 of Lemma 5.6 with negative odd discriminants $\left\langle \frac{a_1}{x} \right\rangle$ and $\left\langle \frac{a_3/2}{P} \right\rangle$. The inequalities $1 \le x \le y$ give the integral positive reduced Laplacian C and its plane graph H as above. Take the full dual H^*, including the loops corresponding to bridges of H. Its flow Gram matrix is C and its cycle rank is four. Subdivide every edge into n_0 edges. Since $n_0 \ge 3$, each loop becomes a loopless cycle; every other subdivided edge is also loopless. Lemma 2.6 gives cycle rank four and flow Gram matrix n_0C. At every odd prime the latter splits as

$$n_0Q_1 \perp (n_2/2)Q_2.$$

At $p \mid n_0$, the matrix $\operatorname{diag}(-1/a_0, -x/a_1)$ has the same discriminant pairing as Q_1 and determinant ratio $1/(2a_0a_1)$, a square by the first hypothesis. Odd local splitting therefore identifies the two matrices. After multiplication by n_0, their negative discriminant is $(\left\langle \frac{a_0}{n_0} \right\rangle \perp \left\langle \frac{a_1}{n_1} \right\rangle)_p$. At $p \mid x$ with $p \nmid n_0$, the scalar n_0 is a unit and the inverse pairing is multiplied by n_0^{-1}, giving the p-part of $\left\langle \frac{a_1}{n_1} \right\rangle$.

At $p \mid n_2$, the second hypothesis identifies Q_2 with $\operatorname{diag}(-2/a_2, -2P/a_3)$ by the same determinant and discriminant argument. Multiplication by $n_2/2$ gives $\operatorname{diag}(-n_2/a_2, -n_3/a_3)$. At $p \mid P$ with $p \nmid n_2$, unit scaling gives the remaining p-part of $\left\langle \frac{a_3}{n_3} \right\rangle$. Thus the negative discriminant of n_0C is the prescribed pairing at every odd prime. Finally,

$$\det(n_0C) = n_0^4 xy^2P = n_0n_1n_2n_3$$

is odd, so there is no two-primary part. Every prime dividing n_0 occurs in all four cyclic factors. The generator lower bound is therefore four, proving optimality. □

Corollary 5.9. *Let $1 < n_1 \mid \cdots \mid n_d$, with all prime divisors congruent to 1 or 7 modulo eight, and let $b = \perp_i \left\langle \frac{1}{n_i} \right\rangle$. For $d \ge 3$,*

$$\mu(A, b) = \begin{cases} d+1, & d \text{ odd and some } p \equiv 7 \pmod 8 \text{ divides } n_1, \\ d, & \text{otherwise.} \end{cases}$$

For $d = 2$ the minimum is two when $n_1n_2 \equiv 1 \pmod 8$, and three when $n_1n_2 \equiv 7 \pmod 8$. All minima are planar.

Proof. Every n_i is congruent to one or seven modulo eight, and $\left(\frac{2}{p}\right) = 1$ at every supported prime. The triple and quartet constructions therefore apply to any three or four factors in their divisibility order. For two factors $n_i \mid n_j$ and $p \mid n_i$, write $n_i = p^s u$, $n_j = p^t v$. Their primary coefficients are u, v, and the prime-to-p part of their product is also uv. The binary determinant character is consequently $(uv)^2$. If the two factors have the same residue modulo eight, their product is one modulo eight and the binary criterion gives two cycles.

Pair factors within the two residue classes. If $d \geq 4$ is even, the two class counts are both even or both odd. In the latter case one count is at least three; remove three factors of that class and one of the other for a quartet, then pair the rest. This gives cycle rank d. For odd $d \geq 3$, one count is odd and the other even. Remove either three factors of the odd-count class, or its sole factor and two of the other class. A four-cycle triple and the remaining binary pairs give rank $d + 1$.

For $p \mid n_1$, put $u_i = n_i / p^{v_p(n_i)}$. The primary coefficient product and the prime-to-p part of $|A|$ are both $\prod_i u_i$. Thus the full-rank determinant character is $\left(\frac{-1}{p}\right)^d$. It is negative precisely in the stated exceptional case, and then excludes rank d. Otherwise, if d is odd, every prime dividing n_1 is one modulo eight. Hence -1 is a square modulo n_1, and the first factor is a cycle pairing. For $d \geq 5$, combine this cycle with the even case on the other $d - 1$ factors. For $d = 3$, the same positive determinant characters give rank three directly by Theorem 4.1.

It remains to treat $d = 2$ when $n_1 n_2 \equiv 7 \pmod 8$. The rational matrix $\mathrm{diag}(-n_1, -n_2)$ has the prescribed negative discriminant at every odd prime. Its Hasse invariant at infinity is -1. Its two unit entries have residue classes $1, 7$ modulo eight in some order, so its two-adic Hasse invariant is 1. Reciprocity gives odd-prime Hasse product -1. Lemma 3.10 forces two-adic Hasse invariant 1 for a unimodular binary lattice of determinant $n_1 n_2$. A positive definite binary presentation would therefore violate reciprocity. Rank two is impossible, and the ternary theorem gives rank three. The generator bound proves optimality in all cases. □

The assertion concerns the displayed coefficient forms, not every pairing on the underlying groups.

5.5. **Primary forms at distinct scales.**

Corollary 5.10. *For $p \equiv 7 \pmod 8$ and $1 \leq s_1 < s_2 < s_3$, the pairing $\perp_{i=1}^{3} \left\langle \frac{1}{p^{s_i}} \right\rangle$ has minimum cycle rank four.*

Proof. In Theorem 5.7, take $x = p^{s_1}$, $y = p^{s_2}$, $z = p^{s_3}$ and all three coefficients equal to one. The condition is $(2/p) = 1$. The determinant condition of Lemma 3.11 excludes rank three, since $(-1/p) = -1$. The generator rank excludes smaller ranks. □

Corollary 5.11. *For $p \equiv 7 \pmod 8$ and $1 \leq s_0 < s_1 < s_2 < s_3$, $\perp_{i=0}^{3} \left\langle \frac{1}{p^{s_i}} \right\rangle$ has minimum cycle rank four.*

Proof. Apply Corollary 5.8; both its characters are $(2/p) = 1$. The generator lower bound is four. □

5.6. **Minimum cycle rank for odd-primary pairings.** Let p be odd and let (A, b) be a nontrivial nonsingular symmetric p-primary pairing. Write an orthogonal cyclic decomposition

$$(A, b) = \perp_{i=1}^{d} \langle a_i / p^{s_i} \rangle, \qquad s_i \geq 1,$$

and define

$$\Delta(A, b) = \left(\frac{(-1)^d \prod_i a_i}{p} \right).$$

This sign is intrinsic by Lemma 3.12: the product of the unit coefficients of the Jordan constituents is an isometry invariant modulo squares. Equivalently, Δ is the determinant obstruction to an exact presentation in rank $d = d(A)$.

Theorem 5.12 (Minimum cycle rank of odd-primary pairings). *For every odd prime p and every nonsingular symmetric p-primary pairing (A, b) with $d(A) \geq 3$,*

$$\boxed{\mu(A, b) = d(A) + \frac{1 - \Delta(A, b)}{2}.}$$

Every minimum is attained by a connected planar loopless graph. In particular, an exact realization exists with at most $d(A) + 1$ cycles, and the determinant condition is the only obstruction to attaining the generator lower bound.

Proof. A cyclic constituent is of cycle type if $(-a_i/p) = 1$. Every cycle-type constituent is the pairing of a cycle. The sign Δ is (-1) to the number of constituents not of cycle type.

If $p \not\equiv 7 \pmod 8$, any two remaining constituents have an exact binary realization, and a single remaining constituent has an exact binary realization as well. Pair the remaining constituents and realize the cycle-type constituents by cycles. This gives rank d when their number is even and $d + 1$ when it is odd.

It remains to treat $p \equiv 7 \pmod 8$. Cycle-type coefficients are then nonresidues; the other coefficients are residues. Two residue constituents of the same exponent parity have an exact binary realization. Suppose first that a cycle-type cyclic orthogonal summand is available. Reserve one such summand, and pair the residue constituents within each exponent parity. If none remains, the total rank is d. A single remaining constituent of even exponent requires two cycles, giving total rank $d + 1$. A single remaining constituent of odd exponent can be combined with the reserved cycle-type summand and realized in three cycles by Corollary 4.2, again giving $d+1$. If one residue constituent of each parity remains, combine them with the reserved cycle-type summand. Their coefficient product is a nonresidue, so the exact ternary determinant condition holds and this triple has minimum cycle rank three; the total cycle rank is d.

If any homogeneous Jordan constituent has rank at least two, a cycle-type cyclic summand is available after changing its orthogonal basis. Indeed, every nonsingular binary form over $\mathbb{F}_p$ represents a nonresidue. To see the representation assertion directly, for each nonzero u the sets $a\{x^2 : x \in \mathbb{F}_p\}$ and $u - b\{y^2 : y \in \mathbb{F}_p\}$ each have $(p + 1)/2$ elements and therefore intersect. A vector with nonzero prescribed norm lifts to a unit-norm vector in the homogeneous constituent and splits off orthogonally.

It remains to treat pairings whose Jordan constituents all have rank one and residue coefficients, with distinct exponents. Each residue coefficient has a unit square root modulo its prime power, by Hensel lifting. Rescaling the cyclic generators therefore makes every coefficient one. Corollary 5.10 realizes any three of these constituents in four cycles.

For four constituents, Corollary 5.8 gives a four-cycle realization: its two determinant characters are both $\left(\frac{2}{p}\right) = 1$. The corollary retains all dual loops before uniform subdivision, so its flow lattice has the required four scales.

For odd d, one parity count is odd and the other even. If the odd count is at least three, select three from that parity; otherwise select its sole exponent and two from the other parity. The remaining counts are even. The four-cycle triple and the binary pairings give $d + 1$ cycles. For even d, if both parity counts are even, pair within parity to obtain d cycles. If both are odd, choose three exponents from one parity and one from the other. This is possible because $d \geq 4$. The four-cycle quartet and the remaining binary pairings again give d cycles. Here $\Delta = (-1)^d$, so these are the asserted upper bounds.

All constructions preserve planarity, and vertex sums combine the pieces without changing their paired Jacobians or adding cycles. The generator lower bound gives $\mu \geq d$. If $\Delta = -1$, the minimal-rank local determinant condition excludes a rank-d presentation. These bounds prove optimality. □

Corollary 5.13. *For every nontrivial odd primary pairing, put $\mu_0 = d + (1 - \Delta)/2$. Then $\mu = \mu_0$, with exactly the following two exceptions, both at primes $p \equiv 7 \pmod 8$:*

(1) $d = 1$, the sole coefficient is a residue, and its exponent is odd; in this case $\mu = 3$ instead of $\mu_0 = 2$.

(2) $d = 2$, *both coefficients are residues, and their exponents have different parities; in this case* $\mu = 3$ *instead of* $\mu_0 = 2$.

Every stated minimum is attained by a connected planar loopless graph. In particular, $\mu \le d + 1$ *for every odd primary pairing with* $d \ge 2$.

Proof. Rank at least three is the theorem. Rank one is the exact odd cyclic classification. For rank two outside $p \equiv 7 \pmod 8$, the binary determinant condition is sufficient and gives the displayed formula. At $p \equiv 7 \pmod 8$, write the coefficient signs as σ_1, σ_2. Opposite signs violate the binary determinant condition and give minimum three. Equal signs give minimum two unless both are residues and the exponents have opposite parity: in that last case the order is seven modulo eight and the odd Hasse product is -1, excluding a binary presentation. The ternary theorem gives three in every excluded rank-two case. □

Corollary 5.14. *Let* $n > 1$ *be odd and let* (A, b) *have underlying group* $(\mathbb{Z}/n\mathbb{Z})^d$, *with* $d \ge 2$. *Then*

$$\boxed{\mu(A,b) = \begin{cases} d, & (A,b) \cong \langle -1/n \rangle^{\perp d}, \\ d+1, & \text{otherwise.} \end{cases}}$$

Every minimum is attained by a planar graph.

Proof. At each $p \mid n$, the homogeneous Jordan constituent has rank d. Its isometry class is determined by rank and determinant square class, by Lemma 3.12. Hence one can prescribe the coefficient square class of each of the first $d - 1$ cyclic summands to agree with the primary part of $\langle -1/n \rangle$. The last coefficient is then determined by the determinant. Combining the local summands gives

$$(A,b) \cong \langle -1/n \rangle^{\perp (d-1)} \perp C$$

for one cyclic pairing C of order n.

If $C \cong \langle -1/n \rangle$, the vertex sum of d cycles is a rank-d realization. Otherwise reserve one of the $d - 1$ cycles and combine its pairing with C. The odd two-generator theorem realizes this pair in three cycles. The other $d - 2$ cyclic factors give a total of $d + 1$.

For necessity at rank d, write $n = p^k n_p$. The p-part of the order of A is p^{kd}, and the prime-to-p part of $|A|$ is n_p^d. If α_p is the determinant coefficient of b_p, the minimal-presentation determinant condition gives

$$\left(\frac{(-1)^d n_p^d \alpha_p}{p} \right) = 1.$$

This is precisely the condition that the rank-d homogeneous pairing b_p have the same determinant as the p-part of $\langle -1/n \rangle^{\perp d}$. The local classification therefore makes the pairings isometric at every prime, hence globally. □

5.7. **Scale multiplicities and minimum rank.** Suppose $N = |A|$ is odd. At each $p \mid N$, write an orthogonal primary decomposition

$$(A_p, b_p) \cong \perp_{s \in S_p} \left((\mathbb{Z}/p^s\mathbb{Z})^{m_{p,s}},\ p^{-s} U_{p,s} \right), \qquad p \nmid \det U_{p,s}. \tag{5.4}$$

The matrices $U_{p,s}$ may be diagonal. Set

$$d_p = \sum_{s \in S_p} m_{p,s}, \quad d = \max_p d_p, \quad j_p = |S_p|, \quad \alpha_p = \prod_{s \in S_p} \det U_{p,s} \quad \text{modulo squares in } \mathbb{F}_p^\times.$$

Thus j_p counts distinct scales, not generators. It depends only on the underlying group. Let

$$P_{\max} = \{p : d_p = d\}, \qquad N_p = N/|A_p|, \qquad \delta_p = \left(\frac{(-1)^d N_p \alpha_p}{p} \right) \quad (p \in P_{\max}).$$

The factor N_p is essential in the mixed-prime problem.

Theorem 5.15 (Minimum cycle rank with two local exponents). *Suppose N is odd, $d \geq 3$, and $j_p \leq 2$ at every prime. Then*

$$\boxed{\mu(A,b) = \begin{cases} d, & \delta_p = 1 \text{ for every } p \in P_{\max}, \\ d+1, & \delta_p = -1 \text{ for at least one } p \in P_{\max}. \end{cases}} \tag{5.5}$$

Every minimum has a planar realization of treewidth at most three. If the minimum is d, a realization is a vertex sum of $d-3$ cycles and one graph of cycle rank at most three. If it is $d+1$, a realization is a vertex sum of $d-2$ cycles and one such graph.

The scales and the nonsingular coefficient forms may vary independently from one prime to another. The realizing graphs may have cut vertices and parallel edges.

Theorem 5.16. *Suppose N is odd and $d \geq 3$. Assume $j_p \leq 3$ for $p \in P_{\max}$ and $j_p \leq 2$ for the other primes. Then*

$$\mu(A,b) = d \quad \Longleftrightarrow \quad \delta_p = 1 \text{ for every } p \in P_{\max}.$$

When equality holds, the same $d-3$ cycle plus ternary-graph normal form applies.

Under these hypotheses, a negative full-rank character gives $\mu(A,b) \geq d(A)+1$.

5.8. **Prescribed norm extraction and global cycles.**

Lemma 5.17. *Let p be odd, $s \geq 1$, and let U be a nonsingular symmetric form on $(\mathbb{Z}/p^s\mathbb{Z})^m$, with $m \geq 2$. For every unit $u \bmod p^s$ there is a primitive vector of norm u. It splits off orthogonally, leaving a nonsingular homogeneous form of rank $m-1$ at the same scale.*

Proof. Diagonalize U over $\mathbb{Z}/p^s\mathbb{Z}$ and select two unit diagonal entries a, b. Let χ be the quadratic character on $\mathbb{F}_p$, extended by $\chi(0) = 0$. For $t \neq 0$, the map $(x,z) \mapsto (x-z, x+z)$ identifies the solutions of $z^2 = x^2 - t$ with pairs (v,w) satisfying $vw = t$. There are $p-1$ such pairs, so

$$\sum_{x \in \mathbb{F}_p} \chi(x^2 - t) = -1.$$

The number of solutions of $ax^2 + by^2 = u$, with $u \neq 0$, is therefore

$$\sum_{x \in \mathbb{F}_p} \left(1 + \chi(b^{-1}(u - ax^2))\right) = p - \chi(-ab) > 0.$$

At a solution at least one coordinate is nonzero. Suppose it is x. If (x_j, y_j) is a solution modulo p^j, keep y_j fixed and put $x_{j+1} = x_j + p^j t_j$. Modulo p^{j+1} the error changes by $2ax_j p^j t_j$. Since $2ax_j$ is a unit modulo p, exactly one value of $t_j \bmod p$ cancels the error. Iteration gives a vector of norm $u \bmod p^s$. If only y is nonzero, vary y instead; the derivative $2by$ is a unit and determines the required correction modulo p.

Let v be the resulting vector. Its unit norm makes it primitive. For every w, the vector $w - u^{-1}(w,v)v$ belongs to $v^\perp$. Hence the module is the direct sum of the line spanned by v and its orthogonal complement. Extend v to a basis and subtract from the other basis vectors their components along v. The resulting vectors form a basis of the complement, which is therefore free of rank $m-1$. If $w \in v^\perp$ and $(w, v^\perp) = 0$, then $(w,v) = 0$ as well; thus w is orthogonal to the whole module and $w = 0$. The restricted form is nonsingular and its rank is $m-1$. □

Thus a homogeneous block of rank m permits $m-1$ successive independently prescribed unit norms. Its last rank-one determinant class is the original determinant class divided by the product of the extracted norm classes.

Lemma 5.18. *Choose $k \geq 0$. At each prime prescribe at most k distinct positions $j \in \{1, \dots, k\}$, assigning to position j a scale $p^{s_{p,j}}$. Suppose no scale s is assigned more than $m_{p,s} - 1$ times. Put*

$$n_j = \prod_{p \text{ assigned to } j} p^{s_{p,j}}.$$

If $n_j > 1$ for every position, then there is an orthogonal decomposition

$$(A, b) \cong \left(\perp_{j=1}^{k} \left\langle \tfrac{-1}{n_j} \right\rangle \right) \perp (B, c), \tag{5.6}$$

where the indicated local cyclic factors have been removed from A_p. Each first summand is the pairing of a cycle of length n_j.

Proof. Determine all orders n_j first. At prime p in position j, put $u_{p,j} = n_j / p^{s_{p,j}}$, a unit at p. Prescribe the norm coefficient $-u_{p,j}$ at scale $p^{s_{p,j}}$. Lemma 5.17 permits all these choices: each original homogeneous block retains at least one line.

The p-primary part of $\left\langle \frac{-1}{n_j} \right\rangle$ is generated by $(n_j / p^{s_{p,j}})[1]$, whose norm is

$$-\frac{u_{p,j}}{p^{s_{p,j}}} \pmod{\mathbb{Z}}.$$

Thus the selected primary factors, assembled across primes, are exactly the cycle pairing $\left\langle \frac{-1}{n_j} \right\rangle$. Primary orthogonality proves (5.6). □

Proof of Theorem 5.16. Necessity is Lemma 3.11. Assume all $\delta_p = 1$, and set $k = d - 3$. At a full-rank prime remove $d - 3$ lines, retaining at least one at each scale. This is possible because $j_p \leq 3$. At any other prime remove $\max(d_p - 2, 0)$ lines; this is possible because $j_p \leq 2$, and the number removed is at most $d - 3$. Assign the removed lines to the k positions of Lemma 5.18. Every position contains a nontrivial factor at every full-rank prime, so every cycle length is at least three.

Let (B, c) be the residual pairing, $M = |B|$, and let C denote the entire extracted cycle pairing. The residual local rank is three exactly at the full-rank primes of A, and at most two elsewhere. Fix a full-rank prime p, and put $C'_p = |C|/|C_p|$. Since every extracted cycle has a nontrivial p-part,

$$\alpha_p(C) = (-1)^k C'_p \quad \text{modulo squares}, \qquad M_p = N_p / C'_p.$$

Multiplicativity of primary determinants gives

$$\left(\frac{-M_p \alpha_p(B)}{p} \right) = \left(\frac{-\dfrac{N_p}{C'_p} \dfrac{\alpha_p(A)}{(-1)^k C'_p}}{p} \right) \tag{5.7}$$

$$= \left(\frac{(-1)^{k+1} N_p \alpha_p(A)}{p} \right) = \left(\frac{(-1)^d N_p \alpha_p(A)}{p} \right) = \delta_p = 1. \tag{5.8}$$

The square $(C'_p)^2$ cancels. Theorem 4.1 realizes the residual pairing in at most three cycles. Vertex summing with the $d - 3$ extracted cycles gives cycle rank at most d, hence exactly d by the generator bound. The graph is planar and has the asserted normal form. □

Proof of Theorem 5.15. When all characters are positive, Theorem 5.16 applies. In general set $k = d - 2$ and remove $\max(d_p - 2, 0)$ lines at each prime, retaining at least one at every scale. The hypothesis $j_p \leq 2$ permits this. Assign the removed lines to distinct positions among $1, \dots, k$. At a full-rank prime exactly k lines are removed, so every position is occupied and its cycle length exceeds one. Lemma 5.18 gives $d - 2$ cycles and a residual pairing with at most two generators. Theorem 4.1 gives the upper bound $(d - 2) + 3 = d + 1$. If a full-rank character is negative, Lemma 3.11 excludes rank d, so this upper bound is exact. Vertex sums preserve planarity and have treewidth equal to the maximum of the summands' treewidths. □

5.9. **Coprime complements of specified order.**

Theorem 5.19 (Cycle rank under coprime orthogonal addition). *Let (A, b) satisfy Theorem 5.15. Let (C, c) be any odd-order paired group with $d(C) \le 2$ and $\gcd(|C|, N) = 1$, and put $m = |C|$. Then*

$$\boxed{\mu\big((A,b) \perp (C,c)\big) = \begin{cases} d, & \left(\frac{m}{p}\right) = \delta_p \text{ for all } p \in P_{\max}, \\ d+1, & \text{otherwise.} \end{cases}} \tag{5.9}$$

The result is independent of the pairing c and of the group structure of C within the stated two-generator class. Optimal planar realizations have treewidth at most three.

Proof. The new primes have local rank at most two, hence at most two scales. They are not full-rank primes, since $d \ge 3$. The old full-rank set is unchanged, while N_p is multiplied by m. Thus each old character becomes $\delta_p \left(\frac{m}{p}\right)$. Apply Theorem 5.15. □

In particular (5.9) applies to every odd integer m coprime to N and every cyclic pairing $\left\langle \frac{a}{m} \right\rangle$. It applies to every individual complementary prime, not only sufficiently large primes or primes selected by a constructed progression. Square-order coprime complements do not alter any character.

Corollary 5.20. *For every odd prime $\ell \nmid N$ and every $a \not\equiv 0 \pmod{\ell}$,*

$$\mu\big((A,b) \perp \left\langle \tfrac{a}{\ell} \right\rangle\big) = d \quad \Longleftrightarrow \quad \left(\frac{\ell}{p}\right) = \delta_p \quad (p \in P_{\max}).$$

Otherwise the minimum is $d+1$. Both cyclic pairing classes at ℓ have the same minimum. If $t = |P_{\max}|$, the primes of minimum d have relative natural density 2^{-t} among all primes.

Proof. For each full-rank prime, its quadratic-character condition selects half of the nonzero residue classes. The Chinese remainder theorem makes the t choices independent. The prime number theorem in fixed arithmetic progressions [12] gives relative density 2^{-t}; discarding primes dividing $2N$ has no effect. □

The cycle summands in the proof can be fixed independently of the complementary group: its primary factors are left inside the ternary residual pairing. There are two fixed decompositions of A, one for each of the d and $d+1$ branches. The ternary graph varies with the complement. The realizing graphs are vertex sums of cycles and a planar graph of cycle rank at most three; they have treewidth at most three.

5.10. **Counting the pairing classes at each minimum.**

Corollary 5.21. *Fix an odd-order group A with $d \ge 3$ and $j_p \le 2$. Put*

$$J = \sum_p j_p, \qquad t = |P_{\max}|.$$

There are exactly 2^J isometry classes of nonsingular symmetric pairings on A. Exactly 2^{J-t} have minimum cycle rank d, and the remaining $2^J - 2^{J-t}$ have minimum $d+1$.

Proof. Lemma 3.12 gives exactly two nonsingular homogeneous classes at each occupied scale, distinguished by determinant square class. Choosing the final diagonal unit realizes either class. Distinct choices at any scale remain distinct in the intrinsic form $J_s(A_p)$, so there are exactly 2^J global classes. At a full-rank prime, δ_p is a fixed sign times the product of the signs at its j_p scales. Choosing the signs at $j_p - 1$ scales determines a unique sign at the last scale with $\delta_p = 1$. Exactly half the local choices therefore have positive character. Different primes have independent choices, giving 2^{J-t} such classes. Theorem 5.15 gives their stated minima. □

Each isometry class is counted with weight one.

5.11. **Orthogonal sums and graph blocks.**

Proposition 5.22. *Let $p \equiv 7 \pmod 8$ and let $s_1 < s_2 < s_3$ be odd positive integers. Put*

$$B = \perp_{i=1}^{3} \langle 1/p^{s_i} \rangle .$$

There is no exact realization of B of cycle rank at most four by a graph with more than one nontrivial block. Equivalently, no orthogonal direct sum of exact binary and ternary graph realizations realizes B in at most four cycles. Every rank-four realization of B has exactly one nontrivial block. After deleting attached trees, the remaining graph is biconnected.

Proof. The intrinsic forms $J_s(B)$ of Lemma 3.12 are one-dimensional at the three indicated scales and zero elsewhere. Under any orthogonal decomposition their dimensions add. At each scale exactly one factor therefore receives the one-dimensional residue form. The same lemma identifies each factor with the sum of its selected constituents. In a nontrivial decomposition, each selected subset is proper. A one-generator factor has odd exponent and residue coefficient at a prime seven modulo eight, so its exact graph minimum is three. A two-generator factor has two residue coefficients at odd scales and therefore has minimum two by the binary criterion. Any nontrivial orthogonal decomposition consequently requires at least $3 + 2 = 5$ independent cycles.

For a connected graph, the paired Jacobian is the orthogonal sum of the paired Jacobians of its blocks, and the cycle ranks add. Every nontrivial loopless block contributes a nontrivial Jacobian. Hence a graph with more than one nontrivial block cannot realize B in rank at most four. Attached bridges and trees do not affect the pairing and may be removed. A two-vertex loopless block has cyclic Jacobian, whereas B requires three generators. The remaining block therefore has at least three vertices and is biconnected. □

Corollary 5.10 gives $\mu(B) = 4$. Among realizations with at least two nontrivial blocks, the minimum is five, attained by the vertex sum of a cyclic realization of rank three and a binary realization of rank two.

5.12. **Optimal realizations with one nontrivial block.**

Theorem 5.23 (Optimal realizations with one nontrivial block). *For every $k \equiv 1 \pmod 4$, $k \geq 1$, there are infinitely many k-tuples of distinct primes $p_i \equiv 7 \pmod{24}$ with the following property. Put*

$$(A, b) = \perp_{i=1}^{k} \left(\langle 1/p_i \rangle \perp \left\langle 1/p_i^3 \right\rangle \perp \left\langle 1/p_i^5 \right\rangle \right) .$$

Then $d(A) = 3$ and $\mu(A, b) = 4$. Among graph realizations with more than one nontrivial block, the minimum cycle rank is exactly five. Therefore every minimum realization has a single nontrivial block.

Every orthogonal decomposition into at least two nontrivial pairings realizable in cycle rank at most three has total minimum cycle rank at least five.

Proof. For $k = 1$, Proposition 5.22 and Theorem 5.7 give minimum four, while the vertex sum of optimal cyclic and binary realizations has cycle rank five. Dirichlet's theorem [15] supplies infinitely many primes $p \equiv 7 \pmod{24}$. Write $k = 4h + 1$ with $h \geq 1$, and index the primes by $\mathbb{Z}/k\mathbb{Z}$. Require

$$\left(\frac{p_j}{p_i} \right) = (-1)^{a_{ij}}, \qquad a_{ij} = \begin{cases} 1, & j - i \in \{1, \dots, 2h\} \pmod k, \\ 0, & j - i \in \{2h+1, \dots, 4h\} \pmod k, \end{cases} \qquad (i \neq j).$$

These requirements are consistent with quadratic reciprocity: $a_{ij} + a_{ji} = 1$, and all primes are three modulo four. Choose the primes successively. The prescribed Legendre symbols specify nonempty sets of nonzero residue classes modulo the already chosen primes. The Chinese remainder theorem combines them with the class seven modulo twenty-four, and Dirichlet's theorem gives infinitely many choices for the next prime.

The matrix $D = (a_{ij})$, with zero diagonal, has row sums $2h$. Its kernel over $\mathbb{F}_2$ consists exactly of the constant vectors. Indeed, if $Dx = 0$, consecutive equations give

$$x_{i+1} = x_{i+2h+1} \quad \text{for all } i.$$

Since $\gcd(2h, 4h+1) = 1$, all coordinates of x agree.

At each prime, the intrinsic forms $J_s(A_p)$ of Lemma 3.12 have dimension one at $s = 1, 3, 5$ and zero elsewhere. Their dimensions add under orthogonal sums; hence every orthogonal factor selects a subset of these three residue constituents. Suppose a graph with more than one nontrivial block realizes (A, b) in at most four cycles. Each nontrivial block has positive cycle rank. If one has rank one, the other blocks have total rank at most three. Otherwise there are exactly two nontrivial blocks, both of rank two. Thus its pairing splits in one of two ways: a rank-one graph pairing plus a pairing realizable in rank at most three, or two pairings each realizable in rank at most two.

Consider the first possibility, $(A, b) = C \perp B$, where C is the pairing of a cycle. Let S be the set of primes at which C_p is nonzero, and put $T = \{1, \dots, k\} \setminus S$. At each $i \in S$, the factor C selects one constituent of odd exponent and residue coefficient. If $n = |C|$, the cycle pairing $\langle -1/n \rangle$ has primary coefficient $-n/p_i^{v_{p_i}(n)}$. Consequently

$$\prod_{j \in S \setminus \{i\}} \left(\frac{p_j}{p_i} \right) = -1 \quad (i \in S).$$

At each $i \in T$, the factor B_{p_i} still has rank three and residue coefficient product. The prime-to-p_i part of $|B|$ has square class $\prod_{j \in T \setminus \{i\}} p_j$: at the primes in S, two odd exponents remain and their sum is even. The exact ternary determinant condition therefore gives

$$\prod_{j \in T \setminus \{i\}} \left(\frac{p_j}{p_i} \right) = -1 \quad (i \in T).$$

In the tournament defined by a_{ij}, every vertex of the induced subtournaments on S and on T must have odd outdegree. A tournament on m vertices with every outdegree odd satisfies

$$m \equiv \binom{m}{2} \pmod 2,$$

and hence $m \equiv 0$ or $3 \pmod 4$. But two integers each congruent to zero or three modulo four cannot sum to $k \equiv 1 \pmod 4$. This excludes the first possibility.

For the second possibility, write $(A, b) = X \perp Y$ with both factors binary-realizable. At every prime, their local ranks must be one and two in some order. Let S be the set of primes where X has rank one; then Y has rank one exactly on the complement T. The order square classes are

$$|X| \equiv \prod_{i \in S} p_i, \qquad |Y| \equiv \prod_{i \in T} p_i \mod (\mathbb{Q}^\times)^2.$$

Every rank-two primary coefficient product is a residue. The binary determinant conditions are therefore

$$\prod_{j \in S} \left(\frac{p_j}{p_i} \right) = 1 \quad (i \in T), \qquad \prod_{j \in T} \left(\frac{p_j}{p_i} \right) = 1 \quad (i \in S).$$

For the indicator vector x of S, these equations read

$$Dx = \operatorname{diag}(D\mathbf{1})x = 0 \quad \text{over } \mathbb{F}_2,$$

because all row sums are even. The kernel calculation forces S to be empty or the whole vertex set.

One factor is consequently cyclic and selects one odd-exponent residue constituent at every prime. Let its order be M. Then $M \equiv 7^k \equiv 7 \pmod 8$. Its odd-prime Hasse product is

$$(-1)^k \prod_{i<j} \left(\frac{p_j}{p_i} \right) \left(\frac{p_i}{p_j} \right) = (-1)^{k + \binom{k}{2}} = -1.$$

The two-adic binary Hasse invariant is forced to be one, so this cyclic factor is not binary-realizable. This excludes the second possibility.

The same tournament parity argument with S empty excludes a rank-three realization of (A, b), because the ternary determinant conditions would require every vertex of the full tournament to have odd outdegree. Thus $\mu(A, b) \geq 4$.

Put $P = \prod_i p_i$. The even row sums of D give

$$\left(\frac{P/p_i}{p_i}\right) = \prod_{j \neq i} \left(\frac{p_j}{p_i}\right) = 1.$$

The primary coefficients of each global cyclic pairing $\langle 1/P^s \rangle$, for $s = 1, 3, 5$, are consequently squares at every p_i. Hence

$$(A, b) \simeq \langle 1/P \rangle \perp \langle 1/P^3 \rangle \perp \langle 1/P^5 \rangle.$$

Theorem 5.7 supplies a planar four-cycle realization. Thus $\mu(A, b) = 4$.

Finally, take the cyclic factor consisting of the exponent-one constituent at every prime. Its exact cycle rank is three by the odd cyclic theorem and the Hasse calculation above. The remaining two-generator pairing has square order and residue coefficient product at every prime, so the binary criterion realizes it in two cycles. Their vertex sum gives a five-cycle planar realization with at least two nontrivial blocks. This proves all the assertions. □

Example 5.24. For $k = 5$, one may take

$$(p_0, p_1, p_2, p_3, p_4) = (7, 31, 199, 631, 751).$$

The matrix of off-diagonal Legendre symbols is

$$\begin{pmatrix} 0 & -1 & -1 & 1 & 1 \\ 1 & 0 & -1 & -1 & 1 \\ 1 & 1 & 0 & -1 & -1 \\ -1 & 1 & 1 & 0 & -1 \\ -1 & -1 & 1 & 1 & 0 \end{pmatrix}.$$

Its negative-symbol matrix has kernel $\{(0, 0, 0, 0, 0), (1, 1, 1, 1, 1)\}$ over $\mathbb{F}_2$. The prime product is 20 463 603 223. Every one of these primary parts individually has exact minimum four by Theorem 5.7; the obstruction concerns their simultaneous orthogonal assembly.

5.13. **Reduction to generator ranks three, four and five.**

Conjecture 5.25. *Every finite nonsingular symmetric pairing of odd order with $d(A) \geq 2$ satisfies*

$$\mu(A, b) \leq d(A) + 1. \tag{5.10}$$

Theorem 5.26. *Assertion* (5.10) *is equivalent to its restriction to generator ranks* 3, 4, *and* 5. *Thus any failure has a counterexample with one of those three generator ranks.*

Proof. Rank two is Theorem 4.1. Classify each primary cyclic constituent by

$$(s \bmod 2, \left(\frac{a}{p}\right)),$$

so there are four types. Pair equal types, obtaining L_p pairs and at most four unpaired constituents at prime p. Remove $\min(k, L_p)$ pairs at each prime and assemble the jth selected pair across primes into one global binary component. Lemma 5.1 realizes each nonzero component in two cycles. The residual local rank is

$$d_p - 2\min(k, L_p).$$

If $d \geq 6$ is even, take $k = (d - 4)/2$. When $L_p \geq k$, the residual rank is at most four; otherwise it is the number of unpaired types, again at most four. Under the rank-three and rank-four cases of (5.10),

the residual pairing has a realization of cycle rank at most five. Residual generator ranks at most two have realizations of cycle rank at most three. Thus the total is at most $2k + 5 = d + 1$.

If $d \geq 7$ is odd, take $k = (d - 5)/2$. The same argument leaves rank at most five. The assumed cases through five realize the residual in at most six cycles, giving $2k + 6 = d + 1$. This covers every remaining rank. □

A counterexample of least generator rank has rank three, four, or five. Theorems 5.15 and 5.12 imply that its order has at least two distinct prime divisors and that some primary group has at least three distinct elementary-divisor exponents.

6. Prime stabilization with prescribed arithmetic

6.1. **Tridiagonal flow matrices on planar ladders.** For $r = 1$, let Q_1 be a triangle. For $r \geq 2$, let Q_r have vertices

$$u_1, \dots, u_{r-1}, v_1, \dots, v_{r-1}.$$

There is one ordinary rung $u_i v_i$ for each $1 \leq i < r$, a top edge $u_i u_{i+1}$ and a bottom edge $v_i v_{i+1}$ for each $1 \leq i < r - 1$, and two additional end edges: one more edge $u_1 v_1$ and one more edge $u_{r-1} v_{r-1}$. All three kinds of edges are distinct. In particular, Q_2 consists of three parallel edges between two vertices. For $r \geq 2$, the graph has $2r - 2$ vertices and $3r - 3$ edges, with every vertex of degree three.

Place the u_i and v_i in two horizontal rows, with the extra end edges drawn outside the left and right ordinary rungs. This gives a plane embedding with r bounded faces, in order: the left digon, the $r - 2$ rectangles, and the right digon. This description also applies to $r = 2$, when there are no rectangles.

Lemma 6.1. *Let $r \geq 1$ and let L be the symmetric integral tridiagonal matrix with diagonal entries $b_1, \dots, b_r$ and adjacent entries $-c_1, \dots, -c_{r-1}$. Fix an integer $g \geq 3$. If $r = 1$, assume $b_1 \geq 3g$. If $r \geq 2$, assume*

$$\begin{aligned} c_i &\geq g && (1 \leq i < r), \\ b_1 - c_1 &\geq g, \qquad b_r - c_{r-1} \geq g, \\ b_i - c_{i-1} - c_i &\geq 2g && (2 \leq i < r). \end{aligned} \tag{6.1}$$

Then a subdivision Γ of the fixed graph Q_r has an integral flow basis whose Gram matrix is exactly L. The graph Γ is simple, planar and biconnected, has all vertex degrees in $\{2, 3\}$, has girth at least $2g$, and has treewidth at most two. Its cycle rank is exactly r, and it has exactly $2r - 2$ vertices of degree three.

Consequently L is positive definite and the entire paired Jacobian of Γ is $-\mathcal{D}(L)$.

Proof. Suppose first that $r = 1$. Replace the three edges of Q_1 by paths of lengths $g, g, b_1 - 2g$, with pairwise disjoint interiors. The result is a cycle of length b_1. Its oriented cycle is an integral flow basis with Gram matrix $[b_1]$. Since $b_1 \geq 3g \geq 3$, this graph is simple and planar, every vertex has degree two, deletion of a vertex leaves a connected path, and its girth is b_1. Its cycle rank is one. If its vertices in order are $x_0, \dots, x_{b_1-1}$, the path of bags

$$\{x_0, x_i, x_{i+1}\}, \qquad 1 \leq i \leq b_1 - 2,$$

is a tree decomposition of width two. It covers every edge, and the bags containing any fixed vertex form an interval.

Assume now that $r \geq 2$, and put

$$c_0 = c_r = 0, \qquad s_i = b_i - c_{i-1} - c_i.$$

Replace the ordinary rung $u_i v_i$ by a path of length c_i. Replace the extra left and right end edges by paths of lengths s_1 and s_r, respectively. For the interior face with index i, $2 \leq i < r$, replace its top edge $u_{i-1} u_i$ and bottom edge $v_{i-1} v_i$ by paths of lengths g and $s_i - g$. All path interiors are pairwise disjoint. The assumptions imply that every replacement path has length at least g. Thus c_i is the

length of the common rung of faces i and $i+1$, while s_i is the total length of the edges belonging only to the boundary of face i among the bounded faces.

The ordinary rungs and bottom edges form a spanning tree of Q_r: the bottom vertices form a path, and every top vertex is attached to its bottom partner by its rung. The edges outside this tree are the extra left edge, the top edges, and the extra right edge. Their fundamental cycles are exactly the bounded facial cycles. Lemma 2.3 therefore makes these cycles an integral basis of the flow lattice.

Orient all bounded face boundaries consistently in the plane. Two consecutive boundaries have opposite coefficients on their common rung. Under subdivision, orient each replacement path along its old edge. The incidence equation at each new internal vertex forces its two edge coefficients in any flow to be equal. Restriction to one coefficient per replacement path and constant extension along the paths are therefore inverse isomorphisms of integral flow groups. The extended facial cycles $z_1, \dots, z_r$ remain an integral basis, and

$$\langle z_i, z_j \rangle = \begin{cases} s_i + c_{i-1} + c_i = b_i, & i = j, \\ -c_i, & j = i+1, \\ -c_j, & i = j+1, \\ 0, & |i-j| > 1. \end{cases} \tag{6.2}$$

Their Gram matrix is precisely L.

The plane embedding survives subdivision. Every old edge lies on a bounded facial cycle, so every new edge lies on a cycle and is not a bridge. The graph is connected. Each old vertex retains degree three, and every new vertex has degree two. Because every old edge has been replaced by a path of length at least three with its own internal vertices, no new edge is a loop and no two new edges have the same endpoints. Thus Γ is simple.

If a vertex w were a cut vertex, each component of $\Gamma - w$ would have at least two edges to w; a unique such edge would be a bridge. At least two components would force $\deg(w) \geq 4$, contrary to the degree bound. Since Γ has at least three vertices, this proves biconnectivity. Every cycle in Γ consists of complete replacement paths, because their internal vertices have degree two. Since Q_r has no loop, it contains at least two paths of length at least g, so the girth is at least $2g$.

A tree decomposition is a tree of vertex bags which covers all vertices and edges and in which the bags containing each fixed graph vertex form a connected subtree. Its width is one less than the maximum bag size. For Q_2, the single bag $\{u_1, v_1\}$ is a decomposition. For $r \geq 3$, take the path of bags

$$B_1, D_1, B_2, D_2, \dots, B_{r-2}, D_{r-2},$$

where

$$B_i = \{u_i, v_i, u_{i+1}\}, \qquad D_i = \{v_i, u_{i+1}, v_{i+1}\} \quad (1 \leq i \leq r-2).$$

Top edges are covered by the B_i, bottom edges by the D_i, and each rung and extra end edge is covered by a bag containing its two endpoints. The bags containing an internal u_i are consecutive among B_{i-1}, D_{i-1}, B_i; those containing an internal v_i are consecutive among D_{i-1}, B_i, D_i. At the ends these lists are truncated. Hence this is a valid decomposition with bags of size at most three.

For each old edge xy replaced by the path $xw_1 \cdots w_k y$, choose a bag containing x, y and attach to it the chain of new bags

$$\{x, y, w_1\},\ \{y, w_1, w_2\},\ \dots,\ \{y, w_{k-1}, w_k\}.$$

These bags cover every new edge. The bags containing x or y remain connected, and each w_i occurs in one or two consecutive new bags. Attach these chains separately for every old edge, including parallel edges. The resulting decomposition still has bags of size at most three, proving treewidth at most two.

The core Q_r has cycle rank $(3r-3) - (2r-2) + 1 = r$, and subdivision preserves cycle rank. It also preserves the degrees of the $2r-2$ old vertices and creates only vertices of degree two. This proves the remaining numerical assertions. A Gram matrix of a basis in a Euclidean lattice is positive definite, and the final pairing assertion is Lemma 2.4. □

6.2. **A primitive arithmetic progression of determinants.**

Lemma 6.2. *Every nonsingular integral symmetric lattice over $\mathbb{Z}_p$ is an orthogonal sum of lines when p is odd, and of lines and scaled even unimodular binary lattices when $p = 2$. In particular, it has a tridiagonal Gram matrix over $\mathbb{Z}_p$ in an integral basis. If the lattice is even at two, every summand is even.*

Proof. Let k be the least valuation of a Gram entry. Suppose a primitive vector v has norm $p^k u$, with u a unit. All pairings with v are divisible by p^k, so

$$x \longmapsto x - \frac{(x,v)}{(v,v)}v$$

is integral and splits the line $\mathbb{Z}_p v$ orthogonally. At an odd prime such a vector exists: if no diagonal entry has valuation k, an off-diagonal entry (v_i, v_j) of valuation k gives $v_i + v_j$ of norm of valuation k.

At two, if no diagonal entry has valuation k, the corresponding pair v_i, v_j has Gram matrix

$$2^k B, \qquad B = \begin{pmatrix} 2a & u \\ u & 2b \end{pmatrix}, \qquad u \in \mathbb{Z}_2^\times.$$

The matrix B is unimodular. Every pairing with the pair is divisible by 2^k, so multiplication by $(2^k B)^{-1}$ gives integral coefficients for the orthogonal projection onto their span. This splits an integral binary summand. In either case the complement is nonsingular and has smaller rank. Induction gives the decomposition. Evenness is inherited by every integral sublattice. Ordering the one- and two-dimensional summands consecutively gives a tridiagonal matrix. □

The cofactor of the last diagonal entry of a tridiagonal matrix is its preceding principal determinant. Making the determinant and this cofactor coprime away from the prescribed primes gives a primitive arithmetic progression; the same cofactor determines the pairing on the entire complementary cyclic group.

Proposition 6.3. *Let $N \geq 1$, $r \geq 1$, and let S be a finite set of primes containing every divisor of $2N$. For each $p \in S$, prescribe an integral symmetric tridiagonal $\mathbb{Z}_p$-matrix C_p of size r with $v_p(\det C_p) = v_p(N)$. Then there are positive tridiagonal integral matrices L_t, $t \geq 0$, with the prescribed local isometry classes and*

$$\det L_t = N(u + vt), \qquad \mathcal{D}(L_t) \cong \left(\perp_{p \in S} \mathcal{D}_p(C_p) \right) \perp \left\langle \tfrac{NF}{u+vt} \right\rangle, \tag{6.3}$$

where u, v, F are positive, $\gcd(u, v) = 1$, and every $u + vt$ is coprime to $NF \prod_{p \in S} p$. Only the last diagonal varies. The adjacent weights and row sums may have any prescribed lower bounds. Any specified row-sum parities satisfied by C_2 are retained.

If $m \geq 1$, $(a, m) = 1$, S contains the divisors of m, and $\det C_p \in Na(\mathbb{Z}_p^\times)^2$ for $p \mid m$, the matrices may also be chosen with $u \equiv a \pmod{m}$ and $m \mid v$, retaining the specified row-sum parities.

Proof. In the last assertion, choose a unit s_p with $s_p^2 \det C_p = Na$ and multiply the first basis vector by s_p. This preserves tridiagonality and the local isometry class. Whenever $p = 2$, the unit s_p is one modulo two, so every matrix entry modulo two, and hence every row-sum parity, is preserved. The determinant is now Na at every $p \mid m$. Without a prescribed residue, make no such basis change.

Choose $e_p \geq 0$ with $p^{e_p} C_p^{-1}$ integral. Take $k_p \geq e_p + 3$, and, where $p \mid m$, also $k_p \geq v_p(N) + v_p(m)$. Put $M = \prod_{p \in S} p^{k_p}$. Choose positive integers c_i, as large as required, with $-c_i \equiv (C_p)_{i,i+1} \pmod{p^{k_p}}$ for all $p \in S$. Let T consist of the prime divisors of $\prod_{i<r} c_i$ outside S. For $r = 1$ the product is one and T is empty. By the Chinese remainder theorem choose diagonal entries a_i with

$$a_i \equiv (C_p)_{ii} \pmod{p^{k_p}} \, (p \in S), \qquad a_1 \equiv 1 \pmod{q}, \quad a_i \equiv 1 + c_{i-1}^2 \pmod{q} \, (q \in T,\ i \geq 2).$$

Increase them independently by positive multiples of $M \prod_{q \in T} q$ until all row sums have the desired positive lower bounds. Let L have diagonal a_i and adjacent entries $-c_i$. For $c_0 = c_r = 0$, its quadratic form is

$$x^{\mathsf{T}} L x = \sum_{i<r} c_i (x_i - x_{i+1})^2 + \sum_i (a_i - c_{i-1} - c_i) x_i^2 > 0 \quad (x \neq 0).$$

Lemma 3.5 preserves every local isometry class. Since M is even, the specified row parities are preserved.

Let Δ_i denote the leading principal determinants and $\Delta_0 = 1$. Expansion in the last row gives

$$\Delta_1 = a_1, \qquad \Delta_i = a_i\Delta_{i-1} - c_{i-1}^2\Delta_{i-2}.$$

They are positive. For $q \in T$, induction gives $\Delta_i \equiv 1 \pmod q$. Set $D = \Delta_r$, $F = \Delta_{r-1}$ and $u = D/N$. The local determinant valuations imply that u is a positive integer coprime to every prime of S. It is also coprime to T. If a prime outside $S \cup T$ divided both u and F, it would divide Δ_r and Δ_{r-1}. The recurrence and the invertibility of every c_i at that prime would successively imply $\Delta_{r-2} = \cdots = \Delta_0 = 0$ modulo the prime, contrary to $\Delta_0 = 1$. For $r = 1$, one has $F = \Delta_0 = 1$ directly. Thus $(u, F) = 1$.

Put $K = M\prod_{q\in T} q$, $v = KF$, and $L_t = L + NKt\, e_r e_r^{\mathsf T}$. Cofactor expansion gives

$$\det L_t = N(u + vt), \qquad (L_t^{-1})_{rr} = \frac{F}{N(u + vt)}.$$

Every prime divisor of K lies in $S \cup T$. Hence $(u, v) = 1$ and $(u + vt, NF\prod_{p\in S} p) = 1$ for every $t \geq 0$. Put $n_t = u + vt$. The adjugate identity shows that $\det L_t = Nn_t$ annihilates the cokernel, so $n_t N[e_r] = 0$. The norm of this class is

$$N^2(L_t^{-1})_{rr} = \frac{NF}{n_t}.$$

Since $(NF, n_t) = 1$, this value has order n_t in $\mathbb{Q}/\mathbb{Z}$. The class $N[e_r]$ therefore has order n_t, and its cyclic subgroup is nonsingular. The sum of the primary parts at S has order N. Pairings between groups of relatively prime orders vanish, and Nn_t is the order of the full cokernel. These subgroups therefore form the orthogonal decomposition (6.3).

For the last assertion, entrywise approximation preserves $\det L \equiv Na \pmod{p^{v_p(N)+v_p(m)}}$ at every $p \mid m$. Dividing by N gives $u \equiv a \pmod m$. The chosen k_p imply $m \mid K$, hence $m \mid v$. Increasing the last diagonal changes no interior row sum. All positivity and length inequalities persist. □

Theorem 6.4 (Minimum cycle rank with a prime complement). *Let (A, b) be finite nonsingular. For any rank $r \geq \max\{1, d(A)\}$, finite set of primes to exclude, and girth bound, infinitely many primes ℓ admit*

$$(\mathrm{Jac}(G_\ell), b_{G_\ell}) \cong (A, b) \perp \left\langle \tfrac{\kappa}{\ell} \right\rangle, \qquad \beta(G_\ell) = r,$$

where $\kappa \neq 0$ is fixed. The graphs are simple, planar, biconnected, of treewidth at most two, with every vertex degree in $\{2, 3\}$ and the prescribed girth. They subdivide Q_r and only one path length varies. The least possible rank when the complement is free is $\max\{1, d(A)\}$.

Proof. At the primes dividing $2|A|$ choose the local presentations of $(A_p, -b_p)$ from Lemma 3.4, with unimodular summands up to rank r. At additional excluded primes prescribe a unimodular matrix. Apply Proposition 6.3 with $N = |A|$, then Lemma 6.1. The graph pairing is the negative flow discriminant, so $\kappa = -NF$. Dirichlet's theorem [15] applies to $(u, v) = 1$ and gives infinitely many prime denominators. A flow matrix of size β presents its discriminant with at most β generators. The prescribed quotient A and the nonzero prime part therefore force $\beta \geq \max\{1, d(A)\}$. □

Corollary 6.5. *Every finite paired group has infinitely many prime-order cyclic completions realized by biconnected outerplanar loopless multigraphs. The prime can avoid an arbitrary finite set. The edge multiplicities, and hence the vertex degrees, may be unbounded.*

Proof. Apply Proposition 6.3 to local presentations of (A_p, b_p), with rank at least two. The matrices have negative adjacent entries $-c_i$ and positive row sums s_i. On vertices $o, v_1, \ldots, v_r$ put c_i parallel edges between v_i, v_{i+1} and s_i edges between o, v_i. The reduced Laplacian is the matrix. Its pairing has positive sign, giving the requested target. The cycle $o, v_1, \ldots, v_r, o$ is a Hamilton cycle; draw the remaining edges on its interior side along nonintersecting spokes from o. This is an outerplanar embedding. Deleting any vertex leaves the spanning path from the Hamilton cycle, so the graph is biconnected. Dirichlet's theorem selects the prime orders. □

6.3. **Prime residue and pairing classes.** Let (A, b) be a nonsingular finite symmetric bilinear pairing and write $N = |A|$. Let m be divisible by $8\,\mathrm{rad}(N_{\mathrm{odd}})$ and let $\gcd(a, m) = 1$. For odd primes $\ell \nmid 2N$, the quadratic character $\left(\frac{-N}{\ell}\right)$ depends only on $\ell \bmod m$; write its value on the class a as $\chi_{-N}(a)$. Let $\varepsilon \in \{1, -1\}$. The pair (a, ε) is admissible at rank $r \geq 1$ if there are integral local lattices K_p, one for each $p \mid 2N$, with

$$\operatorname{rank} K_p = r, \qquad \mathcal{D}_p(K_p) \cong (A_p, -b_p), \qquad \det K_p \in N a(\mathbb{Z}_p^\times)^2,$$

and

$$\prod_{p|2N} h_p(K_p) = \chi_{-N}(a)\varepsilon. \tag{6.4}$$

Evenness at two is not imposed in this bilinear definition.

Lemma 6.6. *Let C be a positive definite integral symmetric matrix of determinant $N\ell$, where ℓ is an odd prime not dividing $2N$. Suppose its discriminant bilinear module is*

$$\mathcal{D}(C) \cong (A, -b) \perp \left\langle \frac{-s}{\ell} \right\rangle.$$

Then

$$h_\ell(C) = \left(\frac{-N}{\ell}\right)\left(\frac{s}{\ell}\right), \qquad \prod_{p|2N} h_p(C) = \left(\frac{-N}{\ell}\right)\left(\frac{s}{\ell}\right).$$

Proof. At ℓ, integral diagonalization gives

$$C \cong U \perp [\ell u],$$

where U is unimodular and u is a unit. Its discriminant pairing on the ramified line has coefficient u^{-1} modulo squares, hence

$$\left(\frac{u}{\ell}\right) = \left(\frac{-s}{\ell}\right).$$

The determinant condition gives $\det U = N/u$ modulo squares. A unimodular form at an odd prime has Hasse invariant one, since Hilbert symbols between two units are one. The direct-sum formula therefore gives

$$h_\ell(C) = (N/u, \ell u)_\ell = \left(\frac{N/u}{\ell}\right) = \left(\frac{-Ns}{\ell}\right).$$

At an odd prime outside $2N\ell$, the entire lattice is unimodular and its Hasse invariant is one. At the real place it is positive definite, so its Hasse invariant is one as well. The product formula proves the second equality. □

Theorem 6.7 (Prescribed prime residue and pairing classes). *For a fixed rank $r \geq 1$, the following are equivalent.*

(1) The pair (a, ε) is admissible at rank r.

(2) For some prime $\ell \equiv a \pmod m$, $\ell \nmid 2N$, there is a connected loopless graph G with $\beta(G) = r$ and

$$(\mathrm{Jac}(G), b_G) \cong (A, b) \perp \left\langle \frac{s}{\ell} \right\rangle, \qquad \left(\frac{s}{\ell}\right) = \varepsilon.$$

(3) For every prescribed girth bound and finite exceptional set of primes, infinitely many such primes outside that set have realizations by simple planar biconnected graphs of cycle rank r, all of whose vertices have degree two or three and whose treewidth is at most two. All realizing graphs may be subdivisions of the fixed graph Q_r. Within the constructed progression, the numerator $s = \kappa$ can be chosen independent of ℓ.

Proof. For (2) implies (1), take the positive integral flow Gram matrix of G. Its discriminant pairing is the negative graph pairing. Localization gives the prescribed discriminant modules. Since $\ell \equiv a \pmod m$, the ratio ℓ/a is a square unit at each $p \mid 2N$, so its determinant square class is Na. Lemma 6.6 gives the Hasse product condition.

For (1) implies (3), enlarge the prime set to include the prescribed exceptions and the prime divisors of m. At a divisor of m not dividing $2N$, prescribe the unimodular matrix $\operatorname{diag}(Na, 1, \dots, 1)$; at every other added prime prescribe the identity matrix. Lemma 6.2 gives an integral tridiagonal Gram matrix for each prescribed lattice K_p. These are integral changes of basis of the prescribed lattices, so their full local isometry classes, determinant square classes, and rational Hasse invariants are retained. Proposition 6.3 now gives $\det L_j = N(u + vj)$, with $u \equiv a \pmod m$, $m \mid v$, $(u, v) = 1$, and the required local isometry classes. For each prime value $\ell = u + vj$, the complementary graph pairing is $\left\langle \frac{\kappa}{\ell} \right\rangle$ with $\kappa = -NF$. Lemma 6.6 gives

$$\chi_{-N}(a)\left(\frac{\kappa}{\ell}\right) = \prod_{p \mid 2N} h_p(K_p) = \chi_{-N}(a)\varepsilon.$$

Thus its Legendre class is ε. Dirichlet's theorem gives infinitely many such primes, and Lemma 6.1 gives every stated graph restriction. Assertion (3) supplies a graph satisfying (2), by choosing one of its prime denominators. □

Theorem 6.8 (Sharp rank bound for prescribed prime classes). *Let (A, b) be any nonsingular finite symmetric pairing, and put $d = d(A)$, $d_2 = d(A_2)$, and*

$$R(A) = \max\{d + 1, d_2 + 3\}.$$

Let $m \geq 1$, $\gcd(a, m) = 1$, and $\varepsilon \in \{1, -1\}$. For every $r \geq R(A)$, every prescribed girth bound, and every finite set of excluded primes, infinitely many primes $\ell \equiv a \pmod m$, $\ell \nmid 2|A|$, admit simple planar biconnected graph realizations

$$(\operatorname{Jac}(G_\ell), b_{G_\ell}) \cong (A, b) \perp \left\langle \frac{\kappa}{\ell} \right\rangle, \qquad \left(\frac{\kappa}{\ell}\right) = \varepsilon, \qquad \beta(G_\ell) = r.$$

The numerator κ is fixed within the constructed family. All vertices have degree two or three, all graphs have treewidth at most two, and all may be subdivisions of Q_r. The rank differences are

$$R(A) - d = \begin{cases} 1, & d \geq d_2 + 2, \\ 2, & d = d_2 + 1, \\ 3, & d = d_2. \end{cases}$$

In each of these three regimes there are pairings and prescriptions for which no smaller rank is possible. In particular, the universal constant three cannot be replaced by two.

Proof. Put $N = |A|$. Refine the prescribed congruence class, if necessary, to a unit class modulo $\operatorname{lcm}(m, 8\operatorname{rad}(N_{\mathrm{odd}}))$. Such a refinement exists by the Chinese remainder theorem. It suffices to construct admissible local lattices for this refined class.

At an odd prime $p \mid N$, start with a minimal-rank integral presentation of $(A_p, -b_p)$. Pad it to rank r by unimodular lines. At least one line is available because $r \geq d + 1$; its unit square class can be chosen to make the total determinant square class Na. Fix these local lattices and their Hasse invariants. At two, choose a minimal-rank integral presentation C_2 of $(A_2, -b_2)$, of rank d_2. There remain $t = r - d_2 \geq 3$ ranks for a unimodular summand. Choose an odd unit D such that

$$\det C_2 \cdot D \in Na(\mathbb{Z}_2^\times)^2.$$

The two unimodular matrices

$$U_+ = \operatorname{diag}(1, 1, D, 1, \dots, 1), \qquad U_- = \operatorname{diag}(-1, -1, D, 1, \dots, 1)$$

have rank t, the same determinant D, and opposite Hasse invariants:

$$h_2(U_+) = 1, \qquad h_2(U_-) = (-1,-1)_2\,(-1,D)_2^2 = -1.$$

Their discriminant pairings are trivial. The cross term $(\det C_2, D)_2$ is the same for both, so the lattices $C_2 \perp U_+$ and $C_2 \perp U_-$ have opposite Hasse invariants and the same required determinant and finite pairing. Choose the sign so that the product over $p \mid 2N$ satisfies (6.4). Theorem 6.7 now gives the asserted realizations. Propositions 6.10, 6.11, and 6.9 give the corresponding lower bounds. □

Proposition 6.9. *Fix $k \geq 2$, and let $\mathcal{E}_{2^k}$ denote the hyperbolic bilinear pairing on $(\mathbb{Z}/2^k\mathbb{Z})^2$. Suppose $\ell \equiv 1 \pmod 8$ is prime and s is a quadratic residue modulo ℓ. If a connected loopless graph satisfies*

$$(\mathrm{Jac}(G), b_G) \cong \mathcal{E}_{2^k} \perp \left\langle \frac{s}{\ell} \right\rangle,$$

then $\beta(G) \geq 5$. For infinitely many such primes there are realizations with $\beta(G) = 5$ and all the restrictions of Theorem 6.8.

Proof. The generator bound gives $\beta(G) \geq 2$. Let C be a positive integral flow Gram matrix, of rank $r = \beta(G)$ and determinant $2^{2k}\ell$. At two its discriminant pairing is $-\mathcal{E}_{2^k} \cong \mathcal{E}_{2^k}$. Integral Jordan splitting gives

$$C \otimes \mathbb{Z}_2 \cong U \perp 2^k B,$$

where U is unimodular of rank $r-2$ and B is a unimodular binary matrix. The finite pairing condition implies that B^{-1} is congruent to H modulo four, after an invertible change of basis. Inverting this congruence shows that B is likewise congruent to H modulo four after an integral unit change of basis. Such a matrix has determinant -1 modulo eight: its diagonal entries are multiples of four and its off-diagonal entry is one modulo four. An odd change-of-basis determinant has square one modulo eight, so

$$\det B \in -(\mathbb{Z}_2^\times)^2.$$

Over $\mathbb{Q}_2$, a nonsingular binary form whose determinant is minus a square is hyperbolic. Thus

$$h_2(2^k B) = 1, \qquad \det(2^k B) \equiv -1 \quad \text{modulo rational squares.}$$

If $r = 2$, this contradicts $\det C = 2^{2k}\ell$, whose unit square class is 1 because $\ell \equiv 1 \pmod 8$. If $r = 3$ or $r = 4$, then U has rank one or two and determinant square class -1. In rank one its Hasse invariant is one by definition; in rank two it is hyperbolic, so its Hasse invariant is again one. Therefore

$$h_2(C) = h_2(U)h_2(2^k B)(\det U, \det(2^k B))_2 = (-1,-1)_2 = -1.$$

But Lemma 6.6 gives

$$h_2(C) = \left(\frac{-2^{2k}}{\ell}\right)\left(\frac{s}{\ell}\right) = 1,$$

since $\ell \equiv 1 \pmod 8$ and s is a residue. This contradiction excludes ranks three and four. The universal construction with $d(\mathcal{E}_{2^k}) = 2$, $r = 5$, class $1 \pmod 8$, and sign $+1$ proves attainability for infinitely many primes. □

Proposition 6.10. *For every integer $d \geq 2$, let*

$$(A, b) = \left\langle \frac{1}{3} \right\rangle^{\perp d}.$$

Prescribe a prime class satisfying $\left(\frac{\ell}{3}\right) = -(-1)^d$, and prescribe either square class for the complementary prime pairing. Every connected loopless graph realization has $\beta(G) \geq d+1$, and infinitely many such primes admit realizations at rank $d+1$ with all the restrictions of Theorem 6.8. Here $d_2 = 0$ and $R(A) = d+1$. In particular, $A = \langle 1/3\rangle^{\perp 2}$ and $\ell \equiv 2 \pmod 3$ give the smallest example in this regime.

Proof. The generator bound gives $r = \beta(G) \geq d$. If $r = d$, integral Jordan splitting at three and the finite pairing prescription give

$$C \otimes \mathbb{Z}_3 \cong -3I_d.$$

Indeed, the unimodular matrix multiplying three has reduction isometric to $-I_d$ over $\mathbb{F}_3$, and this isometry lifts over $\mathbb{Z}_3$. Its determinant has 3-adic unit square class $(-1)^d$. But $\det C = 3^d\ell$ has unit square class ℓ, contrary to the prescribed character. Thus $r \geq d+1$. Since $R(A) = \max\{d+1, 3\} = d+1$, the universal construction proves the attainment assertion for either complementary pairing class. □

Proposition 6.11. *Let*

$$(A, b) = \mathcal{E}_4 \perp \left\langle \frac{1}{3} \right\rangle^{\perp 3}, \qquad |A| = 432,$$

and prescribe $\ell \equiv 19 \pmod{24}$ *and a square complementary pairing class. Every connected loopless graph realization has* $\beta(G) \geq 5$*, and infinitely many such primes admit realizations at rank five with all the restrictions of Theorem 6.8. Here* $d = 3$*,* $d_2 = 2$*, and* $R(A) = 5 = d + 2$*.*

Proof. Let C be a positive integral flow Gram matrix, with $\det C = 432\ell$. The generator bound gives $r \geq 3$. Suppose $r = 3$ or $r = 4$. At two, the argument in Proposition 6.9 gives a ramified hyperbolic binary summand of determinant square class -1 and Hasse invariant one. The unit part of the determinant of C is $27\ell \equiv 1 \pmod 8$, because $\ell \equiv 3 \pmod 8$. The remaining unimodular summand therefore has determinant square class -1 and rank one or two. Its Hasse invariant is one in either case, so

$$h_2(C) = (-1, -1)_2 = -1.$$

If $r = 3$, the local pairing at three forces $C \otimes \mathbb{Z}_3 \cong -3I_3$. Its determinant unit square class is -1, whereas $432\ell = 3^3 \cdot 16\ell$ has unit square class 1 at three, since $\ell \equiv 1 \pmod 3$. This excludes $r = 3$.

If $r = 4$, the local isometry class at three is

$$C \otimes \mathbb{Z}_3 \cong (-3I_3) \perp [-16\ell].$$

The two Hasse factors are

$$h_3(-3I_3) = (-3, -3)_3^3 = -1, \qquad (-27, -16\ell)_3 = \left(\frac{-16\ell}{3}\right) = -1.$$

Consequently $h_3(C) = 1$ and $h_2(C)h_3(C) = -1$. On the other hand,

$$\left(\frac{-432}{\ell}\right) = \left(\frac{-3}{\ell}\right) = \left(\frac{\ell}{3}\right) = 1.$$

Lemma 6.6 would give $h_2(C)h_3(C) = 1$ for a square complementary pairing, a contradiction. This excludes $r = 4$. The rank-five attainment follows from $R(A) = \max\{4, 5\} = 5$. □

6.3.1. *Finite determination of admissible local data.* The admissibility condition can be expressed by the following finite sets of determinant square classes and Hasse invariants. Unimodular summands have trivial discriminant but contribute to both invariants.

Fix $p \mid 2N$ and a proposed rank r. Let e_p be the exponent valuation of A_p, with $e_p = 0$ for the trivial group. At an odd prime, choose a nonsquare unit η_p. Consider orthogonal sums of the blocks

$$[p^k u], \qquad 0 \leq k \leq e_p, \qquad u \in \{1, \eta_p\}.$$

At two consider orthogonal sums of

$$[2^k u], \quad u \in \{1, 3, 5, 7\}, \qquad 2^k H, \qquad 2^k F, \qquad 0 \leq k \leq e_2,$$

where

$$H = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad F = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}.$$

Rank-one blocks of scale $k = 0$ are allowed at two. Lemma 6.2 and Lemma 3.3 give these representatives: rescaling a line by a unit square leaves one of the displayed unit classes, and every scaled even unimodular binary block is $2^k H$ or $2^k F$. Each block of positive scale has exponent p^k in its discriminant group, so $k \le e_p$.

At scale $k = 1$, the blocks $2H$ and $2F$ have the same finite bilinear pairing: in each case the two standard classes have norm zero and mutual pairing $1/2$ in $\mathbb{Q}_2/\mathbb{Z}_2$. Their determinant square classes are -1 and 3, respectively, whereas both rational Hasse invariants are one. Indeed,

$$2H \cong_{\mathbb{Q}_2} \operatorname{diag}(4,-4), \qquad 2F \cong_{\mathbb{Q}_2} \operatorname{diag}(4,3).$$

The first basis is $(e_1 + e_2, e_1 - e_2)$ and the second is $(e_1, e_2 - e_1/2)$; neither is an integral $\mathbb{Z}_2$-basis. The Hilbert symbols $(4,-4)_2$ and $(4,3)_2$ are both one. Thus the determinant condition distinguishes two integral lattices with the same finite bilinear pairing.

Let $\mathscr{L}_p(r, A, b)$ consist of the displayed orthogonal sums C satisfying

$$\operatorname{rank} C = r, \quad v_p(\det C) = v_p(N), \quad \mathcal{D}(C) \cong (A_p, -b_p).$$

There are finitely many block multisets of total rank r. Fix generators $x_1, \dots, x_s$ of A_p and a finite set of defining relations. The last condition is equivalent to the existence of elements $y_1, \dots, y_s$ of coker C which satisfy these relations, generate the cokernel, and obey

$$b_p(x_i, x_j) + y_i^{\mathsf{T}} C^{-1} y_j = 0 \quad \text{in } \mathbb{Q}_p/\mathbb{Z}_p$$

for all i, j. The relations give a surjective homomorphism $x_i \mapsto y_i$; the two groups have order $p^{v_p(N)}$, so it is an isomorphism. Bilinearity extends the displayed identities to every pair of elements. There are finitely many possible tuples. Set

$$\mathscr{E}_p = \{h_p(C) \,:\, C \in \mathscr{L}_p(r, A, b),\ \det C \in Na(\mathbb{Z}_p^{\times})^2\}.$$

For a rational diagonalization $C \cong \operatorname{diag}(c_1, \dots, c_r)$, $h_p(C) = \prod_{i<j} (c_i, c_j)_p$. The Hilbert symbols are as follows. If $x = p^{\alpha} u$ and $y = p^{\beta} v$, with u, v units, then at an odd prime

$$(x, y)_p = (-1)^{\alpha\beta(p-1)/2} \left(\frac{u}{p}\right)^{\beta} \left(\frac{v}{p}\right)^{\alpha}.$$

At two, for odd unit representatives u, v modulo eight,

$$(x, y)_2 = (-1)^{\frac{u-1}{2}\frac{v-1}{2} + \alpha\frac{v^2-1}{8} + \beta\frac{u^2-1}{8}}.$$

The pair (a, ε) is admissible precisely when

$$\chi_{-N}(a)\varepsilon \in \left\{ \prod_{p \mid 2N} \eta_p \,:\, \eta_p \in \mathscr{E}_p \right\}.$$

Every admissible pair has infinitely many prime realizations by Theorem 6.7. This assertion concerns a subprogression of the prescribed class, rather than every prime in that class.

7. Equivariant graphical realization

7.1. **Unimodular forms with prescribed row sums.** An integral symmetric tridiagonal matrix C with adjacent entries $-c_i$ has row sums

$$s_i = C_{ii} - c_{i-1} - c_i, \qquad c_0 = c_g = 0.$$

In the reflection-invariant ladder below, the integrality of the paired rail lengths is equivalent to $s_i \in 2\mathbb{Z}$ for $2 \le i \le g - 1$.

Lemma 7.1. *For $u \geq 1$, put*

$$J_u = \begin{pmatrix} 2 & -1 & & & \\ -1 & 2 & -1 & & \\ & \ddots & \ddots & \ddots & \\ & & -1 & 2 & -1 \\ & & & -1 & 1 \end{pmatrix}, \qquad J_1 = [1].$$

Then J_u is positive definite, $\det J_u = 1$*, and its row sums are* $(1, 0, \dots, 0)$*. If a tridiagonal matrix B has all its entries even, then every interior row sum of $J_u \perp B$ is even. The same holds for B without a unimodular block.*

Proof. The quadratic form is

$$x_1^2 + \sum_{i=1}^{u-1} (x_i - x_{i+1})^2.$$

The change of variables $y_1 = x_1$, $y_{i+1} = x_i - x_{i+1}$ has integral inverse $x_i = y_1 - y_2 - \cdots - y_i$. Thus J_u is integrally congruent to I_u. Multiplication by the all-ones vector gives $J_u \mathbf{1} = e_1$. Every row sum of B is even, so the only odd row sum of $J_u \perp B$ occurs in its first row. □

Lemma 7.2. *Let (A, b) be a finite paired group, let $g \geq \max\{1, d(A)\}$, and let P be a finite set of primes containing every prime dividing $2|A|$. There is a symmetric integral tridiagonal matrix C_0 of size g, such that $\mathcal{D}(C_0)_p \simeq (A_p, b_p)$ for $p \in P$ and all interior row sums of C_0 are even. The matrix may be made positive definite, with negative adjacent entries and arbitrarily large positive row sums.*

Proof. At an odd prime, a cyclic constituent $\left\langle \frac{a}{p^s} \right\rangle$ is the discriminant pairing of $[p^s/a]$ over $\mathbb{Z}_p$. Their orthogonal sum, followed by $g - d(A_p)$ unit lines, has rank g. At two, the cyclic and even binary decomposition [39, 30] gives blocks $2^s U$, $s \geq 1$, where U is symmetric and unimodular over $\mathbb{Z}_2$, of size one or two. Every entry of their block sum B_2 is even; the matrix is tridiagonal of rank $d(A_2)$. Prepend $J_{g-d(A_2)}$ when $g > d(A_2)$. Lemma 7.1 gives even interior row sums and the same two-primary discriminant pairing.

For $p \in P$, let p^{e_p} be the exponent of A_p, with $e_p = 0$ when $A_p = 0$. Approximate these tridiagonal local matrices entrywise by one integral matrix modulo

$$M = \prod_{p \in P} p^{2e_p+1}.$$

If $D = C + E$, $E \in p^{2e+1} \operatorname{Mat}(\mathbb{Z}_p)$ and $C^{-1} \in p^{-e} \operatorname{Mat}(\mathbb{Z}_p)$, put $U = I + C^{-1}E \in I + p^{e+1} \operatorname{Mat}(\mathbb{Z}_p)$. Then $U \in \mathrm{GL}_g(\mathbb{Z}_p)$, $D = CU$, and

$$D\mathbb{Z}_p^g = C\mathbb{Z}_p^g, \qquad D^{-1} - C^{-1} = -U^{-1}C^{-1}EC^{-1} \in p \operatorname{Mat}(\mathbb{Z}_p).$$

The identity on this common cokernel preserves the entire bilinear pairing.

Since M is even, the interior row parities are retained. Choose the adjacent entries negative in their residue classes. Increase each diagonal by a sufficiently large positive multiple of M. This gives strict diagonal dominance and the desired lower bounds on row sums without changing any congruence. □

7.2. **Length-preserving involutions on prime-complement graphs.** The graph Q_g is the ladder of Lemma 6.1.

Lemma 7.3. *Let $g \geq 2$, and let C be a $g \times g$ tridiagonal matrix with adjacent entries $-c_i < 0$ and positive row sums s_i. Suppose the interior row sums are even. Give rung i length c_i, give the two end edges lengths s_1, s_g, and give both rails bordering face i length $s_i/2$ for $2 \leq i \leq g-1$. Then the integral facial-cycle basis has Gram matrix C.*

The involution $\iota : u_i \leftrightarrow v_i$ is length preserving, acts as $-I$ on integral homology, and has tree quotient. It has exactly $g + 1$ fixed metric points. If every replacement length is at least $h \geq 2$, the unit-edge subdivision is simple, planar, biconnected, subcubic, of treewidth at most two and girth at least $2h$.

Proof. Adjacent facial cycles meet in the rung of length c_i, with opposite orientations. A facial cycle has squared length $s_i + c_{i-1} + c_i$. Nonadjacent faces have no common edge. The facial cycles are an integral basis: the rungs and one rail form a spanning tree of Q_g, and the complementary edges have diagonal ± 1 coordinates in the displayed cycles.

Reflection reverses every oriented facial cycle. The quotient consists of a path on $g-1$ vertices, with $g+1$ pendant edges ending at the midpoints of the $g-1$ rungs and the two end edges. These are its only fixed points. On a reversed path of length n, the subdivision vertices numbered $j = 0, \dots, n$ are sent to those numbered $n - j$. For odd n, the central unit edge is reversed and its midpoint is the fixed metric point. The paired rails have equal lengths and are interchanged. Thus the same reflection is an automorphism of the unit-edge subdivision for either parity of n.

The graph is a subdivision of the planar bridgeless cubic ladder. Distinct replacement paths have disjoint interiors, and their lengths are at least two, so the graph is simple. If a vertex separated two components, bridgelessness would require at least two incident edges into each component, contrary to its degree at most three. Every cycle contains at least two core edges and hence at least $2h$ unit edges. The width-two tree decomposition and its extension across subdivided edges are given in Lemma 6.1. □

Theorem 7.4. *Fix a finite paired group (A, b), a rank $g \geq \max\{2, d(A)\}$, a finite avoidance set, and a lower bound for every core edge length. There are positive coprime integers u, v, an integer $\kappa > 0$, and symmetric positive tridiagonal matrices C_t such that*

$$\mathcal{D}(C_t) \simeq (A, b) \perp \left\langle \tfrac{\kappa}{u+vt} \right\rangle, \qquad \gcd(u + vt, 2|A|\kappa) = 1 \quad (t \geq 0).$$

They are the flow Gram matrices of the symmetric ladders in Lemma 7.3. Only the right end length varies. Infinitely many $u + vt$ are prime and avoid the prescribed set.

Proof. Put $N = |A|$, and let P contain the prime divisors of $2N$ and the avoidance set. Lemma 7.2 gives local tridiagonal presentations of rank g with even interior row sums at two. Proposition 6.3, in its first form, gives $\det C_t = N(u + vt)$, $\kappa = NF > 0$, and the displayed orthogonal decomposition. Its congruences preserve every interior row parity; only the last diagonal increases. Choose all adjacent weights and end row sums at least the prescribed length bound, and every interior row sum at least twice that bound. Lemma 7.3 then realizes each C_t by symmetric integral lengths. The relation $(u, v) = 1$ and Dirichlet's theorem give infinitely many prime values of $u + vt$; their coprimality to every prime in P gives the avoidance condition. □

8. Prescribed monodromy of hyperelliptic Jacobians

Let K be a nonarchimedean local field of characteristic zero, with ring of integers R, uniformizer π, residue field k, and $v_K(\pi) = 1$. For a semistable Jacobian J/K, the principal polarization identifies its positive monodromy form with a symmetric integral form q on the toric character lattice X. The geometric component group is the cokernel of the adjoint map $X \to X^\vee$. Define its positive finite pairing by

$$(\Phi_J(\bar{k}), \lambda_J^+) \simeq \mathcal{D}(q), \qquad \lambda_J^+([x], [y]) = x^{\mathsf{T}} q^{-1} y \bmod \mathbb{Z}. \tag{8.1}$$

For a regular semistable curve, q is the length form on the integral homology of its dual graph. A stable node $xy = u\pi^n$, with $u \in R^\times$, contributes an edge of length n; see [13, §2.1–2.2, equations (2.8)–(2.13)].

For comparison, the positive-Laplacian graph convention gives

$$(\mathrm{Jac}(\Gamma), b_\Gamma) \simeq -\mathcal{D}(C) \tag{8.2}$$

when C is a flow Gram matrix. Thus, for the same length graph, the graph pairing is the negative of the positive monodromy discriminant pairing.

Example 8.1 (The one-cycle sign). For a split Tate degeneration with parameter of valuation n, the monodromy map on its rank-one character lattice is $[n]$. The positive finite convention is therefore $\mathcal{D}([n]) = \left\langle \frac{1}{n} \right\rangle$. The unit-edge cycle of length n has graph pairing $\left\langle \frac{-1}{n} \right\rangle$. Thus the two signs already differ in toric rank one.

8.1. **Lifting over the prescribed valuation ring.** Let K'/K be a finite extension of ramification index e. A split node $xy = u\pi^n$ over K has thickness en over K'; hence its monodromy matrix changes from Q to eQ. The construction below is defined over the original valuation ring.

Lemma 8.2. *Let K be a nonarchimedean local field of characteristic zero and odd residue characteristic, with ring of integers R, residue field k and uniformizer π. Give Q_g, $g \geq 2$, positive integral lengths, equal on the two rails in each pair. There is a stable curve $\mathcal{X}/R$ with smooth generic fibre X/K such that:*

(1) its special fibre has dual graph Q_g, every component is $\mathbb{P}^1_k$, and every node and branch is k-rational;
(2) its node corresponding to an edge of length n has completed local smoothing equation $xy = u\pi^n$, with $u \in R^\times$;
(3) the reflection lifts to an involution ι_X of X, whose quotient is $\mathbb{P}^1_K$;
(4) X has a K-rational non-Weierstrass point and is hyperelliptic of genus g.

No base-field extension is made.

Proof. For each vertex w of Q_g take a component $P_w \cong \mathbb{P}^1_k$. Mark its three incident branches by $0, 1, \infty$, with equal labels on reflected components, and identify the marked points specified by each edge. This produces a connected stable nodal curve X_0/k with normalization $\nu : \coprod_w P_w \to X_0$. The reflection induces an automorphism σ_0 of order two. It interchanges the components, interchanges paired rail nodes, and interchanges the two branches at each fixed node. The same identifications of marked sections of $\mathbb{P}^1_R$ give an R-model with all nodes unsmoothed and with the same automorphism.

Put $\mathcal{T}^0 = \mathcal{H}om(\Omega_{X_0/k}, \mathcal{O}_{X_0})$, and let D_w be the three marked points on P_w. At a node, with local ring $A = k[[x, y]]/(xy)$, a derivation has the form $xf(x)\partial_x + yh(y)\partial_y$. Thus

$$\mathcal{T}^0 = \nu_* \bigoplus_w T_{P_w}(-D_w), \qquad T_{P_w}(-D_w) \cong \mathcal{O}_{\mathbb{P}^1_k}(-1), \qquad H^0(\mathcal{T}^0) = H^1(\mathcal{T}^0) = 0.$$

At the same node the exact sequence

$$0 \longrightarrow A \xrightarrow{c \mapsto (cy, cx)} A^2 \longrightarrow \Omega_{A/k} \longrightarrow 0$$

gives $\mathrm{Ext}^1_A(\Omega_{A/k}, A) = A/(x, y) = k$ and $\mathrm{Ext}^2_A(\Omega_{A/k}, A) = 0$. Its first arrow is injective: $cx = cy = 0$ implies $c \in (x) \cap (y) = 0$. The local-to-global Ext sequence therefore gives

$$\mathrm{Ext}^0(\Omega_{X_0/k}, \mathcal{O}_{X_0}) = 0, \qquad \mathrm{Ext}^1(\Omega_{X_0/k}, \mathcal{O}_{X_0}) \cong \bigoplus_{e \in E(Q_g)} k, \qquad \mathrm{Ext}^2(\Omega_{X_0/k}, \mathcal{O}_{X_0}) = 0.$$

Here the sheaf of local first-order deformations is supported at the nodes, so its first cohomology vanishes; coherent second cohomology vanishes on the curve.

Consider deformations over Artinian local R-algebras with residue field k, together with an identification of their special fibre with X_0. The deformation theorem for stable curves [16, Section 1] and the displayed Ext groups identify the representing complete local ring with

$$B = R[[t_e : e \in E(Q_g)]].$$

Here $|E(Q_g)| = 3g - 3$. The vanishing of Ext^0 implies that an isomorphism inducing the identity on the special fibre, when it exists, is unique; induction through square-zero extensions gives this statement over every Artinian base. $\mathrm{Ext}^2 = 0$ removes obstructions, and the isomorphism for Ext^1 makes the node deformations independent. The completed local equation at node e is $xy = t_e$ after a choice of local coordinates. In particular its unsmoothed locus has principal ideal (t_e). The unsmoothed R-model above determines the section $t_e = 0$ for every e. Smoothness of the stable-curve stack over $\mathrm{Spec}\,\mathbb{Z}$ is also [38, Tag 0E9C].

Changing the identification of the special fibre by σ_0 induces an R-automorphism σ of B and a compatible isomorphism of the universal formal family. Uniqueness of isomorphisms reducing to the identity implies $\sigma^2 = 1$ on the base and on the family. The ideals (t_e) are permuted according

to the action on edges. At a fixed node, the local deformation $xy = t_e$ and the branch interchange $(x, y) \mapsto (y, x)$ show that the tangent action on t_e is $+1$. Consequently $\sigma(t_e) = u_e t_e$, where $u_e \in B^\times$ and $u_e \equiv 1 \pmod{\mathfrak{m}_B}$. Replacing t_e by

$$\frac{t_e + \sigma(t_e)}{2}$$

multiplies it by the unit $(1 + u_e)/2$ and gives an invariant generator of the same ideal. For a pair $e \neq \sigma_0(e)$ choose one generator and define the other as its transform. The new parameters have independent relative linear terms, and hence again identify B with a formal power series ring over R. They satisfy $\sigma(t_e) = t_{\sigma_0(e)}$ exactly.

The fixed locus of this action is defined by the ideal

$$I = (t_e - t_{\sigma_0(e)} \,:\, e \in E(Q_g)), \qquad B/I \cong R[[t_{\mathcal{O}} \,:\, \mathcal{O} \in E(Q_g)/\langle\sigma_0\rangle]].$$

The given lengths satisfy $n_e = n_{\sigma_0(e)}$. The continuous map $B/I \to R$ sending $t_{\mathcal{O}}$ to π^{n_e} pulls the universal family back to a proper formal stable curve over R, with an involution and completed node equations $xy = u'_e \pi^{n_e}$, $u'_e \in R^\times$. The image π^{n_e} is invariant also when n_e is odd.

The relative dualizing sheaf is invertible and ample on the special fibre. Its third power is very ample on a stable curve. The formal curve with this relatively ample sheaf algebraizes to a projective R-curve by the polarized Grothendieck existence theorem in [16, Section 1]. Applying full faithfulness to the formal graph of the automorphism algebraizes the involution; its square is the identity because this holds after completion. The nonsmooth locus of a nodal deformation lies over $\bigcup_e V(t_e)$. Since each image π^{n_e} is nonzero in K, the generic fibre X/K is smooth. The normalization sequence on X_0 gives

$$0 \longrightarrow k \longrightarrow k^{V(Q_g)} \longrightarrow k^{E(Q_g)} \longrightarrow H^1(X_0, \mathcal{O}_{X_0}) \longrightarrow 0.$$

Thus its genus is $|E(Q_g)| - |V(Q_g)| + 1 = g$.

Let $M = H^1(\mathcal{X}, \mathcal{O}_{\mathcal{X}})$. Cohomology and base change for this proper flat family of connected nodal curves makes M free of rank g and identifies $M/\pi M$ with $H^1(X_0, \mathcal{O}_{X_0}) \cong H^1(Q_g, k)$. The reflection is -1 on this latter space by Lemma 7.3. Since $2 \in R^\times$, $M^+ = (1 + \sigma)M/2$ is a direct summand of M with $M^+/\pi M^+ = 0$. Nakayama's lemma gives $M^+ = 0$. For the smooth projective quotient $Y = X/\langle\sigma\rangle$, finiteness of $X \to Y$ and the averaging idempotent give

$$H^1(Y, \mathcal{O}_Y) = H^1(X, \mathcal{O}_X)^\sigma = 0.$$

Hence Y has genus zero.

There are $|k| + 1 - 3 = |k| - 2 \geq 1$ rational points of each P_w outside its marked points; this includes $k = \mathbb{F}_3$, where the remaining point is -1. At such a point $\mathcal{X} \to \operatorname{Spec} R$ is smooth. Hensel's lemma gives an R-section, with generic point $P \in X(K)$. Its transform specializes to the distinct component $P_{\sigma_0(w)}$, so $P \neq \sigma(P)$. Its image is a rational point $y_0 \in Y(K)$. Riemann–Roch gives $\dim_K H^0(Y, \mathcal{O}_Y(y_0)) = 2$; a nonconstant section defines a map $Y \to \mathbb{P}^1_K$ of degree one: a nonconstant section has a pole, and its pole divisor is bounded by y_0. Thus $Y \cong \mathbb{P}^1_K$. The degree-two map $X \to Y$ is hyperelliptic and P is not a Weierstrass point. Riemann–Hurwitz gives $2g + 2$ geometric branch points. All constructions have taken place over R and K. □

Hyperelliptic lifting for metrized complexes is treated in [1, Section 4]. The construction in Lemma 8.2 is over R itself, so its node thicknesses are the prescribed integers n_e.

Corollary 8.3. *Let K have odd residue characteristic, let (A, b) be any finite paired group, and let $g \geq \max\{2, d(A)\}$. There are infinitely many primes ℓ and hyperelliptic curves X_ℓ/K of genus g with split totally degenerate reduction and*

$$(\Phi_{\operatorname{Jac} X_\ell}(\bar{k}), \lambda^+) \simeq (A, b) \perp \left\langle \tfrac{\kappa}{\ell} \right\rangle.$$

The positive integer κ is fixed, and the primes have the avoidance and progression properties of Theorem 7.4.

Proof. For every prime value $\ell = u + vt$ in Theorem 7.4, Lemma 8.2 lifts the corresponding symmetric ladder over R. Resolving $xy = u\pi^n$ inserts $n-1$ rational components and replaces its dual edge by a chain of n unit edges. Integral flows have constant coefficients along that chain, so the flow lattice and its length form remain C_t. Equation (8.1) therefore gives the displayed pairing. Every component, node, branch and resolution chain is split, so Frobenius is the identity on the graph, its integral homology and its discriminant group. □

9. Global arithmetic with fixed local pairings

9.1. **Global approximation and absolute simplicity.**

Lemma 9.1. *Each local curve in Corollary 8.3 has a model*

$$y^2 = f_v(x), \qquad f_v \in \mathcal{O}_{F_v}[x]$$

with f_v monic, squarefree, and of degree $2g+2$. A sufficiently small coefficient neighborhood of f_v, within monic polynomials of that degree, preserves its split regular reduction graph and therefore its full component pairing.

Proof. Put $K = F_v$ and $R = \mathcal{O}_{F_v}$. The non-Weierstrass point of Lemma 8.2 and its distinct involutive image are both K-rational. Send their common image in the quotient to infinity. A squarefree equation then has degree $n = 2g+2$ and square leading coefficient, so a rescaling of y makes it monic. If $f = x^n + \sum_{i<n} a_i x^i$, the substitution $x = \pi^{-m}X$, $y = \pi^{-(g+1)m}Y$ gives

$$Y^2 = X^n + \sum_{i<n} a_i \pi^{m(n-i)} X^i.$$

All coefficients are integral for sufficiently large m.

Let $\alpha_1, \dots, \alpha_n$ be the roots of this integral monic polynomial f in a splitting field L/K, and extend v_K to L. All roots are integral. Set

$$a = \max_i v_K(f'(\alpha_i)) = \max_i \sum_{j\neq i} v_K(\alpha_i - \alpha_j), \qquad N \in \mathbb{Z}, \quad N > 2a.$$

Each root-difference valuation is nonnegative and at most a. For a monic $h \in R[x]$ of degree n satisfying $h \equiv f \pmod{\pi^N}$, one has

$$v_K(h(\alpha_i)) \geq N, \qquad v_K(h'(\alpha_i)) = v_K(f'(\alpha_i)) \leq a.$$

Hensel's lemma over L produces a root β_i of h with

$$v_K(\beta_i - \alpha_i) \geq N - v_K(f'(\alpha_i)) > a.$$

The balls $v_K(x - \alpha_i) > a$ are disjoint. Hence the β_i are distinct and comprise every root of h. The unique root in each ball makes $\alpha_i \mapsto \beta_i$ Galois-equivariant, and

$$\frac{\beta_i - \beta_j}{\alpha_i - \alpha_j} \equiv 1 \pmod{\mathfrak{m}_L} \qquad (i \neq j).$$

These are the root-matching hypotheses of [13, Theorem 19.1]; the leading coefficients are both one. That theorem gives semistability of $y^2 = h(x)$ and an isomorphism of minimal regular special fibres over the maximal unramified extension, compatible with Frobenius. In particular, the split dual graphs with unit lengths are isomorphic. Their homology lattices, length forms and discriminant pairings are therefore isometric. Contracting the rational components of valence two also preserves the stable graph and every node thickness. □

Lemma 9.2. *Fix a number field F, an integer $n \geq 5$, and finitely many nonempty coefficient neighborhoods of monic squarefree degree-n polynomials at finite places. There is a monic $f \in \mathcal{O}_F[x]$ in all those neighborhoods if the specified local coefficients are integral. It may be required to have* $\mathrm{Gal}(f/F) = S_n$.

Proof. Replace each neighborhood by finitely many congruence conditions. Choose three further prime ideals of sufficiently large residue-field size. At them prescribe squarefree factorizations of types

$$(n), \qquad (n-1,1), \qquad (2,1,\dots,1).$$

Over a sufficiently large residue field there is an irreducible polynomial of each indicated degree and enough distinct linear factors. Their products give the three prescribed squarefree reductions. The Chinese remainder theorem gives a monic $f \in \mathcal{O}_F[x]$ with these reductions. If $f = gh$ in $F[x]$ with monic factors of positive degree, the coefficients of g, h are integral over $\mathcal{O}_F$, being symmetric polynomials in integral roots of f. Since $\mathcal{O}_F$ is integrally closed, $g, h \in \mathcal{O}_F[x]$. Their reductions remain monic of the same positive degrees, contrary to the irreducible reduction. Thus f is irreducible over F. At each auxiliary prime its discriminant is a unit. The Frobenius permutation of its roots has cycle lengths equal to the degrees of the distinct irreducible residue factors.

Let $G \le S_n$ be its transitive Galois group. An $(n-1)$-cycle shows that G is primitive. Indeed, the block containing its fixed point is invariant under that cycle; if it contains any other point, it contains all the other points and is the whole set. A primitive group containing a transposition is S_n: the graph whose edges are the conjugates of that transposition has components forming a block system, so is connected, and the transpositions along a connected graph generate S_n. □

Theorem 9.3 (Hyperelliptic Jacobians with prescribed monodromy). *Let F be a number field, let S be a finite nonempty set of nonarchimedean places of odd residue characteristic, and prescribe a finite paired group (A_v, b_v) for every $v \in S$. Let*

$$g \ge \max\{2, \max_{v\in S} d(A_v)\}.$$

At each v, also prescribe a finite set of rational primes to be avoided. Then there are integers $\kappa_v > 0$ and infinite sets of primes $\mathcal{P}_v$ with the following property. Every tuple $(\ell_v)_{v\in S} \in \prod_v \mathcal{P}_v$ is realized by a smooth projective hyperelliptic curve C/F of genus g, with two F-rational points and

$$\boxed{(\Phi_{\mathrm{Jac}\,C,v}(\bar{k}_v), \lambda^+_{C,v}) \simeq (A_v, b_v) \perp \left\langle \tfrac{\kappa_v}{\ell_v} \right\rangle} \qquad (v \in S). \tag{9.1}$$

The following additional properties hold.

1. *The curve has split stable reduction at every $v \in S$, with every component rational and dual stable graph the same trivalent ladder Q_g. Its node thicknesses are positive integers, and the associated regular-model graph can be required to be simple, planar, biconnected, subcubic, and of any prescribed lower girth. No extension of F_v is required.*
2. *The Jacobian satisfies $\mathrm{End}_{\bar{F}}(\mathrm{Jac}\,C) = \mathbb{Z}$, and hence is absolutely simple.*
3. *Each ℓ_v is coprime to $2|A_v|\kappa_v$ and avoids the prescribed finite set. Each $\mathcal{P}_v$ consists of the primes in a fixed primitive arithmetic progression, apart from finitely many initial terms. The number κ_v is independent of the tuple.*

The geometric component group is split, so the local Tamagawa number is $|A_v|\ell_v$. If $D = \max_v d(A_v) \ge 2$, one may take $g = D$; this dimension is minimal among all semistable Jacobians whose geometric component groups contain the prescribed A_v as quotients. Varying the complementary primes gives infinitely many F-isomorphism classes of curves.

Proof of Theorem 9.3. At each v, Theorem 7.4 fixes κ_v and a primitive progression of complementary primes, with the specified avoidance and length lower bounds. For any tuple of these primes, Corollary 8.3 gives local curves and Lemma 9.1 gives integral monic coefficient neighborhoods. Lemma 9.2, with $n = 2g+2$, gives a polynomial in their intersection with Galois group S_n. Its smooth projective double cover has genus g by Riemann–Hurwitz. In the chart $t = 1/x$, $z = y/x^{g+1}$, the two points above infinity are $(t,z) = (0, \pm 1)$. The preserved regular special fibres give the pairings (9.1); contraction of their valence-two components gives the stable ladder and its original thicknesses.

Zarhin's theorem [41, Theorem 2.1] applies because F has characteristic zero, $n = 2g+2 \ge 6$, and the polynomial Galois group is S_n. Thus $\mathrm{End}_{\bar{F}}(J) = \mathbb{Z}$. If J had a nonzero proper abelian subvariety

over $\bar{F}$, Poincaré reducibility would give a nontrivial isogeny decomposition and hence an idempotent other than $0, 1$ in $\mathrm{End}_{\bar{F}}(J) \otimes \mathbb{Q} = \mathbb{Q}$, a contradiction.

For any semistable abelian variety, the geometric component group is presented by a monodromy map between lattices of rank equal to its toric rank. Thus

$$d(A_v) \leq d(\Phi_{J,v}) \leq \mathrm{toricrank}_v(J) \leq \dim J$$

whenever A_v is a quotient. Taking the maximum over v proves minimality when $g = D \geq 2$. The split condition gives $\#\Phi_{J,v}(k_v) = |A_v|\ell_v$. Varying a selected prime at one place varies this invariant, proving infinitely many isomorphism classes. □

9.2. **The maximal adelic group**. Fix a number field F, an integer $g \geq 2$, and $n = 2g + 2$. For $\mathbf{a} = (a_0, \dots, a_{n-1}) \in \mathcal{O}_F^n$, put

$$f_{\mathbf{a}}(x) = x^n + \sum_{i=0}^{n-1} a_i x^i.$$

When $\mathrm{disc}(f_{\mathbf{a}}) \neq 0$, let $C_{\mathbf{a}}$ be the smooth projective model of $y^2 = f_{\mathbf{a}}(x)$, and set $J_{\mathbf{a}} = \mathrm{Jac}(C_{\mathbf{a}})$. Let $G_F = \mathrm{Gal}(\bar{F}/F)$ and let $\chi_F : G_F \to \widehat{\mathbb{Z}}^\times$ be the cyclotomic character. The canonical principal polarization gives

$$\rho_{\mathbf{a}} : G_F \longrightarrow \mathrm{GSp}_{2g}(\widehat{\mathbb{Z}}), \qquad \mathrm{mult} \circ \rho_{\mathbf{a}} = \chi_F.$$

The branch-divisor description of $J_{\mathbf{a}}[2]$ [27, Section 3.3] identifies the branch permutation action with the representation of S_n on

$$V = \{(x_1, \dots, x_n) \in \mathbb{F}_2^n : \textstyle\sum_i x_i = 0\}/\langle(1, \dots, 1)\rangle. \tag{9.2}$$

Let $W = \{x \in \mathbb{F}_2^n : \sum_i x_i = 0\}$. Its orthogonal complement for the dot product is $\langle \mathbf{1} \rangle \subset W$. Also $x \cdot x = \sum_i x_i = 0$ for $x \in W$. Hence the quotient V is symplectic of dimension $n - 2 = 2g$. The permutation representation on V is faithful. Indeed, if σ acts trivially, then

$$e_{\sigma(i)} + e_{\sigma(j)} - e_i - e_j \in \{0, \mathbf{1}\} \quad (i \neq j).$$

The left side has support of size at most four, whereas $n \geq 6$; therefore it is zero. Thus σ fixes every two-element subset and consequently every element of $\{1, \dots, n\}$. Write $\mathfrak{S}_n$ for the resulting subgroup of $\mathrm{Sp}_{2g}(\mathbb{F}_2)$ and define

$$H_{g,F} = \{h \in \mathrm{GSp}_{2g}(\widehat{\mathbb{Z}}) : h \bmod 2 \in \mathfrak{S}_n,\ \mathrm{mult}(h) \in \chi_F(G_F)\}. \tag{9.3}$$

All groups are understood up to symplectic conjugacy. In particular, for $g \geq 3$, maximal hyperelliptic image does not mean all of $\mathrm{GSp}_{2g}(\widehat{\mathbb{Z}})$.

Proposition 9.4. *For the monic degree-$2g + 2$ family, put $\delta_F = 2$ when $F = \mathbb{Q}$ and $\delta_F = 1$ otherwise. Ordered by*

$$\|\mathbf{a}\| = \max_{i, \sigma : F \hookrightarrow \mathbb{C}} |\sigma(a_i)|,$$

a density-one subset of squarefree integral coefficient vectors satisfies

$$[H_{g,F} : \rho_{\mathbf{a}}(G_F)] = \delta_F.$$

For every $R > 0$, the proportion of exceptions is $O_{F,g,R}((\log B)^{-R})$ among vectors of norm at most B [27, Theorem 1.2, family $i = 2$].

Over $\mathbb{Q}$ the index two can be described exactly. Assume $\mathrm{Gal}(f_{\mathbf{a}}/\mathbb{Q}) = S_n$, let $D_{\mathbf{a}}$ be the fundamental discriminant of $\mathbb{Q}(\sqrt{\mathrm{disc}(f_{\mathbf{a}})})$, and let $\chi_{D_{\mathbf{a}}}$ be its quadratic Dirichlet character. Let ϵ denote sign on $\mathfrak{S}_n$.

Proposition 9.5. *The image is contained in the index-two subgroup*

$$H_{\mathbf{a}}^{\max} = \{h \in H_{g,\mathbb{Q}} \,:\, \epsilon(h \bmod 2) = \chi_{D_{\mathbf{a}}}(\mathrm{mult}(h))\}. \tag{9.4}$$

If it has the maximal index of Proposition 9.4, then it equals this subgroup. In that case, for every odd positive integer m,

$$\rho_{\mathbf{a},m}(G_{\mathbb{Q}}) = \mathrm{GSp}_{2g}(\mathbb{Z}/m\mathbb{Z}). \tag{9.5}$$

Proof. If the roots are $\alpha_1, \dots, \alpha_n$, the element $\prod_{i<j}(\alpha_i - \alpha_j)$ has square $\mathrm{disc}(f_{\mathbf{a}})$ and transforms by the sign character. Kronecker–Weber identifies the resulting quadratic character with $\chi_{D_{\mathbf{a}}} \circ \chi_{\mathbb{Q}}$. This proves the containment in (9.4).

A transposition (ij) on (9.2) is the symplectic transvection $x \mapsto x + \langle x, e_i + e_j\rangle(e_i + e_j)$. An integral lift of its nonzero vector defines a transvection in $\mathrm{Sp}_{2g}(\mathbb{Z}_2)$. Together with identity components at the odd primes, this gives an element of $H_{g,\mathbb{Q}}$ with multiplier one and sign -1. The character defining (9.4) is therefore nontrivial, and its kernel has index two. Equality with the Galois image follows when that image also has index two.

Let m be odd and let $h_m \in \mathrm{GSp}_{2g}(\mathbb{Z}/m\mathbb{Z})$. Each component for $r^k \| m$ lifts to $\mathrm{GSp}_{2g}(\mathbb{Z}_r)$. Indeed, lift its multiplier to a unit of $\mathbb{Z}_r$ and divide by the corresponding diagonal similitude. The resulting symplectic basis lifts inductively: lift its first vector primitively, lift its partner and divide that partner by their unit pairing, then subtract from each remaining vector its components along these two vectors. This operation preserves their prescribed reductions, and induction gives a symplectic basis over $\mathbb{Z}_r$. Choose the identity at the other odd primes. Give the two-adic component multiplier one. Its sign can be prescribed as either value, by choosing the identity or the transvection above. Choose that sign to equal $\chi_{D_{\mathbf{a}}}$ of the already fixed adelic multiplier. The resulting element lies in $H_{\mathbf{a}}^{\max}$ and reduces to h_m, proving (9.5). □

Since the representation (9.2) is faithful for $n \geq 6$, a maximal-image member over $\mathbb{Q}$ has index

$$2[\mathrm{Sp}_{2g}(\mathbb{F}_2) \,:\, \mathfrak{S}_n] = \frac{2^{g^2+1}\prod_{i=1}^{g}(2^{2i}-1)}{(2g+2)!}.$$

It is 2 in genus two and 72 in genus three.

9.3. **Galois representations in coefficient congruence classes.**

Theorem 9.6. *Let S be a finite set of finite places of F. For every $v \in S$, prescribe a nonempty open coefficient neighborhood $\Omega_v \subset \mathcal{O}_{F_v}^n$ consisting of squarefree monic polynomials. Then there are a nonzero ideal $\mathfrak{a} \subset \mathcal{O}_F$ and a coefficient vector $\mathbf{a}_0 \in \mathcal{O}_F^n$ such that every vector in*

$$\Lambda = \mathbf{a}_0 + \mathfrak{a}^{\oplus n}$$

lies in all the neighborhoods and has the following properties:

1. *its polynomial has Galois group S_n, and $\mathrm{End}_{\bar{F}}(J_{\mathbf{a}}) = \mathbb{Z}$;*
2. *its Jacobian has split semistable toric rank one at an additional place, outside S;*
3. *for that Jacobian, the residual Galois image is $\mathrm{GSp}_{2g}(\mathbb{F}_r)$ for all sufficiently large rational primes r;*
4. *a relative density-one subset of Λ has $[H_{g,F} \,:\, \rho_{\mathbf{a}}(G_F)] = \delta_F$.*

For each $R > 0$, the exceptional proportion in (4) is $O_{\Lambda,F,g,R}((\log B)^{-R})$. The exceptional-prime bound in (3) may depend on $\mathbf{a}$.

Lemma 9.7. *There are arbitrarily many auxiliary finite places w at which a nonempty congruence condition modulo $\mathfrak{p}_w^2$ forces a split irreducible one-node stable special fibre, with toric rank one and node thickness one. It also forces inertia on the roots of the branch polynomial to be a transposition.*

Proof. Choose a rational prime $q \equiv 1 \pmod 4$, $q > 2g$, unramified in F and outside the prescribed finite set, and a place w above q. There are infinitely many such q by Dirichlet's theorem. Write $R = \mathcal{O}_{F_w}$ and choose a uniformizer π. Put

$$h(x) = \prod_{i=1}^{g}(x^2 - i^2), \qquad f_w(x) = (x^2 - \pi)h(x).$$

The reduction of h has $2g$ distinct nonzero roots, and $h(0) = (-1)^g(g!)^2$ is a square unit. Let f be monic with $f \equiv f_w \pmod{\pi^2}$. Since x^2 and $\bar{h}$ are coprime, the factorization form of Hensel's lemma gives

$$f(x) = (x^2 + Ax + B)\widetilde{h}(x), \qquad A \in \pi^2 R, \quad B \equiv -\pi \pmod{\pi^2}, \quad \widetilde{h} \equiv h \pmod{\pi^2}.$$

The congruences modulo π^2 follow from uniqueness of the monic lift of the coprime factorization. In the coordinate $X = x + A/2$, the quadratic factor is $X^2 - d$, where $d = A^2/4 - B \equiv \pi \pmod{\pi^2}$. The series $\widetilde{h}(X - A/2)$ has a unit constant term with square residue. Hensel's lemma in the complete local ring $R[[X]]$ supplies a square root. Dividing y by that root reduces the completed local equation to $y'^2 = X^2 - d$. The invertible linear change $u = X - y'$, $v = X + y'$ gives $uv = d$, with $v_w(d) = 1$.

The projective double cover is obtained by adjoining the chart $t = 1/x$, $z = y/x^{g+1}$, where $z^2 = t^{2g+2}f(1/t)$. Its two points at $t = 0$ are smooth because $2z = \pm 2$ there. The special fibre has equation $y^2 = x^2\bar{h}(x)$. Its only singular point is $(0, 0)$, and its normalization is the smooth projective curve $z^2 = \bar{h}(x)$ of genus $g - 1$. The two points above the node are rational because $\bar{h}(0)$ is a square. The normalization is connected, since the squarefree polynomial $\bar{h}$ is not a square. The resulting irreducible nodal fibre is stable for $g \geq 2$, and its dual graph has one vertex and one loop. Its toric rank is one.

The roots of $\widetilde{h}$ are unramified, being Hensel lifts of its distinct residue roots. The remaining two roots generate the ramified quadratic extension defined by $X^2 = d$, with $v_w(d) = 1$ and residue characteristic odd. Its nontrivial inertia element interchanges exactly these two roots. Equivalently,

$$\operatorname{disc}(f_w) = 4\pi \operatorname{disc}(h) \prod_{i=1}^{g}(\pi - i^2)^4$$

has valuation one; all the factors other than π are units. The same valuation follows for f from the lifted factorization. □

Proof of Theorem 9.6. Shrink each Ω_v to a coefficient congruence class. Add the condition of Lemma 9.7 at a place outside S. At three further places with sufficiently large residue fields, impose squarefree factorization patterns

$$(n), \qquad (n-1, 1), \qquad (2, 1, \dots, 1).$$

Finite fields have irreducible polynomials of each needed degree, and the fields can be chosen large enough for the distinct linear factors. Coefficientwise Chinese remaindering gives a nonempty coset Λ.

Lemma 9.2 applies to these reductions and gives $\operatorname{Gal}(f_{\mathbf{a}}/F) = S_n$ for every $\mathbf{a} \in \Lambda$. The discriminant is a unit at each of the three auxiliary places, so $f_{\mathbf{a}}$ is squarefree.

Zarhin's theorem [41, Theorem 2.1] gives (1), and Lemma 9.7 gives (2). The canonical principal polarization, geometric endomorphism ring $\mathbb{Z}$, and the semistable fibre of toric rank one satisfy Hall's hypotheses [22, Theorem 1]. Thus for each $\mathbf{a} \in \Lambda$ there is a bound $r_0(J_{\mathbf{a}}, F)$ such that (3) holds for every rational prime $r > r_0(J_{\mathbf{a}}, F)$.

Finally let $d_F = [F : \mathbb{Q}]$ and $D = nd_F$. The Minkowski embedding identifies $\mathcal{O}_F^n$ with a full lattice in $\mathbb{R}^D$. Lattice-point counting in the norm ball gives

$$\#\{\mathbf{a} \in \Lambda : \|\mathbf{a}\| \leq B\} = c_{F,n}\,\mathrm{N}(\mathfrak{a})^{-n}B^D + O_\Lambda(B^{D-1}), \qquad c_{F,n} > 0.$$

The norm ball is a product of real intervals and complex discs; its bounded piecewise smooth boundary gives the stated $O_\Lambda(B^{D-1})$ error. The index of $\mathfrak{a}^{\oplus n}$ in $\mathcal{O}_F^n$ is $\mathrm{N}(\mathfrak{a})^n$, which gives the leading constant.

The exceptional count in the whole coefficient space is $O_{F,g,R}(B^D(\log B)^{-R})$ by Proposition 9.4. Its intersection with Λ has the same upper bound. Dividing by the positive main term proves (4), with relative exceptional proportion $O_{\Lambda,F,g,R}((\log B)^{-R})$. □

Corollary 9.8. *Take the pairings and prime families of Theorem 9.3. For every* fixed *tuple of complementary primes, Theorem 9.6 gives a coefficient coset on which all the prescribed component pairings* (9.1) *occur, every Jacobian has geometric endomorphism ring $\mathbb{Z}$, and density one have the maximal admissible adelic image. The genus can be*

$$g = \max_v d(A_v)$$

when this maximum is at least two, and is minimal among semistable realizations with the indicated component-group quotients. The local reduction graphs and their thicknesses at the prescribed places remain fixed on the coset.

Proof. Apply Theorem 9.6 to the neighborhoods of Lemma 9.1, whose regular reduction graphs and discriminant pairings are constant. Choose its auxiliary places outside the prescribed set. The dimension lower bound is

$$d(A_v) \le d(\Phi_{J,v}(\bar{k}_v)) \le \operatorname{toricrank}_v(J) \le \dim J,$$

by the monodromy presentation. Theorem 9.3 gives equality when $g = \max_v d(A_v) \ge 2$. □

9.4. **Nonisogenous realizations with independent branch fields.**

Theorem 9.9 (Nonisogeny and linearly disjoint branch fields). *Fix the neighborhoods of Theorem 9.6, and optionally a finite extension E/F. There is an infinite sequence of curves satisfying those same neighborhoods and having maximal admissible adelic image such that:*

(1) their Jacobians are pairwise nonisogenous over $\bar{F}$;
(2) their branch splitting fields L_i/F, each with group S_n, are jointly linearly disjoint, and are linearly disjoint from the normal closure of E/F.

Consequently the component pairings and the complementary primes in Corollary 9.8 can be held fixed throughout this sequence.

Proof. Suppose $C_1, \dots, C_{j-1}$ satisfy the prescribed local and adelic conditions, their Jacobians are pairwise geometrically nonisogenous, and $[\widetilde{E}L_1 \cdots L_{j-1} : \widetilde{E}] = (n!)^{j-1}$. Choose a place w_j as in Lemma 9.7 at which every J_i, $i < j$, has good reduction and the finite Galois compositum

$$K_{j-1} = \widetilde{E}L_1 \cdots L_{j-1}$$

is unramified. Only finitely many places are excluded by these conditions. Add the one-node congruence at w_j to the fixed neighborhoods. Theorem 9.6 gives a coset with a positive-density subset of maximal-image members. Choose one, denoted C_j, and let L_j be its branch splitting field.

Suppose J_j and J_i, $i < j$, are isogenous over a finite extension F'/F. Choose a rational prime r different from the residue characteristic at w_j. At a place of F' above w_j, inertia acts trivially on V_rJ_i. On V_rJ_j its monodromy operator is eN, where $e \ge 1$ is the ramification index and $\operatorname{rank} N = 1$. Thus $eN \ne 0$ over $\mathbb{Q}_r$. An isogeny would induce an inertia-equivariant isomorphism $V_rJ_i \cong V_rJ_j$, a contradiction. This proves (1).

For (2), the intersection $T = L_j \cap K_{j-1}$ is Galois over F and unramified at w_j. Inertia in L_j/F contains a transposition by Lemma 9.7, and acts trivially on T. Thus $\operatorname{Gal}(L_j/T) \lhd S_n$ contains that transposition. Normality puts every transposition in this kernel, and transpositions generate S_n. Hence $T = F$. Since the two extensions are Galois,

$$[K_{j-1}L_j : K_{j-1}] = [L_j : F] = n!.$$

Induction gives $[\widetilde{E}L_1 \cdots L_j : \widetilde{E}] = (n!)^j$, which is the required joint linear disjointness. □

The faithful representation (9.2) gives $L_i = F(J_i[2])$. The full torsion fields contain $F(\mu_\infty)$ by the Weil pairing.

9.5. **Inertia invariants and the component group.** Let K be a local field with residue characteristic p, and let J/K be a principally polarized Jacobian with split totally degenerate semistable reduction of dimension g. Let M be its integral positive monodromy matrix and let $\Phi = \operatorname{coker} M$.

Proposition 9.10. *For every rational prime $r \neq p$ and every $k \geq 1$,*

$$\boxed{\#J[r^k]^{I_K} = r^{kg}\#\Phi[r^k].} \tag{9.6}$$

In particular

$$\dim_{\mathbb{F}_r} J[r]^{I_K} = g + d(\Phi_r). \tag{9.7}$$

If the Smith factors of M are $s_1, \dots, s_g$, then the right hand side of (9.6) *is $r^{kg+\sum_i \min(k, v_r(s_i))}$.*

Proof. Split toric uniformization gives an exact sequence of Tate modules

$$0 \longrightarrow \mathbb{Z}_r(1)^g \longrightarrow T_r J \longrightarrow \mathbb{Z}_r^g \longrightarrow 0.$$

Choose a module splitting. Inertia acts trivially on both outer terms and, after fixing a generator of the Tate twist, has the form

$$\rho_r(\sigma) = \begin{pmatrix} I_g & t_r(\sigma)M \\ 0 & I_g \end{pmatrix}, \qquad \sigma \in I_K.$$

Here $t_r : I_K \twoheadrightarrow \mathbb{Z}_r$ is the r-adic tame character. Every r^k-th root of a unit lies in an unramified extension after adjoining an r^k-th root of its residue, by Hensel's lemma, whereas compatible roots of π give t_r. Applying this to the period matrix in split toric uniformization gives the displayed valuation matrix M; see [13, Sections 2.2–2.3]. The principal polarization identifies the period and character lattices, so M is the integral monodromy matrix in those bases.

Modulo r^k, a vector (u, v) is invariant exactly when $Mv = 0$. There are r^{kg} choices of u. Smith normal form gives

$$\#\ker(M : (\mathbb{Z}/r^k)^g \to (\mathbb{Z}/r^k)^g) = \prod_i r^{\min(k, v_r(s_i))} = \#\Phi[r^k].$$

This proves both formulas. □

Over $\mathbb{Q}_r$, the matrix M is invertible. A change of basis in the two graded pieces therefore identifies the unpolarized rational Weil–Deligne representation with g copies of the split multiplicative two-dimensional special representation [13, Sections 2.2–2.3]. The Swan conductor is zero, the space of inertia invariants has dimension g, and Frobenius on the inertia invariants in $H^1_{\text{ét}}(J_{\bar{K}}, \mathbb{Q}_r)$ has all eigenvalues one. Hence the conductor exponent is g and $L(J/K, T) = (1 - T)^{-g}$.

For r different from the residue characteristic at v, equation (9.1) gives inertia dimension $g + d((A_v)_r)$ when $r \mid |A_v|$, dimension $g + 1$ when $r = \ell_v$, and dimension g otherwise. These integral invariants are compatible with the adelic conclusion of Corollary 9.8. In the prime families the Tamagawa number is $|A_v|\ell_v$, although the local conductor exponent stays g.

10. Fixed ambient lattices and stable nonembedding

Let Λ_{24} denote the positive Leech lattice. All four-manifolds in this section are topological and oriented; embeddings are locally flat. Freedman's existence theorem [18, Theorem 1.5] supplies a closed simply connected four-manifold X_Λ with intersection lattice Λ_{24}. Each connected sum has the given orientation on every copy. For a closed three-manifold Y, put $g_X(Y) = \inf\{n \geq 0 : Y \hookrightarrow \#^n X\}$, where the infimum of the empty set is $+\infty$ and $\#^0 X = S^4$.

Theorem 10.1. *Let Y be a closed connected oriented rational homology three-sphere with $H_1(Y) \cong \mathbb{Z}/2$. If W is a closed simply connected oriented four-manifold with intersection lattice $\Lambda_{24}^{\perp n}$ for some $n \geq 1$, then Y does not embed locally flatly in W. Consequently,*

$$\boxed{g_{X_\Lambda}(Y) = \infty, \qquad g_{X_\Lambda}(\mathbb{RP}^3) = \infty.} \tag{10.1}$$

10.1. **Homology of the complementary regions.**

Lemma 10.2. *Suppose a closed connected oriented rational homology three-sphere Y embeds locally flatly in a closed simply connected oriented four-manifold W. Write $m = |H_1(Y)|$. The complement has two connected sides, whose closures are compact oriented manifolds U, V with boundaries $Y, -Y$. For either side U, the group $H_2(U)$ is free, $H_1(U)$ is finite, and its nonsingular intersection form satisfies*

$$m = |\det Q_U|\,|H_1(U)|^2. \tag{10.2}$$

If m is squarefree, then $H_1(U) = H_1(V) = 0$ and $|\det Q_U| = |\det Q_V| = m$.

Proof. The orientations trivialize the normal line bundle, and local flatness gives a bicollar of Y. If the complement were connected, a path in it joining the two sides of a short transverse arc would close that arc to a one-cycle with algebraic intersection one with Y. This contradicts $H_1(W;\mathbb{Z}) = 0$. Every component of the complement meets a side of the bicollar, since W is connected. Each side of that bicollar is connected because Y is connected. Thus the complement has exactly two components, with closures U, V, and $W = U \cup_Y V$.

All homology groups in this proof have integral coefficients. Poincaré duality on Y gives $H_2(Y) = H^1(Y) = \mathrm{Hom}(H_1(Y), \mathbb{Z}) = 0$. Mayer–Vietoris contains

$$0 \longrightarrow H_2(U) \oplus H_2(V) \longrightarrow H_2(W) \longrightarrow H_1(Y) \longrightarrow H_1(U) \oplus H_1(V) \longrightarrow 0. \tag{10.3}$$

Poincaré duality and universal coefficients identify $H_2(W)$ with $H^2(W) = \mathrm{Hom}(H_2(W), \mathbb{Z})$, since $H_1(W) = 0$. Hence $H_2(W)$ and its subgroups $H_2(U), H_2(V)$ are free. The surjection from $H_1(Y)$ makes $H_1(U)$ and $H_1(V)$ finite. The rational pair sequence gives $H_2(U;\mathbb{Q}) \cong H_2(U, Y;\mathbb{Q})$, and duality identifies this map with the adjoint of the intersection form. Thus Q_U is nonsingular, and the same argument applies to V.

Write $t = |H_1(U)|$. The boundary map $H_4(U, Y) \to H_3(Y)$ sends the relative orientation class to the orientation class of the connected boundary and is an isomorphism. Poincaré–Lefschetz duality gives $H_3(U, Y) \cong H^1(U) = 0$, whence $H_3(U) = 0$. Since $H_2(U)$ is free, the universal coefficient theorem now gives $H^3(U) = 0$, and therefore $H_1(U, Y) = 0$.

The pair sequence reduces to

$$0 \longrightarrow H_2(U) \xrightarrow{j} H_2(U, Y) \longrightarrow H_1(Y) \longrightarrow H_1(U) \longrightarrow 0. \tag{10.4}$$

By duality and universal coefficients, the middle group has torsion subgroup of order t, and its torsion-free quotient is $H_2(U)^*$. The map induced by j on that quotient is the adjoint of Q_U. It is injective because Q_U is nonsingular, so $j(H_2(U))$ meets the torsion subgroup trivially. Thus

$$|\operatorname{coker} j| = t\,|\det Q_U|.$$

Equation (10.4) also gives $|\operatorname{coker} j| = m/t$. This proves (10.2). If m is squarefree, the divisibility $t^2 \mid m$ forces $t = 1$, for each side. □

Linking-form presentations by bounded four-manifolds are treated in [17, Section 2].

Corollary 10.3. *In Lemma 10.2, assume $H_1(Y) \cong \mathbb{Z}/2$ and that the intersection lattice L of W is even and positive definite. Then the images of the side lattices give an orthogonal full-rank sublattice*

$$K = K_U \perp K_V \subset L,$$

with

$$\det K_U = \det K_V = 2, \qquad L/K \cong \mathbb{Z}/2. \tag{10.5}$$

In particular $2L \subset K$.

Proof. Both side forms are restrictions of the ambient intersection form, and are therefore even and positive definite. Their images are orthogonal: representatives supported on the two sides can be moved into the disjoint interiors. Their ranks sum to rank L by rational Mayer–Vietoris. Lemma 10.2 gives $\det K_U = \det K_V = 2$ and $H_1(U) = H_1(V) = 0$. Equation (10.3) then gives the cokernel $\mathbb{Z}/2$. □

10.2. **The integral sign-change obstruction.**

Lemma 10.4. *An even nonsingular integral lattice of determinant of absolute value two has odd rank.*

Proof. If its rank is r, the Smith factors of a Gram matrix consist of $r-1$ ones and one two. Consequently its reduction modulo two has rank $r-1$. Its diagonal vanishes modulo two, so the reduced symmetric form is alternating. An alternating bilinear form has even rank. Therefore $r-1$ is even. □

Theorem 10.5 (An involution obstruction to locally flat embeddings). *If a closed simply connected oriented four-manifold W has even positive definite intersection lattice L, and contains a locally flat oriented rational homology three-sphere Y with $H_1(Y) \cong \mathbb{Z}/2$, then $O(L)$ contains an involution of determinant -1.*

Proof. Corollary 10.3 gives $K_U \perp K_V \subset L$ with $2L \subset K_U \perp K_V$. Lemma 2.2 therefore extends the rational sign change $+1$ on $K_U \otimes \mathbb{Q}$ and -1 on $K_V \otimes \mathbb{Q}$ to an involution $s \in O(L)$. By Lemma 10.4, the rank of K_V is odd, so $\det s = (-1)^{\operatorname{rank} K_V} = -1$. □

10.3. **Orthogonal powers of the Leech lattice.** The Leech lattice is even, positive, unimodular, of rank twenty-four, and has no vector of norm two. A positive even unimodular lattice has rank divisible by eight; in rank eight it is isometric to E_8 [11].

Lemma 10.6. *The Leech lattice is orthogonally indecomposable. Every isometry of $\Lambda_{24}^{\perp n}$ permutes its n Leech summands.*

Proof. In an orthogonal decomposition $L = L_1 \perp L_2$ of a positive integral unimodular lattice, $1 = \det L = (\det L_1)(\det L_2)$ forces both positive integral determinants to be one. If Λ_{24} decomposed nontrivially, its even unimodular summands would have positive ranks divisible by eight and summing to twenty-four. One summand would have rank eight and hence be E_8, contrary to the absence of roots in Λ_{24}.

For any positive integral lattice L, call a nonzero vector orthogonally irreducible if it is not a sum of two nonzero orthogonal lattice vectors. Splitting a reducible vector decreases the positive integral norm of each summand. Induction on the norm therefore expresses every vector as a sum of orthogonally irreducible vectors. Form a graph on these vectors, with an edge when their inner product is nonzero. For each connected component D let L_D be its integral span. Distinct L_D are orthogonal, and the preceding induction gives $L = \bigoplus_D L_D$. Only finitely many L_D are nonzero because their ranks sum to $\operatorname{rank} L$.

In any orthogonal decomposition of L, an orthogonally irreducible vector lies in a single summand: its projections are orthogonal lattice vectors. A path of nonzero inner products stays in that summand. Thus every L_D lies in one summand. Each L_D is itself indecomposable by the same argument, since its graph is connected and its vertices span it. Consequently the L_D are precisely the summands in any decomposition into indecomposable lattices. Isometries permute them. Applied to $L = \Lambda_{24}^{\perp n}$, they permute the given Leech summands. □

Lemma 10.7. *If $\sigma \in O(\Lambda_{24})$ and $\sigma^2 = \mathrm{id}$, then the negative eigenspace of σ has dimension*

$$0,\ 8,\ 12,\ 16,\ \text{or } 24. \tag{10.6}$$

In particular $\det \sigma = 1$.

Proof. For $\sigma \neq \mathrm{id}$, Conway's classification [11, Chapter 10, Section 3.7] gives four conjugacy classes of linear involutions, with representatives having negative eigenspace dimensions $8, 12, 16, 24$; the last is $-\mathrm{id}$. This is also [36, Theorem 3.3]. The identity has negative dimension zero. Since $\sigma^2 = 1$, the minimal polynomial over $\mathbb{Q}$ divides $(T-1)(T+1)$, so its determinant is $(-1)^{\dim V_-} = 1$ in all five cases. □

Proposition 10.8. *For every $n \geq 1$, every involution of $\Lambda_{24}^{\perp n}$ has determinant $+1$.*

Proof. By Lemma 10.6, the induced permutation of the Leech summands consists of fixed summands and exchanged pairs. On a fixed summand, the negative eigenspace has even dimension by Lemma 10.7. On an exchanged pair, the involution has the form

$$(x, y) \longmapsto (f(y), f^{-1}(x))$$

for an isometry f between the two summands. Its negative eigenspace is $\{(x, -f^{-1}(x)) : x \in \Lambda_{24} \otimes \mathbb{Q}\}$, of dimension twenty-four. The total negative dimension is therefore even, so the determinant is one. □

Proof of Theorem 10.1. A hypothetical embedding in W would produce a determinant-minus-one involution of $\Lambda_{24}^{\perp n}$ by Theorem 10.5. Proposition 10.8 excludes it. Freedman's theorem supplies X_Λ, and the intersection form of $\#^n X_\Lambda$ is $\Lambda_{24}^{\perp n}$. Hence no positive n works. Nor does $n = 0$: in S^4, the injection in (10.3) makes $H_2(U) = 0$, whose determinant is one, contradicting (10.2) with $m = 2$. This proves (10.1). □

Remark 10.9. Conjecture 1.3 in the 21 December 2001 preprint [17] proposes $g_X(Y) < \infty$ for every simply connected X and every homology lens space Y. For $X = S^4$, equation (10.2) excludes an embedding of a rational homology sphere of order two. The following paragraph of that preprint isolates definite indecomposable forms as the remaining case. Theorem 10.1 concerns a nonzero positive definite indecomposable form and excludes every orthogonal power of it. The connected sums in $g_X(Y)$ contain copies of X with the same orientation. The intersection forms of $X_\Lambda \# (-X_\Lambda)$ and $X_\Lambda \# (S^2 \times S^2)$ are indefinite; neither is an orthogonal power of the positive Leech lattice.

11. Further realization questions

There is a positive integral lattice K of rank four with $-\mathcal{D}(K) \cong \left\langle \frac{1}{8} \right\rangle$ (Remark B.5), whereas $\mu(\left\langle \frac{1}{8} \right\rangle) = 7$. Thus the minimum rank of a positive integral lattice with negative discriminant (A, b) can be strictly smaller than $\mu(A, b)$.

Two exact realization questions remain:

(1) Does every odd-order pairing with $d(A) \geq 2$ satisfy $\mu(A, b) \leq d(A) + 1$? Theorem 5.26 reduces this assertion to ranks three, four and five, without bounding the orders or the number of primes.

(2) Does every cyclic pairing except $\left\langle \frac{1}{8} \right\rangle$ have a graphical presentation of cycle rank at most four? Theorem B.1 settles the two-primary case and Theorem 4.11 settles the odd-order case. For even composite orders, the question concerns the classes excluded by Theorem 4.16 in ranks at most three.

Chua–Kummer–Sturmfels describe the four-dimensional cographic cones [8]; Mandelshtam's conorm criterion [29] characterizes the cographic locus. The second question asks for a positive rank-four representative of the prescribed negative discriminant in a cographic cone with nonnegative integral edge lengths. Zero lengths correspond to contraction.

A coprime cyclic complement, without a rank or planarity condition, also follows from [23, 31]. Fix a finite pairing (A, b) and a finite set of excluded primes. Choose an integer $R \geq 3$ exceeding those primes and every prime divisor of $|A|$. Write $\exp(A_p) = p^{a_p}$, with $a_p = 0$ when $A_p = 0$, and put

$$e = \prod_{p<R} p^{a_p+1}.$$

For a finite abelian group T, the isomorphism $T/eT \cong A$ holds if and only if $T_p \cong A_p$ for every $p < R$. Indeed, a cyclic summand $\mathbb{Z}/p^b\mathbb{Z}$ of T_p has image of order $p^{\min\{b, a_p+1\}}$ in T/eT. Thus $T/eT \cong A$ forces $\exp(T_p) \leq p^{a_p}$, and then $T_p/p^{a_p+1}T_p = T_p$. The components at primes $p \geq R$ have zero quotient. In the random-graph model $G(n, 1/2)$, prescribe (A, b) at the primes below R, with trivial primary

part at the additional primes. Corollary 10.2 and the primary-subgroup argument of Corollary 10.5 in [23] give limiting probability

$$c_R = \frac{1}{|A|\,|\operatorname{Aut}(A,b)|}\prod_{p<R}\prod_{j\ge 1}(1-p^{1-2j}).$$

Changing the Laplacian sign replaces b by $-b$ and does not change this probability. The product over $j \ge 2$ is bounded below by a positive constant independent of R, since $\sum_p \sum_{j\ge 2} p^{1-2j} < \infty$. Moreover,

$$\prod_{p<R}(1-p^{-1}) \ge \prod_{m=2}^{R-1}(1-m^{-1}) = \frac{1}{R-1}.$$

Thus $c_R \ge c_A/R$ for a constant $c_A > 0$. Let E_R be the event specifying the primary pairings below R, and let B_R be the event that a primary part at some $p \ge R$ is noncyclic. Put $d = n-1$, the size of the reduced Laplacian. Propositions 2.1 and 2.5 of [31] give a constant $c > 0$ such that, for sufficiently large d,

$$\Pr(B_R) \ll \sum_{R \le p \le \exp(d^{c/2})} \left(p^{-3} + e^{-d^c}\right) + d^{-2} \ll R^{-2} + e^{-d^c/2} + d^{-2}.$$

Indeed, a noncyclic primary cokernel has dimension at least two modulo p, and hence the reduced Laplacian has rank at most $d-2$. The sum of p^{-3} is at most $\sum_{j\ge R} j^{-3} \ll R^{-2}$, and there are at most $\exp(d^{c/2})$ primes in the sum. There is consequently a constant C independent of R such that

$$\liminf_{n\to\infty} \Pr(E_R \cap B_R^{c}) \ge c_R - \limsup_{n\to\infty} \Pr(B_R) \ge \frac{c_A}{R} - \frac{C}{R^2} > 0 \qquad (R > C/c_A).$$

The probability that $G(n,1/2)$ is disconnected tends to zero:

$$\Pr(G(n,1/2)\ \text{disconnected}) \le \sum_{s=1}^{\lfloor n/2\rfloor} \binom{n}{s} 2^{-s(n-s)} \le \sum_{s=1}^{\lfloor n/2\rfloor} (n2^{-n/2})^{s} = o(1).$$

Hence some connected graph has the prescribed primary pairings below R and cyclic primary parts at all other primes. The orthogonal sum of the latter parts is cyclic of order coprime to $|A|$ and to every excluded prime.

For smooth definite fillings of lens spaces, see [2]; for locally flat embeddings in topological four-manifolds, see [17].

Appendix A. Quadratic refinements and prime classes

A.1. **Even presentations and full local stability.** A finite quadratic module is a finite abelian group A with a function $q : A \longrightarrow \mathbb{Q}/\mathbb{Z}$ such that $q(nx) = n^2 q(x)$ for every integer n, and such that

$$b_q(x,y) = q(x+y) - q(x) - q(y)$$

is a nonsingular bilinear pairing. At a prime p, the natural map $\mathbb{Q} \to \mathbb{Q}_p$ identifies the p-primary subgroup of $\mathbb{Q}/\mathbb{Z}$ with $\mathbb{Q}_p/\mathbb{Z}_p$. For a nonsingular symmetric matrix $C \in \operatorname{Mat}_r(\mathbb{Z}_p)$, with even diagonal when $p = 2$, put

$$\mathcal{Q}_p(C) = \left(\mathbb{Z}_p^r/C\mathbb{Z}_p^r, [x] \longmapsto \frac{1}{2}x^{\mathsf T}C^{-1}x \pmod{\mathbb{Z}_p}\right).$$

The expression is well defined. Replacing x by $x + Cz$ changes it by $x^{\mathsf T}z + z^{\mathsf T}Cz/2$, which belongs to $\mathbb{Z}_p$. For an even nonsingular integral matrix C, define $\mathcal{Q}(C)$ by the same formula in $\mathbb{Q}/\mathbb{Z}$; its p-primary part is canonically identified with $\mathcal{Q}_p(C)$.

Lemma A.1. *Let (A, q) be a finite quadratic module, let d_p be the least number of generators of A_p, and let $r \geq d_p$. For an odd prime p, there is a nonsingular symmetric diagonal matrix $C_p \in \mathrm{Mat}_r(\mathbb{Z}_p)$ such that $\mathcal{Q}_p(C_p) \cong (A_p, q_p)$. For $p = 2$, there is a nonsingular symmetric tridiagonal matrix C_2 with even diagonal and $\mathcal{Q}_2(C_2) \cong (A_2, q_2)$ if and only if*

$$r \equiv d_2 \pmod 2.$$

The entries in all these matrices can be chosen in $\mathbb{Z}_{(p)} = \{a/b \in \mathbb{Q} : p \nmid b\}$.

Proof. The primary quadratic decomposition gives, at an odd prime p, cyclic summands

$$\left(\mathbb{Z}/p^k\mathbb{Z}, x \longmapsto \frac{ax^2}{p^k}\right), \qquad k \geq 1, \quad p \nmid a.$$

The rank-one matrix $[2ap^k]$ presents this quadratic summand locally: the generator $[2a]$ has quadratic value a/p^k. Its order is p^k. The orthogonal sum of these rank-one matrices has size d_p. Appending $r - d_p$ copies of $[1]$ adds no local discriminant module.

At two, the quadratic decomposition has cyclic summands

$$\left(\mathbb{Z}/2^k\mathbb{Z}, x \longmapsto \frac{ax^2}{2^{k+1}}\right), \qquad k \geq 1, \quad a \text{ odd},$$

and binary summands

$$\left((\mathbb{Z}/2^k\mathbb{Z})^2, (x, y) \longmapsto \frac{xy}{2^k}\right), \qquad \left((\mathbb{Z}/2^k\mathbb{Z})^2, (x, y) \longmapsto \frac{x^2 + xy + y^2}{2^k}\right).$$

These are precisely the blocks of the quadratic decomposition; see [42, Definition 3.11 and Theorem 3.19]. Set

$$H = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad F = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}.$$

The cyclic summand is presented by $[2^k a]$: its generator $[a]$ has quadratic value $a/2^{k+1}$. The two binary summands are presented by $2^k H$ and $2^k F$. Indeed, for either $B = H$ or $B = F$, the map

$$(\mathbb{Z}_2/2^k\mathbb{Z}_2)^2 \longrightarrow \mathbb{Z}_2^2/(2^k B)\mathbb{Z}_2^2, \qquad x \longmapsto [Bx]$$

is an isomorphism, since B is unimodular over $\mathbb{Z}_2$, and its quadratic value is $x^{\mathsf{T}}Bx/2^{k+1}$. Their orthogonal sum is tridiagonal, has even diagonal, and has size d_2. If $r - d_2$ is even, append $(r - d_2)/2$ copies of H at unit scale. These are even unimodular matrices and contribute no local discriminant module. The resulting matrix has the required size.

Conversely, if C_2 is an even nonsingular matrix of size r, then its reduction modulo two is alternating. Therefore its rank over $\mathbb{F}_2$ is even. Reduction of its cokernel modulo two gives

$$d_2 = r - \mathrm{rank}_{\mathbb{F}_2}(C_2 \bmod 2),$$

which proves the parity condition. The displayed block matrices are integral, so the final assertion follows as well. □

Remark A.2. The two binary quadratic blocks at $k = 1$ are distinct. Their associated bilinear pairings are isometric, but their quadratic forms have opposite Arf invariants. Thus a bilinear local prescription at two does not replace the quadratic prescription in Lemma A.1.

Corollary A.3. *Let (A, q) be a finite quadratic module, and let S be a finite set of primes containing two and every prime dividing $|A|$. Suppose*

$$r \geq d(A) := \max_p d(A_p), \qquad r \equiv d(A_2) \pmod 2.$$

Then there is a positive definite even integral tridiagonal matrix C of size r such that

$$\mathcal{Q}_p(C) \cong (A_p, q_p) \quad (p \in S).$$

When $r \geq 2$, its adjacent entries may all be chosen strictly negative, and its diagonal entries may satisfy any prescribed strict diagonal dominance margins. Its nonadjacent entries are zero.

Proof. Choose the matrices of Lemma A.1 at each $p \in S$. Let p^{e_p} annihilate A_p, taking $e_p = 0$ when $A_p = 0$. Their inverses multiplied by p^{e_p} are integral, because this integrality is equivalent to annihilation of the local cokernel. The Chinese remainder theorem gives simultaneous integral approximations to each diagonal and adjacent entry modulo p^{2e_p+3} for all $p \in S$. Keep the nonadjacent entries equal to zero. Replace the adjacent entries within their congruence classes by negative integers. Then replace each diagonal entry by a sufficiently large positive integer in its congruence class to obtain the required strict diagonal dominance. All diagonal entries are even, since their congruences at two preserve the even diagonals of C_2. Strict diagonal dominance with positive diagonal makes C positive definite. Lemma 3.5 proves every local quadratic isometry. The argument also applies to $r = 1$; for $r = 0$, the hypotheses force $A = 0$ and the empty matrix provides the corresponding degenerate-size convention. □

Remark A.4 (Rank-zero and rank-one conventions). The empty matrix has determinant one and zero discriminant module, but cannot produce a nontrivial prime-order complement. A prime- completion statement must therefore impose $r \geq 1$. If $A = 0$, the parity condition makes the least possible such rank equal to two. At rank one an even integral matrix is $[2k]$, so its 2-primary cokernel is nonzero and cyclic. Hence rank one is available only when $d(A) = d(A_2) = 1$; its quadratic prime-complement construction is obtained by varying this single even diagonal in an appropriate arithmetic progression.

A.1.1. *Gauss sums and the Brown invariant.* For a nondegenerate finite homogeneous quadratic module (A, q), define the Brown invariant by

$$|A|^{-1/2} \sum_{x \in A} \exp(2\pi i q(x)) = \exp\bigl(2\pi i \operatorname{Br}(q)/8\bigr).$$

Thus the Brown invariant is additive under orthogonal sum, changes sign under $q \mapsto -q$, and equals the signature modulo eight for the discriminant quadratic module of an even integral lattice. The trivial module has Brown invariant zero. These are the positive-exponential conventions for Milgram's formula; see [42, Theorem 5.1 and Proposition 5.2], whose exponential convention has the opposite sign.

Lemma A.5. *Let $d_2 = d(A_2)$. Then*

$$\operatorname{Br}(q) \equiv d_2 \pmod 2.$$

Every nondegenerate quadratic module of odd prime order has Brown invariant in $\{0, 2, 4, 6\}$.

Proof. The primary quadratic block decomposition in Lemma A.1 reduces the calculation to the displayed cyclic and binary forms. For an odd prime p, the normalized Gauss sum of ax^2/p^k is one if k is even, and is $\left(\frac{a}{p}\right)\epsilon_p$ if k is odd, where $\epsilon_p = 1$ for $p \equiv 1 \pmod 4$ and $\epsilon_p = i$ for $p \equiv 3 \pmod 4$. Its Brown invariant is therefore even. The normalized Gauss sums of the three 2-primary blocks are

q	normalized Gauss sum
$ax^2/2^{k+1}$	$\left(\frac{2}{a}\right)^k \exp(2\pi i a/8)$
$xy/2^k$	1
$(x^2+xy+y^2)/2^k$	$(-1)^k$

for $k \geq 1$ and odd a, with $\left(\frac{2}{a}\right) = (-1)^{(a^2-1)/8}$. For the two-primary cyclic sum write $G_k(a) = \sum_{x \bmod 2^k} \exp(2\pi i a x^2/2^{k+1})$. For $k \geq 1$, write $x = y + 2^{k+1}t$, with $y \bmod 2^{k+1}$ and $t \in \{0, 1\}$. Summing over t gives the factor $1 + (-1)^y$. Only $y = 2z$ remain, and hence $G_{k+2}(a) = 2G_k(a)$. The two base values are $G_1(a) = 1 + i^a$ and $G_2(a) = 2\exp(2\pi i a/8)$. For the hyperbolic binary sum, summing first over y leaves only $x = 0$, giving 2^k. For the other binary sum B_{k+2}, write $x = X + 2^{k+1}s$ and $y = Y + 2^{k+1}t$, with $X, Y \bmod 2^{k+1}$ and $s, t \in \{0, 1\}$. The sum over s, t is zero unless X, Y are both even, when it contributes a factor four. Putting $X = 2x'$ and $Y = 2y'$ gives $B_{k+2} = 4B_k$. The base values are $B_1 = -2$ and $B_2 = 4$. These recurrences give the tabulated normalized values. The odd-prime base

evaluation is the quadratic Gauss-sum formula, in the convention of [42, Section 5]. For its prime-power extension, writing $x = y + p^{k+1}t$ in the sum of modulus p^{k+2} gives $\sum_{t \bmod p} \exp(2\pi i\, 2ayt/p)$, which vanishes unless $p \mid y$ and equals p otherwise. Thus the unnormalized sums satisfy $S_{k+2} = pS_k$. Each cyclic 2-primary block therefore has Brown invariant odd, and each binary 2-primary block has Brown invariant zero or four. The least number of generators of the 2-primary group is the number of cyclic blocks plus twice the number of binary blocks. Additivity proves the parity assertion. More explicitly, a quadratic module of odd prime order has the form

$$q_{\ell,\kappa}(x) = \frac{\kappa x^2}{\ell} \pmod{\mathbb{Z}}, \qquad \ell \nmid \kappa,$$

and its normalized Gauss sum is

$$\left(\frac{\kappa}{\ell}\right) \begin{cases} 1, & \ell \equiv 1 \pmod 4, \\ i, & \ell \equiv 3 \pmod 4. \end{cases}$$

This also proves the second assertion. □

A.2. **The quadratic refinement of a bipartite graph.** The quadratic refinement is defined by the characteristic-discriminant construction of [14, Section 2.1.2]. The parity of the flow lattice is also recorded in [3, Proposition 1].

Fix an orientation of a finite connected bipartite graph G. Let $\partial : \mathbb{Z}^{E(G)} \longrightarrow \mathbb{Z}^{V(G)}$ be its incidence map and let $L = \partial\partial^{\mathsf{T}}$ be its Laplacian. Let $\chi : V(G) \longrightarrow \{0, 1\}$ be either bipartition indicator. For a degree-zero integral divisor D, choose a rational vector f with $Lf = D$ and set

$$q_G([D]) = \frac{1}{2}\left(D^{\mathsf{T}} f - \chi^{\mathsf{T}} D\right) \pmod{\mathbb{Z}}.$$

Proposition A.6. *The function q_G is a well-defined homogeneous quadratic refinement of the positive monodromy pairing on* $\mathrm{Jac}(G)$*. It is independent of the orientation, the choice of f, and the choice between the two bipartition indicators. Under the canonical antiisometry between the cut and flow discriminant bilinear groups, it corresponds to the negative discriminant quadratic form of the integral flow lattice. Consequently*

$$\mathrm{Br}(q_G) \equiv -\beta(G) \pmod 8.$$

Proof. Changing f by a constant leaves $D^{\mathsf{T}} f$ unchanged, since D has degree zero. Replacing χ by $1 - \chi$ changes q_G by $\chi^{\mathsf{T}} D \in \mathbb{Z}$. Both L and the displayed expression are independent of the orientation. If D is replaced by $D + Lz$, with z integral, choose $f + z$ as its potential. The change in q_G is

$$D^{\mathsf{T}} z + \frac{1}{2}\left(z^{\mathsf{T}} L z - \chi^{\mathsf{T}} L z\right).$$

For every oriented edge, put $k = z_u - z_v$ and $\epsilon = \chi_u - \chi_v \in \{1, -1\}$. Its contribution to the parenthesis is $k^2 - \epsilon k$, an even integer. Thus q_G is well defined on the Jacobian. Symmetry of L gives

$$q_G([D + E]) - q_G([D]) - q_G([E]) = b_G([D], [E]).$$

Moreover

$$q_G(n[D]) - n^2 q_G([D]) = \frac{n^2 - n}{2} \chi^{\mathsf{T}} D \in \mathbb{Z}.$$

It remains to identify the quadratic form on the flow lattice. Write

$$\mathcal{F} = \ker \partial \cap \mathbb{Z}^{E(G)}, \qquad u = \partial^{\mathsf{T}} f, \qquad w = \partial^{\mathsf{T}} \chi.$$

Every coordinate of w is 1 or -1. In particular, the integral flow lattice is even: for $c \in \mathcal{F}$, one has $c^{\mathsf{T}} c \equiv c^{\mathsf{T}} w = 0 \pmod 2$. Choose $a \in \mathbb{Z}^{E(G)}$ with $\partial a = D$, possible by connectedness, and put $v = a - u$. Then v belongs to the rational flow space. For $c \in \mathcal{F}$, one has $v^{\mathsf{T}} c = a^{\mathsf{T}} c \in \mathbb{Z}$, so $v \in \mathcal{F}^*$. Changing

a changes v by an integral flow. Its discriminant class is the image of $[D]$ in the flow discriminant group. Since u and v are orthogonal,

$$u^{\mathsf{T}}u + v^{\mathsf{T}}v = a^{\mathsf{T}}a, \qquad a^{\mathsf{T}}w = \chi^{\mathsf{T}}D.$$

It follows that

$$q_G([D]) = \frac{1}{2}\left(a^{\mathsf{T}}a - a^{\mathsf{T}}w\right) - \frac{1}{2}v^{\mathsf{T}}v \equiv -\frac{1}{2}v^{\mathsf{T}}v \pmod{\mathbb{Z}},$$

since every coordinate of w is odd. This proves the quadratic identification. The flow lattice is positive definite of rank $\beta(G)$, so Milgram's formula gives the Brown invariant. □

A.3. **A local criterion for prime residue classes.** For a finite quadratic module (A, q) write $N = |A|$. Fix an integer $r \geq 1$, an integer m divisible by $8\,\mathrm{rad}(N_{\mathrm{odd}})$, and an integer a prime to m. The class $a \bmod m$ is admissible at rank r if, for every prime $p \mid 2N$, there is a nonsingular integral $\mathbb{Z}_p$-lattice K_p of rank r, even when $p = 2$, such that

$$\mathcal{Q}_p(K_p) \cong (A_p, -q_p), \qquad \det K_p \in Na\,(\mathbb{Z}_p^{\times})^2.$$

The valuation of $\det K_p$ is necessarily v_pN. Thus the determinant condition is a condition on its unit square class. Admissibility depends only on the residue class $a \bmod m$.

Theorem A.7 (Quadratic prime complements in prescribed residue classes). *The following conditions are equivalent.*

(1) The class $a \bmod m$ is admissible at rank r.

(2) There are an odd prime $\ell \equiv a \pmod{m}$, with $\ell \nmid N$, and a finite connected bipartite graph G such that

$$\beta(G) = r, \qquad (\mathrm{Jac}(G), q_G) \cong (A, q) \perp (C, q_C), \qquad |C| = \ell.$$

(3) For every prescribed integer $g \geq 3$ and every prescribed finite set of primes, infinitely many such primes ℓ outside that set have realizations by simple planar biconnected bipartite graphs of cycle rank r, with all vertex degrees in $\{2, 3\}$, girth at least $2g$, and treewidth at most two. For fixed r, all realizing graphs may be chosen as subdivisions of the same fixed planar multigraph Q_r. For each construction there is a fixed nonzero integer κ such that its cyclic quadratic complements are

$$\left(\mathbb{Z}/\ell\mathbb{Z}, x \longmapsto \frac{\kappa x^2}{\ell} \pmod{\mathbb{Z}}\right).$$

Proof. Suppose (2) holds. The integral flow lattice of G is even, has rank r, and has discriminant quadratic module $(A, -q) \perp (C, -q_C)$ by Proposition A.6. Its determinant is $N\ell$. At every $p \mid 2N$, the complementary group vanishes locally. Moreover ℓ/a is a square unit in $\mathbb{Z}_p$: at odd p it is congruent to one modulo p, and at two it is congruent to one modulo eight. Thus the localized flow lattice proves (1).

Assume (1). Add the prime divisors of m and the exceptional set. At a prime dividing m but not $2N$, prescribe $\mathrm{diag}(Na, 1, \dots, 1)$; at other new primes prescribe a unimodular form. By Lemma 6.2, each prescribed lattice K_p admits an integral orthogonal decomposition into lines and, at two, scaled even unimodular binary blocks. Their ordered Gram matrices are tridiagonal and represent the same integral lattices. In particular, they retain the determinant square classes, rational Hasse invariants, evenness at two, and quadratic discriminant modules. Apply Proposition 6.3 to these matrices. Its determinant-normalizing change of basis preserves evenness. Lemma 3.5 preserves the full local lattices, so the resulting L_j have the prescribed quadratic discriminants. The complementary element $N[e_r]$ has order $n_j = u + vj$, bilinear norm NF/n_j, and quadratic value $NF/(2n_j)$. The primary summands are orthogonal for the bilinear pairing and therefore for the quadratic form.

The integer NF is even. This follows from $2 \mid N$ when N is even. Otherwise n_j is odd, so $\det L_j = Nn_j$ is odd and $L_j \bmod 2$ is nonsingular alternating. Its rank is even; its preceding odd-dimensional principal submatrix is alternating and has even determinant F. Thus the complementary

quadratic form is well defined on the cyclic group of odd order n_j, and the graph quadratic numerator is $\kappa = -NF/2 \in \mathbb{Z} \setminus \{0\}$.

Lemma 6.1 realizes the matrices. Each cycle vector has norm equal to the cycle length. Evenness of the lattice therefore makes every cycle even, so the graph is bipartite. Proposition A.6 identifies its quadratic module as the negative lattice discriminant. Dirichlet's theorem selects infinitely many primes from the progression $u + vj \equiv a \pmod{m}$. All stated restrictions follow from the same graph construction. Choosing one prime from the family in (3) proves (2). □

A.3.1. *Finite determinant conditions.* The local determinant condition is determined by finitely many integral forms. At an odd prime p, choose a nonsquare unit η_p. Every integral local lattice is an orthogonal sum of lines

$$[p^k u], \qquad k \geq 0, \quad u \in \{1, \eta_p\}.$$

A line has rank one, determinant valuation k, and unit determinant class u. For $k \geq 1$, the generator $[u]$ identifies its quadratic discriminant module with $x \mapsto ux^2/(2p^k)$; for $k = 0$ it is trivial. At two, every even integral local lattice is an orthogonal sum of blocks from the following table.

block	range	rank	v_2 det	unit determinant class
$[2^k u]$	$k \geq 1,\ u \in \{1,3,5,7\}$	1	k	u
$2^k H$	$k \geq 0$	2	$2k$	-1
$2^k F$	$k \geq 0$	2	$2k$	3

The quadratic discriminant modules for $k \geq 1$ are respectively

$$\frac{ux^2}{2^{k+1}}, \qquad \frac{xy}{2^k}, \qquad \frac{x^2 + xy + y^2}{2^k};$$

the two binary blocks at $k = 0$ have trivial discriminant.

Let e_p be the exponent valuation of A_p, with $e_p = 0$ if $A_p = 0$. Let $\mathscr{Q}_p$ be the set of block sums from these lists of rank r, determinant valuation $v_p(N)$, and quadratic discriminant isometric to $(A_p, -q_p)$. Every nonunimodular scale satisfies $k \leq e_p$, so $\mathscr{Q}_p$ is finite. Fix generators $x_1, \dots, x_s$ of A_p and a finite set of defining relations. For such a block sum C, write q_C for its discriminant quadratic form. The isometry condition is equivalent to the existence of elements $y_1, \dots, y_s$ of coker C which satisfy those relations, generate the cokernel, and obey

$$q_C(y_i) = -q_p(x_i), \qquad b_{q_C}(y_i, y_j) = -b_{q_p}(x_i, x_j) \quad (i < j).$$

The relations give a surjective homomorphism $x_i \mapsto y_i$. Both groups have order $p^{v_p(N)}$, so this homomorphism is an isomorphism. The identity

$$q\left(\sum_i n_i x_i\right) = \sum_i n_i^2 q(x_i) + \sum_{i<j} n_i n_j b_q(x_i, x_j)$$

then proves preservation of every quadratic value. Equivalently, one may prescribe the values on all generators and their pairwise sums. Generator values alone do not suffice: the forms $(x^2 + y^2)/5$ and $(x^2 + xy + y^2)/5$ on $(\mathbb{Z}/5\mathbb{Z})^2$ agree on the standard generators, while their polar matrices have determinants 4 and 3 modulo five, respectively. These determinant classes differ by a nonsquare, so the forms are not isometric. The tuples $(y_1, \dots, y_s)$ range over the finite set $(\operatorname{coker} C)^s$. The class $a \bmod m$ is admissible if and only if

$$Na/p^{v_p(N)} \in \bigcup_{C \in \mathscr{Q}_p} p^{-v_p(N)} \det C \, (\mathbb{Z}_p^\times)^2 \quad \text{for every } p \mid 2N.$$

For a fixed cyclic quadratic block of order two, the two lifts of its coefficient modulo four give different determinant unit classes modulo eight. Both are included in $\mathscr{Q}_2$.

The lists exhaust the integral local lattices by Lemma 6.2 and Lemma 3.3. At two, evenness excludes unit-scale lines; a line of positive scale 2^k has $k \geq 1$. Rescaling by unit squares gives precisely the displayed unit representatives. The cokernel of each positive-scale block has exponent p^k, proving the bound $k \leq e_p$.

A.3.2. *The stable-rank simplification.*

Lemma A.8. *Let C be an even nonsingular matrix over $\mathbb{Z}_2$ of rank r, and write* $\det C = 2^s u$ *with u odd. Then*

$$u \equiv (-1)^{(r-\mathrm{Br}(Q_2(C)))/2} \pmod 4.$$

The exponent is integral, and its parity is independent of the representative of the Brown invariant modulo eight.

Proof. Apply the local block decomposition. For a cyclic block $[2^k u]$, the elementary quadratic Gauss sum gives $\mathrm{Br} \equiv u \pmod 4$. For a scaled H or F block, the Brown invariant is divisible by four, while its rank is two and its unit determinant is -1 modulo four. The statement also holds for unit-scale H, F, whose discriminant module is trivial. Both sides multiply under orthogonal direct sum, proving the formula. □

Corollary A.9. *Suppose*

$$r > d(A), \qquad r \equiv d(A_2) \pmod 2.$$

Put $N_{\mathrm{odd}} = N/2^{v_2 N}$ *and* $\sigma_2 = \mathrm{Br}(A_2, q_2) \in \mathbb{Z}/8\mathbb{Z}$. *Then a* mod *m is admissible at rank r if and only if*

$$\boxed{N_{\mathrm{odd}} a \equiv (-1)^{(r+\sigma_2)/2} \pmod 4.}$$

Thus every coprime residue class satisfying this single congruence contains infinitely many prime complements with all the graph restrictions of Theorem A.7.

Proof. At an odd prime, a minimal-rank local presentation of $(A_p, -q_p)$ may be padded to rank r by unimodular lines. Since $r > d(A) \geq d(A_p)$, at least one such line is available, and its unit square class may be chosen arbitrarily. Hence there is no determinant obstruction at an odd prime. At two, put $d_2 = d(A_2)$. The integer $r - d_2$ is positive and even, so there are at least two ranks for a unimodular summand. Start with any rank-d_2 even local presentation and pad by even unimodular binary blocks. Replacing one H unimodular block by F changes its determinant unit class by -3, which is 5 modulo eight, and leaves its quadratic discriminant module unchanged. The two resulting determinant classes are precisely the two odd unit square classes with the required residue modulo four. Lemma A.8, applied to discriminant form $-q_2$, identifies that residue as $(-1)^{(r+\sigma_2)/2}$. This proves necessity and sufficiency. □

A.4. **The exact cycle rank with a prescribed prime Brown invariant.**

Corollary A.10 (Minimum cycle rank with prescribed prime Brown invariant). *Let (A, q) be a nondegenerate finite homogeneous quadratic module, put $d = d(A)$, and prescribe $c \in \{0, 2, 4, 6\}$. Define*

$$r_c = \min\Big\{ r \geq \max\{1, d\} \,:\, r + \mathrm{Br}(q) + c \equiv 0 \pmod 8 \Big\}.$$

Then r_c is the minimum cycle rank among finite connected bipartite graphs G admitting a quadratic prime completion

$$(\mathrm{Jac}(G), q_G) \cong (A, q) \perp (\mathbb{Z}/\ell\mathbb{Z}, q_C), \qquad \ell \nmid 2|A|, \quad \mathrm{Br}(q_C) = c.$$

For every prescribed girth bound and finite set of excluded primes, infinitely many such odd primes have realizations at rank r_c by simple planar biconnected bipartite graphs, with all vertex degrees in $\{2, 3\}$ and treewidth at most two. All these graphs may be subdivisions of the fixed graph Q_{r_c}. Within each constructed family, the prime quadratic complements have a fixed numerator:

$$q_C(x) = \frac{\kappa x^2}{\ell} \pmod{\mathbb{Z}}, \qquad \kappa \in \mathbb{Z} \setminus \{0\}.$$

The same existence assertion holds at every rank $r \geq \max\{1, d\}$ with $r + \mathrm{Br}(q) + c \equiv 0 \pmod 8$. No prime residue class is prescribed externally in this corollary.

Proof. Let G be any graph in the stated minimum. Its positive definite integral flow lattice has rank $r = \beta(G)$ and discriminant group isomorphic to its Jacobian. Therefore

$$r \geq d\big(A \oplus \mathbb{Z}/\ell\mathbb{Z}\big) = \max\{d, 1\}.$$

Since G is bipartite, the flow lattice is even. Its discriminant quadratic module is the negative of the canonical graph quadratic module. Proposition A.6 and Milgram's formula give

$$-r \equiv \operatorname{Br}(q_G) = \operatorname{Br}(q) + c \pmod 8.$$

This proves the lower bound $r \geq r_c$.

Conversely, fix any rank $r \geq \max\{1, d\}$ satisfying the displayed Brown congruence. By Lemma A.5,

$$r \equiv -\operatorname{Br}(q) - c \equiv d(A_2) \pmod 2.$$

For each $p \mid 2N$, where $N = |A|$, choose an integral local presentation K_p of $(A_p, -q_p)$ of rank r, even at two, by Lemma A.1. Its determinant has valuation $v_p N$. Consequently

$$\delta_p := \frac{\det K_p}{N} \in \mathbb{Z}_p^\times.$$

Set $m = 8\operatorname{rad}(N_{\mathrm{odd}})$, and choose an integer a by the Chinese remainder theorem so that

$$a \equiv \delta_2 \pmod 8, \qquad a \equiv \delta_p \pmod p \quad (p \mid N,\ p \text{ odd}).$$

These residues are units, so $\gcd(a, m) = 1$. A unit congruent to one modulo p is a square in $\mathbb{Z}_p^\times$ for odd p, and a 2-adic unit congruent to one modulo eight is a square. Hence

$$\det K_p \in N a(\mathbb{Z}_p^\times)^2 \quad (p \mid 2N).$$

The class a mod m is therefore admissible at rank r in Theorem A.7. That theorem gives infinitely many odd prime completions, outside the prescribed finite set, with all the graph restrictions and the fixed numerator here. Applying Milgram's formula to each resulting graph gives

$$\operatorname{Br}(q_C) \equiv -r - \operatorname{Br}(q) \equiv c \pmod 8.$$

This proves attainability at r_c and at every other permitted rank. The local determinants determine the residue class of the complementary primes. □

Remark A.11 (Interpretation of the prime Brown invariant). For $q_C(x) = \kappa x^2/\ell$, the four prescriptions are exactly

c	$\ell \bmod 4$	$\left(\frac{\kappa}{\ell}\right)$
0	1	$+1$
2	3	$+1$
4	1	-1
6	3	-1

The coefficient here is the quadratic numerator κ; the associated bilinear numerator is 2κ. The construction may impose further congruences on ℓ inside the indicated class modulo four.

Remark A.12 (The trivial module and rank one). If $A = 0$, then $d = 0$ and $\operatorname{Br}(q) = 0$, so the exact ranks are

c	0	2	4	6
r_c	8	6	4	2.

Rank zero cannot produce a nontrivial prime Jacobian. A rank-one bipartite flow lattice has Gram matrix $[2k]$ and therefore has nontrivial 2-primary discriminant. Accordingly, rank one is possible in the corollary precisely when

$$d(A) = d(A_2) = 1, \qquad 1 + \operatorname{Br}(q) + c \equiv 0 \pmod 8.$$

The local construction then has just one diagonal entry, and the resulting graphs may be even cycles of length $N\ell$. Their lengths are unbounded along the prime progression, so simplicity and every prescribed girth bound remain available in this case.

Corollary A.13. *If the prime quadratic complement may have any Brown invariant, the minimum cycle rank is*

$$r_{\mathrm{free}} = \min\{r \geq \max\{1, d(A)\} : r \equiv d(A_2) \pmod 2\}.$$

For $A \neq 0$, this equals $d(A)$ when $d(A)$ and $d(A_2)$ have the same parity, and equals $d(A)+1$ otherwise. For $A = 0$ it equals two. This minimum has infinitely many prime realizations with all the graph restrictions in Corollary A.10.

Proof. For any even local presentation at two, reduction modulo two is alternating. Thus a graph in the assertion necessarily satisfies $r \equiv d(A_2) \pmod 2$; the generator bound gives the other inequality. At the least rank satisfying these two conditions, the residue $c = -r - \mathrm{Br}(q)$ is even by Lemma A.5. Choosing its representative in $\{0, 2, 4, 6\}$ and applying Corollary A.10 proves attainment. □

Example A.14 (A rank difference of seven). The formula gives $r_c \leq \max\{1, d(A)\} + 7$, and this allowance is necessary in general. Take $A = \mathbb{Z}/3\mathbb{Z}$, $q(x) = x^2/3$, and $c = 6$. Then $\mathrm{Br}(q) = 2$, so the minimum is $r_c = 8$, while $d(A) = 1$. The two quadratic refinements $q_H(x, y) = xy/2$ and $q_F(x, y) = (x^2 + xy + y^2)/2$ on $(\mathbb{Z}/2\mathbb{Z})^2$ have the same hyperbolic bilinear pairing, but Brown invariants zero and four. For $c = 0$, their exact minimum ranks are respectively eight and four. Thus the quadratic data change the sharp graph realization problem even when the underlying bilinear pairing is unchanged.

Appendix B. Cyclic two-primary minima

Corollary 4.17 determines the minima at most three. Explicit graphs determine the larger minima.

Theorem B.1 (Minimum cycle rank of cyclic two-primary pairings). *Let $k \geq 1$ and a be odd. The minimum cycle rank of a graph with paired Jacobian $\left\langle \frac{a}{2^k} \right\rangle$ is as follows. At $k = 1$ it is one. At $k = 2$ it is three for $a = 1 \bmod 4$ and one for $a = 3 \bmod 4$. For $k \geq 3$ it is given by*

$a \bmod 8$	1	3	5	7
$k = 3$	7	3	2	1
$k \geq 4$ *even*	4	2	3	1
$k \geq 5$ *odd*	4	3	2	1.

Every minimum is attained by a connected planar loopless multigraph. In particular every cyclic pairing of order 2^k, $k \geq 4$, has an exact planar realization with at most four cycles, and four is necessary for precisely the unit square class.

Lemma B.2. *Let $z \geq j \geq 1$ and $q > j$ be integers. Set $m = 3z + 1$ and $n = mq - 3j^2$. There is a connected planar loopless graph of cycle rank four with flow Gram matrix*

$$C(z, j, q) = \begin{pmatrix} 1+z & z & z & j \\ z & 1+z & z & j \\ z & z & 1+z & j \\ j & j & j & q \end{pmatrix}. \tag{B.1}$$

It has determinant n and $(C^{-1})_{44} = m/n$. If $\gcd(m, n) = 1$, its entire paired Jacobian is cyclic with generator $[e_4]$ of norm $-m/n$.

Proof. Join two vertices by three distinct edges and a path of length z. Let w be the vertex on the long path at distance j from the first endpoint. Add a path of length $q - j$ between this endpoint and w, with new interior vertices. Place the added path next to the corresponding segment of the old path in a plane embedding. The graph is loopless and its cycle rank is four. Take the three cycles comparing the unit edges with the long path, followed by the cycle comparing the new path with the segment of length j. The long path and all but one edge of the new path form a spanning tree. The three old unit edges and the omitted new edge are the four complementary edges. The four displayed cycles have coefficients forming a diagonal matrix with entries ± 1 on them; they are therefore an integral

fundamental cycle basis. Choose their signs so that shared segments have equal signs. Their Gram matrix is (B.1).

The leading ternary block is $I_3 + zJ_3$, of determinant m and inverse $I_3 - (z/m)J_3$. Its Schur complement gives

$$\det C = m\left(q - \frac{3j^2}{m}\right) = n, \qquad (C^{-1})_{44} = \frac{m}{n}.$$

The graph construction gives positive definiteness. If m is a unit modulo n, the self-pairing of $[e_4]$ has denominator n, so its order is n and it generates the whole discriminant group. □

Proposition B.3. *For every $k \geq 4$, the pairing $\left\langle \frac{1}{2^k} \right\rangle$ has a connected planar loopless realization of cycle rank four.*

Proof. In Lemma B.2, it suffices to arrange

$$n = 2^k, \qquad m \equiv 7 \pmod 8.$$

Then $-m$ is a unit square modulo 2^k, so the displayed pairing is isometric to $\left\langle \frac{1}{2^k} \right\rangle$.

For $k = 4$, take $(z, j, q) = (2, 2, 4)$; then $m = 7$ and $n = 16$. For odd $k \geq 5$, take the following values:

$k \bmod 4$	j	q	m
1	1	5	$(2^k + 3)/5$
3	2	20	$(2^{k-2} + 3)/5$.

(B.2)

In both rows put $z = (m - 1)/3$. The quantities are integers: in the first row $2^k = 2 \bmod 15$, and in the second $2^{k-2} = 2 \bmod 15$. Moreover $m = 7 \bmod 8$, $z \geq j$, and $mq - 3j^2 = 2^k$. At the first endpoints $k = 5, 7$, one has $z = 2$; thereafter z increases.

For even $k \geq 8$, set $q = 13$. Let j be the unique odd member of the pair of residues

$$\{2^{k/2+1}, -2^{k/2+1}\} \pmod{13}$$

represented in $\{1, \dots, 12\}$. Thus $j \in \{1, 3, 5, 7, 9, 11\}$ and $j^2 = 4 \cdot 2^k \bmod 13$. Put

$$m = \frac{2^k + 3j^2}{13}, \qquad z = \frac{m - 1}{3}. \tag{B.3}$$

The first expression is integral because $1 + 3 \cdot 4 = 13$. Since k is even, its numerator is 1 mod 3, and $13 = 1 \bmod 3$, so z is integral. As j is odd, $m = 3/13 = 7 \bmod 8$. For $k = 8$, the choice is $j = 7$, $m = 31$, $z = 10$. For $k \geq 10$,

$$z \geq \frac{2^k/13 - 1}{3} > 11 \geq j.$$

Also $q = 13 > j$. These choices satisfy the lemma.

For $k = 6$, put

$$C_{64} = \begin{pmatrix} 2 & -1 & 0 & 0 \\ -1 & 3 & -1 & 0 \\ 0 & -1 & 5 & -1 \\ 0 & 0 & -1 & 3 \end{pmatrix}. \tag{B.4}$$

Its leading determinants are $2, 5, 23, 64$, and

$$C_{64}^{-1} e_4 = \frac{1}{64}(1, 2, 5, 23)^{\mathsf{T}}.$$

The generator $5[e_4]$ has negative discriminant norm $-575/64 = 1/64 \bmod \mathbb{Z}$.

Begin with a triangle A, B, C having two AB edges, two AC edges, and one BC edge. Replace one AB edge by $A - w - x - y - B$, a path of length four, and add a path $A - z - w$ of length two beside the edge Aw in the plane. The graph is planar and loopless, with seven vertices and ten edges, so

its cycle rank is four. Orient each edge as its name indicates, and denote the two edges from A to C by f_1, f_2. The edges AB, f_1, Aw, wx, xy, Az form a spanning tree. Its fundamental cycles, with signs chosen as follows, are

$$f_1 - f_2, \qquad AB + BC - f_1, \qquad Aw + wx + xy + yB - AB, \qquad Az + zw - Aw.$$

Their lengths are $2, 3, 5, 3$. Consecutive cycles have exactly one common edge, with opposite signs, and all other pairs are edge-disjoint. Their Gram matrix is (B.4). □

Lemma B.4. *If a loopless biconnected multigraph G has at least three vertices, then $\tau(G) \geq 2\beta(G) + 1$.*

Proof. The simple support of G is connected, has at least three vertices, and has no cut vertex. It cannot be a tree, since a tree on at least three vertices has a cut vertex. Hence it contains a cycle H of length at least three. Start with this cycle. If $V(H) \neq V(G)$, a component of $G - V(H)$ has at least two distinct neighbours u, v in H: a single neighbour would be a cut vertex of G. Choose a path from u to v with interior in that component and without repeated vertices. Adjoining this path preserves biconnectivity. Indeed, deleting an interior path vertex leaves its two remaining segments attached to the connected graph H; deleting a vertex of H leaves H minus that vertex connected, and every surviving path segment remains attached to it. Repetition includes every vertex. Each remaining edge is then an ear of length one. Thus G is obtained from a cycle of length at least three by open ears, all intermediate graphs being biconnected.

Suppose an ear of length a is adjoined to an intermediate graph H between distinct vertices u, v. Put $T = \tau(H)$, and let $F_{u,v}$ be the number of spanning forests of H with exactly two components, with u and v in different components. A spanning tree of the new graph either omits one ear edge and restricts to a tree of H, or contains the whole ear and restricts to such a two-component forest. It cannot omit two ear edges, since a segment of internal vertices would then be disconnected. Consequently the new tree count is

$$T' = aT + F_{u,v}, \qquad \beta' = \beta(H) + 1.$$

There exists a u–v path in H of length at least two. If u, v are adjacent, the component of $H - \{u, v\}$ containing any other vertex has neighbours at both u and v, since neither is a cut vertex; otherwise any path has the required length. Extend the edges of such a path to a spanning tree of H. Deleting each of two different path edges gives two distinct forests counted by $F_{u,v}$; hence $F_{u,v} \geq 2$. Therefore $T' - T = (a - 1)T + F_{u,v} \geq 2$. The initial cycle has $\beta = 1$ and at least three spanning trees. Induction on the number of ears gives $\tau(G) \geq 2\beta(G) + 1$. □

Proof of Theorem B.1. Corollary 4.17 proves all entries except the upper bounds in the unit-square column. Proposition B.3 supplies those bounds for $k \geq 4$. For the pairing $\left\langle \frac{1}{8} \right\rangle$, Theorem 4.16 excludes cycle rank at most three. By Lemma 2.7, a graph with cyclic Jacobian of order eight has only one nontrivial block: two nontrivial blocks would contribute a direct product of two nontrivial two-groups, which is not cyclic. The remaining blocks are bridges and contribute neither a discriminant group nor cycle rank. Thus the nontrivial block has the pairing $\left\langle \frac{1}{8} \right\rangle$ and the cycle rank of the graph. If its nontrivial block had at least three vertices, Lemma B.4 would force its cycle rank to be at most three. Hence the block has two vertices and eight parallel edges. Its cycle rank is seven and its pairing is $\left\langle \frac{1}{8} \right\rangle$. This graph attains the remaining entry. □

Remark B.5 (The graphical obstruction in rank four). Let

$$C = \begin{pmatrix} 2 & -1 & -1 & -1 \\ -1 & 2 & 0 & 0 \\ -1 & 0 & 2 & 0 \\ -1 & 0 & 0 & 3 \end{pmatrix}.$$

Its leading principal determinants are $2, 3, 4, 8$, so it is positive definite. Moreover $(C^{-1})_{22} = 7/8$, and the class $[e_2]$ has order eight. Thus $\mathcal{D}(C) \cong -\left\langle \frac{1}{8} \right\rangle$, whereas every graph with paired Jacobian $\left\langle \frac{1}{8} \right\rangle$ has cycle rank at least seven. In particular, a positive integral presentation of the negative pairing need not be a graph flow lattice.

Appendix C. The pairing of a complete graph

The integral cut and flow lattices of complete graphs are described in [3, Section 9].
Put

$$H = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad F = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}, \qquad \mathcal{E}_N = \big((\mathbb{Z}/N\mathbb{Z})^2, H/N\big), \qquad \mathcal{F}_N = \big((\mathbb{Z}/N\mathbb{Z})^2, F/N\big).$$

In the notation $\mathcal{F}_N$, assume $3 \nmid N$, so that the pairing is nonsingular. Here J_d is the $d \times d$ matrix all of whose entries are one, and I_d is the identity matrix.

$$P^{\mathsf{T}} B P \equiv B' \pmod N, \quad P \in \mathrm{GL}_d(\mathbb{Z}/N) \quad \Longrightarrow \quad \big((\mathbb{Z}/N)^d, B/N\big) \cong \big((\mathbb{Z}/N)^d, B'/N\big). \tag{C.1}$$

$$(\mathrm{Jac}(K_N), b_{K_N}) \cong ((\mathbb{Z}/N)^{N-2}, (I_{N-2} + J_{N-2})/N) \qquad (N \geq 3). \tag{C.2}$$

Theorem C.1. *For every integer $r \geq 3$,*

$$(\mathrm{Jac}(K_{2^r}), b_{K_{2^r}}) \cong \mathcal{E}_{2^r}^{\perp(2^{r-1}-1)}. \tag{C.3}$$

In particular,

$$(\mathrm{Jac}(K_8), b_{K_8}) \cong \mathcal{E}_8^{\perp 3}. \tag{C.4}$$

C.1. Divisor generators and their pairings.

Proposition C.2. *Let $N \geq 3$ and number the vertices of K_N by $1, \dots, N$. For $1 \leq i \leq N-2$, set $D_i = \mathbf{e}_i - \mathbf{e}_{N-1}$. The homomorphism*

$$(\mathbb{Z}/N\mathbb{Z})^{N-2} \longrightarrow \mathrm{Jac}(K_N), \qquad (a_i) \longmapsto \sum_{i=1}^{N-2} a_i [D_i] \tag{C.5}$$

is an isomorphism, and

$$b_{K_N}([D_i], [D_j]) = \frac{\delta_{ij} + 1}{N} \pmod{\mathbb{Z}}. \tag{C.6}$$

Consequently (C.2) *holds.*

Proof. The Laplacian is

$$L = N I_N - J_N. \tag{C.7}$$

Since $\sum_v (D_i)_v = 0$, one has $L D_i = N D_i$. Thus $N[D_i] = 0$, and (C.5) is well defined. For an arbitrary $D \in \mathrm{Div}^0(K_N)$, set $t = D_N$. The N-th coordinate of $L\mathbf{e}_1$ is -1; hence $D' = D + tL\mathbf{e}_1$ has $D'_N = 0$. It still has coordinate sum zero and represents the class of D. Therefore

$$D' = \sum_{i=1}^{N-2} D'_i (\mathbf{e}_i - \mathbf{e}_{N-1}). \tag{C.8}$$

This proves surjectivity of (C.5). Suppose $\sum_{i=1}^{N-2} a_i D_i = Lf$ for $f \in \mathbb{Z}^N$, and write $S = \sum_{v=1}^{N} f_v$. The N-th coordinate gives $0 = N f_N - S$. The i-th coordinate, for $i \leq N-2$, consequently gives

$$a_i = N f_i - S = N(f_i - f_N). \tag{C.9}$$

Thus every a_i is divisible by N, proving injectivity. The vector D_j/N is a rational potential for D_j by (C.7). Since $D_i^{\mathsf{T}} D_j = \delta_{ij} + 1$, Equation (2.2) gives (C.6). □

C.2. Hyperbolic reduction at the prime two.

C.2.1. *Quadratic forms over* $\mathbb{F}_2$. Let W be a finite-dimensional vector space over $\mathbb{F}_2$. A quadratic form $q : W \to \mathbb{F}_2$ has an associated bilinear form

$$\beta(x, y) = q(x + y) - q(x) - q(y). \tag{C.10}$$

The form q is nondegenerate when β is nondegenerate. The hyperbolic quadratic plane has coordinates (a, b) and $q(a, b) = ab$. A hyperbolic basis of a $2k$-dimensional quadratic space consists of vectors u_i, v_i with

$$q(u_i) = q(v_i) = 0, \qquad \beta(u_i, v_j) = \delta_{ij}, \qquad \beta(u_i, u_j) = \beta(v_i, v_j) = 0. \tag{C.11}$$

Define the integer

$$S(q) = \sum_{x \in W} (-1)^{q(x)}. \tag{C.12}$$

Lemma C.3. *A nondegenerate quadratic form on a $2k$-dimensional $\mathbb{F}_2$-vector space is hyperbolic if and only if $S(q) > 0$. In that case $S(q) = 2^k$.*

Proof. For $k = 0$, the space consists of its zero vector, $q(0) = 0$, and $S(q) = 1$; its empty basis is hyperbolic. Suppose $k \geq 1$ and $S(q) > 0$. The number of zeros is

$$\#q^{-1}(0) = \frac{2^{2k} + S(q)}{2} > 1. \tag{C.13}$$

Choose $u \neq 0$ with $q(u) = 0$. Nondegeneracy supplies v with $\beta(u, v) = 1$. Put $v' = v + q(v)u$. Equation (C.10) gives $q(v') = q(v) + q(v)\beta(v, u) = 0$ and $\beta(u, v') = 1$. The vectors u, v' are independent, since pairing a relation $au + bv' = 0$ with u, v' gives $b = a = 0$. Their polar matrix is H, so $U = \operatorname{span}\{u, v'\}$ is nondegenerate. For each $x \in W$, the vector

$$x - \beta(x, v')u - \beta(x, u)v' \tag{C.14}$$

is orthogonal to U. Since the polar form on U is nonsingular, $U \cap U^\perp = 0$, so $W = U \perp U^\perp$. The complement is nondegenerate because its radical would be orthogonal to all of W. On U, the quadratic form is $q(au + bv') = ab$, so $S(q|_U) = 2$. For an orthogonal decomposition the quadratic form is the sum of its restrictions, and summing independently over the two summands gives

$$S(q) = 2S(q|_{U^\perp}). \tag{C.15}$$

Thus the character sum of the complement is positive. Induction gives a hyperbolic basis of $U^\perp$, and adjoining u, v' gives one of W. Conversely, each hyperbolic plane has character sum 2; multiplicativity gives $S(q) = 2^k$ for an orthogonal sum of k such planes. □

Let B be a symmetric integral matrix with even diagonal. The expression $x^\mathsf{T} Bx$ is even for every integral x. Define

$$q_B(\bar{x}) = \frac{x^\mathsf{T} Bx}{2} \pmod 2, \qquad \bar{x} \in \mathbb{F}_2^d. \tag{C.16}$$

This is independent of the integral lift, because replacing x by $x + 2z$ changes the half-norm by

$$2x^\mathsf{T} Bz + 2z^\mathsf{T} Bz \equiv 0 \pmod 2. \tag{C.17}$$

Expanding $(x + y)^\mathsf{T} B(x + y)$ gives its polar form $\bar{x}^\mathsf{T}(B \bmod 2)\bar{y}$. Thus q_B is nondegenerate when $\det B$ is odd.

Lemma C.4. *For a nonnegative integer $d \equiv 6 \pmod 8$, the quadratic form q_B associated with $B = I_d + J_d$ is hyperbolic.*

Proof. The diagonal of B is 2. Expanding the determinant by multilinearity in the columns of $I_d + \mathbf{1}\mathbf{1}^\mathsf{T}$ gives

$$\det(I_d + J_d) = 1 + d. \tag{C.18}$$

Indeed, terms containing two columns equal to $\mathbf{1}$ vanish; the term containing none is 1, and each of the d terms containing exactly one is 1. Since d is even, (C.18) is odd. Therefore q_B is nondegenerate. Represent $\bar{x} \in \mathbb{F}_2^d$ by a vector with entries $0, 1$, and let w be the number of its nonzero entries. Then

$$x^{\mathsf{T}} B x = w + w^2, \qquad q_B(\bar{x}) = \frac{w(w+1)}{2} \pmod 2. \tag{C.19}$$

For integral $w \geq 0$, both $(-1)^{w(w+1)/2}$ and $\mathrm{Re}((1+i)i^w)$ have the successive values $1, -1, -1, 1$ as w runs modulo four. Hence the binomial formula gives

$$S(q_B) = \sum_{w=0}^{d} \binom{d}{w} (-1)^{w(w+1)/2} = \mathrm{Re}\left((1+i) \sum_{w=0}^{d} \binom{d}{w} i^w \right) \tag{C.20}$$

$$= \mathrm{Re}(1+i)^{d+1} = 2^{d/2}. \tag{C.21}$$

Indeed, for $d = 8t+6$, $(1+i)^{d+1} = 16^t(8-8i)$ and $8 \cdot 16^t = 2^{d/2}$. Lemma C.3 gives the hyperbolic decomposition. □

C.2.2. *Lifting modulo powers of two.*

Lemma C.5. *Let B be a symmetric integral $2k \times 2k$ matrix with even diagonal and odd determinant. If q_B is hyperbolic, then for every integer $s \geq 2$ there is a matrix $P \in \mathrm{GL}_{2k}(\mathbb{Z}/2^s\mathbb{Z})$ such that*

$$P^{\mathsf{T}} B P = H^{\perp k} \pmod{2^s}. \tag{C.22}$$

Proof. Fix $s \geq 2$ and induct on k. For $k = 0$, the empty matrix is invertible on the zero module and satisfies the asserted congruence. For $k > 0$, choose a hyperbolic basis of q_B, and lift its vectors to integral vectors whose reductions form that basis, denoted $u, v, w_1, \dots, w_{2k-2}$. Their column matrix has odd determinant, so it is invertible modulo 2^s. The first pair satisfies

$$u^{\mathsf{T}} B u \equiv v^{\mathsf{T}} B v \equiv 0 \pmod 4, \qquad u^{\mathsf{T}} B v \equiv 1 \pmod 2. \tag{C.23}$$

Suppose $2 \leq j < s$ and $u^{\mathsf{T}} B u$ is divisible by 2^j. For $\varepsilon \in \{0, 1\}$, replace u by $u + \varepsilon 2^{j-1} v$. Its norm is

$$u^{\mathsf{T}} B u + \varepsilon 2^j u^{\mathsf{T}} B v + \varepsilon^2 2^{2j-2} v^{\mathsf{T}} B v. \tag{C.24}$$

The last term is divisible by 2^{2j}, hence by 2^{j+1}. Write $u^{\mathsf{T}} B u = 2^j m$ and choose $\varepsilon \equiv m \pmod 2$. Since $u^{\mathsf{T}} B v$ is odd, $m + \varepsilon u^{\mathsf{T}} B v$ is even; hence (C.24) is divisible by 2^{j+1}. This replacement does not change u modulo two or the oddness of $u^{\mathsf{T}} B v$. Starting at $j = 2$ and repeating up to $j = s-1$ gives

$$u^{\mathsf{T}} B u \equiv 0 \pmod{2^s}. \tag{C.25}$$

When $s = 2$, (C.25) already follows from (C.23) and no replacement is made. Choose an odd integer c satisfying $c\, u^{\mathsf{T}} B v \equiv 1 \pmod{2^s}$ and replace v by cv. Its norm is still divisible by four, and now $u^{\mathsf{T}} B v \equiv 1 \pmod{2^s}$. Put $a = v^{\mathsf{T}} B v / 2$, an even integer, and replace v by $v - au$. The new norm and mixed pairing satisfy

$$(v - au)^{\mathsf{T}} B (v - au) = v^{\mathsf{T}} B v - 2a\, u^{\mathsf{T}} B v + a^2 u^{\mathsf{T}} B u \equiv 0 \pmod{2^s}, \tag{C.26}$$

$$u^{\mathsf{T}} B (v - au) \equiv 1 \pmod{2^s}. \tag{C.27}$$

Both replacements preserve v modulo two. Renaming this vector v, the Gram matrix of u, v is H modulo 2^s. For each remaining vector set

$$w_i' = w_i - (w_i^{\mathsf{T}} B v) u - (w_i^{\mathsf{T}} B u) v. \tag{C.28}$$

Set $\alpha_i = w_i^{\mathsf{T}} B v$ and $\beta_i = w_i^{\mathsf{T}} B u$. Then

$$(w_i')^{\mathsf{T}} B u = \beta_i - \alpha_i u^{\mathsf{T}} B u - \beta_i v^{\mathsf{T}} B u \equiv 0 \pmod{2^s}, \tag{C.29}$$

$$(w_i')^{\mathsf{T}} B v = \alpha_i - \alpha_i u^{\mathsf{T}} B v - \beta_i v^{\mathsf{T}} B v \equiv 0 \pmod{2^s}. \tag{C.30}$$

The two coefficients subtracted in (C.28) are even: the reductions of w_i are orthogonal to those of u, v in the original hyperbolic basis. Hence $w_i' \equiv w_i \pmod 2$. The full column matrix is still invertible modulo 2^s. Let $C = ((w_i')^{\mathsf{T}} B w_j')_{i,j}$. It is symmetric, has even diagonal, and has odd determinant, because modulo two it is the nonsingular complementary Gram matrix. For $y \in \mathbb{Z}^{2k-2}$, the equality

$$q_C(\bar{y}) = q_B\left(\sum_i \bar{y}_i \bar{w}_i'\right) \tag{C.31}$$

follows by taking the half-norm of $\sum_i y_i w_i'$. Thus q_C is the hyperbolic complement of the first plane in q_B. The induction hypothesis gives a congruence of C to $H^{\perp(k-1)}$ modulo 2^s. Extend that change of basis by the identity on u, v and compose it with the preceding column matrix. This proves (C.22). □

Proof of Theorem C.1. Set $N = 2^r$ and $d = N - 2$. Since $r \geq 3$, one has $d \equiv 6 \pmod 8$. Proposition C.2 gives the pairing matrix $(I_d + J_d)/N$ on $(\mathbb{Z}/N\mathbb{Z})^d$. By Lemma C.4, its associated quadratic form over $\mathbb{F}_2$ is hyperbolic, and Lemma C.5, with $s = r$, gives an invertible congruence

$$I_d + J_d \cong H^{\perp d/2} \pmod{2^r}. \tag{C.32}$$

Since $d/2 = 2^{r-1} - 1$, (C.1) gives (C.3). For $r = 3$, this is (C.4). □

Corollary C.6. *For $r \geq 3$ and $t \geq 1$, the paired group $\mathcal{E}_{2^r}^{\perp t(2^{r-1}-1)}$ is realized by a simple graph.*

Proof. Identify one vertex in each of t disjoint copies of K_{2^r}. Edges within one copy remain distinct, and distinct copies share no vertex other than the identified one; hence the resulting graph is simple. Apply Lemma 2.6 and Theorem C.1. □

Remark C.7. The identity $(\mathrm{Jac}(K_4), b_{K_4}) \cong \mathcal{F}_4$ occurs in [19, 20]. The relation $\mathcal{F}_4 \perp \mathcal{F}_4 \cong \mathcal{E}_4 \perp \mathcal{E}_4$ is [30, Table 1.2, relation (IV)]. Explicitly, the matrix

$$P = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 3 & 1 \\ 1 & 1 & 2 & 2 \end{pmatrix}$$

has determinant -1, and

$$P^{\mathsf{T}}(F \perp F)P = \begin{pmatrix} 4 & 5 & 8 & 8 \\ 5 & 8 & 16 & 12 \\ 8 & 16 & 40 & 25 \\ 8 & 12 & 25 & 20 \end{pmatrix} \equiv H \perp H \pmod 4.$$

Thus $(\mathrm{Jac}(K_4 \vee K_4), b_{K_4 \vee K_4}) \cong \mathcal{E}_4^{\perp 2}$. This is a counterexample to [20, Conjecture 27]. Theorem C.1 gives biconnected examples at every exponent 2^r with $r \geq 3$.

Appendix D. Explicit integral and arithmetic examples

D.1. **Pairings with minimum cycle ranks four and five.** Put

$$A = (\mathbb{Z}/3\mathbb{Z})^2 \oplus (\mathbb{Z}/9\mathbb{Z})^2 \oplus \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/23\mathbb{Z}, \qquad |A| = 83835,$$

and define

$$b_+ = \left\langle \tfrac{1}{3} \right\rangle \perp \left\langle \tfrac{1}{3} \right\rangle \perp \left\langle \tfrac{1}{9} \right\rangle \perp \left\langle \tfrac{1}{9} \right\rangle \perp \left\langle \tfrac{2}{5} \right\rangle \perp \left\langle \tfrac{1}{23} \right\rangle,$$
$$b_- = \left\langle \tfrac{2}{3} \right\rangle \perp \left\langle \tfrac{1}{3} \right\rangle \perp \left\langle \tfrac{1}{9} \right\rangle \perp \left\langle \tfrac{1}{9} \right\rangle \perp \left\langle \tfrac{2}{5} \right\rangle \perp \left\langle \tfrac{1}{23} \right\rangle.$$

Only $p = 3$ has local generator rank four. Here $N_3 = 115 \equiv 1 \pmod 3$, and the products of the three-primary Jordan determinants for b_+ and b_- are respectively 1 and 2 modulo three. Their full-rank characters are therefore $+1$ and -1. Theorem 5.15 gives

$$\mu(A, b_+) = 4, \qquad \mu(A, b_-) = 5.$$

There are two occupied scales at three, one at five and one at twenty-three. Each scale has two determinant square classes, giving $2^4 = 16$ pairing isometry classes on A. Exactly half have either value of the three-primary character, so eight have each minimum.

An explicit graph for b_+ is the vertex sum of a 15-cycle and a four-path banana with path lengths $9, 27, 6, 9$. The banana has 51 edges and 49 vertices, so the vertex sum has 63 vertices and 66 edges. Orient all four paths from one endpoint to the other. The differences between the paths of lengths $9, 9, 27$ and the path of length 6 form an integral flow basis with Gram matrix

$$C_+ = \begin{pmatrix} 15 & 6 & 6 \\ 6 & 15 & 6 \\ 6 & 6 & 33 \end{pmatrix}, \qquad \det C_+ = 5589 = 3^5 \cdot 23.$$

An obtuse-basis matrix is

$$\begin{pmatrix} 36 & -27 & 0 \\ -27 & 33 & -6 \\ 0 & -6 & 15 \end{pmatrix},$$

with cycle-support conorms $9, 27, 6, 9$. The negative discriminant at 3 is $\left\langle \frac{1}{3} \right\rangle \perp \left\langle \frac{1}{9} \right\rangle^{\perp 2}$ and at 23 is $\left\langle \frac{1}{23} \right\rangle$. The cycle of length fifteen adds $\left\langle \frac{1}{3} \right\rangle \perp \left\langle \frac{2}{5} \right\rangle$.

For b_-, take cycles of lengths three and nine, and the plane dual of the weighted tetrahedron with edge multiplicities

$$(m_{01}, m_{02}, m_{03}, m_{12}, m_{13}, m_{23}) = (2, 5, 19, 7, 2, 5).$$

Its reduced Laplacian is

$$C_- = \begin{pmatrix} 11 & -7 & -2 \\ -7 & 17 & -5 \\ -2 & -5 & 26 \end{pmatrix}, \qquad \det C_- = 3105 = 3^3 \cdot 5 \cdot 23.$$

The weighted tetrahedron has 4 vertices and 40 edges, so its plane dual has 38 vertices and 40 edges. Adjoining the two cycles by vertex sums gives 48 vertices and 52 edges. Every core edge of the dual tetrahedron is subdivided at least twice, so this graph is simple; the four paths and the cycle in the first example also have disjoint interiors and lengths at least two.

The local pairings follow from the congruences

$$U_+ = \begin{pmatrix} 1 & -2/5 & -2/7 \\ 0 & 1 & -2/7 \\ 0 & 0 & 1 \end{pmatrix}, \qquad U_+^{\mathsf{T}} C_+ U_+ = \operatorname{diag}(15, 63/5, 207/7),$$

$$U_- = \begin{pmatrix} 1 & 7/11 & 1/2 \\ 0 & 1 & 1/2 \\ 0 & 0 & 1 \end{pmatrix}, \qquad U_-^{\mathsf{T}} C_- U_- = \operatorname{diag}(11, 138/11, 45/2).$$

The matrices U_+ and U_- have determinant one and are integral at all primes dividing the corresponding determinants. At three the negative discriminant coefficients of C_+, at scales $3, 9, 9$, are $-1/5, -5/7, -7/23$, each a square modulo three. At twenty-three its coefficient is $-7/9 \equiv 12 = 9^2$. For C_- the coefficients are $-11/46$ at scale 3, $-2/5$ at scale 9, $-2/9$ at scale 5, and $-11/6$ at scale 23. Their respective residue classes are $1, 2, 2, 2$; the last is $5^2 \pmod{23}$. Finally the two nonsquare lines at scale nine become square lines, since

$$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}^{\mathsf{T}} (2I_2) \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = 4I_2,$$

and 4 is a unit square in $\mathbb{Z}_3$. This gives the stated pairings after adjoining the cycle summands.

For the first graph, adding either pairing at a new prime $\ell \equiv 1 \pmod 3$ keeps the minimum four; a prime $\ell \equiv 2 \pmod 3$ makes it five. For the second graph these conclusions are reversed. For instance adding either pairing on $\mathbb{Z}/11\mathbb{Z}$ lowers its minimum from five to four.

Two further examples have three and four occupied scales. Put

$$C^{(1)} = \begin{pmatrix} 3 & -3 & 0 & 0 \\ -3 & 13 & -5 & 0 \\ 0 & -5 & 340 & 0 \\ 0 & 0 & 0 & 1125 \end{pmatrix}, \qquad C^{(2)} = 15\begin{pmatrix} 5 & -5 & 0 & 0 \\ -5 & 11 & -3 & 0 \\ 0 & -3 & 339 & 0 \\ 0 & 0 & 0 & 1125 \end{pmatrix}.$$

Their negative discriminant pairings are respectively

$$\left\langle \tfrac{1}{15} \right\rangle \perp \left\langle \tfrac{1}{225} \right\rangle \perp \left\langle \tfrac{2}{3375} \right\rangle, \qquad \left\langle \tfrac{1}{15} \right\rangle \perp \left\langle \tfrac{2}{225} \right\rangle \perp \left\langle \tfrac{1}{3375} \right\rangle \perp \left\langle \tfrac{2}{50625} \right\rangle.$$

Indeed, the same matrix

$$U = \begin{pmatrix} 1 & 1 & 1/2 & 0 \\ 0 & 1 & 1/2 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

has determinant one and gives

$$U^{\mathsf{T}} C^{(1)} U = \operatorname{diag}(3, 10, 675/2, 1125), \qquad U^{\mathsf{T}} C^{(2)} U = \operatorname{diag}(75, 90, 10125/2, 16875).$$

The determinants are 15^6 and 15^{10}, so no other primes occur. The following rows list, in increasing primary scale, the unit coefficients of the negative discriminants modulo p and those of the displayed pairings:

	p	matrix coefficients	pairing coefficients
$C^{(1)}$	3	$(2, 1, 1)$	$(2, 1, 1)$
$C^{(1)}$	5	$(2, 4, 1)$	$(3, 4, 4)$
$C^{(2)}$	3	$(2, 2, 2, 2)$	$(2, 2, 2, 2)$
$C^{(2)}$	5	$(3, 3, 3, 2)$	$(3, 3, 2, 2)$

Every corresponding ratio is a square modulo p, hence a square unit in $\mathbb{Z}_p$ by Hensel's lemma. The primary cyclic pairings are therefore isometric.

Replacing the second basis vector by $e_1 + e_2$ gives integral orthogonal decompositions

$$C^{(1)} \cong [3] \perp \begin{pmatrix} 10 & -5 \\ -5 & 340 \end{pmatrix} \perp [1125], \qquad C^{(2)} \cong [75] \perp \begin{pmatrix} 90 & -45 \\ -45 & 5085 \end{pmatrix} \perp [16875].$$

The binary blocks are flow forms of three-path bananas of lengths $(5, 5, 335)$ and $(45, 45, 5040)$; the rank-one blocks are cycles. Thus both pairings have planar realizations of cycle rank four. For the first pairing, $d(A) = 3$, $N_5 = 3^6$, and $\alpha_5 \equiv 3 \cdot 4 \cdot 4 \equiv 3 \pmod 5$. Hence $\left(\frac{(-1)^3 N_5 \alpha_5}{5}\right) = -1$, excluding cycle rank three by Lemma 3.11. The second pairing has four generators and therefore cannot occur in smaller cycle rank.

D.2. **Two prime-complement pairings.**

D.2.1. *A genus-three prime progression.* For $t \geq 0$, put

$$C_t = 3\begin{pmatrix} 2 & -1 & 0 \\ -1 & 4 & -1 \\ 0 & -1 & 7 + 6t \end{pmatrix}, \qquad \ell_t = 47 + 42t. \tag{D.1}$$

Then $\det C_t = 27\ell_t$ and its row sums are $(3, 6, 18 + 18t)$. The symmetric ladder has rung lengths $3, 3$, two equal rail lengths $3, 3$, and end lengths $3, 18 + 18t$. The first progression primes include $47, 89, 131, 173$.

The full positive discriminant is

$$\mathcal{D}(C_t) \simeq \left\langle \tfrac{2}{3} \right\rangle^{\perp 3} \perp \left\langle \tfrac{189}{\ell_t} \right\rangle \tag{D.2}$$

for every $t \geq 0$, and in particular whenever ℓ_t is prime. At $t = 0$, $189 \equiv 1 \pmod{47}$.

Put

$$P = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}, \qquad Z_t = \ell_t P, \qquad h = 9e_3.$$

Put $d = 7 + 6t$ and $B_t = C_t/3$. Then

$$\operatorname{adj}(B_t) = \begin{pmatrix} 4d-1 & d & 1 \\ d & 2d & 2 \\ 1 & 2 & 7 \end{pmatrix}, \qquad \det B_t = 7d - 2 = \ell_t.$$

Consequently

$$C_t^{-1}(3Z_t) = \operatorname{adj}(B_t)P, \qquad Z_t^{\mathsf{T}} C_t^{-1} Z_t = \frac{\ell_t}{3} \begin{pmatrix} 7 & 9 & 3 \\ 9 & 2d+11 & 3d+3 \\ 3 & 3d+3 & 8d-1 \end{pmatrix},$$

and

$$Z_t^{\mathsf{T}} C_t^{-1} Z_t \equiv \frac{2}{3} I_3 \pmod{\operatorname{Mat}_3(\mathbb{Z})}, \qquad Z_t^{\mathsf{T}} C_t^{-1} h = (21, 27, 9)^{\mathsf{T}}.$$

The congruence follows from $d \equiv 1 \pmod 3$ and $\ell_t \equiv 2 \pmod 3$. Each column of Z_t is killed by three in the discriminant group. If a linear combination of them vanishes, pairing with each column makes every coefficient divisible by three. They therefore generate a nondegenerate subgroup of order 27. The class of h has norm $189/\ell_t$ and order ℓ_t, since $\ell_t h \in C_t\mathbb{Z}^3$ and $\gcd(189, \ell_t) = 1$. Their orthogonal sum has order $27\ell_t = \det C_t$. The unit-edge graph at $t = 0$ has 31 vertices and 33 edges. Its graph pairing is the negative of (D.2); its positive monodromy discriminant is (D.2).

D.2.2. *A two-primary target in a larger genus.* The matrix

$$C = \begin{pmatrix} 4 & -1 & 0 \\ -1 & 7 & -2 \\ 0 & -2 & 6 \end{pmatrix}$$

has determinant $146 = 2 \cdot 73$ and row sums $(3, 4, 4)$. Its symmetric ladder has rung lengths $1, 2$, rail lengths $2, 2$, and end lengths $3, 4$, hence 14 unit edges and 12 vertices. Since

$$C^{-1}e_3 = \frac{1}{146}(2, 8, 27)^{\mathsf{T}},$$

the class $[e_3]$ has order 146. In $D(C)$ the classes $z = 73[e_3]$ and $h = 2[e_3]$ satisfy

$$\operatorname{ord}(z) = 2, \quad \operatorname{ord}(h) = 73, \quad b(z,z) = \frac{1}{2}, \quad b(h,h) = \frac{54}{73}, \quad b(z,h) = 0 \mod \mathbb{Z}.$$

Thus $D(C) = \left\langle \frac{1}{2} \right\rangle \perp \left\langle \frac{54}{73} \right\rangle$. Here the genus exceeds the generator rank of the prescribed group, and the interior row sum remains even. Lemma 7.2 treats arbitrary two-primary pairings.

D.3. **An explicit genus-three coefficient progression.** Take $F = \mathbb{Q}$ throughout this subsection. Over $\mathbb{Q}_5$, consider the equation

$$f_5(x) = \prod_{i=0}^{3} \left((x-i)^2 - 5^{m_i} \right), \qquad (m_0, m_1, m_2, m_3) = (3, 3, 3, 6). \tag{D.3}$$

Its reduction is $\prod_{i=0}^{3}(x-i)^2$. The stable special fibre has two rational components, given by $y = \pm \prod_i (x-i)$, meeting in four rational nodes. Near the node at i, all the other factors form a formal square unit: their reduction at i is a product of squares of nonzero differences. Dividing y by its square root gives

$$y'^2 = (x-i)^2 - 5^{m_i}.$$

The coordinates $u = (x - i) - y'$, $v = (x - i) + y'$ give $uv = 5^{m_i}$, so the node is split of thickness m_i. Orient the four edges of its two-vertex length graph from the first vertex to the second. Their differences $e_i - e_4$, $1 \le i \le 3$, form an integral cycle basis. Its Gram matrix is

$$M = \operatorname{diag}(3,3,3) + 6\mathbf{1}\mathbf{1}^{\mathsf{T}} = \begin{pmatrix} 9 & 6 & 6 \\ 6 & 9 & 6 \\ 6 & 6 & 9 \end{pmatrix}. \tag{D.4}$$

It has determinant 189 and Smith factors $(3, 3, 21)$.

Put

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

One has

$$M^{-1} = \frac{1}{3} I_3 - \frac{2}{21}\mathbf{1}\mathbf{1}^{\mathsf{T}}, \qquad (7P)^{\mathsf{T}} M^{-1} (7P) = \frac{49}{3} I_3 + 7\mathbf{1}\mathbf{1}^{\mathsf{T}}, \qquad (7P)^{\mathsf{T}} M^{-1} (3e_1) = (-1,-1,6)^{\mathsf{T}}.$$

Moreover $M^{-1}(21P)$ is integral and $\det P = -4$ is prime to three. Thus the columns of $7P$ generate a nondegenerate subgroup isometric to $\left\langle \frac{1}{3} \right\rangle^{\perp 3}$. The class $3[e_1]$ is killed by seven and has norm $15/7 \equiv 1/7$, hence exact order seven. The displayed mixed pairings are integral. Since $27 \cdot 7 = \det M$, the entire pairing is

$$\mathcal{D}(M) = \left\langle \tfrac{1}{3} \right\rangle^{\perp 3} \perp \left\langle \tfrac{1}{7} \right\rangle. \tag{D.5}$$

For every prime $r \neq 5$, Proposition 9.10 computes the fixed torsion; for example the dimensions of the inertia invariants in $J[r]$ are 6 for $r = 3$, 4 for $r = 7$, and 3 for all other $r \neq 5$. The conductor exponent at five is three.

Over $\mathbb{Q}_{17}$, let

$$f_{17}(x) = (x^2 - 17)(x^2 - 1)(x^2 - 4)(x^2 - 9) = x^8 - 31x^6 + 287x^4 - 869x^2 + 612.$$

It has the split one-node reduction of Lemma 9.7 and discriminant valuation one. At three good auxiliary primes impose

$$\begin{aligned} f &\equiv x^8 + x + 2 && \pmod{19}, \\ f &\equiv x(x^7 + 5x + 11) && \pmod{23}, \\ f &\equiv (x^2 - 2)\prod_{i=0}^{5}(x - i) && \pmod{29}. \end{aligned}$$

Write $F_{19} = x^8 + x + 2$ and $F_{23} = x^7 + 5x + 11$ in their respective residue fields. The following identities hold:

p	$x^{p^{\deg F_p}} \bmod F_p$	R_p
19	x	$-9x^7 - 9x^6 + 3x^5 + 3x^4 - x^3 + x^2 - 7x + 4$
23	x	$-10x^5 + 3x^4 + 2x^3 + 3x^2 - x$

Here $R_{19} \equiv x^{19^4} - x \pmod{F_{19}}$ and $R_{23} \equiv x^{23} - x \pmod{F_{23}}$. Explicit Bézout identities $A_p F_p + B_p R_p = 1$ are given by

$$\begin{aligned} A_{19} &= 8x^6 + 3x^5 - 8x^4 + 9x^3 - 9x^2 + 7x, \\ B_{19} &= 3x^7 - 9x^6 + 7x^5 - 8x^4 + 6x^3 - 9x + 5, \\ A_{23} &= -4x^4 - 4x^3 - 5x^2 - x - 2, \\ B_{23} &= -5x^6 + 5x^5 + 4x^3 + 3x^2 - 8x + 2. \end{aligned}$$

The irreducible factors of $x^{p^d} - x$ are precisely the monic irreducible polynomials whose degrees divide d. The Frobenius remainder gives $F_{19} \mid x^{19^8} - x$, while its Bézout identity excludes factors

dividing $x^{19^4} - x$. The proper divisors $1, 2, 4$ of eight are thus excluded, so F_{19} is irreducible. Likewise $F_{23} \mid x^{23^7} - x$ and its Bézout identity exclude the only proper divisor, one, of seven. Thus F_{23} is irreducible. Finally $\left(\frac{2}{29}\right) = -1$, so $x^2 - 2$ is irreducible over $\mathbb{F}_{29}$. The displayed linear factors are distinct and have no root in common with their indicated irreducible factors. All three reductions are squarefree. Their factor degrees are (8), $(7, 1)$ and $(2, 1, 1, 1, 1, 1, 1)$.

Impose also $f \equiv f_5 \pmod{5^7}$ and $f \equiv f_{17} \pmod{17^2}$. A centered Chinese-remainder solution is

$$\begin{aligned} f_0(x) = x^8 &+ 23299921863x^7 - 12983375317x^6 - 56498183894x^5 \\ &- 104919389432x^4 - 111987034132x^3 + 2914642161x^2 \\ &+ 18799016500x - 64489145125. \end{aligned} \tag{D.6}$$

The full coefficient modulus is

$$M_0 = 5^7 \cdot 17^2 \cdot 19 \cdot 23 \cdot 29 = 286132578125. \tag{D.7}$$

For every $h \in \mathbb{Z}[x]$ of degree at most seven, let $C_h/\mathbb{Q}$ be the smooth projective model of

$$y^2 = f_0(x) + M_0 h(x). \tag{D.8}$$

The defining polynomial is squarefree and has Galois group S_8 over $\mathbb{Q}$ by Lemma 9.2. At five, Hensel factorization gives four monic quadratics $q_i \equiv (x - i)^2 - 5^{m_i} \pmod{5^7}$. Their discriminants have valuations m_i, since $m_i < 7$, and their pairwise resultants are units, since their reductions have distinct roots. More explicitly, write $q_i = (x - i)^2 + a_i(x - i) + b_i$, where $a_i \in 5^7\mathbb{Z}_5$ and $b_i \equiv -5^{m_i} \pmod{5^7}$. Completing the square gives

$$q_i = \left(x - i + \frac{a_i}{2}\right)^2 - d_i, \qquad d_i = \frac{a_i^2}{4} - b_i \equiv 5^{m_i} \pmod{5^7}.$$

The other three factors form a square unit in the completed local ring at i. Dividing y by its square root and then factoring the difference of two squares gives $uv = d_i$. Thus the four split node thicknesses remain $3, 3, 3, 6$. At seventeen the factorization in Lemma 9.7 gives one quadratic of discriminant valuation one and an unramified factor. Thus the split nodes have the same thicknesses throughout the coefficient class, and the component pairing is (D.5) at five, with toric rank one at seventeen. For every defining polynomial $f = f_0 + M_0 h$, the discriminant product formula gives

$$v_5(\operatorname{disc} f) = 3 + 3 + 3 + 6 = 15, \qquad v_{17}(\operatorname{disc} f) = 1.$$

Zarhin's theorem gives $\operatorname{End}_{\bar{\mathbb{Q}}}(\operatorname{Jac} C_h) = \mathbb{Z}$ for every h, and the split toric-rank-one fibre at seventeen implies $\rho_{h,r}(G_{\mathbb{Q}}) = \mathrm{GSp}_6(\mathbb{F}_r)$ for every sufficiently large prime r, with the bound depending on h, by Hall's theorem. Proposition 9.4 and the coefficient-coset count in the proof of Theorem 9.6 give a density-one subset of this coset with adelic index

$$2[\mathrm{Sp}_6(\mathbb{F}_2) : S_8] = \frac{2^{10}(2^2 - 1)(2^4 - 1)(2^6 - 1)}{8!} = 72.$$

For each member of that subset, Proposition 9.5 gives $\rho_{h,m}(G_{\mathbb{Q}}) = \mathrm{GSp}_6(\mathbb{Z}/m\mathbb{Z})$ for every odd $m \geq 1$.

D.4. **An index-two orthogonal sublattice of E_8.** Let Q be the E_8 Cartan matrix with diagonal entries two and entries minus one on the edges

$$(0, 1), (1, 2), (2, 3), (3, 4), (4, 5), (5, 6), (2, 7).$$

Its first seven leading principal submatrices are the Cartan matrices of $A_1, \dots, A_7$, with determinants $2, 3, 4, 5, 6, 7, 8$. Deleting the third vertex of A_7 leaves $A_2 \perp A_4$, whose determinant is $3 \cdot 5 = 15$. Expansion at the last row and column therefore gives $\det Q = 2 \det A_7 - \det A_2 \det A_4 = 16 - 15 = 1$. These leading determinants are positive, so Q is positive definite. Let $r = e_0$. The orthogonality equation for x is $2x_0 - x_1 = 0$. A basis of $r^{\perp}$ is

$$e_0 + 2e_1,\ e_2, \dots, e_7.$$

The lattice generated by r and these seven vectors has index two in E_8; its orthogonal factors have determinants two and two. The corresponding reflection is

$$s_r(x) = x - (x, r)r,$$

whose matrix has first row $(-1, 1, 0, \dots, 0)$ and whose remaining rows agree with the identity. Since $(r, r) = 2$, one has

$$s_r^2 = I, \qquad (s_r x, s_r y) = (x, y) - 2(x, r)(y, r) + 2(x, r)(y, r) = (x, y).$$

It acts by -1 on $\mathbb{Q}r$ and by $+1$ on $r^\perp \otimes \mathbb{Q}$, so its determinant is -1. If T is the matrix whose columns are $r, e_0 + 2e_1, e_2, \dots, e_7$, then $\det T = 2$ and $T^{\mathsf{T}} Q T = [2] \perp Q_{r^\perp}$. Since $\det Q = 1$, $\det Q_{r^\perp} = 2$.

D.5. **Cyclic pairings of order at most 2048.** Write $n = 2^k m$ with m odd and $\gcd(a, n) = 1$. By Theorems 4.11 and 4.16, the pairing $\left\langle \frac{a}{n} \right\rangle$ has no graph realization of cycle rank at most three precisely when

$$k \geq 3, \qquad a \equiv 1 \pmod 8, \qquad \left(\frac{a}{m}\right) = 1. \tag{D.9}$$

Orient the triangular prism on vertices U, V, a, b, c, d by the ordered edge list

$$UV,\ Ua,\ Ub,\ Vc,\ Vd,\ ab,\ ac,\ bd,\ cd.$$

The first five edges form a spanning tree. The rows of

$$B = \begin{pmatrix} 0 & 1 & -1 & 0 & 0 & 1 & 0 & 0 & 0 \\ -1 & 1 & 0 & -1 & 0 & 0 & 1 & 0 & 0 \\ -1 & 0 & 1 & 0 & -1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & -1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

have zero boundary and restrict to the identity matrix on the last four edges. If x is an integral flow, subtracting the linear combination of these rows with coefficients x_6, x_7, x_8, x_9 leaves a flow on the spanning tree. At a leaf of a tree the incidence equation makes the coefficient of its unique edge zero; induction on the number of edges makes the remaining flow zero. The identity submatrix also makes the four rows independent. Thus they form an integral basis of the cycle group. For $l = (l_1, \dots, l_9) \in \mathbb{Z}^9_{\geq 0}$, put

$$Q(l) = B \operatorname{diag}(l) B^{\mathsf{T}} = \begin{pmatrix} l_2 + l_3 + l_6 & l_2 & -l_3 & 0 \\ l_2 & l_1 + l_2 + l_4 + l_7 & l_1 & -l_4 \\ -l_3 & l_1 & l_1 + l_3 + l_5 + l_8 & l_5 \\ 0 & -l_4 & l_5 & l_4 + l_5 + l_9 \end{pmatrix}. \tag{D.10}$$

Lemma D.1. *Suppose $Q(l)$ is positive definite,* $\det Q(l) = n > 1$, *and $z \in \mathbb{Z}^4$ satisfies*

$$\gcd(n, w_1, w_2, w_3, w_4) = 1, \qquad -z^{\mathsf{T}} w \equiv a \pmod n, \qquad w = \operatorname{adj}(Q(l))z, \qquad \gcd(a, n) = 1.$$

Then $\left\langle \frac{a}{n} \right\rangle$ has a connected planar loopless realization of cycle rank at most four.

Proof. The edges with $l_i = 0$ form a forest. Otherwise a nonzero integral cycle supported on those edges would be an integral linear combination xB of the rows of B and would satisfy $xQ(l)x^{\mathsf{T}} = 0$, contrary to positive definiteness. Contract that forest. Restriction of a flow to the remaining edges is an integral isomorphism of cycle groups. Indeed, the incidence equation at a contracted vertex says that the sum of the prescribed boundary coefficients on the corresponding tree is zero. Leaf elimination therefore determines integral coefficients on its edges, and the last vertex equation is the sum of the preceding ones. The same elimination gives uniqueness. The contracted edges have zero length, so this isomorphism preserves the length form. Subdivide every remaining edge into l_i edges. Extension with constant coefficients on each subdivided path identifies the flow lattices. Thus the resulting connected planar graph has flow Gram matrix $Q(l)$ and cycle rank four. A loop of length

one gives an orthogonal summand [1] in its flow lattice. Delete any such loops. This preserves its finite discriminant pairing and yields a loopless graph of cycle rank at most four.

In $\mathbb{Z}^4/Q(l)\mathbb{Z}^4$, an integer t kills $[z]$ if and only if $tQ(l)^{-1}z = tw/n$ is integral. The least positive such t is $n/\gcd(n, w_1, w_2, w_3, w_4) = n$. Hence $[z]$ generates the whole cokernel, whose order is n. Its negative discriminant norm is $-z^{\mathsf{T}}w/n = a/n \pmod{\mathbb{Z}}$. The cut–flow anti-isometry identifies this pairing with the graph pairing. □

Proposition D.2. *There are* 391 *cyclic-pairing isometry classes of order at most* 2048 *satisfying* (D.9). *Of these,* 390 *have minimum cycle rank four, attained by planar loopless graphs. The remaining class is* $\left\langle \frac{1}{8} \right\rangle$, *whose minimum is seven.*

Proof. For $n = 2^k m$ with $k \geq 3$ and m odd, a unit square class with $a \equiv 1 \pmod 8$ is determined by the signs $\left(\frac{a}{p}\right)$, $p \mid m$. The condition $\left(\frac{a}{m}\right) = 1$ is $\prod_{p|m} \left(\frac{a}{p}\right)^{v_p(m)} = 1$. Write $\omega(m)$ for the number of distinct prime factors of m, and put

$$c(m) = \begin{cases} 2^{\omega(m)}, & m \text{ is a square,} \\ 2^{\omega(m)-1}, & m \text{ is not a square.} \end{cases}$$

The Chinese remainder theorem supplies every sign tuple. The numbers $\sum_{m \leq 2048/2^k,\ m \text{ odd}} c(m)$ are

k	3	4	5	6	7	8	9	10	11
	211	97	45	20	10	4	2	1	1.

Their sum is 391.

Each row (n, a, l, z) of Table 1 satisfies

$$\begin{aligned} \det Q(l)_{[1,j]} > 0 \quad (1 \leq j \leq 4), \qquad \det Q(l) = n, \\ \gcd(n, \operatorname{adj}(Q(l))z) = 1, \qquad -z^{\mathsf{T}} \operatorname{adj}(Q(l))z \equiv a \pmod n. \end{aligned} \tag{D.11}$$

Here the gcd includes all four coordinates. The determinants and cofactors are given by

$$\det M = \sum_{\sigma \in S_j} \operatorname{sgn}(\sigma) \prod_{i=1}^{j} M_{i,\sigma(i)}, \qquad (\operatorname{adj} Q)_{uv} = (-1)^{u+v} \det Q_{\widehat{v},\widehat{u}},$$

where M is a $j \times j$ matrix and $Q_{\widehat{v},\widehat{u}}$ has row v and column u deleted. These formulas, with the entries in (D.10), give (D.11) for every row. The pairs (n, a) in the table give 390 distinct lists of local unit square classes satisfying (D.9); together with $(8, 1)$ they exhaust the above count. Lemma D.1 gives the upper bound four for every row. Equation (D.9) excludes all ranks at most three. Theorem B.1 gives $\mu(\left\langle \frac{1}{8} \right\rangle) = 7$. □

For example, the edge lengths $(1, 2, 1, 1, 1, 2, 2, 0, 0)$ give

$$Q_{72} = \begin{pmatrix} 5 & 2 & -1 & 0 \\ 2 & 6 & 1 & -1 \\ -1 & 1 & 3 & 1 \\ 0 & -1 & 1 & 2 \end{pmatrix}, \qquad \det Q_{72} = 72.$$

The first adjugate diagonal is 23, so $5e_1$ has negative norm $-25 \cdot 23/72 \equiv 1/72 \pmod{\mathbb{Z}}$. It generates the entire cyclic cokernel. Thus $\mu(\langle 1/72 \rangle) = 4$.

TABLE 1. Integral presentations in (D.10).

n	a	$(l_1, \dots, l_9)$	(z_1, z_2, z_3, z_4)
16	1	(0, 0, 1, 1, 1, 2, 2, 0, 0)	(3, 0, 0, 0)
24	1	(1, 1, 1, 1, 1, 3, 0, 0, 0)	(4, 3, 0, 0)
32	1	(1, 0, 1, 1, 4, 1, 1, 0, 0)	(5, 0, 0, 0)
40	1	(1, 1, 0, 1, 2, 2, 2, 0, 0)	(5, 0, 6, 0)
48	1	(1, 2, 0, 1, 1, 2, 3, 0, 0)	(15, 0, 20, 0)
56	1	(0, 1, 1, 1, 2, 8, 0, 0, 0)	(35, 40, 0, 0)
64	1	(1, 3, 1, 1, 1, 1, 2, 0, 0)	(0, 5, 0, 0)
72	1	(1, 2, 1, 1, 1, 2, 2, 0, 0)	(49, 0, 0, 0)
72	17	(0, 0, 1, 1, 1, 2, 10, 0, 0)	(49, 0, 0, 0)
80	1	(0, 1, 1, 1, 5, 5, 0, 0, 0)	(42, 35, 0, 0)
88	1	(1, 1, 1, 1, 1, 11, 0, 0, 0)	(20, 11, 0, 0)
96	1	(0, 1, 1, 2, 6, 3, 0, 0, 0)	(20, 0, 0, 15)
104	1	(1, 1, 0, 1, 6, 2, 2, 0, 0)	(13, 0, 22, 0)
112	1	(0, 1, 1, 1, 2, 16, 0, 0, 0)	(21, 24, 0, 0)
120	1	(1, 1, 1, 5, 0, 8, 0, 0, 0)	(15, 10, 0, 6)
120	17	(1, 1, 2, 3, 0, 8, 0, 0, 0)	(105, 42, 0, 70)
128	1	(0, 0, 1, 1, 1, 2, 18, 0, 0)	(11, 0, 0, 0)
136	1	(3, 0, 2, 1, 1, 2, 3, 0, 0)	(43, 0, 0, 0)
144	1	(1, 3, 2, 2, 2, 1, 1, 0, 0)	(4, 0, 0, 3)
144	17	(1, 0, 1, 1, 20, 1, 1, 0, 0)	(77, 0, 0, 0)
152	1	(1, 1, 1, 1, 1, 19, 0, 0, 0)	(68, 57, 0, 0)
160	1	(1, 1, 0, 1, 2, 2, 10, 0, 0)	(15, 0, 18, 0)
168	1	(1, 2, 2, 3, 0, 7, 0, 0, 0)	(60, 63, 0, 140)
168	17	(0, 1, 1, 1, 2, 24, 0, 0, 0)	(77, 12, 0, 0)
176	1	(1, 2, 0, 1, 5, 2, 3, 0, 0)	(99, 0, 108, 0)
184	1	(0, 0, 1, 1, 1, 2, 26, 0, 0)	(157, 0, 0, 0)
192	1	(1, 1, 0, 1, 1, 4, 12, 0, 0)	(15, 0, 20, 0)
200	1	(4, 0, 1, 1, 2, 1, 6, 0, 0)	(18, 15, 0, 0)
200	17	(1, 0, 1, 1, 28, 1, 1, 0, 0)	(9, 0, 0, 0)
208	1	(0, 1, 1, 1, 5, 13, 0, 0, 0)	(154, 143, 0, 0)
216	1	(1, 1, 1, 1, 1, 27, 0, 0, 0)	(76, 57, 0, 0)
224	1	(0, 1, 1, 1, 2, 32, 0, 0, 0)	(91, 104, 0, 0)
232	1	(1, 1, 0, 1, 14, 2, 2, 0, 0)	(203, 0, 226, 0)
240	1	(1, 1, 2, 3, 0, 16, 0, 0, 0)	(15, 6, 0, 10)
240	17	(1, 1, 1, 5, 0, 16, 0, 0, 0)	(15, 10, 0, 6)
248	1	(0, 1, 1, 1, 10, 8, 0, 0, 0)	(31, 40, 0, 0)
256	1	(1, 0, 1, 1, 36, 1, 1, 0, 0)	(53, 0, 0, 0)
264	1	(5, 1, 1, 1, 1, 11, 0, 0, 0)	(84, 121, 0, 0)
264	17	(1, 1, 1, 1, 17, 3, 0, 0, 0)	(22, 45, 0, 0)
272	1	(2, 0, 1, 4, 7, 1, 2, 0, 0)	(90, 85, 0, 0)
280	1	(1, 1, 1, 4, 4, 5, 0, 0, 0)	(168, 90, 0, 175)
280	17	(0, 1, 1, 1, 2, 40, 0, 0, 0)	(63, 90, 0, 0)
288	1	(1, 0, 1, 1, 1, 4, 12, 0, 0)	(3, 4, 0, 0)
288	17	(1, 0, 1, 4, 17, 1, 1, 0, 0)	(91, 0, 0, 0)
296	1	(0, 0, 1, 1, 1, 2, 42, 0, 0)	(91, 0, 0, 0)
304	1	(0, 0, 1, 1, 2, 2, 25, 0, 0)	(281, 0, 0, 0)
312	1	(1, 1, 6, 3, 0, 8, 0, 0, 0)	(39, 66, 0, 52)
312	41	(1, 1, 1, 8, 0, 13, 0, 0, 0)	(66, 52, 0, 39)
320	1	(0, 1, 1, 1, 21, 5, 0, 0, 0)	(6, 5, 0, 0)
328	1	(4, 0, 1, 1, 1, 2, 10, 0, 0)	(103, 0, 0, 0)
336	1	(4, 1, 2, 1, 2, 7, 0, 0, 0)	(36, 28, 21, 0)
336	17	(0, 1, 1, 1, 2, 48, 0, 0, 0)	(161, 276, 0, 0)
344	1	(1, 1, 1, 1, 1, 43, 0, 0, 0)	(340, 301, 0, 0)
352	1	(0, 1, 1, 2, 6, 11, 0, 0, 0)	(276, 0, 0, 253)
360	1	(1, 2, 0, 1, 2, 2, 17, 0, 0)	(325, 0, 78, 0)
360	41	(1, 1, 0, 1, 22, 2, 2, 0, 0)	(105, 0, 136, 0)
368	1	(1, 1, 1, 1, 4, 16, 0, 0, 0)	(115, 136, 0, 0)
376	1	(0, 1, 1, 2, 9, 8, 0, 0, 0)	(141, 184, 0, 0)
384	1	(1, 1, 1, 1, 25, 3, 0, 0, 0)	(68, 51, 0, 0)
392	1	(4, 0, 1, 5, 6, 1, 2, 0, 0)	(120, 105, 0, 0)
392	17	(2, 0, 1, 4, 4, 1, 5, 0, 0)	(376, 0, 0, 329)
400	1	(9, 0, 1, 1, 12, 1, 1, 0, 0)	(337, 0, 0, 0)
400	17	(0, 0, 1, 1, 2, 2, 33, 0, 0)	(293, 0, 0, 0)
408	1	(1, 1, 1, 1, 1, 51, 0, 0, 0)	(164, 153, 0, 0)
408	41	(0, 1, 1, 6, 10, 3, 0, 0, 0)	(34, 234, 0, 255)
416	1	(1, 1, 0, 1, 6, 2, 10, 0, 0)	(195, 0, 210, 0)
424	1	(1, 1, 0, 1, 26, 2, 2, 0, 0)	(371, 0, 386, 0)
432	1	(1, 2, 0, 1, 13, 2, 3, 0, 0)	(75, 0, 100, 0)
440	1	(1, 1, 2, 8, 0, 11, 0, 0, 0)	(380, 374, 0, 385)
440	17	(1, 1, 5, 5, 0, 8, 0, 0, 0)	(385, 380, 0, 374)
448	1	(0, 1, 1, 1, 2, 64, 0, 0, 0)	(427, 40, 0, 0)
456	1	(0, 1, 1, 2, 30, 3, 0, 0, 0)	(76, 336, 0, 285)
456	41	(5, 1, 1, 1, 1, 19, 0, 0, 0)	(144, 95, 0, 0)
464	1	(0, 1, 1, 1, 5, 29, 0, 0, 0)	(90, 87, 0, 0)
472	1	(1, 1, 1, 1, 1, 59, 0, 0, 0)	(68, 59, 0, 0)
480	1	(1, 1, 1, 5, 0, 32, 0, 0, 0)	(105, 70, 0, 42)
480	17	(1, 1, 2, 3, 0, 32, 0, 0, 0)	(15, 6, 0, 10)
488	1	(0, 0, 1, 1, 2, 9, 10, 0, 0)	(102, 61, 0, 0)
496	1	(0, 1, 1, 1, 10, 16, 0, 0, 0)	(279, 336, 0, 0)
504	1	(5, 1, 1, 1, 4, 8, 0, 0, 0)	(105, 344, 0, 0)
504	65	(0, 1, 1, 1, 2, 72, 0, 0, 0)	(287, 180, 0, 0)
512	1	(2, 0, 1, 3, 4, 2, 5, 0, 0)	(97, 0, 0, 0)
520	1	(0, 1, 1, 1, 13, 13, 0, 0, 0)	(320, 117, 0, 0)
520	33	(0, 0, 1, 1, 1, 2, 74, 0, 0)	(147, 0, 0, 0)
528	1	(2, 1, 1, 4, 12, 3, 0, 0, 0)	(154, 84, 0, 231)
528	17	(1, 1, 1, 1, 9, 11, 0, 0, 0)	(372, 121, 0, 0)
536	1	(1, 1, 1, 1, 1, 67, 0, 0, 0)	(340, 335, 0, 0)
544	1	(1, 0, 1, 4, 33, 1, 1, 0, 0)	(293, 0, 0, 0)
552	1	(1, 1, 1, 1, 4, 24, 0, 0, 0)	(253, 192, 0, 0)
552	17	(1, 2, 2, 3, 0, 23, 0, 0, 0)	(264, 207, 0, 506)
560	1	(1, 2, 0, 5, 5, 2, 3, 0, 0)	(315, 0, 50, 392)
560	17	(0, 1, 1, 1, 2, 80, 0, 0, 0)	(7, 170, 0, 0)
568	1	(0, 1, 1, 5, 6, 8, 0, 0, 0)	(213, 224, 0, 0)
576	1	(1, 1, 1, 1, 1, 3, 24, 0, 0)	(476, 357, 0, 0)
576	17	(0, 0, 1, 1, 1, 2, 82, 0, 0)	(131, 0, 0, 0)
584	1	(1, 0, 1, 1, 4, 1, 25, 0, 0)	(477, 0, 0, 0)
592	1	(0, 1, 1, 1, 5, 37, 0, 0, 0)	(54, 37, 0, 0)
600	1	(4, 1, 1, 2, 14, 3, 0, 0, 0)	(10, 6, 0, 15)

TABLE 1. Integral presentations in (D.10).

n	a	$(l_1, \dots, l_9)$	(z_1, z_2, z_3, z_4)
600	73	$(1, 1, 1, 1, 1, 75, 0, 0, 0)$	$(208, 195, 0, 0)$
608	1	$(0, 1, 1, 2, 6, 19, 0, 0, 0)$	$(4, 0, 0, 551)$
616	1	$(0, 1, 1, 1, 2, 88, 0, 0, 0)$	$(511, 594, 0, 0)$
616	17	$(1, 2, 2, 7, 0, 11, 0, 0, 0)$	$(224, 539, 0, 330)$
624	1	$(1, 1, 1, 13, 0, 16, 0, 0, 0)$	$(117, 364, 0, 6)$
624	41	$(1, 1, 6, 3, 0, 16, 0, 0, 0)$	$(39, 66, 0, 52)$
632	1	$(0, 1, 1, 1, 26, 8, 0, 0, 0)$	$(553, 560, 0, 0)$
640	1	$(1, 1, 0, 1, 2, 2, 42, 0, 0)$	$(305, 0, 366, 0)$
648	1	$(1, 0, 1, 5, 8, 1, 5, 0, 0)$	$(455, 0, 0, 0)$
648	17	$(1, 0, 1, 1, 92, 1, 1, 0, 0)$	$(301, 0, 0, 0)$
656	1	$(1, 0, 1, 1, 1, 4, 28, 0, 0)$	$(345, 0, 0, 0)$
664	1	$(1, 1, 1, 1, 1, 83, 0, 0, 0)$	$(604, 581, 0, 0)$
672	1	$(1, 2, 10, 3, 0, 7, 0, 0, 0)$	$(12, 399, 0, 532)$
672	17	$(0, 1, 1, 1, 2, 96, 0, 0, 0)$	$(665, 132, 0, 0)$
680	1	$(0, 1, 1, 1, 45, 5, 0, 0, 0)$	$(408, 655, 0, 0)$
680	57	$(1, 2, 0, 1, 2, 2, 33, 0, 0)$	$(235, 0, 136, 0)$
688	1	$(0, 0, 1, 1, 1, 2, 98, 0, 0)$	$(467, 0, 0, 0)$
696	1	$(1, 1, 1, 8, 0, 29, 0, 0, 0)$	$(414, 58, 0, 435)$
696	17	$(1, 1, 14, 3, 0, 8, 0, 0, 0)$	$(87, 30, 0, 58)$
704	1	$(1, 1, 0, 1, 5, 4, 12, 0, 0)$	$(517, 0, 628, 0)$
712	1	$(3, 0, 2, 1, 1, 2, 19, 0, 0)$	$(227, 0, 0, 0)$
720	1	$(7, 1, 1, 2, 6, 5, 0, 0, 0)$	$(6, 10, 0, 15)$
720	41	$(0, 1, 1, 1, 5, 45, 0, 0, 0)$	$(208, 195, 0, 0)$
728	1	$(1, 1, 1, 4, 4, 13, 0, 0, 0)$	$(238, 598, 0, 91)$
728	33	$(0, 1, 1, 1, 2, 104, 0, 0, 0)$	$(161, 78, 0, 0)$
736	1	$(1, 1, 1, 1, 4, 32, 0, 0, 0)$	$(115, 120, 0, 0)$
744	1	$(1, 2, 2, 3, 0, 31, 0, 0, 0)$	$(276, 279, 0, 620)$
744	17	$(0, 1, 1, 1, 10, 24, 0, 0, 0)$	$(341, 36, 0, 0)$
752	1	$(0, 1, 1, 2, 9, 16, 0, 0, 0)$	$(47, 80, 0, 0)$
760	1	$(1, 1, 2, 8, 0, 19, 0, 0, 0)$	$(60, 228, 0, 285)$
760	33	$(1, 1, 9, 5, 0, 8, 0, 0, 0)$	$(95, 180, 0, 684)$
768	1	$(1, 2, 0, 1, 1, 3, 50, 0, 0)$	$(0, 69, 92, 0)$
776	1	$(23, 0, 2, 1, 1, 2, 3, 0, 0)$	$(641, 0, 0, 0)$
784	1	$(0, 0, 1, 1, 2, 2, 65, 0, 0)$	$(37, 0, 0, 0)$
784	17	$(2, 0, 1, 4, 23, 1, 2, 0, 0)$	$(696, 609, 0, 0)$
792	1	$(1, 1, 1, 1, 1, 99, 0, 0, 0)$	$(398, 363, 0, 0)$
792	89	$(0, 1, 1, 2, 14, 11, 0, 0, 0)$	$(492, 110, 0, 561)$
800	1	$(1, 0, 1, 4, 49, 1, 1, 0, 0)$	$(157, 0, 0, 0)$
800	17	$(0, 0, 1, 1, 1, 2, 114, 0, 0)$	$(509, 0, 0, 0)$
808	1	$(1, 1, 0, 1, 50, 2, 2, 0, 0)$	$(505, 0, 510, 0)$
816	1	$(0, 1, 1, 2, 54, 3, 0, 0, 0)$	$(34, 18, 0, 51)$
816	41	$(0, 0, 1, 1, 1, 10, 26, 0, 0)$	$(325, 0, 0, 0)$
824	1	$(0, 1, 1, 1, 34, 8, 0, 0, 0)$	$(721, 816, 0, 0)$
832	1	$(0, 1, 1, 1, 21, 13, 0, 0, 0)$	$(170, 39, 0, 0)$
840	1	$(3, 1, 2, 2, 2, 15, 0, 0, 0)$	$(812, 360, 0, 105)$
840	41	$(1, 1, 2, 3, 0, 56, 0, 0, 0)$	$(225, 126, 0, 70)$
840	73	$(1, 1, 1, 5, 0, 56, 0, 0, 0)$	$(135, 770, 0, 378)$
840	113	$(0, 1, 1, 1, 2, 120, 0, 0, 0)$	$(679, 600, 0, 0)$
848	1	$(0, 1, 1, 1, 5, 53, 0, 0, 0)$	$(458, 371, 0, 0)$
856	1	$(0, 0, 1, 1, 1, 2, 122, 0, 0)$	$(311, 0, 0, 0)$
864	1	$(0, 1, 1, 2, 6, 27, 0, 0, 0)$	$(92, 0, 0, 69)$
872	1	$(1, 1, 0, 1, 54, 2, 2, 0, 0)$	$(763, 0, 834, 0)$
880	1	$(1, 1, 5, 5, 0, 16, 0, 0, 0)$	$(605, 60, 0, 22)$
880	17	$(1, 1, 2, 11, 0, 16, 0, 0, 0)$	$(165, 374, 0, 140)$
888	1	$(1, 1, 18, 3, 0, 8, 0, 0, 0)$	$(333, 318, 0, 740)$
888	17	$(1, 1, 1, 8, 0, 37, 0, 0, 0)$	$(546, 740, 0, 111)$
896	1	$(0, 1, 1, 1, 2, 128, 0, 0, 0)$	$(203, 360, 0, 0)$
904	1	$(0, 0, 1, 1, 2, 10, 17, 0, 0)$	$(781, 0, 0, 0)$
912	1	$(1, 1, 1, 1, 9, 19, 0, 0, 0)$	$(576, 589, 0, 0)$
912	41	$(0, 1, 1, 10, 14, 3, 0, 0, 0)$	$(836, 672, 0, 171)$
920	1	$(0, 1, 1, 1, 61, 5, 0, 0, 0)$	$(46, 205, 0, 0)$
920	17	$(1, 1, 1, 1, 1, 115, 0, 0, 0)$	$(836, 805, 0, 0)$
928	1	$(1, 1, 0, 1, 14, 2, 10, 0, 0)$	$(667, 0, 722, 0)$
936	1	$(1, 3, 0, 2, 2, 4, 15, 0, 0)$	$(294, 572, 0, 897)$
936	17	$(1, 1, 0, 1, 58, 2, 2, 0, 0)$	$(195, 0, 590, 0)$
944	1	$(0, 0, 1, 2, 2, 5, 21, 0, 0)$	$(140, 0, 0, 59)$
952	1	$(1, 2, 5, 7, 0, 8, 0, 0, 0)$	$(119, 42, 0, 340)$
952	41	$(0, 1, 1, 1, 2, 136, 0, 0, 0)$	$(693, 748, 0, 0)$
960	1	$(1, 1, 2, 3, 0, 64, 0, 0, 0)$	$(345, 138, 0, 230)$
960	17	$(1, 1, 1, 5, 0, 64, 0, 0, 0)$	$(255, 170, 0, 102)$
968	1	$(0, 0, 1, 1, 1, 2, 138, 0, 0)$	$(757, 0, 0, 0)$
968	17	$(1, 0, 1, 1, 20, 1, 9, 0, 0)$	$(617, 0, 0, 0)$
976	1	$(0, 1, 1, 1, 5, 61, 0, 0, 0)$	$(714, 671, 0, 0)$
984	1	$(1, 1, 1, 1, 1, 123, 0, 0, 0)$	$(628, 615, 0, 0)$
984	17	$(0, 3, 4, 4, 7, 3, 0, 0, 0)$	$(574, 342, 861, 0)$
992	1	$(0, 1, 1, 1, 10, 32, 0, 0, 0)$	$(527, 640, 0, 0)$
1000	1	$(1, 1, 0, 1, 62, 2, 2, 0, 0)$	$(445, 0, 534, 0)$
1008	1	$(1, 1, 1, 1, 12, 16, 0, 0, 0)$	$(273, 832, 0, 0)$
1008	65	$(0, 1, 1, 1, 2, 144, 0, 0, 0)$	$(217, 900, 0, 0)$
1016	1	$(0, 1, 1, 1, 42, 8, 0, 0, 0)$	$(635, 664, 0, 0)$
1024	1	$(0, 0, 1, 1, 1, 2, 146, 0, 0)$	$(181, 0, 0, 0)$
1032	1	$(0, 1, 1, 6, 26, 3, 0, 0, 0)$	$(172, 1008, 0, 387)$
1032	65	$(5, 1, 1, 1, 1, 43, 0, 0, 0)$	$(1008, 559, 0, 0)$
1040	1	$(1, 1, 0, 1, 2, 10, 18, 0, 0)$	$(945, 0, 234, 0)$
1040	33	$(0, 1, 1, 1, 69, 5, 0, 0, 0)$	$(702, 755, 0, 0)$
1048	1	$(1, 1, 1, 1, 1, 131, 0, 0, 0)$	$(924, 917, 0, 0)$
1056	1	$(4, 1, 1, 2, 6, 11, 0, 0, 0)$	$(156, 286, 0, 429)$
1056	17	$(0, 1, 1, 2, 70, 3, 0, 0, 0)$	$(374, 204, 0, 561)$
1064	1	$(1, 2, 2, 7, 0, 19, 0, 0, 0)$	$(322, 665, 0, 646)$
1064	33	$(0, 1, 1, 1, 2, 152, 0, 0, 0)$	$(469, 114, 0, 0)$
1072	1	$(0, 0, 1, 1, 2, 2, 89, 0, 0)$	$(327, 0, 0, 0)$
1080	1	$(1, 1, 13, 5, 0, 8, 0, 0, 0)$	$(255, 170, 0, 102)$
1080	17	$(1, 1, 2, 8, 0, 27, 0, 0, 0)$	$(110, 66, 0, 165)$
1088	1	$(5, 0, 1, 13, 16, 1, 1, 0, 0)$	$(1073, 0, 0, 0)$
1096	1	$(1, 0, 1, 1, 12, 1, 17, 0, 0)$	$(829, 0, 0, 0)$
1104	1	$(1, 1, 1, 1, 4, 48, 0, 0, 0)$	$(115, 72, 0, 0)$
1104	17	$(0, 1, 1, 1, 5, 69, 0, 0, 0)$	$(118, 69, 0, 0)$
1112	1	$(1, 1, 1, 1, 1, 139, 0, 0, 0)$	$(196, 139, 0, 0)$

TABLE 1. Integral presentations in (D.10).

n	a	$(l_1, \dots, l_9)$	(z_1, z_2, z_3, z_4)
1120	1	(2, 1, 1, 3, 19, 5, 0, 0, 0)	(56, 125, 0, 0)
1120	17	(0, 1, 1, 1, 2, 160, 0, 0, 0)	(273, 150, 0, 0)
1128	1	(0, 1, 1, 2, 9, 24, 0, 0, 0)	(517, 360, 0, 0)
1128	41	(1, 2, 2, 3, 0, 47, 0, 0, 0)	(1104, 987, 0, 1034)
1136	1	(0, 1, 1, 5, 6, 16, 0, 0, 0)	(355, 360, 0, 0)
1144	1	(1, 1, 5, 8, 0, 13, 0, 0, 0)	(374, 130, 0, 429)
1144	41	(1, 1, 6, 8, 0, 11, 0, 0, 0)	(546, 462, 0, 1001)
1152	1	(1, 1, 3, 1, 2, 3, 15, 0, 0)	(679, 0, 0, 0)
1152	17	(1, 0, 1, 1, 164, 1, 1, 0, 0)	(707, 0, 0, 0)
1160	1	(1, 2, 0, 1, 2, 2, 57, 0, 0)	(125, 0, 812, 0)
1160	17	(0, 1, 1, 1, 13, 29, 0, 0, 0)	(670, 841, 0, 0)
1168	1	(0, 0, 1, 1, 2, 2, 97, 0, 0)	(163, 0, 0, 0)
1176	1	(7, 1, 10, 2, 2, 3, 0, 0, 0)	(28, 372, 0, 903)
1176	73	(0, 1, 1, 2, 78, 3, 0, 0, 0)	(1036, 156, 0, 777)
1184	1	(1, 1, 0, 1, 18, 2, 10, 0, 0)	(111, 0, 242, 0)
1192	1	(0, 0, 1, 1, 1, 2, 170, 0, 0)	(367, 0, 0, 0)
1200	1	(1, 4, 0, 1, 1, 9, 28, 0, 0)	(282, 705, 470, 0)
1200	73	(1, 2, 0, 1, 1, 2, 99, 0, 0)	(207, 0, 670, 0)
1208	1	(0, 1, 1, 1, 50, 8, 0, 0, 0)	(453, 536, 0, 0)
1216	1	(1, 1, 0, 1, 9, 4, 12, 0, 0)	(247, 0, 452, 0)
1224	1	(6, 0, 1, 3, 24, 1, 2, 0, 0)	(198, 561, 0, 374)
1224	89	(1, 0, 2, 3, 15, 2, 3, 0, 0)	(759, 0, 0, 374)
1232	1	(0, 1, 1, 1, 2, 176, 0, 0, 0)	(665, 110, 0, 0)
1232	17	(0, 1, 1, 1, 5, 77, 0, 0, 0)	(1046, 1001, 0, 0)
1240	1	(0, 1, 1, 1, 10, 40, 0, 0, 0)	(837, 1040, 0, 0)
1240	17	(0, 0, 1, 1, 2, 9, 26, 0, 0)	(522, 155, 0, 0)
1248	1	(1, 1, 6, 3, 0, 32, 0, 0, 0)	(741, 6, 0, 988)
1248	41	(1, 1, 1, 13, 0, 32, 0, 0, 0)	(273, 364, 0, 462)
1256	1	(1, 1, 0, 1, 78, 2, 2, 0, 0)	(1099, 0, 1242, 0)
1264	1	(0, 1, 1, 1, 26, 16, 0, 0, 0)	(553, 624, 0, 0)
1272	1	(1, 1, 1, 8, 0, 53, 0, 0, 0)	(750, 106, 0, 795)
1272	41	(1, 1, 26, 3, 0, 8, 0, 0, 0)	(159, 54, 0, 106)
1280	1	(0, 1, 1, 1, 85, 5, 0, 0, 0)	(378, 315, 0, 0)
1288	1	(0, 1, 1, 1, 2, 184, 0, 0, 0)	(63, 276, 0, 0)
1288	17	(1, 1, 1, 1, 4, 56, 0, 0, 0)	(851, 154, 0, 0)
1296	1	(0, 0, 1, 2, 2, 5, 29, 0, 0)	(244, 0, 0, 183)
1296	17	(1, 0, 1, 1, 1, 12, 20, 0, 0)	(805, 0, 0, 0)
1304	1	(0, 0, 1, 1, 1, 2, 186, 0, 0)	(1029, 0, 0, 0)
1312	1	(0, 0, 1, 1, 1, 10, 42, 0, 0)	(1009, 0, 0, 0)
1320	1	(1, 2, 2, 3, 0, 55, 0, 0, 0)	(84, 825, 0, 1100)
1320	41	(1, 1, 1, 5, 0, 88, 0, 0, 0)	(525, 220, 0, 1254)
1320	73	(1, 1, 2, 3, 0, 88, 0, 0, 0)	(375, 66, 0, 220)
1320	113	(1, 1, 2, 11, 0, 24, 0, 0, 0)	(385, 594, 0, 1050)
1328	1	(0, 0, 1, 2, 2, 9, 17, 0, 0)	(1324, 0, 0, 1245)
1336	1	(0, 1, 1, 2, 33, 8, 0, 0, 0)	(501, 624, 0, 0)
1344	1	(3, 1, 2, 2, 10, 7, 0, 0, 0)	(612, 476, 0, 357)
1344	17	(0, 1, 1, 1, 2, 192, 0, 0, 0)	(329, 516, 0, 0)
1352	1	(7, 0, 2, 1, 1, 2, 19, 0, 0)	(567, 0, 0, 0)
1352	33	(3, 0, 2, 1, 17, 2, 3, 0, 0)	(453, 0, 0, 0)
1360	1	(0, 1, 1, 1, 5, 85, 0, 0, 0)	(288, 85, 0, 0)
1360	57	(0, 0, 1, 1, 1, 2, 194, 0, 0)	(1119, 0, 0, 0)
1368	1	(0, 1, 1, 2, 14, 19, 0, 0, 0)	(48, 836, 0, 285)
1368	17	(2, 1, 1, 4, 4, 19, 0, 0, 0)	(624, 1292, 0, 627)
1376	1	(0, 1, 1, 2, 6, 43, 0, 0, 0)	(428, 0, 0, 387)
1384	1	(1, 1, 0, 1, 86, 2, 2, 0, 0)	(865, 0, 998, 0)
1392	1	(1, 1, 14, 3, 0, 16, 0, 0, 0)	(435, 1110, 0, 754)
1392	17	(1, 1, 1, 16, 0, 29, 0, 0, 0)	(1290, 1102, 0, 957)
1400	1	(0, 1, 1, 1, 58, 8, 0, 0, 0)	(1295, 1122, 0, 0)
1400	57	(0, 1, 1, 1, 2, 200, 0, 0, 0)	(1057, 1350, 0, 0)
1408	1	(1, 1, 1, 1, 25, 11, 0, 0, 0)	(60, 55, 0, 0)
1416	1	(5, 1, 1, 1, 1, 59, 0, 0, 0)	(852, 1003, 0, 0)
1416	65	(0, 1, 1, 2, 94, 3, 0, 0, 0)	(118, 852, 0, 885)
1424	1	(2, 0, 1, 3, 31, 2, 2, 0, 0)	(1389, 0, 0, 0)
1432	1	(1, 1, 1, 1, 1, 179, 0, 0, 0)	(1004, 895, 0, 0)
1440	1	(1, 2, 0, 2, 10, 5, 5, 0, 0)	(464, 0, 0, 345)
1440	41	(1, 1, 0, 1, 22, 2, 10, 0, 0)	(645, 0, 688, 0)
1448	1	(0, 0, 1, 1, 1, 18, 26, 0, 0)	(499, 0, 0, 0)
1456	1	(0, 0, 1, 1, 2, 2, 121, 0, 0)	(215, 0, 0, 0)
1456	33	(0, 1, 1, 1, 2, 208, 0, 0, 0)	(567, 754, 0, 0)
1464	1	(1, 1, 30, 3, 0, 8, 0, 0, 0)	(549, 462, 0, 1220)
1464	17	(1, 1, 1, 8, 0, 61, 0, 0, 0)	(138, 1220, 0, 915)
1472	1	(0, 0, 1, 1, 1, 2, 210, 0, 0)	(1269, 0, 0, 0)
1480	1	(0, 1, 1, 1, 13, 37, 0, 0, 0)	(340, 481, 0, 0)
1480	17	(1, 1, 0, 1, 2, 2, 98, 0, 0)	(525, 0, 296, 0)
1488	1	(4, 1, 2, 1, 2, 31, 0, 0, 0)	(1476, 868, 279, 0)
1488	17	(0, 1, 1, 1, 5, 93, 0, 0, 0)	(104, 1023, 0, 0)
1496	1	(1, 1, 1, 1, 1, 187, 0, 0, 0)	(244, 187, 0, 0)
1496	41	(0, 1, 1, 6, 10, 11, 0, 0, 0)	(102, 462, 0, 561)
1504	1	(0, 1, 1, 2, 9, 32, 0, 0, 0)	(423, 656, 0, 0)
1512	1	(1, 2, 2, 7, 0, 27, 0, 0, 0)	(532, 1155, 0, 36)
1512	17	(0, 1, 1, 1, 2, 216, 0, 0, 0)	(1379, 612, 0, 0)
1520	1	(1, 1, 9, 5, 0, 16, 0, 0, 0)	(855, 820, 0, 76)
1520	33	(1, 1, 2, 16, 0, 19, 0, 0, 0)	(1420, 836, 0, 665)
1528	1	(0, 0, 1, 1, 1, 2, 218, 0, 0)	(1185, 0, 0, 0)
1536	1	(0, 1, 1, 2, 102, 3, 0, 0, 0)	(916, 0, 0, 687)
1544	1	(1, 0, 1, 1, 220, 1, 1, 0, 0)	(1305, 0, 0, 0)
1552	1	(0, 0, 1, 1, 2, 2, 129, 0, 0)	(1429, 0, 0, 0)
1560	1	(1, 1, 1, 13, 0, 40, 0, 0, 0)	(741, 1430, 0, 180)
1560	17	(1, 1, 9, 4, 4, 5, 0, 0, 0)	(1092, 180, 130, 975)
1560	41	(1, 1, 2, 3, 0, 104, 0, 0, 0)	(1425, 1092, 0, 1430)
1560	73	(1, 1, 1, 5, 0, 104, 0, 0, 0)	(315, 650, 0, 1404)
1568	1	(4, 0, 1, 1, 1, 2, 50, 0, 0)	(1065, 0, 0, 0)
1568	17	(1, 0, 1, 3, 16, 2, 6, 0, 0)	(795, 0, 0, 0)
1576	1	(1, 1, 0, 1, 98, 2, 2, 0, 0)	(1379, 0, 1386, 0)
1584	1	(1, 2, 0, 1, 5, 2, 35, 0, 0)	(1045, 0, 228, 0)
1584	89	(0, 0, 1, 1, 1, 2, 226, 0, 0)	(761, 0, 0, 0)
1592	1	(0, 1, 1, 1, 66, 8, 0, 0, 0)	(199, 328, 0, 0)
1600	1	(1, 0, 1, 3, 4, 2, 22, 0, 0)	(567, 0, 0, 0)

TABLE 1. Integral presentations in (D.10).

n	a	$(l_1, \ldots, l_9)$	(z_1, z_2, z_3, z_4)
1600	17	(0, 0, 1, 1, 2, 17, 18, 0, 0)	(558, 465, 0, 0)
1608	1	(0, 1, 1, 14, 18, 3, 0, 0, 0)	(1340, 1296, 0, 1407)
1608	41	(5, 1, 1, 1, 1, 67, 0, 0, 0)	(1176, 1273, 0, 0)
1616	1	(0, 1, 1, 1, 5, 101, 0, 0, 0)	(154, 1515, 0, 0)
1624	1	(0, 1, 1, 1, 2, 232, 0, 0, 0)	(1365, 1160, 0, 0)
1624	17	(1, 1, 1, 1, 1, 203, 0, 0, 0)	(642, 203, 0, 0)
1632	1	(0, 1, 1, 2, 6, 51, 0, 0, 0)	(836, 0, 0, 663)
1632	41	(2, 1, 1, 8, 24, 3, 0, 0, 0)	(850, 1314, 0, 459)
1640	1	(1, 1, 0, 1, 102, 2, 2, 0, 0)	(615, 0, 344, 0)
1640	17	(0, 1, 1, 1, 109, 5, 0, 0, 0)	(1066, 1405, 0, 0)
1648	1	(0, 1, 1, 1, 34, 16, 0, 0, 0)	(1339, 1496, 0, 0)
1656	1	(1, 1, 1, 1, 4, 72, 0, 0, 0)	(253, 816, 0, 0)
1656	41	(0, 1, 1, 2, 41, 8, 0, 0, 0)	(1173, 1190, 0, 0)
1664	1	(1, 1, 0, 1, 6, 2, 42, 0, 0)	(1027, 0, 1106, 0)
1672	1	(1, 1, 1, 1, 17, 19, 0, 0, 0)	(1342, 1235, 0, 0)
1672	41	(0, 1, 1, 2, 30, 11, 0, 0, 0)	(1406, 198, 0, 1045)
1680	1	(3, 1, 1, 2, 6, 21, 0, 0, 0)	(410, 1386, 0, 1155)
1680	41	(1, 1, 1, 5, 0, 112, 0, 0, 0)	(1665, 70, 0, 462)
1680	73	(1, 1, 2, 3, 0, 112, 0, 0, 0)	(135, 1218, 0, 1610)
1680	113	(0, 1, 1, 1, 2, 240, 0, 0, 0)	(931, 360, 0, 0)
1688	1	(1, 1, 1, 1, 1, 211, 0, 0, 0)	(1612, 1477, 0, 0)
1696	1	(0, 0, 1, 1, 1, 2, 242, 0, 0)	(347, 0, 0, 0)
1704	1	(0, 1, 1, 5, 6, 24, 0, 0, 0)	(781, 576, 0, 0)
1704	17	(1, 2, 2, 3, 0, 71, 0, 0, 0)	(960, 1065, 0, 142)
1712	1	(1, 2, 0, 1, 53, 2, 3, 0, 0)	(963, 0, 1196, 0)
1720	1	(1, 1, 21, 5, 0, 8, 0, 0, 0)	(1505, 590, 0, 946)
1720	33	(1, 1, 2, 8, 0, 43, 0, 0, 0)	(1010, 86, 0, 1075)
1728	1	(1, 1, 0, 1, 13, 4, 12, 0, 0)	(165, 0, 220, 0)
1736	1	(0, 1, 1, 1, 10, 56, 0, 0, 0)	(403, 616, 0, 0)
1736	17	(0, 1, 1, 1, 2, 248, 0, 0, 0)	(1015, 1612, 0, 0)
1744	1	(0, 1, 1, 1, 5, 109, 0, 0, 0)	(346, 327, 0, 0)
1752	1	(1, 1, 1, 1, 1, 219, 0, 0, 0)	(1238, 1533, 0, 0)
1752	17	(0, 0, 1, 1, 1, 2, 250, 0, 0)	(959, 0, 0, 0)
1760	1	(1, 1, 2, 11, 0, 32, 0, 0, 0)	(605, 22, 0, 140)
1760	17	(1, 1, 5, 5, 0, 32, 0, 0, 0)	(165, 300, 0, 198)
1768	1	(1, 1, 0, 1, 110, 2, 2, 0, 0)	(1547, 0, 1634, 0)
1768	41	(0, 1, 1, 1, 45, 13, 0, 0, 0)	(782, 611, 0, 0)
1776	1	(1, 1, 1, 16, 0, 37, 0, 0, 0)	(618, 740, 0, 999)
1776	17	(1, 1, 18, 3, 0, 16, 0, 0, 0)	(111, 1434, 0, 740)
1784	1	(0, 1, 1, 1, 74, 8, 0, 0, 0)	(223, 352, 0, 0)
1792	1	(0, 1, 1, 1, 2, 256, 0, 0, 0)	(203, 232, 0, 0)
1800	1	(2, 0, 1, 3, 24, 1, 6, 0, 0)	(546, 1365, 0, 910)
1800	17	(2, 0, 1, 12, 23, 1, 2, 0, 0)	(1456, 1365, 0, 0)
1800	41	(5, 0, 3, 2, 2, 4, 7, 0, 0)	(246, 0, 410, 615)
1800	73	(1, 0, 1, 1, 1, 12, 28, 0, 0)	(217, 0, 0, 0)
1808	1	(0, 0, 1, 1, 1, 2, 258, 0, 0)	(85, 0, 0, 0)
1816	1	(1, 1, 1, 1, 1, 227, 0, 0, 0)	(1188, 1135, 0, 0)
1824	1	(1, 1, 1, 1, 121, 3, 0, 0, 0)	(836, 1779, 0, 0)
1824	41	(4, 1, 1, 2, 6, 19, 0, 0, 0)	(384, 1748, 0, 1311)
1832	1	(1, 1, 0, 1, 114, 2, 2, 0, 0)	(1145, 0, 1206, 0)
1840	1	(1, 1, 0, 1, 2, 2, 122, 0, 0)	(255, 0, 1426, 0)
1840	17	(0, 1, 1, 5, 33, 5, 0, 0, 0)	(506, 235, 0, 0)
1848	1	(1, 1, 1, 8, 0, 77, 0, 0, 0)	(444, 1694, 0, 693)
1848	65	(3, 7, 0, 8, 0, 11, 0, 0, 0)	(882, 594, 154, 1155)
1848	73	(1, 1, 10, 8, 0, 11, 0, 0, 0)	(1302, 836, 0, 693)
1848	89	(1, 1, 5, 8, 0, 21, 0, 0, 0)	(572, 1050, 0, 1155)
1856	1	(0, 1, 1, 1, 21, 29, 0, 0, 0)	(42, 1711, 0, 0)
1864	1	(0, 0, 1, 1, 1, 2, 266, 0, 0)	(527, 0, 0, 0)
1872	1	(1, 1, 1, 4, 12, 13, 0, 0, 0)	(330, 260, 0, 195)
1872	17	(0, 1, 1, 1, 5, 117, 0, 0, 0)	(386, 1365, 0, 0)
1880	1	(0, 1, 1, 1, 125, 5, 0, 0, 0)	(1128, 1865, 0, 0)
1880	33	(0, 1, 1, 2, 9, 40, 0, 0, 0)	(141, 830, 0, 0)
1888	1	(0, 1, 1, 2, 6, 59, 0, 0, 0)	(1028, 0, 0, 885)
1896	1	(1, 2, 2, 3, 0, 79, 0, 0, 0)	(924, 1659, 0, 316)
1896	17	(0, 1, 1, 1, 26, 24, 0, 0, 0)	(1343, 1644, 0, 0)
1904	1	(1, 2, 5, 7, 0, 16, 0, 0, 0)	(1309, 350, 0, 1700)
1904	41	(0, 1, 1, 1, 2, 272, 0, 0, 0)	(693, 1836, 0, 0)
1912	1	(1, 1, 2, 3, 16, 8, 0, 0, 0)	(1673, 1880, 0, 0)
1920	1	(1, 1, 1, 5, 0, 128, 0, 0, 0)	(615, 410, 0, 246)
1920	17	(1, 1, 2, 3, 0, 128, 0, 0, 0)	(255, 102, 0, 170)
1928	1	(1, 0, 2, 3, 7, 2, 11, 0, 0)	(699, 0, 0, 0)
1936	1	(0, 0, 1, 2, 2, 9, 25, 0, 0)	(212, 0, 0, 33)
1936	17	(0, 0, 1, 1, 2, 2, 161, 0, 0)	(805, 0, 0, 0)
1944	1	(1, 1, 1, 1, 1, 243, 0, 0, 0)	(508, 381, 0, 0)
1952	1	(1, 1, 0, 1, 30, 2, 10, 0, 0)	(549, 0, 750, 0)
1960	1	(1, 1, 0, 2, 2, 2, 81, 0, 0)	(642, 0, 0, 175)
1960	41	(1, 1, 0, 1, 2, 2, 130, 0, 0)	(585, 0, 1008, 0)
1968	1	(0, 1, 1, 6, 50, 3, 0, 0, 0)	(82, 138, 0, 123)
1968	17	(1, 2, 0, 1, 1, 2, 163, 0, 0)	(1155, 0, 574, 0)
1976	1	(1, 1, 9, 8, 0, 13, 0, 0, 0)	(1216, 1066, 0, 741)
1976	33	(1, 1, 6, 8, 0, 19, 0, 0, 0)	(130, 1216, 0, 1729)
1984	1	(0, 1, 1, 1, 10, 64, 0, 0, 0)	(1519, 1568, 0, 0)
1992	1	(0, 0, 1, 1, 2, 9, 42, 0, 0)	(910, 747, 0, 0)
1992	89	(1, 2, 2, 8, 15, 3, 0, 0, 0)	(830, 1737, 0, 0)
2000	1	(0, 1, 1, 1, 5, 125, 0, 0, 0)	(1602, 1335, 0, 0)
2008	1	(1, 1, 1, 1, 1, 251, 0, 0, 0)	(964, 753, 0, 0)
2016	1	(5, 1, 1, 1, 4, 32, 0, 0, 0)	(273, 928, 0, 0)
2016	65	(0, 1, 1, 1, 2, 288, 0, 0, 0)	(721, 1476, 0, 0)
2024	1	(1, 2, 2, 11, 0, 23, 0, 0, 0)	(748, 759, 0, 1564)
2024	17	(1, 1, 1, 1, 4, 88, 0, 0, 0)	(1173, 1980, 0, 0)
2032	1	(0, 1, 1, 1, 42, 16, 0, 0, 0)	(1143, 1248, 0, 0)
2040	1	(1, 1, 2, 3, 0, 136, 0, 0, 0)	(1425, 1326, 0, 340)
2040	41	(1, 1, 1, 8, 0, 85, 0, 0, 0)	(1194, 1700, 0, 255)
2040	73	(1, 1, 25, 5, 0, 8, 0, 0, 0)	(1275, 1940, 0, 1938)
2040	137	(1, 1, 1, 5, 0, 136, 0, 0, 0)	(1425, 340, 0, 1326)
2048	1	(1, 0, 3, 1, 2, 4, 28, 0, 0)	(357, 0, 0, 0)

References

[1] O. Amini, M. Baker, E. Brugallé and J. Rabinoff, *Lifting harmonic morphisms II: tropical curves and metrized complexes*, Algebra Number Theory **9** (2015), no. 2, 267–315. https://doi.org/10.2140/ant.2015.9.267.

[2] P. Aceto, D. McCoy and J. Park, *Definite fillings of lens spaces*, J. Differential Geom. **131** (2025), no. 1, 1–41. 10.4310/jdg/1755541518. https://arxiv.org/abs/2208.02586v2.

[3] R. Bacher, P. de la Harpe and T. Nagnibeda, *The lattice of integral flows and the lattice of integral cuts on a finite graph*, Bull. Soc. Math. France **125** (1997), 167–198. https://doi.org/10.24033/bsmf.2303.

[4] M. Baker and S. Norine, *Harmonic morphisms and hyperelliptic graphs*, Int. Math. Res. Not. IMRN **2009** (2009), no. 15, 2914–2955. 10.1093/imrn/rnp037.

[5] S. Bosch and D. Lorenzini, *Grothendieck's pairing on component groups of Jacobians*, Invent. Math. **148** (2002), no. 2, 353–396. 10.1007/s002220100195.

[6] H. Chen and B. Mohar, *The sandpile group of a polygon flower*, Discrete Appl. Math. **270** (2019), 68–82. 10.1016/j.dam.2019.07.020.

[7] H. Chen and B. Mohar, *The sandpile group of polygon rings and twisted polygon rings*, Graphs Combin. **38** (2022), no. 4, article 113. 10.1007/s00373-022-02514-x.

[8] L. Chua, M. Kummer and B. Sturmfels, *Schottky algorithms: classical meets tropical*, Math. Comp. **88** (2019), no. 319, 2541–2558. 10.1090/mcom/3406.

[9] J. Clancy, N. Kaplan, T. Leake, S. Payne and M. M. Wood, *On a Cohen–Lenstra heuristic for Jacobians of random graphs*, J. Algebraic Combin. **42** (2015), no. 3, 701–723. 10.1007/s10801-015-0598-x.

[10] J. H. Conway and N. J. A. Sloane, *Low-dimensional lattices. VI. Voronoi reduction of three-dimensional lattices*, Proc. Roy. Soc. London Ser. A **436** (1992), 55–68. https://doi.org/10.1098/rspa.1992.0004. https://neilsloane.com/doc/Me169.pdf.

[11] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, 3rd ed., Grundlehren 290, Springer, 1999, Chapter 10, Section 3.7.

[12] H. Davenport, *Multiplicative Number Theory*, third edition, revised by H. L. Montgomery, Graduate Texts in Mathematics 74, Springer-Verlag, New York, 2000.

[13] T. Dokchitser, V. Dokchitser, C. Maistret and A. Morgan, *Arithmetic of hyperelliptic curves over local fields*, Math. Ann. **385** (2023), 1213–1322. https://doi.org/10.1007/s00208-021-02319-y. https://arxiv.org/abs/1808.02936v2.

[14] F. Deloup and G. Massuyeau, *Quadratic functions and complex spin structures on three-manifolds*, Topology **44** (2005), 509–555. https://doi.org/10.1016/j.top.2004.11.003.

[15] P. G. Lejeune Dirichlet, *There are infinitely many prime numbers in all arithmetic progressions with first term and difference coprime*, English translation by R. Stephan of the 1837 paper. https://arxiv.org/abs/0808.1408.

[16] P. Deligne and D. Mumford, *The irreducibility of the space of curves of given genus*, Publ. Math. IHES **36** (1969), 75–109. https://doi.org/10.1007/BF02684599.

[17] A. L. Edmonds, *Homology lens spaces in topological 4-manifolds*, arXiv:math/0112245v1, 21 December 2001.

[18] M. H. Freedman, *The topology of four-dimensional manifolds*, J. Differential Geom. **17** (1982), no. 3, 357–453. Theorem 1.5. https://doi.org/10.4310/jdg/1214437136.

[19] L. Gaudet, D. Jensen, D. Ranganathan, N. Wawrykow and T. Weisman, *Realization of groups with pairing as Jacobians of finite graphs*, Ann. Comb. **22** (2018), 781–801. https://doi.org/10.1007/s00026-018-0406-0.

[20] L. Gaudet, D. Jensen, D. Ranganathan, N. Wawrykow and T. Weisman, *Realization of groups with pairing as Jacobians of finite graphs*, arXiv:1410.5144v2 (2017). https://arxiv.org/abs/1410.5144v2.

[21] J. E. Greene, *The lens space realization problem*, Ann. of Math. (2) **177** (2013), 449–511. https://doi.org/10.4007/annals.2013.177.2.3.

[22] C. Hall, *An open-image theorem for a general class of abelian varieties*, Bull. Lond. Math. Soc. **43** (2011), 703–711. https://doi.org/10.1112/blms/bdr004. Theorem 1 in arXiv:0803.1682.

[23] E. Hodges, *The distribution of sandpile groups of random graphs with their pairings*, Trans. Amer. Math. Soc. **377** (2024), no. 12, 8769–8815. 10.1090/tran/9244. arXiv:2311.07078v1 (2023), Corollaries 10.2 and 10.5.

[24] A. Kawauchi and S. Kojima, *Algebraic classification of linking pairings on 3-manifolds*, Math. Ann. **253** (1980), no. 1, 29–42. 10.1007/BF01457818.

[25] M. Kneser and D. Puppe, *Quadratische Formen und Verschlingungsinvarianten von Knoten*, Math. Z. **58** (1953), 376–384. https://webhomes.maths.ed.ac.uk/~v1ranick/papers/knespupp.pdf.

[26] V. Kurlin, *A complete isometry classification of 3-dimensional lattices*, preprint, April 2026. https://www.kurlin.org/projects/lattice-geometry/lattices3Dmaths.pdf.

[27] A. Landesman, A. A. Swaminathan, J. Tao and Y. Xu, *Hyperelliptic curves with maximal Galois action on the torsion points of their Jacobians*, Indiana Univ. Math. J. **69** (2020), no. 7, 2461–2492. https://doi.org/10.1512/iumj.2020.69.8178. https://arxiv.org/abs/1705.08777v3.

[28] A. Landesman, A. A. Swaminathan, J. Tao and Y. Xu, *Surjectivity of Galois representations in rational families of abelian varieties*, Algebra Number Theory **13** (2019), 995–1038. https://doi.org/10.2140/ant.2019.13.995.

[29] Y. Mandelshtam, *Nonnegative conorms, regular matroids, and the tropical Schottky problem*, arXiv:2608.28783, version 1 (28 August 2026). https://arxiv.org/abs/2608.28783.

[30] R. Miranda, *Nondegenerate symmetric bilinear forms on finite abelian 2-groups*, Trans. Amer. Math. Soc. **284** (1984), 535–542. https://doi.org/10.1090/S0002-9947-1984-0743731-1.

[31] H. H. Nguyen and M. M. Wood, *Local and global universality of random matrix cokernels*, Math. Ann. **391** (2025), 5117–5210. 10.1007/s00208-024-03050-0. arXiv:2210.08526v1 (2022), Theorem 1.22.

[32] V. V. Nikulin, *Integral symmetric bilinear forms and some of their applications*, Math. USSR Izv. **14** (1980), 103–167. 10.1070/IM1980v014n01ABEH001060.

[33] R. Schulze-Pillot, *Lecture Notes on Quadratic Forms and their Arithmetic*, arXiv:2008.12847v2. https://arxiv.org/abs/2008.12847v2.

[34] E. Selling, *Ueber die binären und ternären quadratischen Formen*, J. Reine Angew. Math. **77** (1874), 143–229. https://eudml.org/doc/148235.

[35] J. Shen, *Quantative universality for cokernels of matrices with symmetries*, arXiv:2601.09704v1 (2026). https://arxiv.org/abs/2601.09704.

[36] I. Shimada, *Involutions in the affine Conway group*, arXiv:2608.29065v1, 29 August 2026. https://arxiv.org/abs/2608.29065v1.

[37] F. Shokrieh, *The monodromy pairing and discrete logarithm on the Jacobian of finite graphs*, J. Math. Cryptol. **4** (2010), 43–56. 10.1515/JMC.2010.002.

[38] The Stacks Project Authors, *The Stacks Project*, Tags 0E00, 0E73 and 0E9C, nodal curves and the stack of stable curves. https://stacks.math.columbia.edu/tag/0E9C.

[39] C. T. C. Wall, *Quadratic forms on finite groups, and related topics*, Topology **2** (1963), 281–298. 10.1016/0040-9383(63)90012-0.

[40] M. M. Wood, *The distribution of sandpile groups of random graphs*, J. Amer. Math. Soc. **30** (2017), no. 4, 915–958. 10.1090/jams/866. Errata: https://people.math.harvard.edu/~mmwood/Publications/SandpileJAMSErrata.pdf.

[41] Y. G. Zarhin, *Hyperelliptic Jacobians without complex multiplication*, Math. Res. Lett. **7** (2000), 123–132. https://doi.org/10.4310/MRL.2000.v7.n1.a11. Theorem 2.1 in arXiv:math/9909052.

[42] X.-J. Zhu, *Finite quadratic modules and lattices*, Comm. Algebra **52** (2024), 604–629. https://doi.org/10.1080/00927872.2023.2245924. Preprint: https://arxiv.org/abs/2110.06783.

Toulouse, France
Email address: nifa.anass@gmail.com