PRIME-ORDER COMPLEMENTS IN PLANAR GRAPH JACOBIANS

ANASS NIFA

ABSTRACT. Let (A, b) be a finite abelian group with a nondegenerate symmetric pairing into $\mathbb{Q}/\mathbb{Z}$, and let $r(A)$ be its least number of generators. For infinitely many primes ℓ, we realize $(A, b) \perp \langle \kappa/\ell \rangle$ as the entire paired Jacobian of a simple planar biconnected graph, with one nonzero integer κ independent of ℓ. The primes avoid any prescribed finite set. Every vertex has degree two or three. The graphs have arbitrarily large prescribed girth, treewidth at most two, and cycle rank $\max\{1, r(A)\}$, which is optimal. For each cycle rank they are subdivisions of one fixed planar multigraph. We construct a family whose complementary orders form a primitive arithmetic progression; an explicit cofactor determines the complementary pairing. Dirichlet's theorem gives the prime-order conclusion. A separate construction retains outerplanarity, allowing parallel edges and unbounded degree. Finally, for $r \geq 3$, the paired Jacobian of K_{2^r} is the orthogonal sum of $2^{r-1} - 1$ hyperbolic planes over $\mathbb{Z}/2^r\mathbb{Z}$. The case K_8 contradicts the exceptional-pairing conjecture of Gaudet, Jensen, Ranganathan, Wawrykow and Weisman.

CONTENTS

2020 *Mathematics Subject Classification.* 05C25, 05C50, 05C10, 11E08, 11N13, 20K01.

Key words and phrases. Graph Jacobian, monodromy pairing, hyperbolic form, planar graph, prime-order completion, treewidth, finite abelian group.

1. Introduction

The Jacobian of a finite connected graph carries more information than its underlying abelian group. Its canonical symmetric pairing takes values in $\mathbb{Q}/\mathbb{Z}$, and a group isomorphism need not preserve this pairing. We study realization with the pairing prescribed. The main result realizes every finite nondegenerate symmetric pairing after adjoining one orthogonal summand of prime order. The realizing graphs are simple, planar and biconnected. Their cycle rank is the smallest possible, their degrees are two or three, and their girth has an arbitrary prescribed lower bound.

A *finite paired group* is a finite abelian group A with a symmetric bilinear map $b : A \times A \to \mathbb{Q}/\mathbb{Z}$ such that $b(x, A) = 0$ implies $x = 0$. Isometries preserve both the group and the pairing. Write $\perp$ for orthogonal sum, A_p for the p-primary subgroup with its restricted pairing, and $r(A)$ for the least number of generators of A. The zero group has order and exponent one, and $r(0) = 0$. For coprime integers a, n with $n \geq 2$, put

$$\left\langle \tfrac{a}{n} \right\rangle = \left(\mathbb{Z}/n\mathbb{Z},\ (x, y) \longmapsto \frac{axy}{n} \pmod{\mathbb{Z}} \right). \tag{1.1}$$

A cyclic pairing with denominator one denotes the zero group. For a connected graph G, put $\beta(G) = |E(G)| - |V(G)| + 1$. Graphs are finite, undirected and connected. They have no loops; parallel edges are permitted unless simplicity is stated, and every edge has weight one. A graph is *biconnected* if it has at least three vertices and remains connected after deletion of any vertex. It is *outerplanar* if it has a plane embedding with every vertex on the boundary of the unbounded face.

The integral cut and flow lattices give two presentations of the Jacobian [1]. Shokrieh identifies its monodromy pairing by rational potentials and by the inverse of a reduced Laplacian [14, Theorem 3.4 and Proposition 3.7]. We use the positive Laplacian: vertex degrees on the diagonal and negative edge multiplicities off the diagonal. With this convention, the cut lattice gives the monodromy pairing, whereas the flow lattice gives its negative. Section 8 proves this sign relation integrally. The decomposition of finite pairings into cyclic and rank-two summands is due to Wall [15]; Miranda treats the 2-primary normal forms [10]. We give the splitting arguments needed below rather than assume canonical normal forms.

1.1. Prime-order complements and minimum cycle rank.

Theorem 1.1. *Let (A, b) be a finite paired group. For every pair of integers $h \geq 1$ and $g \geq 3$, there are infinitely many primes ℓ not dividing $2h|A|$ and simple planar biconnected graphs G_ℓ such that*

$$(\mathrm{Jac}(G_\ell), b_{G_\ell}) \cong (A, b) \perp \left\langle \tfrac{\kappa}{\ell} \right\rangle, \qquad \ell \nmid \kappa, \tag{1.2}$$

where the nonzero integer κ is independent of ℓ. Every vertex has degree two or three, the girth is at least g, and the treewidth is at most two. Set $d = \max\{1, r(A)\}$. All the graphs G_ℓ can be chosen as subdivisions of one fixed planar multigraph Q_d, depending only on d, with

$$\beta(G_\ell) = d, \qquad \#\{v \in V(G_\ell) : \deg(v) = 3\} = 2d - 2. \tag{1.3}$$

The graph Q_1 is a triangle; Q_d is cubic for $d \geq 2$. The number d is the least possible cycle rank among all connected graphs with a paired Jacobian as in (1.2).

The graph Q_d is independent of the pairing, its exponent, and h, g. Its subdivision lengths depend on these data. When $d = 2$, Q_d has two vertices joined by three parallel edges; the final graphs are theta graphs. They are not required to be cubic: only the vertices inherited from Q_d have degree three. Nor is outerplanarity part of this conclusion. The prime ℓ and the isometry class of its cyclic pairing are not prescribed in advance. Choosing h divisible by a prescribed finite set of primes excludes that set from all complementary orders.

We prove a formula for every member of a family, before imposing primality. Theorem 9.3 constructs positive coprime integers u, v, a nonzero integer κ, and subdivisions Γ_t of Q_d, for every integer $t \geq 0$, such that

$$(\mathrm{Jac}(\Gamma_t), b_{\Gamma_t}) \cong (A, b) \perp \left\langle \tfrac{\kappa}{u+vt} \right\rangle, \qquad \gcd(u + vt, 2h|A|\kappa) = 1. \tag{1.4}$$

Only one path length varies with t. Dirichlet's theorem on primes in an arithmetic progression [6] then gives Theorem 1.1. No assertion about prime values of a polynomial of degree greater than one is used.

There are two distinct probabilistic antecedents. Nguyen and Wood [11, Theorem 1.22] prescribe an underlying finite group together with a cyclic complement whose prime factors avoid a fixed finite range. Hodges prescribes the pairings on finitely many primary subgroups of random graph Jacobians [9, Theorem 1.1 and Corollaries 10.2, 10.5]. His theorem extends Wood's result for the groups [16]; Clancy, Kaplan, Leake, Payne and Wood had treated the paired symmetric-matrix model [5]. Shen subsequently obtained quantitative universality for paired cokernels of symmetric random integral matrices with independent upper-triangular entries [13, Theorem 1.2]. These results distinguish a prescribed primary part from a prescribed entire cokernel. The assertion in Theorem 1.1 is the simultaneous prescription of the pairing on A, a complement of prime order, and the stated geometric restrictions with minimum cycle rank. No random-matrix or random-graph theorem is used in its proof.

The graphs in the construction are subdivisions of ladders. Chen and Mohar compute sandpile groups for polygon flowers [3] and for polygon rings, including ladder families [4]. The facial cycle basis and its tridiagonal determinant recurrence are established constructions. Here the lengths of the paths shared by adjacent faces are independent congruence variables. Their choice prescribes the primary pairings; a further choice of the diagonal entries makes the complementary determinant a primitive arithmetic progression.

1.2. **Outerplanar realization and prescribed primary parts.**

Theorem 1.2. *Let (A, b) be a finite paired group, and let $h \geq 1$ be an integer. There exist a biconnected outerplanar loopless multigraph G and a nondegenerate pairing c on a finite cyclic group C such that*

$$(\mathrm{Jac}(G), b_G) \cong (A, b) \perp (C, c), \qquad \gcd(|C|, 2h|A|) = 1. \tag{1.5}$$

The group C may be zero.

Section 7 proves this by a tridiagonal reduced Laplacian construction. Corollary 9.4 subsequently makes $|C|$ prime, with infinitely many possible primes. These outerplanar graphs may have parallel edges and unbounded degree. Thus the outerplanar conclusion is separate from the simple subcubic conclusion of Theorem 1.1. A complement cannot be omitted uniformly: the hyperbolic pairing on $(\mathbb{Z}/2\mathbb{Z})^2$ is not the entire paired Jacobian of any graph [7, Proposition 26]. Corollary 2.5 proves this obstruction from the Laplacian energy identity.

Corollary 1.3. *Let S be a finite set of primes, and let (A_p, b_p) be a finite paired p-group for each $p \in S$. For every integer $g \geq 3$, there are infinitely many pairwise nonisomorphic simple planar biconnected graphs G of maximum degree at most three and girth at least g such that*

$$(\mathrm{Jac}(G)_p, b_G|_{\mathrm{Jac}(G)_p}) \cong (A_p, b_p) \qquad (p \in S). \tag{1.6}$$

The groups A_p may be zero.

Apply Theorem 1.1 to $(A, b) = \perp_{p \in S} (A_p, b_p)$ and $h = \prod_{p \in S} p$. The complementary prime is outside S, so its primary parts at those primes vanish. Distinct complementary primes give different Jacobian orders and hence nonisomorphic graphs. An independent proof in Section 8 gives the vertex-replacement and subdivision formulas used to compare cycle lattices.

Without the graph restrictions, the existence in Corollary 1.3 already follows from the positive limiting probabilities in Hodges's theorem. His Laplacian has the opposite sign; replacing the prescribed pairing by its negative gives the present convention. The additional restrictions here are imposed together. Degree two could not replace degree three in a universal statement: a simple biconnected graph with maximum degree two is a cycle, whose Jacobian is cyclic. None of these results asserts exact realization of every finite pairing without a complementary summand.

1.3. **Complete graphs and hyperbolic pairings.** For $N \geq 2$, put

$$H = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \mathcal{E}_N = \left((\mathbb{Z}/N\mathbb{Z})^2,\ (x,y) \longmapsto \frac{x^{\mathsf{T}} H y}{N} \pmod{\mathbb{Z}} \right). \tag{1.7}$$

This is the hyperbolic pairing. For $N = 2^r$ the notation agrees with [7, Section 2.4].

Gaudet, Jensen, Ranganathan, Wawrykow and Weisman conjectured that $\mathcal{E}_{2^r}^{\perp k}$ is not the entire paired Jacobian of a graph for positive integers r, k [7, arXiv version 2, Conjecture 27]. Their observation that $\mathcal{E}_2$ can occur as a primary subgroup does not contradict this assertion. The following is an isometry of the entire paired group and does contradict it.

Theorem 1.4. *For every integer $r \geq 3$,*

$$(\mathrm{Jac}(K_{2^r}), b_{K_{2^r}}) \cong \mathcal{E}_{2^r}^{\perp(2^{r-1}-1)}. \tag{1.8}$$

In particular,

$$(\mathrm{Jac}(K_8), b_{K_8}) \cong \mathcal{E}_8^{\perp 3}. \tag{1.9}$$

The group $\mathrm{Jac}(K_N)$ and the associated integral lattices were already computed in [1, Section 9, pp. 194–195], which also discusses their Witt classes. Proposition 3.1 gives the pairing in explicit divisor coordinates:

$$(\mathrm{Jac}(K_N), b_{K_N}) \cong \left((\mathbb{Z}/N\mathbb{Z})^{N-2}, \frac{I_{N-2} + J_{N-2}}{N} \right), \qquad N \geq 3. \tag{1.10}$$

Here J_d is the all-ones matrix. For $N = 2^r$, $r \geq 3$, the half-norm of the numerator reduces to a hyperbolic quadratic form over $\mathbb{F}_2$. Successive integral changes of basis lift a hyperbolic quadratic basis to a bilinear hyperbolic basis modulo 2^r. This proves the isometry, not only equality of Witt classes.

1.4. **Cyclic pairings and their antecedents.** Every nondegenerate pairing on a nonzero cyclic group is $\left\langle \frac{a}{n} \right\rangle$ for some $n > a > 0$ with $\gcd(a, n) = 1$: if z is a generator and $b(z, z) = a/n$, a common divisor $d > 1$ would put the nonzero element $(n/d)z$ in the radical.

The negative continued fraction $n/a = [b_1, \ldots, b_\ell]^-$, with $b_i \geq 2$, determines a linear lattice with matrix

$$C_{ii} = b_i, \qquad C_{i,i+1} = C_{i+1,i} = -1, \qquad C_{ij} = 0 \quad (|i - j| > 1). \tag{1.11}$$

Greene realizes this matrix as a graph lattice [8, Section 3.3, p. 466]: join consecutive basis vertices, adjoin one further vertex, and add edges to it until the basis vertices have degrees b_i. Thus C is already a reduced Laplacian in that construction. The inverse-matrix pairing formula then gives cyclic realization. We include the argument to specify an integral generator, a rational potential and the vertex bound.

Proposition 1.5. *For $n > a > 0$ with $\gcd(n, a) = 1$, there is a connected planar loopless multigraph $G(n, a)$ and a generator $z \in \mathrm{Jac}(G(n, a))$ such that*

$$\mathrm{ord}(z) = n, \qquad b_{G(n,a)}(z, z) = \frac{a}{n} \pmod{\mathbb{Z}}. \tag{1.12}$$

The graph has at most n vertices. In particular, $(\mathrm{Jac}(G(n, a)), b_{G(n,a)}) \cong \left\langle \frac{a}{n} \right\rangle$.

Corollary 1.6. *Every finite paired group of odd order is the paired Jacobian of a connected planar loopless multigraph. For a nonzero group A, the graph can be chosen with at most $|A|$ vertices.*

This corollary follows from cyclic realization, the odd-primary decomposition and identification of one vertex in each graph. It is therefore a consequence of the antecedents just described. Gaudet et al. obtain odd-order realization under the generalized Riemann hypothesis [7, Theorem 2] and prove realization of cyclic 2-primary pairings [7, Theorem 25]. The continued-fraction proof used here requires no unproved number-theoretic hypothesis.

Bosch and Lorenzini realize every finite pairing by an arithmetical graph [2, Proposition 5.2]. Such a graph includes a primitive positive vertex-multiplicity vector R satisfying $MR = 0$; the constructions permit nonconstant R. This category is larger than ordinary graph Laplacians, whose kernel vector is $\mathbf{1}$. In particular, their theorem is not an exact ordinary-graph realization theorem. The distinction is retained throughout this paper.

1.5. **Congruences and the determinant construction.** For a nonsingular symmetric integral matrix C, write

$$\mathcal{D}(C) = \left(\mathbb{Z}^d/C\mathbb{Z}^d, (x,y) \longmapsto x^{\mathsf{T}}C^{-1}y \bmod \mathbb{Z}\right).$$

If $\mathcal{D}(C)_p$ has exponent p^e, the congruence $D \equiv C \pmod{p^{2e+1}}$ preserves its entire p-primary pairing (Lemma 7.2), including $p = 2$ and $e = 0$. We construct a presentation of A_p with $r(A_p)$ rows and append unimodular rows to reach the common size $\max\{1, \max_p r(A_p)\}$. Entrywise Chinese remainder congruences then give one tridiagonal matrix of size $\max\{1, r(A)\}$.

For a tridiagonal matrix with diagonal entries a_i and adjacent entries $-c_i$, its leading principal determinants satisfy

$$\Delta_0 = 1, \quad \Delta_1 = a_1, \quad \Delta_i = a_i\Delta_{i-1} - c_{i-1}^2\Delta_{i-2}.$$

At every extra prime dividing $\prod_i c_i$, suitable diagonal congruences give $\Delta_i \equiv 1$. At all other extra primes the recurrence excludes a common divisor of two consecutive Δ_i. Consequently, if $D = \det L$ and F is the preceding principal determinant, then $\gcd(D/|A|, F) = 1$. Varying only the last diagonal entry gives (1.4). The class $|A|[e_d]$ generates the whole complementary group; its self-pairing in the graph is $-|A|F/(u + vt)$. Both the complementary order and the numerator are thus determined.

The preceding manuscript [12] also uses rational potentials. Its graph H_{t+1} has pairing

$$\left\langle \tfrac{5}{8} \right\rangle^{\perp\lceil t/2\rceil} \perp \left\langle \tfrac{7}{8} \right\rangle^{\perp\lfloor t/2\rfloor} \qquad (t \geq 1); \tag{1.13}$$

see [12, Corollary 6.5]. This pairing has a self-value $5/8$, whereas the self-values of $\mathcal{E}_8^{\perp k}$ belong to $\frac{1}{4}\mathbb{Z}/\mathbb{Z}$. It therefore does not give the isometry (1.9). None of the proofs below depends on a theorem from that manuscript.

Section 2 fixes the pairing convention. Sections 3 and 4 prove the complete-graph formula. Sections 5 and 6 give cyclic and odd-order realization. Section 7 proves finite-congruence invariance and the outerplanar completion. Section 8 proves the integral cut–flow comparison and the vertex-replacement formulas. Finally, Section 9 constructs the primitive progression, realizes its matrices on Q_d, and proves the optimal cycle rank.

2. Rational potentials and reduced Laplacians

Let $V = V(G)$, and let m_{vw} be the number of edges between distinct vertices v, w. The positive Laplacian is

$$(L_G x)_v = \sum_{w \neq v} m_{vw}(x_v - x_w). \tag{2.1}$$

Define

$$\mathrm{Div}^0(G) = \left\{ D \in \mathbb{Z}^V \,:\, \sum_{v \in V} D_v = 0 \right\}, \qquad \mathrm{Jac}(G) = \mathrm{Div}^0(G)/L_G\mathbb{Z}^V. \tag{2.2}$$

The image $L_G\mathbb{Z}^V$ lies in $\mathrm{Div}^0(G)$ because L_G is symmetric and has zero row sums. For the graph on one vertex this group is zero. An empty matrix has determinant one and presents the zero paired group.

For $x \in \mathbb{R}^V$, expansion of (2.1) gives

$$x^{\mathsf{T}}L_G x = \sum_{\{v,w\} \subset V} m_{vw}(x_v - x_w)^2. \tag{2.3}$$

Connectedness implies $\ker_{\mathbb{Q}} L_G = \mathbb{Q}\mathbf{1}$: equality to zero in (2.3) implies equality of the coordinates at the ends of every edge. Symmetry and the rank $|V|-1$ then give

$$L_G\mathbb{Q}^V = \left\{ D \in \mathbb{Q}^V \,:\, \sum_{v\in V} D_v = 0 \right\}. \tag{2.4}$$

A vector $x_D \in \mathbb{Q}^V$ with $L_G x_D = D$ is called a rational potential for D.

Lemma 2.1. *For every nonsingular integral matrix C of size d, one has*

$$\left|\mathbb{Z}^d / C\mathbb{Z}^d\right| = |\det C|. \tag{2.5}$$

For $d = 0$, both sides are one. A positive definite real symmetric matrix has positive determinant.

Proof. Induct on d. The assertion for $d = 0$ follows from the stated conventions. For $d > 0$, the first column is nonzero. If a, b are two integers not both zero, put $g = \gcd(a, b) > 0$ and choose $u, v \in \mathbb{Z}$ with $ua + vb = g$. Then

$$\begin{pmatrix} u & v \\ -b/g & a/g \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} g \\ 0 \end{pmatrix}, \qquad \det \begin{pmatrix} u & v \\ -b/g & a/g \end{pmatrix} = 1.$$

Apply these operations to the first column, permitting also row permutations and changes of sign. A permutation first puts a nonzero entry in the first row; successive two-row operations eliminate the remaining entries. For a one-row matrix, a change of sign makes the entry positive. There is $U \in \mathrm{GL}_d(\mathbb{Z})$ such that

$$UC = \begin{pmatrix} g & w \\ 0 & C_1 \end{pmatrix}, \qquad g > 0, \tag{2.6}$$

where C_1 is nonsingular. Multiplication by U induces an isomorphism of cokernels and changes the determinant at most by a sign.

Projection onto the last $d-1$ coordinates induces a surjection from the cokernel in (2.6) onto $\mathbb{Z}^{d-1}/C_1\mathbb{Z}^{d-1}$. If the last coordinates of a representative are $C_1 z$, subtraction of $(UC)(0, z)^{\mathsf{T}}$ leaves a multiple of e_1. Moreover,

$$k e_1 = (UC)(m, z)^{\mathsf{T}} \implies C_1 z = 0 \implies z = 0, \quad k = gm.$$

Thus the kernel is cyclic of order g. Every fibre of the surjection is a coset of that kernel. By induction the order of the cokernel is $g|\det C_1| = |\det C|$, proving (2.5).

For the last assertion, induct on the size of a positive definite real symmetric matrix. Write it as $C = \left(\begin{smallmatrix} a & b^{\mathsf{T}} \\ b & D \end{smallmatrix}\right)$. Then $a > 0$, and for $y \neq 0$,

$$y^{\mathsf{T}}(D - a^{-1} b\, b^{\mathsf{T}})y = (-a^{-1} b^{\mathsf{T}} y, y)^{\mathsf{T}} C (-a^{-1} b^{\mathsf{T}} y, y) > 0.$$

Subtracting b_i/a times the first row from row $i+1$ gives $\det C = a \det(D - a^{-1} b\, b^{\mathsf{T}}) > 0$ by induction. The size-one assertion is $a > 0$. □

Lemma 2.2. *Assume $|V| \geq 2$, fix $o \in V$, and let A be the matrix obtained from L_G by deleting row and column o. Then A is positive definite, and restriction to $V \setminus \{o\}$ induces an isomorphism*

$$\mathrm{Jac}(G) \cong \mathbb{Z}^{V\setminus\{o\}} / A\mathbb{Z}^{V\setminus\{o\}}. \tag{2.7}$$

In particular, $\mathrm{Jac}(G)$ *is finite and has order* $\det A$.

Proof. Given $y \in \mathbb{R}^{V\setminus\{o\}}$, extend it by $x_o = 0$. Then $y^{\mathsf{T}} A y = x^{\mathsf{T}} L_G x \geq 0$. Equality implies that x is constant; its coordinate at o is zero, so $y = 0$. This proves positive definiteness.

Restriction $\rho : \mathrm{Div}^0(G) \to \mathbb{Z}^{V\setminus\{o\}}$ has inverse

$$(\rho^{-1} y)_v = y_v \ (v \neq o), \qquad (\rho^{-1} y)_o = -\sum_{v\neq o} y_v. \tag{2.8}$$

For $v \neq o$, one has $\rho(L_G \mathbf{e}_v) = A\mathbf{e}_v$. The identity $L_G\mathbf{1} = 0$ gives $\rho(L_G\mathbf{e}_o) = -\sum_{v\neq o} A\mathbf{e}_v$. Hence $\rho(L_G\mathbb{Z}^V) = A\mathbb{Z}^{V\setminus\{o\}}$, proving (2.7). Finally, $\det A$ is a nonzero integer and $A\,\mathrm{adj}(A) = (\det A)I$. The cokernel is generated by $|V|-1$ elements and annihilated by $\det A$, so it is finite. Lemma 2.1 gives its order $\det A$, which is positive because A is positive definite. □

Lemma 2.3. *For $D, E \in \mathrm{Div}^0(G)$, the formula*

$$b_G([D],[E]) = D^{\mathsf{T}} x_E \pmod{\mathbb{Z}}, \qquad L_G x_E = E, \tag{2.9}$$

defines a nondegenerate symmetric bilinear pairing on $\mathrm{Jac}(G)$. *In the reduced coordinates of Lemma 2.2, it is*

$$b_G([u],[v]) = u^{\mathsf{T}} A^{-1} v \pmod{\mathbb{Z}}. \tag{2.10}$$

Proof. Two rational potentials for E differ by a constant vector, which pairs to zero with D. Replacing D by $D + L_G f$, with $f \in \mathbb{Z}^V$, changes $D^{\mathsf{T}} x_E$ by $f^{\mathsf{T}} E \in \mathbb{Z}$. Replacing E by $E + L_G h$, with $h \in \mathbb{Z}^V$, permits replacing x_E by $x_E + h$ and changes the value by $D^{\mathsf{T}} h \in \mathbb{Z}$. Thus (2.9) is well defined. Potentials add under addition of divisors, so the pairing is bilinear. If $L_G x_D = D$, symmetry follows from

$$D^{\mathsf{T}} x_E = x_D^{\mathsf{T}} L_G x_E = E^{\mathsf{T}} x_D. \tag{2.11}$$

Suppose $[D]$ pairs to zero with every class. Subtract a constant from x_D so that $x_{D,o} = 0$. Pairing with $\mathbf{e}_v - \mathbf{e}_o$ and using (2.11) gives $x_{D,v} \in \mathbb{Z}$ for every v. Therefore $D = L_G x_D$ is principal. For (2.10), extend $A^{-1}v$ by zero at o. The resulting vector has Laplacian $\rho^{-1}v$: equality holds away from o, and the remaining coordinate follows from the zero sum. Substitution in (2.9) proves the formula. □

Lemma 2.4. *Let e be an edge of a connected loopless multigraph, with distinct endpoints v, w. Put $D = e_v - e_w$, choose $L_G x = D$, and set $\rho_e = x_v - x_w$. Then $0 < \rho_e \leq 1$. If $G - e$ contains a path from v to w, then $\rho_e < 1$.*

Proof. For an edge f with endpoints a_f, b_f, put $d_f = x_{a_f} - x_{b_f}$. Its square is independent of their order. The energy identity gives

$$\rho_e = D^{\mathsf{T}} x = x^{\mathsf{T}} L_G x = \rho_e^2 + \sum_{f\neq e} d_f^2. \tag{2.12}$$

The vector x is not constant, since $L_G x = D \neq 0$. Connectedness therefore gives $\rho_e > 0$. The inequality $\rho_e \geq \rho_e^2$ implies $\rho_e \leq 1$. If $\rho_e = 1$, every d_f with $f \neq e$ is zero. Along a path from v to w avoiding e, summing the signed values d_f would then give $x_v - x_w = 0$, a contradiction. □

Corollary 2.5. *If $b_G(z,z) = 0$ for every $z \in \mathrm{Jac}(G)$, then $\mathrm{Jac}(G) = 0$. Consequently, $\mathcal{E}_2^{\perp k}$ is not the paired Jacobian of a graph for any $k \geq 1$.*

Proof. For every edge $e = vw$, Lemma 2.3 gives $b_G([e_v - e_w],[e_v - e_w]) = \rho_e \bmod \mathbb{Z}$. The hypothesis and Lemma 2.4 imply $\rho_e = 1$. Hence $G - e$ has no path joining the endpoints of e. Choose a spanning tree by successively adjoining an edge reaching a new vertex. An edge outside that tree would have its endpoints joined by the tree path, contrary to the preceding conclusion. Thus G is a tree.

Fix a root o. For each edge e of the tree, let w_e be its endpoint farther from o and v_e its other endpoint. Let f_e be the characteristic function of the component of $G - e$ containing w_e. Only e joins that component to its complement, so $L_G f_e = e_{w_e} - e_{v_e}$. For every vertex v, summing these identities over the root path from o to v expresses $e_v - e_o$ as an integral Laplacian. These differences generate $\mathrm{Div}^0(G)$; hence $\mathrm{Jac}(G) = 0$. For $\mathcal{E}_2^{\perp k}$, the self-pairing of $(a_1, b_1, \ldots, a_k, b_k)$ is $\sum_i a_i b_i = 0 \bmod \mathbb{Z}$, whereas its group has order $2^{2k} > 1$. This proves the last assertion. □

We will also use the following elementary matrix convention. If B is a symmetric integral $d \times d$ matrix, then $(B/N)(x,y) = x^{\mathsf{T}} B y / N$ modulo $\mathbb{Z}$ is a bilinear form on $(\mathbb{Z}/N\mathbb{Z})^d$. If P is invertible modulo N, the map $x \mapsto Px$ is an isometry

$$\left((\mathbb{Z}/N\mathbb{Z})^d, \frac{P^{\mathsf{T}} B P}{N}\right) \longrightarrow \left((\mathbb{Z}/N\mathbb{Z})^d, \frac{B}{N}\right). \tag{2.13}$$

Changing the numerator matrix by a matrix divisible by N does not change the pairing. In particular, the congruence in (2.13) is a congruence over $\mathbb{Z}/N\mathbb{Z}$; no integral unimodularity of a lift of P is required.

Lemma 2.6. *Let $G_1, \dots, G_t$ be connected loopless multigraphs with chosen vertices o_i. Form G by identifying all the o_i to one vertex. Then*

$$(\mathrm{Jac}(G), b_G) \cong \bigperp_{i=1}^{t} (\mathrm{Jac}(G_i), b_{G_i}). \tag{2.14}$$

If the G_i are planar, so is G.

Proof. A one-vertex factor may be omitted, since its degree-zero divisor group is zero. If all factors have one vertex, the assertion follows from the same observation. Otherwise, delete the identified vertex. No edge joins the remaining vertices of distinct G_i, so the reduced Laplacian of G is the block matrix $\mathrm{diag}(A_1, \dots, A_t)$, where A_i is the reduced Laplacian of G_i at o_i. Its cokernel is the direct sum of their cokernels, and its inverse is $\mathrm{diag}(A_1^{-1}, \dots, A_t^{-1})$. Equations (2.7) and (2.10) give (2.14). For planarity, regard an embedding of each G_i as an embedding in the sphere, choose a face incident with o_i as the outer face, and place the drawings in discs with disjoint interiors meeting only at the point representing the identified vertices. No interiors of edges from different drawings meet. The resulting graph is connected and has no loops. □

3. The pairing of a complete graph

Proposition 3.1. *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*

$$(\mathbb{Z}/N\mathbb{Z})^{N-2} \longrightarrow \mathrm{Jac}(K_N), \qquad (a_i) \longmapsto \sum_{i=1}^{N-2} a_i [D_i] \tag{3.1}$$

is an isomorphism, and

$$b_{K_N}([D_i], [D_j]) = \frac{\delta_{ij} + 1}{N} \pmod{\mathbb{Z}}. \tag{3.2}$$

Consequently (1.10) *holds.*

Proof. The Laplacian is

$$L = NI_N - J_N. \tag{3.3}$$

Since $\sum_v (D_i)_v = 0$, one has $LD_i = ND_i$. Thus $N[D_i] = 0$, and (3.1) 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

$$D' = \sum_{i=1}^{N-2} D'_i (\mathbf{e}_i - \mathbf{e}_{N-1}). \tag{3.4}$$

This proves surjectivity of (3.1).

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 $0 = Nf_N - S$. The i-th coordinate, for $i \leq N-2$, consequently gives

$$a_i = Nf_i - S = N(f_i - f_N). \tag{3.5}$$

Thus every a_i is divisible by N, proving injectivity.

The vector D_j/N is a rational potential for D_j by (3.3). Since $D_i^{\mathsf{T}} D_j = \delta_{ij} + 1$, Lemma 2.3 gives (3.2). □

4. Hyperbolic reduction at the prime two

4.1. **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

$$\beta(x, y) = q(x + y) - q(x) - q(y). \tag{4.1}$$

We call q 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

$$q(u_i) = q(v_i) = 0, \qquad \beta(u_i, v_j) = \delta_{ij}, \qquad \beta(u_i, u_j) = \beta(v_i, v_j) = 0. \tag{4.2}$$

Define the integer

$$S(q) = \sum_{x \in W} (-1)^{q(x)}. \tag{4.3}$$

Lemma 4.1. *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

$$\#q^{-1}(0) = \frac{2^{2k} + S(q)}{2} > 1. \tag{4.4}$$

Choose $u \neq 0$ with $q(u) = 0$. Nondegeneracy supplies v with $\beta(u, v) = 1$. Put $v' = v + q(v)u$. Equation (4.1) 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

$$x - \beta(x, v')u - \beta(x, u)v' \tag{4.5}$$

is orthogonal to u and v'. This proves $W = U + U^\perp$. If $au + bv' \in U^\perp$, pairing with u and v' gives $b = a = 0$. Thus $W = U \perp U^\perp$. The complement is nondegenerate: an element of its radical would be orthogonal to both summands, hence to 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

$$S(q) = 2S(q|_{U^\perp}). \tag{4.6}$$

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

$$q_B(\bar{x}) = \frac{x^\mathsf{T} Bx}{2} \pmod 2, \qquad \bar{x} \in \mathbb{F}_2^d. \tag{4.7}$$

This is independent of the integral lift, because replacing x by $x + 2z$ changes the half-norm by

$$2x^\mathsf{T} Bz + 2z^\mathsf{T} Bz \equiv 0 \pmod 2. \tag{4.8}$$

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 4.2. *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

$$\det(I_d + J_d) = 1 + d. \tag{4.9}$$

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, (4.9) 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

$$x^{\mathsf{T}}Bx = w + w^2, \qquad q_B(\bar{x}) = \frac{w(w+1)}{2} \pmod 2. \tag{4.10}$$

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

$$S(q_B) = \sum_{w=0}^{d} \binom{d}{w} (-1)^{w(w+1)/2} = \mathrm{Re}\left((1+i) \sum_{w=0}^{d} \binom{d}{w} i^w \right) \tag{4.11}$$

$$= \mathrm{Re}(1+i)^{d+1} = 2^{d/2}. \tag{4.12}$$

For the last equality, write $d = 8t + 6$ and use $(1+i)^8 = 16$ and $(1+i)^7 = 8 - 8i$. Lemma 4.1 now proves the assertion. □

4.2. **Lifting modulo powers of two.**

Lemma 4.3. *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*

$$P^{\mathsf{T}}BP = H^{\perp k} \pmod{2^s}. \tag{4.13}$$

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 $u, v, w_1, \ldots, w_{2k-2}$. Their column matrix has odd determinant, so it is invertible modulo 2^s. The first pair satisfies

$$u^{\mathsf{T}}Bu \equiv v^{\mathsf{T}}Bv \equiv 0 \pmod 4, \qquad u^{\mathsf{T}}Bv \equiv 1 \pmod 2. \tag{4.14}$$

Suppose $2 \leq j < s$ and $u^{\mathsf{T}}Bu$ is divisible by 2^j. For $\varepsilon \in \{0, 1\}$, replace u by $u + \varepsilon 2^{j-1}v$. Its norm is

$$u^{\mathsf{T}}Bu + \varepsilon 2^j u^{\mathsf{T}}Bv + \varepsilon^2 2^{2j-2} v^{\mathsf{T}}Bv. \tag{4.15}$$

The last term is divisible by 2^{2j}, hence by 2^{j+1}. Write $u^{\mathsf{T}}Bu = 2^j m$ and choose $\varepsilon \equiv m \pmod 2$. Since $u^{\mathsf{T}}Bv$ is odd, $m + \varepsilon u^{\mathsf{T}}Bv$ is even; hence (4.15) is divisible by 2^{j+1}. This replacement does not change u modulo two or the oddness of $u^{\mathsf{T}}Bv$. Starting at $j = 2$ and repeating up to $j = s - 1$ gives

$$u^{\mathsf{T}}Bu \equiv 0 \pmod{2^s}. \tag{4.16}$$

When $s = 2$, (4.16) already follows from (4.14) and no replacement is made.

Choose an odd integer c satisfying $c\, u^{\mathsf{T}}Bv \equiv 1 \pmod{2^s}$ and replace v by cv. Its norm is still divisible by four, and now $u^{\mathsf{T}}Bv \equiv 1 \pmod{2^s}$. Put $a = v^{\mathsf{T}}Bv/2$, an even integer, and replace v by $v - au$. The new norm and mixed pairing satisfy

$$(v - au)^{\mathsf{T}}B(v - au) = v^{\mathsf{T}}Bv - 2a\, u^{\mathsf{T}}Bv + a^2 u^{\mathsf{T}}Bu \equiv 0 \pmod{2^s}, \tag{4.17}$$

$$u^{\mathsf{T}}B(v - au) \equiv 1 \pmod{2^s}. \tag{4.18}$$

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

$$w_i' = w_i - (w_i^{\mathsf{T}}Bv)u - (w_i^{\mathsf{T}}Bu)v. \tag{4.19}$$

Set $\alpha_i = w_i^{\mathsf{T}} B v$ and $\beta_i = w_i^{\mathsf{T}} B u$. Then

$$(w_i')^{\mathsf{T}} B u = \beta_i - \alpha_i u^{\mathsf{T}} B u - \beta_i v^{\mathsf{T}} B u \equiv 0 \pmod{2^s}, \tag{4.20}$$

$$(w_i')^{\mathsf{T}} B v = \alpha_i - \alpha_i u^{\mathsf{T}} B v - \beta_i v^{\mathsf{T}} B v \equiv 0 \pmod{2^s}. \tag{4.21}$$

The two coefficients subtracted in (4.19) 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

$$q_C(\bar{y}) = q_B\left(\sum_i \bar{y}_i \bar{w}_i'\right) \tag{4.22}$$

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 (4.13). □

Proof of Theorem 1.4. Set $N = 2^r$ and $d = N - 2$. Since $r \geq 3$, one has $d \equiv 6 \pmod 8$. Proposition 3.1 gives the pairing matrix $(I_d + J_d)/N$ on $(\mathbb{Z}/N\mathbb{Z})^d$. By Lemma 4.2, its associated quadratic form over $\mathbb{F}_2$ is hyperbolic, and Lemma 4.3, with $s = r$, gives an invertible congruence

$$I_d + J_d \cong H^{\perp d/2} \pmod{2^r}. \tag{4.23}$$

Apply (2.13) and use $d/2 = 2^{r-1} - 1$. Taking $r = 3$ gives (1.9). □

Corollary 4.4. *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 1.4. □

5. Continued fractions and cyclic pairings

The path-and-root graph in this section is Greene's linear graph-lattice construction [8, Section 3.3, p. 466]. We give the integral presentation and the rational potential determining its pairing.

5.1. **The integral matrix.**

Lemma 5.1. *Let $n > a > 0$ be coprime integers. There are integers $b_1, \dots, b_\ell \geq 2$ and*

$$s_0 = n, \quad s_1 = a, \quad s_0 > s_1 > \cdots > s_\ell = 1, \quad s_{\ell+1} = 0 \tag{5.1}$$

satisfying

$$s_{i-1} = b_i s_i - s_{i+1} \qquad (1 \leq i \leq \ell). \tag{5.2}$$

They give

$$\frac{n}{a} = [b_1, \dots, b_\ell]^- = b_1 - \cfrac{1}{b_2 - \cfrac{1}{\ddots - \cfrac{1}{b_\ell}}}, \qquad \ell \leq a. \tag{5.3}$$

For $\ell = 1$, the continued fraction is $[b_1]^- = b_1$.

Proof. Start with $s_0 = n$, $s_1 = a$. As long as $s_i > 0$, set

$$b_i = \left\lceil \frac{s_{i-1}}{s_i} \right\rceil, \qquad s_{i+1} = b_i s_i - s_{i-1}. \tag{5.4}$$

The inequalities $b_i - 1 < s_{i-1}/s_i \le b_i$ give $0 \le b_i s_i - s_{i-1} < s_i$. Since $s_{i-1}/s_i > 1$, one has $b_i \ge 2$. The positive remainders strictly decrease, so a first zero is reached. A common divisor of s_{i-1}, s_i divides $s_{i+1} = b_i s_i - s_{i-1}$, and a common divisor of s_i, s_{i+1} divides $s_{i-1} = b_i s_i - s_{i+1}$. Therefore $\gcd(s_i, s_{i+1}) = \gcd(s_{i-1}, s_i)$, and the last positive remainder is $\gcd(n, a) = 1$. There are at most a positive remainders beginning with s_1, which gives $\ell \le a$. For $i < \ell$, divide (5.2) by s_i to obtain $s_{i-1}/s_i = b_i - 1/(s_i/s_{i+1})$. At $i = \ell$, the ratio is $s_{\ell-1}/s_\ell = b_\ell$. Successive substitution gives (5.3). □

Lemma 5.2. *For the integers in Lemma 5.1, let C be the symmetric tridiagonal matrix*

$$C_{ij} = \begin{cases} b_i, & i = j, \\ -1, & |i-j| = 1, \\ 0, & |i-j| \ge 2. \end{cases} \tag{5.5}$$

Then

$$\det C = n, \qquad (C^{-1})_{11} = \frac{a}{n}, \tag{5.6}$$

and the integral vector $s = (s_1, \dots, s_\ell)^{\mathsf{T}}$ satisfies

$$Cs = n\mathbf{e}_1. \tag{5.7}$$

Proof. Let Δ_i be the determinant of the trailing submatrix on indices $i, \dots, \ell$, with $\Delta_{\ell+1} = 1$ and $\Delta_{\ell+2} = 0$. Expanding along its first row gives

$$\Delta_i = b_i \Delta_{i+1} - \Delta_{i+2}. \tag{5.8}$$

For the second term, the minor matrix obtained by deleting the first row and second column has first column $(-1, 0, \dots, 0)^{\mathsf{T}}$. Its determinant is $-\Delta_{i+2}$. Multiplication by the entry -1 and the cofactor sign -1 leaves this term unchanged. For a block of size one, the recurrence reads $\Delta_\ell = b_\ell \cdot 1 - 0 = b_\ell$. Equations (5.2) and (5.8), read backwards from the two terminal values, give $\Delta_i = s_{i-1}$. Thus $\Delta_1 = n$ and $\Delta_2 = a$. The $(1,1)$ cofactor formula gives $(C^{-1})_{11} = \Delta_2/\Delta_1 = a/n$, including $\ell = 1$.

The first coordinate of Cs is $b_1 s_1 - s_2 = s_0 = n$. For $1 < i < \ell$, the i-th coordinate is $b_i s_i - s_{i-1} - s_{i+1} = 0$. The last coordinate, when $\ell > 1$, is $b_\ell s_\ell - s_{\ell-1} = s_{\ell+1} = 0$. When $\ell = 1$, the first-coordinate computation alone applies. This proves (5.7). □

5.2. **The planar graph.** For n, a as above, take vertices $o, v_1, \dots, v_\ell$. Join v_i to v_{i+1} by one edge for $1 \le i < \ell$. For each i, join v_i to o by exactly

$$c_i = b_i - \mathbf{1}_{\{i>1\}} - \mathbf{1}_{\{i<\ell\}} \tag{5.9}$$

parallel edges. This defines $G(n, a)$. If $\ell = 1$, then $c_1 = b_1$. If $\ell \ge 2$, then $c_1, c_\ell \ge 1$ and all other $c_i \ge 0$, because every $b_i \ge 2$.

Lemma 5.3. *The graph $G(n, a)$ is connected, planar and loopless. Its reduced Laplacian at o is C, and*

$$|V(G(n,a))| = \ell + 1 \le a + 1 \le n, \qquad |E(G(n,a))| = \sum_{i=1}^{\ell} b_i - \ell + 1. \tag{5.10}$$

Proof. For $\ell = 1$, the two vertices are joined by $b_1 \ge 2$ edges, which can be drawn as disjoint arcs except at their endpoints. For $\ell \ge 2$, the vertices v_i form a path and o is joined to its two endpoints, so the graph is connected. Place $o, v_1, \dots, v_\ell$ in this cyclic order on a convex polygon. Draw the path on its boundary and draw one straight segment from o to each v_i for which $c_i > 0$. The interiors of these segments are disjoint. For each segment, replace it by c_i nearby arcs, choosing disjoint thin neighborhoods away from the vertices and disjoint sectors at each vertex. This yields a planar embedding with the prescribed parallel edges. Every edge has distinct endpoints, so there are no loops.

The degree of v_i is b_i by (5.9); there is one edge between consecutive path vertices and no edge between other pairs of path vertices. Thus the reduced Laplacian is exactly (5.5). There are $\ell + 1$ vertices. The length bound in Lemma 5.1 gives the vertex inequality. The path has $\ell - 1$ edges, and $\sum_i c_i = \sum_i b_i - 2(\ell - 1)$, including $\ell = 1$. Adding the two counts proves the edge formula. □

Proof of Proposition 1.5. Use the graph of Lemma 5.3. By Lemma 2.2, write its Jacobian as $\mathbb{Z}^\ell/C\mathbb{Z}^\ell$, and denote the class of $\mathbf{e}_i$ by z_i. For $1 \le i < \ell$, the i-th column relation is

$$z_{i+1} = b_i z_i - z_{i-1}, \qquad z_0 = 0. \tag{5.11}$$

It follows by induction on i that every z_i is an integral multiple of z_1. For $\ell = 1$, this conclusion holds without any relation. Thus $z = z_1$ generates the group.

Equation (5.7) gives $nz = 0$ and the rational potential $C^{-1}\mathbf{e}_1 = s/n$. By (2.10),

$$b_{G(n,a)}(z,z) = \frac{s_1}{n} = \frac{a}{n} \pmod{\mathbb{Z}}. \tag{5.12}$$

If $kz = 0$, bilinearity implies $ka/n \in \mathbb{Z}$. Since $\gcd(n,a) = 1$, one has $n \mid k$. Therefore z has order exactly n, and bilinearity determines the full pairing from (5.12). The required graph properties and size bound are those of Lemma 5.3. □

Example 5.4. For $n = 17$, $a = 3$, one has $17/3 = [6,3]^-$ and

$$C = \begin{pmatrix} 6 & -1 \\ -1 & 3 \end{pmatrix}, \qquad C^{-1} = \frac{1}{17}\begin{pmatrix} 3 & 1 \\ 1 & 6 \end{pmatrix}. \tag{5.13}$$

The graph has one edge v_1v_2, five edges ov_1 and two edges ov_2. The class of $v_1 - o$ generates its Jacobian and has self-pairing $3/17$. For $a = 1$ the construction is the graph on two vertices with n parallel edges, realizing $\left\langle \frac{1}{n} \right\rangle$. For $a = n-1$ the remainder sequence is $s_i = n - i$; all $b_i = 2$ and the graph is the cycle on n vertices (the two-edge cycle when $n = 2$), realizing $\left\langle \frac{(n-1)}{n} \right\rangle$.

6. Orthogonal sums and odd-order groups

Proposition 6.1. *Every finite orthogonal sum of nondegenerate cyclic pairings is the paired Jacobian of a connected planar loopless multigraph. For a nonempty sum $\perp_{j=1}^{t} \left\langle \frac{a_j}{n_j} \right\rangle$, with $n_j > a_j > 0$ coprime, one can use at most $1 + \sum_{j=1}^{t} a_j$ vertices.*

Proof. Realize the j-th summand by $G(n_j, a_j)$ and identify the vertices denoted by o. The graph has $1 + \sum_j \ell_j \le 1 + \sum_j a_j$ vertices. Proposition 1.5 and Lemma 2.6 give its pairing and planarity. The empty orthogonal sum is realized by a single vertex, whose degree-zero divisor group is zero. □

Lemma 6.2. *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 $q \ne p$. Such integers exist because the prime powers are pairwise coprime, by repeated use of Bézout's identity. Modulo n they satisfy $\sum_p e_p = 1$ and $e_p e_q = 0$ for $p \ne q$. Thus

$$A = \bigoplus_p A_p, \qquad A_p = e_p A = \{x \in A : p^{r_p} x = 0\}. \tag{6.1}$$

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 (6.1). For $x \in A_p$ and $y \in A_q$ with $p \ne q$, 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

$$b(x,x) = \frac{u}{p^r}, \qquad b(y,y) = \frac{v}{p^r}, \qquad b(x,y) = \frac{w}{p^r}, \qquad p \nmid w, \tag{6.2}$$

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

$$b(z,z) = \frac{c}{p^r}, \qquad p \nmid c. \tag{6.3}$$

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 $kz \in C^\perp$, (6.3) implies $kc \equiv 0 \pmod{p^r}$, hence $kz = 0$. Thus

$$(A, b) = (C, b|_C) \perp (C^\perp, b|_{C^\perp}). \tag{6.4}$$

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 (6.1) completes the general case. □

Proof of Corollary 1.6. For $A \neq 0$, Lemma 6.2 gives an orthogonal sum of cyclic pairings of orders $n_1, \dots, n_t \geq 3$. Choose coprime representatives $0 < a_j < n_j$ for their self-pairing numerators and apply Proposition 6.1. The number of vertices is at most

$$1 + \sum_{j=1}^{t} a_j \leq 1 + \sum_{j=1}^{t} (n_j - 1) \leq \prod_{j=1}^{t} n_j = |A|. \tag{6.5}$$

For the middle inequality, expand $\prod_j (1 + (n_j - 1))$: the constant and linear terms give the left-hand side, and all higher terms are nonnegative. The zero group is realized by the one-vertex graph. □

7. Cyclic completion of arbitrary finite pairings

7.1. **Localization and finite congruences.** For a nonsingular symmetric integral matrix C of size d, put

$$\mathcal{D}(C) = \left(\mathbb{Z}^d/C\mathbb{Z}^d,\ ([x],[y]) \longmapsto x^{\mathsf{T}}C^{-1}y \pmod{\mathbb{Z}}\right). \tag{7.1}$$

Lemma 2.1 gives the finite order $|\det C|$. Replacing x by $x + Cz$ changes the pairing by $z^{\mathsf{T}}y \in \mathbb{Z}$; replacing y gives the corresponding assertion. Symmetry follows from $(C^{-1})^{\mathsf{T}} = C^{-1}$. If $[x]$ pairs to zero with every coordinate class, then $C^{-1}x \in \mathbb{Z}^d$, so $[x] = 0$. Thus (7.1) is a finite paired group.

For a prime p, let $R_p = \mathbb{Z}_{(p)} \subset \mathbb{Q}$, the ring of fractions whose denominator is prime to p. Its units are the fractions whose numerator and denominator are both prime to p.

Lemma 7.1. *The map induced by $\mathbb{Z}^d \subset R_p^d$ identifies the p-primary part of $\mathcal{D}(C)$ with*

$$\left(R_p^d/CR_p^d,\ ([x],[y]) \longmapsto x^{\mathsf{T}}C^{-1}y \pmod{R_p}\right). \tag{7.2}$$

The coefficient group $\mathbb{Q}/R_p$ is identified with the p-primary subgroup of $\mathbb{Q}/\mathbb{Z}$ by the inverse of the natural quotient map.

Proof. A rational class of p-power order has a representative a/p^k. If this representative belongs to R_p, then $p^k \mid a$; hence the natural map is injective on these classes. For any fraction $a/(p^k s)$ with $p \nmid s$, choose $b \in \mathbb{Z}$ with $bs \equiv a \pmod{p^k}$. Then

$$\frac{a}{p^k s} - \frac{b}{p^k} = \frac{a - bs}{p^k s} \in R_p. \tag{7.3}$$

This proves the asserted coefficient isomorphism.

Write $A = \mathbb{Z}^d/C\mathbb{Z}^d$, and let the exponent of A_p be p^e. The primary decomposition proved in (6.1) does not require oddness of $|A|$. Every primary subgroup at a prime other than p maps to zero in R_p^d/CR_p^d: it is annihilated by a power of that prime, which is a unit of R_p. If $[x] \in A_p$ maps to zero, write $x = Cy$ with $y \in R_p^d$. Choose s prime to p with $sy \in \mathbb{Z}^d$. Then $s[x] = 0$ in A_p. An integer b with $bs \equiv 1 \pmod{p^e}$ gives $[x] = bs[x] = 0$. Thus the map on A_p is injective.

For $y \in R_p^d$, choose s prime to p with $sy \in \mathbb{Z}^d$ and decompose $[sy] \in A$ into its primary parts. Let $x \in A_p$ be its p-primary part. In the localized quotient, $s[y]$ equals the image of x. Choose b with $bs \equiv 1 \pmod{p^e}$. Multiplication by s is invertible on the localized quotient; therefore the image of bx is $[y]$. This proves surjectivity. The equality of pairings follows by applying the coefficient map to the formula in (7.1). □

Lemma 7.2. *Let C, D be nonsingular symmetric integral matrices of the same size. Suppose the exponent of $\mathcal{D}(C)_p$ is p^e, where $e = 0$ means that this group is zero. If*

$$D - C \in p^{2e+1}\,\mathrm{Mat}_d(\mathbb{Z}), \tag{7.4}$$

then $\mathcal{D}(D)_p \cong \mathcal{D}(C)_p$ as paired groups.

Proof. By Lemma 7.1, the exponent hypothesis is $p^e R_p^d \subset CR_p^d$. Apply C^{-1} to each vector $p^e e_i$. The resulting vectors lie in R_p^d; equivalently,

$$C^{-1} \in p^{-e}\,\mathrm{Mat}_d(R_p). \tag{7.5}$$

Set $E = D - C$ and $U = I + C^{-1}E$. Equations (7.4) and (7.5) imply

$$U \in I + p^{e+1}\,\mathrm{Mat}_d(R_p), \qquad \det U \equiv 1 \pmod{pR_p}. \tag{7.6}$$

Thus $\det U$ is a unit of R_p and $U^{-1} = (\det U)^{-1}\,\mathrm{adj}(U)$ has entries in R_p. Since $D = CU$, one has $DR_p^d = CR_p^d$.

The identity $U^{-1} - I = -U^{-1}(U - I)$ gives

$$D^{-1} - C^{-1} = -U^{-1}C^{-1}EC^{-1} \in p\,\mathrm{Mat}_d(R_p). \tag{7.7}$$

Indeed, the two inverse factors contribute p^{-2e} and E contributes p^{2e+1}. For $x, y \in R_p^d$, the value $x^{\mathsf{T}}(D^{-1} - C^{-1})y$ consequently belongs to R_p. The identity on the common quotient preserves the pairings in (7.2). Apply Lemma 7.1. This proof also applies to $p = 2$ and to $e = 0$. □

7.2. **Binary summands at the prime two.**

Lemma 7.3. *Every finite paired group is an orthogonal sum of nondegenerate cyclic pairings and pairings*

$$\left((\mathbb{Z}/N\mathbb{Z})^2, B/N\right), \qquad N = 2^r, \quad r \geq 1, \tag{7.8}$$

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

Proof. Primary subgroups are mutually orthogonal and nondegenerate by the proof of Lemma 6.2; 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

$$B = \begin{pmatrix} 2a & c \\ c & 2d \end{pmatrix}. \tag{7.9}$$

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 7.4. *Let $N = 2^r$, $r \geq 1$, and let B satisfy* (7.8)*. Let Q be a finite set of odd primes. Fix a positive odd integer c satisfying*

$$-c \equiv (B^{-1})_{12} \pmod{N}. \tag{7.10}$$

There are even integers $a, d > c$ such that, for

$$C = \begin{pmatrix} a & -c \\ -c & d \end{pmatrix}, \qquad t = ad - c^2, \tag{7.11}$$

one has

$$C \equiv B^{-1} \pmod{N}, \quad \gcd(a,c) = 1, \quad t > 0, \quad \gcd\left(t, 2\prod_{q\in Q} q\right) = 1. \tag{7.12}$$

The matrix NC is a reduced Laplacian of a three-vertex outerplanar loopless multigraph, and

$$\mathcal{D}(NC) \cong \left((\mathbb{Z}/N\mathbb{Z})^2, B/N\right) \perp (C_t, \gamma), \tag{7.13}$$

where C_t is cyclic of order t and γ is nondegenerate. In the congruences, B^{-1} denotes the inverse over $\mathbb{Z}/N\mathbb{Z}$.

Proof. The adjugate of B has even diagonal and odd off-diagonal entries. Its multiplication by the inverse of the odd integer $\det B$ preserves those parities. Thus a positive odd c in (7.10) exists. The moduli N, c are coprime. Choose $a > c$ satisfying

$$a \equiv (B^{-1})_{11} \pmod{N}, \qquad a \equiv 1 \pmod{c}. \tag{7.14}$$

These congruences imply that a is even and $\gcd(a,c) = 1$. For each $q \in Q$ with $q \nmid a$, impose

$$d \equiv a^{-1}(c^2+1) \pmod{q}, \qquad d \equiv (B^{-1})_{22} \pmod{N}. \tag{7.15}$$

All the moduli are pairwise coprime, so these conditions have a solution; adding a positive multiple of their product gives $d > c$. The last condition makes d even. If $q \nmid a$, then $t \equiv 1 \pmod{q}$. If $q \mid a$, then $q \nmid c$ and $t \equiv -c^2 \not\equiv 0 \pmod{q}$. Also t is odd and $ad > c^2$. This proves (7.12). The choices follow from Bézout's identity, applied successively to the coprime moduli.

Take $N(a-c)$ edges between o, v_1, $N(d-c)$ edges between o, v_2, and Nc edges between v_1, v_2. All multiplicities are positive integers. The reduced Laplacian at o is NC. Draw one copy of each edge as a triangle and all additional copies on its interior side. This is an outerplanar embedding, with the three vertices on its exterior triangle. In particular, NC is positive definite by Lemma 2.2.

Choose integers u, v with $ua - vc = 1$, and put $k = -uc + vd$. The two matrices

$$U = \begin{pmatrix} u & v \\ c & a \end{pmatrix}, \qquad V = \begin{pmatrix} 1 & -k \\ 0 & 1 \end{pmatrix} \tag{7.16}$$

have determinant one. Multiplication gives

$$UC = \begin{pmatrix} 1 & k \\ 0 & t \end{pmatrix}, \qquad U(NC)V = \begin{pmatrix} N & 0 \\ 0 & Nt \end{pmatrix}. \tag{7.17}$$

Thus the underlying cokernel is $\mathbb{Z}/N\mathbb{Z} \oplus \mathbb{Z}/Nt\mathbb{Z}$. This row-and-column equivalence determines the group only; the pairing is computed below.

Let $\bar{e}_i$ be the coordinate classes in $\mathcal{D}(NC)$. The classes $t\bar{e}_1, t\bar{e}_2$ are annihilated by N, since $Nte_i = NC\,\mathrm{adj}(C)e_i$. If $t(x_1e_1 + x_2e_2) \in NC\mathbb{Z}^2$, each coordinate is divisible by N. Since $\gcd(t, N) = 1$, one has $N \mid x_1, x_2$. They therefore generate a subgroup isomorphic to $(\mathbb{Z}/N\mathbb{Z})^2$. Equation (7.17) shows that the full 2-primary subgroup has order N^2; hence they form its basis. Their Gram matrix is

$$t^2(NC)^{-1} = \frac{t}{N}\,\mathrm{adj}(C). \tag{7.18}$$

Choose $w \in \mathbb{Z}$ with $wt \equiv 1 \pmod N$. Multiplying both basis vectors by w is invertible on this subgroup, and the new numerator satisfies

$$w^2 t\,\mathrm{adj}(C) \equiv t^{-1}\,\mathrm{adj}(C) \equiv C^{-1} \equiv B \pmod N. \tag{7.19}$$

By (7.17) the odd-primary subgroup is cyclic of order t. Primary orthogonality and nondegeneracy of the entire pairing prove (7.13). □

Proposition 7.5. *For $N = 2^r$, $r \geq 1$, let T_N have three vertices and edge multiplicities $N, N, N(N-1)$. Then*

$$(\mathrm{Jac}(T_N), b_{T_N}) \cong \mathcal{E}_N \perp \left\langle \tfrac{1}{2N-1} \right\rangle. \tag{7.20}$$

Proof. Put $t = 2N - 1$ and root the graph at the common endpoint of the two edge families of multiplicity N. The reduced Laplacian and its inverse are

$$L = N\begin{pmatrix} N & -(N-1) \\ -(N-1) & N \end{pmatrix}, \qquad L^{-1} = \frac{1}{Nt}\begin{pmatrix} N & N-1 \\ N-1 & N \end{pmatrix}. \tag{7.21}$$

The product of the two displayed numerator matrices is tI_2, since $N^2 - (N-1)^2 = t$ and the mixed entries cancel. The argument of (7.17) gives cokernel $\mathbb{Z}/N\mathbb{Z} \oplus \mathbb{Z}/Nt\mathbb{Z}$.

As in the proof of Lemma 7.4, $t\bar{e}_1, t\bar{e}_2$ form a basis of the 2-primary part. Their self-pairings are $t \in \mathbb{Z}$ and their mixed pairing is

$$\frac{t(N-1)}{N} = 2N - 3 + \frac{1}{N}. \tag{7.22}$$

Thus they give $\mathcal{E}_N$. The element $N\bar{e}_1$ is annihilated by t, by the adjugate identity, and has self-pairing N^2/t. Since $\gcd(N, t) = 1$, this value has order t; hence the element generates the odd part. If $vN \equiv 1 \pmod t$, the generator $vN\bar{e}_1$ has self-pairing $1/t$ modulo $\mathbb{Z}$. Primary orthogonality proves the assertion. □

7.3. **Tridiagonal reduced Laplacians.**

Lemma 7.6. *Let L be an integral symmetric tridiagonal matrix of size $d \geq 2$. Suppose*

$$c_i = -L_{i,i+1} > 0 \quad (1 \leq i < d), \qquad s_i = \sum_j L_{ij} \geq 0, \qquad s_1, s_d > 0. \tag{7.23}$$

Then L is the reduced Laplacian of a loopless multigraph with an outerplanar embedding whose exterior boundary is a Hamilton cycle. The graph is biconnected. If P is a finite set of primes containing all prime divisors of $\prod_{i=1}^{d-1} c_i$, then $\mathcal{D}(L)_\ell$ is cyclic for every prime $\ell \notin P$.

Proof. Take vertices $o, v_1, \ldots, v_d$, with c_i edges between v_i, v_{i+1} and s_i edges between o, v_i. The diagonal degree at v_i is $s_i + c_{i-1} + c_i = L_{ii}$, where $c_0 = c_d = 0$. The off-diagonal entries are those of L. Choose one edge from each adjacent family and one edge from each of the two endpoint families. They form the cycle

$$o, v_1, v_2, \ldots, v_d, o. \tag{7.24}$$

Embed this cycle as a convex polygon. The segments from o to v_i have disjoint interiors. Draw every remaining parallel edge on the interior side of its chosen segment or polygon side, inside disjoint narrow strips away from vertices and disjoint sectors at vertices. The exterior boundary remains (7.24). Deleting any vertex leaves the path obtained by deleting it from this cycle; that path contains

all remaining vertices. Hence the graph is biconnected. Its connectedness also proves that L is positive definite.

Delete row one and column d from L. In row i of the resulting matrix, a possibly nonzero entry has column at least i; its diagonal entry is $-c_i$. Its determinant is therefore

$$(-1)^{d-1}\prod_{i=1}^{d-1} c_i. \tag{7.25}$$

If $\ell \notin P$, this minor is a unit modulo ℓ, so $\operatorname{rank}_{\mathbb{F}_\ell}(L \bmod \ell) \geq d-1$. For $A = \mathbb{Z}^d/L\mathbb{Z}^d$, reduction of its presentation gives

$$A/\ell A \cong \mathbb{F}_\ell^d/(L \bmod \ell)\mathbb{F}_\ell^d, \qquad \dim_{\mathbb{F}_\ell}(A/\ell A) \leq 1. \tag{7.26}$$

Multiplication by ℓ is bijective on every primary subgroup of A at a prime other than ℓ. Hence $A/\ell A = A_\ell/\ell A_\ell$. Choose $x \in A_\ell$ whose class generates this quotient, using $x = 0$ when it is zero. Then $A_\ell = \langle x\rangle + \ell A_\ell$. The quotient $K = A_\ell/\langle x\rangle$ satisfies $K = \ell K$. For an integer m with $\ell^m K = 0$, iteration gives $K = \ell^m K = 0$. Thus $A_\ell = \langle x\rangle$ is cyclic. □

Proof of Theorem 1.2. Let P be the set of prime divisors of $2h|A|$. For $p \in P$, let p^{e_p} be the exponent of A_p, with $e_p = 0$ if $A_p = 0$. Decompose (A, b) using Lemma 7.3. For each cyclic summand use the matrix of Proposition 1.5. It has nonnegative row sums and positive endpoint row sums, including a one-row block. Its adjacent entries, when present, are -1.

For every binary summand, choose c as in (7.10) before choosing its two diagonal entries. Let T be the set of primes outside P dividing any of these integers c. They are odd because each c is odd. Apply Lemma 7.4 with $Q = (P \cup T) \setminus \{2\}$ to every binary summand. A binary block NC has positive row sums $N(a-c), N(d-c)$; every prime divisor of its adjacent entry $-Nc$ belongs to $P \cup T$. Denote the resulting blocks by $L_1, \dots, L_s$ and put

$$L_0 = \operatorname{diag}(L_1, \dots, L_s). \tag{7.27}$$

Block inversion, the exact cyclic realizations and (7.13) give

$$\mathcal{D}(L_0)_p \cong (A_p, b|_{A_p}) \quad (p \in P), \qquad \mathcal{D}(L_0)_q = 0 \quad (q \in T). \tag{7.28}$$

The last assertion follows because the original summands have no q-torsion and every added odd order is prime to q.

If L_0 has fewer than two rows, append copies of the one-row matrix $[b]$ until it has two rows, where

$$b = 1 + \prod_{p \in P \cup T} p. \tag{7.29}$$

Since $2 \in P$, this integer is odd and at least three. It is congruent to one at every prime of $P \cup T$; thus appending these matrices preserves (7.28). Their row sums are positive. This also treats $A = 0$, for which the initial matrix has size zero. Continue to denote the enlarged block matrix by L_0; let its size be $d \geq 2$.

Let J be the set of indices i at which two consecutive blocks meet. Define

$$w = \left(\prod_{p \in P} p^{2e_p+1}\right)\left(\prod_{q \in T} q\right), \qquad L = L_0 + w\sum_{i \in J}(e_i - e_{i+1})(e_i - e_{i+1})^{\mathsf{T}}. \tag{7.30}$$

For any $x \in \mathbb{R}^d$, the added quadratic form is $w\sum_{i\in J}(x_i - x_{i+1})^2 \geq 0$. Each block of L_0 is positive definite; hence L is positive definite. Each added matrix has zero row sums. It replaces the zero adjacent entry at the corresponding block boundary by $-w$. All other adjacent entries are unchanged, so every adjacent entry is strictly negative. The row sums remain nonnegative and the first and last remain positive. Lemma 7.6 therefore constructs an outerplanar biconnected graph G with reduced Laplacian L and exterior Hamilton cycle (7.24).

For $p \in P$, the difference $L - L_0$ is divisible by p^{2e_p+1}. For $q \in T$, it is divisible by q and the q-primary part of $\mathcal{D}(L_0)$ is zero. Lemma 7.2 yields

$$\mathcal{D}(L)_p \cong (A_p, b|_{A_p}) \quad (p \in P), \qquad \mathcal{D}(L)_q = 0 \quad (q \in T). \tag{7.31}$$

The prime divisors of every adjacent entry of L belong to $P \cup T$. Lemma 7.6 shows that $\mathcal{D}(L)_\ell$ is cyclic for every $\ell \notin P \cup T$.

Let C be the sum of these latter primary subgroups. Only finitely many are nonzero, since $\mathcal{D}(L)$ is finite. If x_ℓ generates its ℓ-primary part of order m_ℓ, then $\sum_\ell x_\ell$ has order $\prod_\ell m_\ell$: an integer annihilates this sum precisely when it is divisible by every m_ℓ, and these integers are pairwise coprime. Thus C is cyclic. Its order is prime to $2h|A|$ and its restricted pairing is nondegenerate by primary orthogonality. Combining (7.31) with Lemma 2.3 gives (1.5). □

Remark 7.7. The trivial complementary group is permitted. It cannot be required for every finite paired group: Corollary 2.5 excludes $\mathcal{E}_2$ as an entire paired Jacobian; compare [7, Proposition 26]. The complement can therefore always be cyclic but cannot always be zero. Theorem 1.2 does not prescribe $|C|$ or c; it prescribes primes which do not divide $|C|$.

8. Simple planar graphs with prescribed primary pairings

8.1. **Integral cycles and cuts.** Give each edge of a connected loopless graph G an orientation. Let $D : \mathbb{Z}^{E(G)} \to \mathbb{Z}^{V(G)}$ send an oriented edge to its head minus its tail. Give the edge group its Euclidean scalar product. Then $DD^{\mathsf{T}} = L_G$. Put

$$F = \ker D, \qquad B = D^{\mathsf{T}}\mathbb{Z}^{V(G)}, \qquad F_{\mathbb{Q}} = F \otimes \mathbb{Q}, \quad B_{\mathbb{Q}} = B \otimes \mathbb{Q}. \tag{8.1}$$

The group F is the group of integral cycles. Equipped with the restricted scalar product, it is the integral cycle lattice. For an integral positive-definite lattice K, define

$$K^* = \{x \in K \otimes \mathbb{Q} : (x, K) \subset \mathbb{Z}\}. \tag{8.2}$$

The discriminant pairing on K^*/K is the scalar product modulo $\mathbb{Z}$. The zero-rank case has zero discriminant group.

Lemma 8.1. *The subgroups F, B are direct summands of $\mathbb{Z}^{E(G)}$. Their rational spans are orthogonal complements. Every integral linear functional on either subgroup extends to the edge group.*

Proof. Choose a spanning tree T of G. It exists by adjoining, to one vertex, an edge reaching a new vertex until all vertices have been reached; connectedness permits each step and no cycle is created. For each $e \notin E(T)$, let p_e be the signed chain on the unique tree path from the tail of e to its head, so that $Dp_e = De$. Set $z_e = e - p_e \in F$. For $z \in F$, subtract $\sum_{e \notin E(T)} z(e) z_e$. The remaining cycle is supported on T. Its coefficient on a leaf edge is zero by the incidence equation at that leaf. Removing the leaf and repeating gives zero. Thus the z_e span F. Their coefficients on edges outside T are coordinate vectors, so they are independent. They form an integral basis of F. Together with the tree-edge coordinate vectors, they form a basis of the entire edge group: the inverse substitution is $e = z_e + p_e$ for $e \notin E(T)$.

Fix a root o. A potential f with $f(o) = 0$ is uniquely determined by its signed differences on the tree edges, because integration along the unique root paths recovers every $f(v)$. Every assignment of integral tree differences gives integral values of f. Therefore restriction to tree-edge coordinates maps B isomorphically onto $\mathbb{Z}^{E(T)}$. Every integral edge vector x consequently has a unique expression $x = b + c$, where $b \in B$ has the same tree coordinates as x and c is supported off T. This proves that B is a direct summand. Extend a functional on F or B by zero on a chosen complement to obtain an integral functional on the edge group.

For $z \in F$ and $f \in \mathbb{Q}^{V(G)}$, one has $(z, D^{\mathsf{T}} f) = (Dz, f) = 0$. The displayed bases give $\operatorname{rank} F = |E| - |V| + 1$ and $\operatorname{rank} B = |V| - 1$. Their ranks sum to $|E|$, so $F_{\mathbb{Q}}$ and $B_{\mathbb{Q}}$ are orthogonal complements. □

Lemma 8.2. *If C is the Gram matrix of an integral basis of F, then*

$$(\mathrm{Jac}(G), b_G) \cong \left(\mathbb{Z}^{\operatorname{rank} F}/C\mathbb{Z}^{\operatorname{rank} F}, -C^{-1} \pmod{\mathbb{Z}}\right). \tag{8.3}$$

Proof. Let π_F, π_B denote the rational orthogonal projections onto $F_{\mathbb{Q}}, B_{\mathbb{Q}}$. For $z \in \mathbb{Z}^{E(G)}$ and $f \in F$, $(\pi_F z, f) = (z, f) \in \mathbb{Z}$, so $\pi_F z \in F^*$. The corresponding argument gives $\pi_B z \in B^*$. Let $u \in F^*$. The functional $(u, -)$ on F extends integrally to the edge group by Lemma 8.1. Every such functional is $(z, -)$ for some integral edge vector z. Then $u - \pi_F z \in F_{\mathbb{Q}}$ is orthogonal to F, so $u = \pi_F z$. If $u \in B^*$, extend $(u, -)$ on B instead; its integral representative z satisfies $u = \pi_B z$ by the same nondegeneracy argument in $B_{\mathbb{Q}}$.

A direct summand K of an integral free group satisfies $(K \otimes \mathbb{Q}) \cap \mathbb{Z}^{E(G)} = K$: project an integral vector onto the complementary summand and use torsion-freeness there. If $\pi_F z \in F$, then $z - \pi_F z \in B_{\mathbb{Q}} \cap \mathbb{Z}^{E(G)} = B$. Conversely, every $z \in F + B$ has $\pi_F z \in F$. The kernel of $z \mapsto [\pi_F z]$ is therefore $F + B$. If $\pi_B z \in B$, the vector $z - \pi_B z$ belongs to $F_{\mathbb{Q}} \cap \mathbb{Z}^{E(G)} = F$, and the converse also holds. Thus the two projections induce isomorphisms

$$\mathbb{Z}^{E(G)}/(F + B) \xrightarrow{\sim} F^*/F, \qquad \mathbb{Z}^{E(G)}/(F + B) \xrightarrow{\sim} B^*/B. \tag{8.4}$$

For integral z, z', orthogonality gives

$$(\pi_F z, \pi_F z') + (\pi_B z, \pi_B z') = (z, z') \in \mathbb{Z}. \tag{8.5}$$

Hence the two pairings transported to the common quotient have opposite signs. The map D sends a signed path to the difference of its endpoints. These differences generate $\mathrm{Div}^0(G)$, so D is onto that group. It sends $F + B$ onto $L_G\mathbb{Z}^{V(G)}$. If $Dz = L_G f$ with f integral, then $z - D^{\mathsf{T}} f \in F$; hence the induced map

$$\mathbb{Z}^{E(G)}/(F + B) \longrightarrow \mathrm{Jac}(G) \tag{8.6}$$

is both surjective and injective.

Choose a rational f with $L_G f = Dz$, using (2.4). Then $D(z - D^{\mathsf{T}} f) = 0$, so $\pi_B z = D^{\mathsf{T}} f$. For $z' \in \mathbb{Z}^{E(G)}$,

$$(\pi_B z, \pi_B z') = (D^{\mathsf{T}} f, z') = f^{\mathsf{T}} D z' = b_G([Dz], [Dz']) \pmod{\mathbb{Z}}. \tag{8.7}$$

The last equality uses Lemma 2.3 and its symmetry. Thus (8.6) identifies the cut discriminant pairing with b_G.

Let $f_1, \dots, f_k$ be the chosen cycle basis and let C be its Gram matrix. In these coordinates the dual lattice is $C^{-1}\mathbb{Z}^k$, and the map $\mathbb{Z}^k/C\mathbb{Z}^k \to C^{-1}\mathbb{Z}^k/\mathbb{Z}^k$ sends $[a]$ to $[C^{-1}a]$. Its scalar product is $(C^{-1}a)^{\mathsf{T}} C (C^{-1}b) = a^{\mathsf{T}} C^{-1} b$. Combining this with (8.5) and (8.7) proves (8.3). □

8.2. **Vertex replacement and subdivision.**

Lemma 8.3. *Let G_0 be a loopless plane multigraph whose exterior boundary is a Hamilton cycle. There is a loopless planar Hamiltonian multigraph H of maximum degree at most three obtained by replacing vertices by paths. Contraction of these paths induces an isomorphism $F(H) \to F(G_0)$ of groups of integral cycles. If C_0 is the Gram matrix of a basis of $F(G_0)$, and ℓ_f is the column vector of coefficients on a new edge f in its lifted basis, then the Gram matrix of $F(H)$ is*

$$C_0 + R, \qquad R = \sum_{f \text{ new}} \ell_f \ell_f^{\mathsf{T}}. \tag{8.8}$$

No assertion of isometry is made for the contraction map.

Proof. At a vertex of degree $d \geq 4$, label the incident half-edges $e_1, \dots, e_d$ in cyclic order so that e_1, e_d are the two exterior Hamilton-cycle half-edges. This order exists because the sector between these two half-edges is incident to the exterior face. In a small vertex disc replace the vertex by a path $x_1, \dots, x_{d-2}$. Attach e_1, e_2 to x_1, attach e_{d-1}, e_d to x_{d-2}, and attach e_j to x_{j-1} for $3 \leq j \leq d - 2$. For $d = 4$ the middle list is empty. All new vertices have degree three.

The modification has a planar embedding with the prescribed boundary half-edges. One construction separates the consecutive pair e_1, e_2 from the remaining half-edges by an arc in the vertex disc, places x_1 on that side, and replaces the residual vertex by the same construction. At each step the separated and remaining boundary endpoints are consecutive intervals; their attachment arcs are disjoint. Iterating gives the stated path and retains the cyclic order of the old half-edges. Choose disjoint vertex discs, and leave vertices of degree two or three unchanged. Every old edge still has distinct endpoints because its endpoints belonged to distinct old vertices. New edges lie on paths with distinct vertices. Hence H is loopless. The Hamilton cycle enters each replacement at x_1, traverses the entire path, and leaves at x_{d-2}. It visits every vertex of H once, so H is Hamiltonian, connected and bridgeless.

Orient the old edges as in G_0 and each replacement path from x_1 to x_m, where $m = d - 2$. For a cycle on H, summing the incidence equations over a replacement path cancels every new-edge term. Its old-edge coefficients therefore satisfy the incidence equation at the corresponding vertex of G_0. Conversely, prescribe a cycle on G_0, and let b_j be the contribution of old edges at x_j. The original incidence equation is $\sum_{j=1}^{m} b_j = 0$. Give the oriented edge $x_j x_{j+1}$ the coefficient

$$a_j = \sum_{i=1}^{j} b_i = -\sum_{i=j+1}^{m} b_i \qquad (1 \le j < m). \tag{8.9}$$

The new incidence equations are

$$b_1 - a_1 = 0, \qquad b_j + a_{j-1} - a_j = 0 \ (1 < j < m), \qquad b_m + a_{m-1} = 0.$$

All follow by substitution. The first equation determines a_1; the interior equations determine each subsequent a_j. Thus the extension exists, is integral, and is unique. Restriction and extension are additive inverse maps between the two cycle groups.

For the lifted basis, let a_e be the column of coefficients on an old edge e. Its old-edge contribution to the Gram matrix is $\sum_{e \text{ old}} a_e a_e^{\mathsf{T}} = C_0$. Each new edge contributes $\ell_f \ell_f^{\mathsf{T}}$. Adding the contributions proves (8.8). □

Lemma 8.4. *In Lemma 8.3, fix integers $M, t \ge 1$. Replace each old edge of H by a path of length $1 + Mt$ and each new edge by a path of length Mt, with all path interiors disjoint. Call the resulting graph G_t. In the transported integral cycle basis its Gram matrix is*

$$C_t = (1 + Mt)C_0 + MtR \equiv C_0 \pmod{M}. \tag{8.10}$$

If $Mt \ge 2$, the graph G_t is simple, planar, biconnected, of maximum degree at most three, and has girth at least Mt. Its number of vertices is strictly increasing as a function of t.

Proof. Orient each subdivided path consistently with the edge it replaces. At each new vertex of that path, the incidence equation equates its two coefficients. A cycle is therefore constant along the path; restriction and constant extension identify the integral cycle groups. A path of length k contributes $k a_e a_e^{\mathsf{T}}$ to the Gram matrix if its coefficient column is a_e. The old and new contributions are consequently $(1 + Mt)C_0$ and MtR, proving (8.10). Since C_0 is positive definite and R is positive semidefinite, C_t is positive definite.

Subdivide within the given plane embedding of H. Connectedness is preserved, and every new vertex has degree two; hence the maximum degree remains at most three. If $Mt \ge 2$, each edge is replaced by a path with an interior vertex. Each new edge has an interior endpoint belonging to that path only. Within a path the vertices are distinct, and distinct paths have disjoint interiors. The absence of loops in H now excludes both loops and parallel edges in G_t.

The Hamilton cycle contains each of its own edges. For any other edge of H, join its distinct endpoints by a Hamilton-cycle arc. That arc together with the edge is a cycle. Thus every edge of H lies on a cycle. Subdivision replaces such a cycle by a cycle through every edge of the corresponding paths. Thus G_t is bridgeless. Suppose that deleting a vertex v disconnects G_t. Each component of $G_t - v$ must have at least two edges to v: with only one, that edge would be a bridge. Two distinct

components would then give $\deg(v) \geq 4$, a contradiction. The graph has at least three vertices, so it is biconnected.

A cycle that contains an interior vertex of a subdivided path must use both incident edges there. Repeating along the path shows that it traverses the entire path. Every edge belongs to such a path, so any cycle contains an entire path of length at least Mt. Its length is at least Mt. Let m_o, m_n be the numbers of old and new edges of H. The vertex count is

$$|V(G_t)| = |V(H)| + m_o Mt + m_n(Mt - 1). \tag{8.11}$$

Here $m_o + m_n > 0$, since H has a Hamilton cycle. Increasing t by one adds $M(m_o + m_n) > 0$ vertices. □

Proof of Corollary 1.3. Set $(A, b) = \perp_{p \in S}(A_p, b_p)$ and $h = \prod_{p \in S} p$, with empty product one. Use the graph G_0 constructed in the proof of Theorem 1.2. By Lemma 7.6, its chosen plane embedding has an exterior Hamilton cycle. The complementary order in that theorem is prime to every $p \in S$, including those for which $A_p = 0$. Thus

$$(\mathrm{Jac}(G_0)_p, b_{G_0}|_{\mathrm{Jac}(G_0)_p}) \cong (A_p, b_p) \qquad (p \in S). \tag{8.12}$$

Put $P = S \cup \{2\}$, and let p^{e_p} be the exponent of $\mathrm{Jac}(G_0)_p$, with $e_p = 0$ for a zero group. Define

$$M = \prod_{p \in P} p^{2e_p + 1}. \tag{8.13}$$

Choose an integral cycle basis of G_0 using Lemma 8.1, with Gram matrix C_0. The Hamilton cycle is a nonzero integral cycle, so this basis has positive rank. Apply Lemmas 8.3 and 8.4. By Lemma 8.2, $\mathcal{D}(C_0)_p$ has exponent p^{e_p}; the minus sign there changes no group order or exponent. For every $p \in P$, equation (8.10) gives $C_t - C_0 \in p^{2e_p+1}\,\mathrm{Mat}(\mathbb{Z})$. Lemma 7.2 gives an isometry of the p-primary discriminant pairings. Negating both pairings preserves that isometry. Lemma 8.2 therefore yields

$$(\mathrm{Jac}(G_t)_p, b_{G_t}|_{\mathrm{Jac}(G_t)_p}) \cong (\mathrm{Jac}(G_0)_p, b_{G_0}|_{\mathrm{Jac}(G_0)_p}) \qquad (p \in P). \tag{8.14}$$

Combine this with (8.12).

Choose any integer t with $Mt \geq g$. Since $g \geq 3$, Lemma 8.4 gives simplicity, planarity, biconnectivity, maximum degree at most three and girth at least g. There are infinitely many such t. Their vertex counts are strictly increasing by (8.11), so the graphs are pairwise nonisomorphic. If S is empty, the construction starts with the zero paired group and the same proof applies. □

Remark 8.5. Corollary 1.3 prescribes the entire primary paired groups at the primes in S. The proof just given does not prescribe the primary groups at other primes or assert that their sum is cyclic. The stronger construction in Section 9 makes that sum have prime order. Neither construction requires the final graph to be outerplanar or regular of degree three. The degree bound cannot be replaced by two in a universal statement. Indeed, biconnectivity implies minimum degree at least two: a vertex of degree one would be isolated by deletion of its neighbour. A finite connected graph all of whose degrees equal two is a cycle: following edges without reversal first produces a cycle, and its vertices have no additional incident edges, so connectedness excludes any remaining vertices. Its Jacobian is cyclic by Proposition 1.5, applied to $m/(m-1) = [2, \ldots, 2]^-$. It cannot realize a noncyclic primary group.

9. Prime-order complements on a fixed graph

9.1. **Tridiagonal matrices with prescribed primary pairings.**

Lemma 9.1. *Let (A, b) be a finite paired group, and put $d = \max\{1, r(A)\}$. For every finite set P of primes containing the prime divisors of $2|A|$, there is a positive definite symmetric integral tridiagonal matrix C_0 of size d such that*

$$\mathcal{D}(C_0)_p \cong (A_p, b_p) \qquad (p \in P). \tag{9.1}$$

Proof. Put $r_p = \dim_{\mathbb{F}_p}(A_p/pA_p)$. A generating set of A maps to a spanning set of this quotient, so $r(A) \geq r_p$. Conversely, the cyclic–binary decomposition in Lemma 7.3 supplies r_p generators of A_p: a nonzero cyclic block contributes one dimension to A_p/pA_p, and a binary block contributes two. Append zeros to these generating lists to obtain the common length $r = \max_p r_p$. Sum their ith entries over the primes to obtain elements $z_i \in A$, $1 \leq i \leq r$. The primary projection of A onto A_p is multiplication by an integer which is one modulo $\exp A_p$ and zero modulo the exponents of the other primary subgroups. Such an integer exists by the Chinese remainder theorem. Multiplying z_i by it recovers the ith primary generator. Thus $z_1, \dots, z_r$ generate A, and $r(A) = \max_p r_p$. The maximum for $A = 0$ is interpreted as zero.

For each $p \in P$, fix the cyclic–binary decomposition of (A_p, b_p). For a cyclic summand $\left\langle \frac{a}{n} \right\rangle$ with $n = p^s$ and $0 < a < n$, use the one-row matrix $[na]$. In its cokernel the class $a[e_1]$ has order n and self-pairing a/n; since $p \nmid a$, it is the entire p-primary subgroup. For each binary summand at two, use the two-row matrix of Lemma 7.4, with Q empty. Only its 2-primary pairing is relevant here. The block diagonal sum for the prime p has size r_p and has the required p-primary pairing. Append $[1]$ blocks to obtain a positive definite tridiagonal matrix $C^{(p)}$ of size d. If $A_p = 0$, take $C^{(p)} = I_d$.

Write $p^{e_p} = \exp A_p$, with $e_p = 0$ when $A_p = 0$. Choose every diagonal and adjacent entry of a symmetric tridiagonal matrix C_0 to satisfy

$$C_0 \equiv C^{(p)} \pmod{p^{2e_p+1}} \qquad (p \in P). \tag{9.2}$$

These congruences are compatible entry by entry. Choose the adjacent entries negative. Increasing diagonal entries by positive multiples of $\prod_{p\in P} p^{2e_p+1}$ makes each diagonal exceed the sum of the absolute values of its adjacent entries. Put $c_i = -(C_0)_{i,i+1} > 0$, $c_0 = c_d = 0$, and $s_i = (C_0)_{ii} - c_{i-1} - c_i > 0$. Then

$$x^{\mathsf{T}} C_0 x = \sum_{i=1}^{d-1} c_i (x_i - x_{i+1})^2 + \sum_{i=1}^{d} s_i x_i^2 > 0 \qquad (x \neq 0). \tag{9.3}$$

For $d = 1$, the first sum is empty and the single diagonal entry is chosen positive. Lemma 7.2, applied separately with reference matrix $C^{(p)}$, proves (9.1). □

9.2. **An integral cycle basis on a fixed planar graph.** Set Q_1 equal to a triangle. For $d \geq 2$, define a loopless multigraph Q_d on the vertices

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

There is a rung $r_i = u_i v_i$ for each $1 \leq i < d$, a top edge $u_i u_{i+1}$ and a bottom edge $v_i v_{i+1}$ for each $1 \leq i < d-1$, and two further edges: $\ell = u_1 v_1$ and $r = u_{d-1} v_{d-1}$. These further edges are distinct from all the rungs. In particular, Q_2 has two vertices and three parallel edges. The graph has $2d-2$ vertices and $3d-3$ edges; every vertex has degree three. Draw the u_i and v_i in two parallel rows, with ℓ to the left and r to the right. This gives a plane embedding with d bounded faces. In order, these are the left digon, the $d-2$ rectangles, and the right digon.

A tree decomposition of a finite graph consists of a finite tree $\mathcal{T}$ and subsets $X_t \subset V(G)$, called bags, one for each vertex t of $\mathcal{T}$, with the following properties. Every graph vertex belongs to some X_t; every graph edge has both endpoints in some X_t; and, for every $v \in V(G)$, the set of vertices t with $v \in X_t$ induces a connected subtree of $\mathcal{T}$. Its width is $\max_t |X_t| - 1$. The treewidth is the least width of such a decomposition. Parallel edges impose the same endpoint condition as one edge.

Lemma 9.2. *Let $d \geq 1$, and let L be the tridiagonal matrix with diagonal $a_1, \dots, a_d$ and adjacent entries $-c_1, \dots, -c_{d-1}$. Put*

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

Fix an integer $g \geq 3$. If $d = 1$, suppose that $a_1 \geq 3g$. If $d \geq 2$, suppose that

$$c_i \geq g \ (1 \leq i < d), \qquad s_1, s_d \geq g, \qquad s_i \geq 2g \ (2 \leq i < d). \tag{9.4}$$

Then a subdivision Γ of Q_d has an integral cycle basis with Gram matrix L. The graph Γ is simple, planar and biconnected, all its degrees belong to $\{2,3\}$, its girth is at least $2g$, and its treewidth is at most two. Its cycle rank is d, and it has exactly $2d-2$ vertices of degree three.

Proof. Suppose first that $d = 1$. Subdivide the three edges of Q_1 into paths of lengths $g, g, a_1 - 2g$. The resulting graph is a cycle of length a_1. Its oriented cycle is an integral basis with Gram matrix $[a_1]$. It is simple, planar and biconnected, all degrees are two, and its girth is $a_1 \geq 3g$. Label its vertices consecutively $x_0, \dots, x_{a_1-1}$. The path of bags $\{x_0, x_i, x_{i+1}\}$, $1 \leq i \leq a_1 - 2$, is a tree decomposition of width two: it covers every edge, and the bags containing a fixed vertex are consecutive. Its cycle rank is one and it has no degree-three vertex. This proves the lemma for $d = 1$.

Assume henceforth that $d \geq 2$. Replace r_i by a path of length c_i, ℓ by a path of length s_1, and r by a path of length s_d. For $2 \leq i < d$, replace $u_{i-1}u_i$ and $v_{i-1}v_i$ by paths of lengths g and $s_i - g$, respectively. All interiors are pairwise disjoint. Every replacement length is an integer at least g.

In Q_d, the ordinary rungs and the bottom edges form a spanning tree. Its remaining d edges are ℓ, the top edges, and r. Their fundamental cycles are precisely the bounded facial cycles. They form an integral basis by Lemma 8.1. Orient all bounded face boundaries consistently in the plane. Adjacent face boundaries have opposite coefficients on their common rung. On a subdivided path, the incidence equation at each internal vertex forces the two incident coefficients to be equal, when the edges are oriented along the path. Thus restriction to the original edges and constant extension along the replacement paths are inverse isomorphisms of integral cycle groups. The extended facial cycles $z_1, \dots, z_d$ remain an integral basis. Their scalar products are

$$\langle z_i, z_j \rangle = \begin{cases} s_i + c_{i-1} + c_i = a_i, & i = j, \\ -c_i, & j = i+1, \\ -c_j, & i = j+1, \\ 0, & |i-j| > 1. \end{cases} \tag{9.5}$$

This proves the Gram-matrix assertion.

The embedding survives subdivision. Every old edge belongs to a bounded facial cycle, so every new edge belongs to a cycle. An edge lying on a cycle is not a bridge: its endpoints remain joined by the rest of that cycle after its deletion. The graph is connected and bridgeless. Its original vertices have degree three and all other vertices have degree two. Since every old edge has been subdivided, no two edges have the same endpoints, and no edge is a loop; hence Γ is simple. If a vertex w were a cut vertex, each component of $\Gamma - w$ would have at least two edges to w. Otherwise its unique edge to w would be a bridge. At least two components would therefore imply $\deg(w) \geq 4$, a contradiction. Thus Γ is biconnected. A cycle in Γ uses entire replacement paths, because their internal vertices have degree two. It cannot use just one such path: Q_d has no loops. It uses at least two paths, each of length at least g, and therefore has length at least $2g$.

For $d = 2$, the single bag $\{u_1, v_1\}$ is a decomposition of Q_2. For $d \geq 3$, use the bags

$$B_i = \{u_i, v_i, u_{i+1}\}, \qquad D_i = \{v_i, u_{i+1}, v_{i+1}\} \quad (1 \leq i \leq d-2), \tag{9.6}$$

ordered on a path as $B_1, D_1, B_2, D_2, \dots, B_{d-2}, D_{d-2}$. The top edges lie in the B_i, the bottom edges in the D_i, and every rung lies in a bag containing its two endpoints. The same bags cover the additional end edges. For an internal index i, the bags containing u_i are consecutive among B_{i-1}, D_{i-1}, B_i, and those containing v_i are consecutive among D_{i-1}, B_i, D_i. Endpoint indices give subintervals of the same lists. This verifies the connected-subtree condition.

If an edge xy is replaced by $xw_1 \cdots w_k y$, choose a bag containing x, y and attach to it the following chain of new bags:

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

Every new edge is covered. The bags containing x remain connected, those containing y acquire a chain attached to one of their bags, and each new w_i belongs to one or two consecutive new bags.

Perform this operation separately for every old edge. All bags have size at most three. The treewidth is therefore at most two. Subdivision preserves $|E| - |V| + 1 = d$ and changes none of the original degrees. This proves the remaining assertions. □

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

Theorem 9.3. *Let (A, b) be a finite paired group and put $N = |A|$. Put $d = \max\{1, r(A)\}$. For every $h \geq 1$ and $g \geq 3$, there exist positive integers u, v, ω, a nonzero integer κ, and subdivisions Γ_t of Q_d, indexed by integers $t \geq 0$, such that*

$$(\mathrm{Jac}(\Gamma_t), b_{\Gamma_t}) \cong (A, b) \perp \left\langle \tfrac{\kappa}{u+vt} \right\rangle, \tag{9.7}$$

$$\gcd(u, v) = 1, \qquad \gcd(u + vt, 2hN\kappa) = 1 \qquad (t \geq 0). \tag{9.8}$$

Here a cyclic pairing of denominator one means the zero group. Every Γ_t is simple, planar and biconnected, has all degrees in $\{2, 3\}$, girth at least $2g$ and treewidth at most two. Only one replacement path changes with t: the right end path for $d \geq 2$, or a fixed edge path of the triangle for $d = 1$. Its length increases by ωt. In particular,

$$|V(\Gamma_t)| = |V(\Gamma_0)| + \omega t. \tag{9.9}$$

Proof. Let P be the set of prime divisors of $2hN$. Apply Lemma 9.1 to $(A, -b)$, and let C_0 be the resulting matrix. This sign is necessary because Lemma 8.2 identifies the graph pairing with the negative cycle discriminant pairing. The integer d depends only on the generator rank of A. For $p \in P$, write p^{e_p} for the exponent of A_p, with $e_p = 0$ if $A_p = 0$, and set

$$M = \prod_{p \in P} p^{2e_p+1}. \tag{9.10}$$

For $1 \leq i < d$, choose an integer $c_i \geq g$ satisfying

$$-c_i \equiv (C_0)_{i,i+1} \pmod{M}. \tag{9.11}$$

Define the finite set

$$T = \{q : q \text{ prime},\ q \notin P,\ q \mid c_1 \cdots c_{d-1}\}. \tag{9.12}$$

The set T is disjoint from P. If $d = 1$, the product in (9.12) is one and T is empty.

Choose integers $a_1, \ldots, a_d$ subject to

$$\begin{aligned} a_i &\equiv (C_0)_{ii} \pmod{M} && (1 \leq i \leq d), \\ a_1 &\equiv 1 \pmod{q} && (q \in T), \\ a_i &\equiv 1 + c_{i-1}^2 \pmod{q} && (q \in T,\ 2 \leq i \leq d). \end{aligned} \tag{9.13}$$

The moduli M and the primes in T are pairwise coprime, so the Chinese remainder theorem gives solutions. Each a_i may be increased independently by a positive multiple of $M \prod_{q \in T} q$. If $d = 1$, arrange $a_1 \geq 3g$. If $d \geq 2$, arrange

$$a_1 - c_1 \geq g, \quad a_d - c_{d-1} \geq g, \quad a_i - c_{i-1} - c_i \geq 2g \quad (2 \leq i < d). \tag{9.14}$$

Let L have diagonal a_i and adjacent entries $-c_i$, with $c_0 = c_d = 0$ also when $d = 1$. Its quadratic form is

$$x^{\mathsf{T}} L x = \sum_{i=1}^{d-1} c_i (x_i - x_{i+1})^2 + \sum_{i=1}^{d} (a_i - c_{i-1} - c_i) x_i^2. \tag{9.15}$$

All coefficients in the last sum are positive; hence L is positive definite. Equations (9.11) and (9.13) give $L \equiv C_0 \pmod{M}$. Lemma 7.2 yields

$$\mathcal{D}(L)_p \cong (A_p, -b_p) \qquad (p \in P). \tag{9.16}$$

Let Δ_i be the determinant of the leading $i \times i$ block of L, and put $\Delta_0 = 1$. Expansion in the last row gives

$$\Delta_1 = a_1, \qquad \Delta_i = a_i\Delta_{i-1} - c_{i-1}^2\Delta_{i-2} \quad (2 \le i \le d). \tag{9.17}$$

Indeed, the last diagonal term contributes $a_i\Delta_{i-1}$; the term using the last off-diagonal entry must also use its symmetric partner and contributes $-c_{i-1}^2\Delta_{i-2}$. By (9.13), induction on i gives

$$\Delta_i \equiv 1 \pmod{q} \qquad (q \in T,\ 0 \le i \le d). \tag{9.18}$$

Every leading block is positive definite by restriction of (9.15), so its determinant is positive. Put

$$D = \Delta_d > 0, \qquad F = \Delta_{d-1} > 0. \tag{9.19}$$

By Lemma 2.1, $|\mathcal{D}(L)| = D$. For a prime p and a positive integer m, let $v_p(m)$ be the largest integer $j \ge 0$ with $p^j \mid m$. Equation (9.16) gives $v_p(D) = v_p(|A_p|) = v_p(N)$ for every $p \in P$. Every prime divisor of N belongs to P. Hence

$$u = D/N \in \mathbb{Z}_{>0}, \qquad \gcd\left(u, \prod_{p\in P} p\right) = 1. \tag{9.20}$$

For $q \in T$, one has $q \nmid N$ and $D \equiv 1 \pmod{q}$, so $q \nmid u$.

Set

$$K = M\prod_{q\in T} q, \qquad v = KF, \qquad \omega = NK. \tag{9.21}$$

These integers satisfy

$$\gcd(u, v) = \gcd(u, NF) = 1. \tag{9.22}$$

No prime in $P \cup T$ divides u. If $d = 1$, then $F = \Delta_0 = 1$, so $\gcd(u, F) = 1$. Suppose now that $d \ge 2$. If a prime $q \notin P \cup T$ divided both u and F, then it would divide D and F and would divide none of the c_i. Reducing (9.17) modulo q, the equalities $\Delta_d = \Delta_{d-1} = 0$ would imply $\Delta_{d-2} = 0$. Repetition would imply $\Delta_0 = 0$, contrary to $\Delta_0 = 1$. Thus $\gcd(u, F) = 1$. All prime divisors of K and N belong to $P \cup T$, which proves (9.22).

For $t \ge 0$, define

$$L_t = L + \omega t\, e_d e_d^{\mathsf{T}}, \qquad c(t) = u + vt. \tag{9.23}$$

Only the last diagonal entry changes. Its cofactor is F, independent of t, and therefore

$$\det L_t = D + \omega F t = Nc(t), \qquad (L_t^{-1})_{dd} = \frac{F}{Nc(t)}. \tag{9.24}$$

Since $L_t - L$ is divisible by M, Lemma 7.2 preserves (9.16) for every t. The matrix L_t is positive definite, since $x^{\mathsf{T}}L_t x = x^{\mathsf{T}}Lx + \omega t x_d^2 > 0$ for $x \ne 0$. Each prime divisor of $2hN$ divides K and hence v, but does not divide u. Also $F \mid v$ and $\gcd(u, F) = 1$. Consequently

$$\gcd(c(t), 2hNF) = 1 \qquad (t \ge 0). \tag{9.25}$$

In $\mathcal{D}(L_t)$ let $x_t = N[e_d]$. The adjugate identity $L_t\,\mathrm{adj}(L_t) = Nc(t)I$ gives $c(t)x_t = 0$. By (9.24), its self-pairing is

$$b_{\mathcal{D}(L_t)}(x_t, x_t) = \frac{NF}{c(t)} \pmod{\mathbb{Z}}. \tag{9.26}$$

This value has order $c(t)$ by (9.25). Thus x_t has order exactly $c(t)$. Its cyclic subgroup is nondegenerate: if kx_t pairs trivially with x_t, then $c(t) \mid kNF$, hence $c(t) \mid k$. The sum of the primary subgroups at primes in P has order N and pairing $(A, -b)$; the order of the entire group is $Nc(t)$. Since $c(t)$ is prime to every prime in P, $\langle x_t\rangle$ is precisely the sum of all remaining primary subgroups. Primary orthogonality gives

$$\mathcal{D}(L_t) \cong (A, -b) \perp \left\langle \tfrac{NF}{c(t)} \right\rangle. \tag{9.27}$$

This also holds when $c(t) = 1$.

Apply Lemma 9.2 to L_t with the fixed parameter g. All lengths remain fixed except that of the right end path when $d \geq 2$, or the third triangle-edge path when $d = 1$; that length increases by ωt. Its integral cycle Gram matrix is L_t. Lemma 8.2 and (9.27) prove (9.7) with $\kappa = -NF$. Equation (9.25) proves the second assertion of (9.8); the first is (9.22). Adding ωt edges to one subdivided path adds exactly ωt vertices, proving (9.9). All graph-theoretic assertions follow from Lemma 9.2. □

Proof of Theorem 1.1. Apply Theorem 9.3. Dirichlet's theorem [6] states that if u, v are positive coprime integers, then $u + vt$ is prime for infinitely many integers $t \geq 0$. For each such t, put $\ell = u + vt$ and take $G_\ell = \Gamma_t$. Equation (9.8) gives $\ell \nmid 2h|A|\kappa$, and (9.7) gives the required entire paired Jacobian. Its order is $|A|\ell$, so different primes give nonisomorphic graphs. The stronger girth bound $2g$ implies the stated bound g. The fixed graph is Q_d; it depends only on $d = \max\{1, r(A)\}$.

For any connected graph H, Lemma 8.2 presents $\mathrm{Jac}(H)$ by a square matrix of size $\beta(H)$. Thus it has at most $\beta(H)$ generators. If $\mathrm{Jac}(H)$ has a quotient isomorphic to A, then $\beta(H) \geq r(A)$. A nontrivial prime-order summand also gives $\beta(H) \geq 1$. Consequently every graph in the statement has $\beta(H) \geq d$, and the constructed graphs attain equality. In any biconnected graph of maximum degree three, every vertex has degree two or three. If n_2, n_3 count these vertices, then $2|E| = 2n_2 + 3n_3$ and $|V| = n_2 + n_3$, so

$$\beta(H) = 1 + \frac{n_3}{2}.$$

The number $2d - 2$ of degree-three vertices is therefore also minimal within that class. □

Corollary 9.4. *Theorem 1.2 holds with $|C|$ prime. More precisely, there are infinitely many such primes, avoiding the prime divisors of $2h|A|$, and pairwise nonisomorphic biconnected outerplanar loopless multigraphs realizing the corresponding orthogonal sums.*

Proof. If $r(A) \leq 1$, Theorem 1.1 realizes the desired sums by cycles, which are outerplanar. Suppose that $r(A) \geq 2$. Perform the construction in the proof of Theorem 9.3 with $(A, -b)$ in place of (A, b). Then (9.27) has first summand (A, b). The matrices L_t have negative adjacent entries and positive row sums by (9.14) and (9.23). Lemma 7.6 realizes L_t as the reduced Laplacian of a biconnected outerplanar loopless multigraph. Its pairing is the positive discriminant pairing, by Lemma 2.3. Thus its paired Jacobian is $(A, b) \perp \left\langle \frac{NF}{u+vt} \right\rangle$. Dirichlet's theorem selects infinitely many prime denominators; (9.25) gives the asserted avoidance. The Jacobian orders distinguish the graphs. □

9.4. **A hyperbolic plane and one prime-order summand.**

Proposition 9.5. *For every prime $q \equiv 7 \pmod 8$, let Θ_q have two vertices joined by three internally disjoint paths of lengths $2, 6, (q-3)/2$. Then*

$$(\mathrm{Jac}(\Theta_q), b_{\Theta_q}) \cong \mathcal{E}_2 \perp \left\langle \tfrac{-2}{q} \right\rangle. \tag{9.28}$$

The graph is simple, planar and biconnected and has maximum degree three. There are infinitely many such primes.

Proof. All three lengths are integers at least two. Orient the three paths from the first common endpoint to the second, in the order $2, 6, (q-3)/2$. An integral cycle is constant on each path and has coefficients (α, β, γ) with $\alpha + \beta + \gamma = 0$. The vectors $z_1 = (1, -1, 0)$ and $z_2 = (-1, 0, 1)$ are an integral basis, because $(\alpha, \beta, \gamma) = -\beta z_1 + \gamma z_2$. Their Gram matrix is

$$C_q = \begin{pmatrix} 8 & -2 \\ -2 & (q+1)/2 \end{pmatrix} = 2B_q, \quad B_q = \begin{pmatrix} 4 & -1 \\ -1 & (q+1)/4 \end{pmatrix}, \quad \det B_q = q. \tag{9.29}$$

In particular, $\det C_q = 4q$ and

$$C_q^{-1} = \frac{1}{4q} \begin{pmatrix} (q+1)/2 & 2 \\ 2 & 8 \end{pmatrix}.$$

The identity $B_q \operatorname{adj}(B_q) = qI$ shows that every class of $\mathcal{D}(C_q)$ is annihilated by $2q$. The classes $q[e_1], q[e_2]$ are annihilated by two and are independent modulo two: if $q(xe_1 + ye_2) \in 2B_q\mathbb{Z}^2$, then x, y are even. They form the full subgroup of order four. In the negative cycle pairing their self-pairings are $-q(q+1)/8$ and $-2q$, both integers, and their mixed pairing is $-q/2 = 1/2$ modulo $\mathbb{Z}$. Thus this subgroup has pairing $\mathcal{E}_2$.

The class $4[e_2]$ is annihilated by q, has self-pairing $-32/q$, and therefore has order q. Choose w with $4w \equiv 1 \pmod{q}$. The self-pairing of $4w[e_2]$ is $-32w^2/q$. Since $16w^2 \equiv 1 \pmod{q}$, it equals $-2/q$ modulo $\mathbb{Z}$. The two primary subgroups are orthogonal and their orders multiply to $4q$, proving (9.28).

Draw three arcs with the same two endpoints and disjoint interiors in the sphere, and subdivide them into the prescribed paths. This gives a planar drawing. Each path has length at least two and its interior is disjoint from those of the other paths, so there are neither loops nor parallel edges. The two common endpoints have degree three and every other vertex has degree two. Deleting a common endpoint leaves three paths joined at the other endpoint. Deleting an interior vertex of one path leaves the other two paths joined at both endpoints, with each remaining portion of the broken path attached at one endpoint. Thus every one-vertex deletion leaves a connected graph. The graph has at least three vertices, so it is biconnected. Finally, 7 and 8 are positive and coprime; Dirichlet's theorem gives infinitely many primes of the form $7 + 8t$, with $t \geq 0$. □

Remark 9.6. Theorem 1.1 does not prescribe the prime ℓ or the isometry class of its cyclic pairing. The proof prescribes a primitive arithmetic progression of possible orders and a constant numerator κ. It neither makes the graph regular of degree three nor bounds its number of vertices independently of ℓ. The graph is not asserted to be outerplanar. The number of degree-three vertices depends only on $r(A)$ and is the least possible within the biconnected subcubic class with the prescribed paired Jacobian. Corollary 2.5 excludes an exact graph realization of $\mathcal{E}_2$ without a nontrivial complementary group; Proposition 9.5 exhibits prime-order complements for that pairing. For $r(A) = 2$, the fixed graph Q_2 has three parallel edges. Thus every finite paired group of generator rank two admits such prime-order completions by theta graphs with arbitrarily long paths.

References

[1] 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), no. 2, 167–198. 10.24033/bsmf.2303.

[2] S. Bosch and D. Lorenzini, *Grothendieck's pairing on component groups of Jacobians*, Invent. Math. **148** (2002), no. 2, 353–396. 10.1007/s002220100195.

[3] 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. arXiv:1907.08450v1 (2019).

[4] H. Chen and B. Mohar, *The sandpile group of polygon rings and twisted polygon rings*, Graphs Combin. **38** (2022), no. 4, Paper No. 113. 10.1007/s00373-022-02514-x. arXiv:2011.08702v1 (2020).

[5] 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. arXiv:1402.5129v2.

[6] 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, arXiv:0808.1408v2 (2014).

[7] 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), no. 4, 781–801. 10.1007/s00026-018-0406-0. The conjecture and theorem numbering used here is that of arXiv:1410.5144v2 (18 September 2017).

[8] J. E. Greene, *The lens space realization problem*, Ann. of Math. (2) **177** (2013), no. 2, 449–511. 10.4007/annals.2013.177.2.3.

[9] 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. The numbering cited here is that of arXiv:2311.07078v1 (2023).

[10] R. Miranda, *Nondegenerate symmetric bilinear forms on finite abelian 2-groups*, Trans. Amer. Math. Soc. **284** (1984), no. 2, 535–542. 10.1090/S0002-9947-1984-0743731-1.

[11] 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. The numbering cited here is that of arXiv:2210.08526v1 (2022).

[12] A. Nifa, *Homocyclic Jacobians of planar biconnected graphs*, preprint, 13 pp., 10.5281/zenodo.22859833.

[13] J. Shen, *Quantative universality for cokernels of matrices with symmetries*, preprint, arXiv:2601.09704v1 (2026), Theorem 1.2.

[14] F. Shokrieh, *The monodromy pairing and discrete logarithm on the Jacobian of finite graphs*, J. Math. Cryptol. **4** (2010), no. 1, 43–56. 10.1515/JMC.2010.002.

[15] C. T. C. Wall, *Quadratic forms on finite groups, and related topics*, Topology **2** (1963), no. 4, 281–298. 10.1016/0040-9383(63)90012-0.

[16] 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. arXiv:1402.5149v2. See also the author's errata.

Toulouse, France
Email address: nifa.anass@gmail.com