Ann. Comb. 22 (2018) 781–801

Published online November 2, 2018
https://doi.org/10.1007/s00026-018-0406-0

Annals of Combinatorics

Realization of Groups with Pairing as Jacobians of Finite Graphs

Louis Gaudet, David Jensen, Dhruv Ranganathan, Nicholas Wawrykow and Theodore Weisman

Abstract. We study which groups with pairing can occur as the Jacobian of a finite graph. We provide explicit constructions of graphs whose Jacobian realizes a large fraction of odd groups with a given pairing. Conditional on the generalized Riemann hypothesis, these constructions yield all groups with pairing of odd order, and unconditionally, they yield all groups with pairing whose prime factors are sufficiently large. For groups with pairing of even order, we provide a partial answer to this question, for a certain restricted class of pairings. Finally, we explore which finite abelian groups occur as the Jacobian of a simple graph. There exist infinite families of finite abelian groups that do not occur as the Jacobians of simple graphs.

Mathematics Subject Classification. 05C25, 14T05.

Keywords. Graph Jacobians, Groups with pairing.

1. Introduction

Given a finite graph G, there is naturally associated group $\mathrm{Jac}(G)$, the *Jacobian* of G. The group $\Gamma = \mathrm{Jac}(G)$ comes with a symmetric, bilinear, nondegenerate pairing [10,14]:

$$\langle \cdot, \cdot \rangle : \Gamma \times \Gamma \to \mathbb{Q}/\mathbb{Z},$$

known as the *monodromy pairing*. Groups with such a pairing will be referred to simply as *groups with pairing*. Clancy et al. [6] observed that the Jacobian of a randomly generated graph is cyclic with probability close to 0.79. This probability agrees with the well-known Cohen–Lenstra heuristics, which predict that a finite abelian group Γ should occur with probability proportional to $\frac{1}{|\mathrm{Aut}(\Gamma)|}$. However, other classes of groups violate these heuristics. This is because the Jacobian of a graph should really be thought of as a group, together with a duality pairing. In loc. cit., it is conjectured that a group with pairing $(\Gamma, \langle\cdot,\cdot\rangle)$ should occur with probability proportional to $\frac{1}{|\Gamma||\mathrm{Aut}(\Gamma,\langle\cdot,\cdot\rangle)|}$. This is further suggested by the empirical evidence of [5] and proven in [16].

Given a finite abelian group with pairing Γ, the probability that a random graph has Jacobian isomorphic to Γ is zero [16], so it is possible that some groups with pairing do not occur at all. In the present text, we investigate precisely which finite abelian groups with pairing can occur as the Jacobian of a finite graph. Our main result is the following.

Theorem 1.1. *Let Γ be a finite abelian group with pairing. There exists a finite set of primes $\mathscr{P} \subset \mathbb{Z}$ such that, if $|\Gamma|$ is not divisible by any $p \in \mathscr{P}$, then there exists a graph G such that*

$$\Gamma \cong \mathrm{Jac}(G)$$

as groups with pairing.

It is our expectation that the set of primes $\mathscr{P}$ appearing in Theorem 1.1 consists of only the prime 2. We have the following result, conditional on the generalized Riemann hypothesis [8].

Theorem 1.2 (Conditional on GRH). *Let Γ be a finite abelian group with pairing of odd order. Then, there exists a graph G such that*

$$\Gamma \cong \mathrm{Jac}(G)$$

as groups with pairing.

Remark 1.3. The above results are related to the following purely number theoretic question. *Given a prime p, does there exist a prime $q < 2\sqrt{p}$, with $q \equiv 3 \mod 4$, such that q is a quadratic nonresidue modulo p?* Numerical evidence suggests that this condition should be satisfied for all sufficiently large primes p.

An interesting variation on the question considered here was studied by Bosch and Lorenzini in [4, Proposition 5.2]. They consider the representation of groups with pairing arising from *arithmetical graphs*. While the strategy of our proof bears some similarities to that found in loc. cit., the presence of arithmetical structure simplifies the classification problem. Indeed, as shown in [4, Example 5.4], in the case of arithmetical graphs, one can take the underlying graph to be a tree. Our setting is motivated by considerations in tropical geometry and the graph theoretic Abel–Jacobi theory of Baker and Norine.

Jacobians of wedge sums of graphs decompose canonically as the orthogonal direct sum of the Jacobians of their components. A structure theorem for groups with pairing, therefore, allows us to focus primarily on the case where Γ is cyclic. When Γ is a 2-group, however, this structure result is more complicated. There are 4 *nonexceptional* natural pairings on the group $\mathbb{Z}/2^r\mathbb{Z}$, and we find graphs which realize these groups with pairings. There are, in addition, 2 exceptional families of pairings on the group $(\mathbb{Z}/2^r\mathbb{Z})^2$ that do not decompose as the orthogonal direct sum of cyclic groups with pairing. We refer to Sect. 2 for background regarding pairings on 2-groups.

Theorem 1.4. *Let $\Gamma \cong (\mathbb{Z}/2^r\mathbb{Z}, \langle\cdot,\cdot\rangle)$ be a cyclic 2-group with nonexceptional pairing $\langle\cdot,\cdot\rangle$. Then, there exists a graph G such that*

$$\Gamma \cong \mathrm{Jac}(G)$$

as groups with pairing.

We discuss groups with exceptional pairings in further detail in Sect. 4.2.

If we forget the structure of the pairing on Γ, it is elementary to observe that every finite abelian group Γ occurs as the Jacobian of a multigraph G. Naively, however, the construction often necessitates the use of graphs with multiple edges. Since the Erdős–Rényi random graphs studied in [5,6,16] are always simple, we find it natural to ask the following.

Question. Which finite abelian groups (without a specified pairing) occur as the Jacobian of a simple graph?

We find that there are infinite families of finite groups that do not occur as the Jacobians of simple graphs.

Theorem 1.5. *For any $k \geq 1$, there exists no simple graph G such that*

$$\mathrm{Jac}(G) \cong (\mathbb{Z}/2\mathbb{Z})^k.$$

More generally, we have the following result for groups with a large number of $\mathbb{Z}/2\mathbb{Z}$ invariant factors.

Theorem 1.6. *Let H be a finite abelian group. Then, there exists a natural number k_H depending on H, such that for all $k > k_H$, there does not exist a simple graph G with*

$$\mathrm{Jac}(G) \cong (\mathbb{Z}/2\mathbb{Z})^k \times H.$$

2. Background

2.1. Jacobians of Graphs

We briefly recall the basics of divisor theory on graphs. We refer to [2] for further details. In this paper, a *graph* will mean a finite connected graph, possibly with multiple edges, but without loops at vertices. A *simple graph* is a graph without multiple edges. A *divisor* on a graph is an integral linear combination of vertices, and we write a divisor as

$$D = \sum_{v \in V(G)} D(v)v,$$

where each $D(v)$ is an integer. The *degree* of a divisor D is as follows:

$$\deg(D) = \sum_{v \in V(G)} D(v).$$

It is common to think of a divisor as a configuration of "chips" and "anti-chips" on the vertices of the graph, so that the degree is just the total number of chips.

Let $\mathcal{M}(G) := \text{Hom}(V(G), \mathbb{Z})$ be the group of integer-valued functions on the vertices of G. For $f \in \mathcal{M}(G)$, we define

$$\text{ord}_v(f) := \sum_{e=vw \text{ edge containing } v} (f(v) - f(w)),$$

and

$$\text{div}(f) := \sum_{v \in V(G)} \text{ord}_v(f) v.$$

Divisors that arise as $\text{div}(f)$ for a function $f \in \mathcal{M}(G)$ are referred to as *principal*. We say that two divisors D_1 and D_2 are *equivalent*, and write $D_1 \sim D_2$, if their difference is principal.

Equivalence of divisors is related to the well-known "chip-firing game" on graphs, which can be described as follows. Given a divisor D and a vertex v, the *chip-firing move* centered at v corresponds to the vertex v giving one chip to each of its neighbors. That is, the vertex v loses a number of chips equal to its valence, and each neighbor gains exactly 1 chip. Two divisors are equivalent if one can be obtained from the other by a sequence of chip-firing moves.

Note that the degree of a divisor is invariant under equivalence. The *Jacobian* $\text{Jac}(G)$ is the group of equivalence classes of divisors of degree zero. The Jacobian of a connected graph is always a finite group, with order equal to the number of spanning trees in G (see [3]).

For the most part, we will not need any deep structural results about the Jacobians of graphs. The following result, however, will greatly simplify one of our proofs in the later sections.

Theorem 2.1 ([7, Theorem 2]). *Let G be a planar graph and let $G^\star$ be a planar dual of G. Then, the Jacobian of G and $G^\star$ are isomorphic as groups.*

The Jacobian of a graph comes equipped with a bilinear pairing, known as the *monodromy pairing*, defined as follows. Given two divisors $D_1, D_2 \in \text{Jac}(G)$, first find an integer m such that mD_1 is principal—that is, there exists a function $f \in \mathcal{M}(G)$ such that $\text{div}(f) = mD_1$. Then, we define the following:

$$\langle D_1, D_2 \rangle = \frac{1}{m} \sum_{v \in V(G)} D_2(v) f(v).$$

It is of course not immediately clear that the pairing above is nondegenerate. A proof may be found in [14, Theorem 3.4].

Remark 2.2. Note that the isomorphism of Jacobians of planar dual graphs does *not*, in general, preserve the pairings (see, for instance, Corollary 3.3).

2.2. Reduced Divisors and Dhar's Burning Algorithm

Given a divisor D and a vertex v_0, we say that D is v_0-*reduced* if

1. $D(v) \geq 0$ for all vertices $v \neq v_0$, and

2. every nonempty set $A \subseteq V(G) \smallsetminus \{v_0\}$ contains a vertex v such that $\mathrm{outdeg}_A(v) > D(v)$.

By [2, Proposition 3.1], every divisor is equivalent to a unique v_0-reduced divisor.

There is a simple algorithm for determining whether a given divisor satisfying (1) above is v_0-reduced, known as *Dhar's burning algorithm*. For $v \neq v_0$, imagine that there are $D(v)$ buckets of water at v. Now, light a fire at v_0. The fire consumes the graph, burning an edge if one of its endpoints is burnt, and burning a vertex v if the number of burnt edges adjacent to v is greater than $D(v)$ (that is, there is not enough water to fight the fire). The divisor D is v_0-reduced if and only if the fire consumes the whole graph. For a detailed account of this algorithm, we refer to [3, Section 5.1] and [9].

2.3. Jacobians of Wedge Sums of Graphs

Given two graphs with distinguished vertices (G_1, v_1) and (G_2, v_2), the *wedge sum* is the graph formed by identifying v_1 and v_2. We suppress the dependence on the choice of distinguished vertices in what follows, as the choice will not matter, denoting the wedge sum as $G_1 \vee G_2$. A key tool in our proof is the fact that the Jacobian of a wedge sum of graphs is the orthogonal direct sum of the Jacobians.

Proposition 2.3. *Let G_1 and G_2 be graphs. Then*

$$\mathrm{Jac}(G_1 \vee G_2) \cong \mathrm{Jac}(G_1) \oplus \mathrm{Jac}(G_2),$$

where $\oplus$ denotes the orthogonal direct sum of finite abelian groups with pairing.

Proof. This follows from the fact that any piecewise linear function on G corresponds to a piecewise linear function on G_i by restriction, and conversely, any function on G_i can be extended to a function on G by giving it a constant value on $G \smallsetminus G_i$. $\square$

2.4. Structure Results for Groups with Pairing

Our arguments will rely heavily on the classification of finite abelian groups with pairing from [12, 15]. A first step in this classification is the following.

Lemma 2.4. *Let Γ be a group with pairing $\langle \cdot, \cdot \rangle$, and suppose that there exist subgroups $\Gamma_1, \Gamma_2 \subseteq \Gamma$ such that $\Gamma \cong \Gamma_1 \times \Gamma_2$ as groups. If the orders of Γ_1 and Γ_2 are relatively prime, then Γ is isomorphic to the orthogonal direct sum $\Gamma_1 \oplus \Gamma_2$.*

Lemma 2.4 reduces the classification of finite abelian groups with pairing to the classification of p-groups with pairing. In light of Proposition 2.3, this lemma allows us to focus on constructing graphs whose Jacobian is a given p-group with pairing.

If p is an odd prime, then there are precisely two isomorphism classes of pairings on $\mathbb{Z}/p^r\mathbb{Z}$, for $r \geq 1$. More precisely, every nondegenerate pairing on $\mathbb{Z}/p^r\mathbb{Z}$ is of the form:

$$\langle x, y \rangle_a = \frac{axy}{p^r},$$

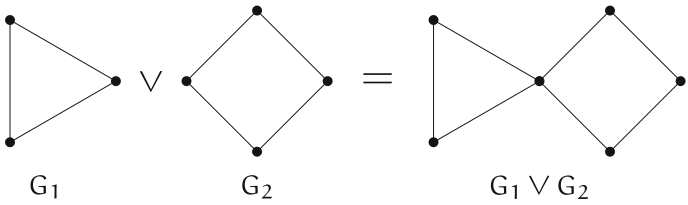

Figure 1. Wedge sum operation on graphs. In this case, $\mathrm{Jac}(G_1) \cong \mathbb{Z}/3\mathbb{Z}$, $\mathrm{Jac}(G_2) \cong \mathbb{Z}/4\mathbb{Z}$, and $\mathrm{Jac}(G_1 \vee G_2) \cong \mathbb{Z}/12\mathbb{Z}$

for some integer a not divisible by p. Two such pairings $\langle \cdot, \cdot \rangle_a, \langle \cdot, \cdot \rangle_b$ are isomorphic if and only if the Legendre symbols of a and b are equal. We will refer to these two pairings as the *residue* and *nonresidue* pairings. The following is a fundamental result for groups with pairing (see Fig. 1).

Theorem 2.5. *If p is an odd prime, then every finite abelian p-group with pairing decomposes as an orthogonal direct sum of cyclic groups with pairing.*

When $p = 2$, the situation is somewhat more intricate. Up to isomorphism, there are four distinct isomorphism classes of pairings on $\mathbb{Z}/2^r\mathbb{Z}$, which we refer to as the *nonexceptional pairings*. These are given as follows:

$$\mathcal{A}_{2^r} \cong (\mathbb{Z}/2^r\mathbb{Z}, \langle \cdot, \cdot \rangle), r \geq 1; \quad \langle x, y \rangle = \frac{xy}{2^r}$$
$$\mathcal{B}_{2^r} \cong (\mathbb{Z}/2^r\mathbb{Z}, \langle \cdot, \cdot \rangle), r \geq 2; \quad \langle x, y \rangle = \frac{-xy}{2^r}$$
$$\mathcal{C}_{2^r} \cong (\mathbb{Z}/2^r\mathbb{Z}, \langle \cdot, \cdot \rangle), r \geq 3; \quad \langle x, y \rangle = \frac{5xy}{2^r}$$
$$\mathcal{D}_{2^r} \cong (\mathbb{Z}/2^r\mathbb{Z}, \langle \cdot, \cdot \rangle), r \geq 3; \quad \langle x, y \rangle = \frac{-5xy}{2^r}.$$

In addition, on $(\mathbb{Z}/2^r\mathbb{Z})^2$, there are two isomorphism classes of pairings that do not decompose as an orthogonal direct sum of cyclic groups with pairing. We refer to these as the *exceptional pairings*:

$$\mathcal{E}_{2^r} \cong ((\mathbb{Z}/2^r\mathbb{Z})^2, \langle \cdot, \cdot \rangle), r \geq 1; \quad \langle e_i, e_j \rangle = \begin{cases} 0, & i = j \\ \frac{1}{2^r}, & \text{otherwise} \end{cases}$$
$$\mathcal{F}_{2^r} \cong ((\mathbb{Z}/2^r\mathbb{Z})^2, \langle \cdot, \cdot \rangle), r \geq 2; \quad \langle e_i, e_j \rangle = \begin{cases} \frac{1}{2^{r-1}}, & i = j \\ \frac{1}{2^r}, & \text{otherwise,} \end{cases}$$

where e_i and e_j are generators for $(\mathbb{Z}/2^r\mathbb{Z})^2$.

We note the following two results of Miranda [12].

Lemma 2.6. *Let Γ be a finite abelian group of order 2^r, with pairing $\langle \cdot, \cdot \rangle$. If $\langle x, x \rangle = \frac{a}{2^r}$ for some $x \in \Gamma$ and odd positive integer a, then Γ is cyclic generated by x. Furthermore, for some $c \in \{\pm 1, \pm 5\}$, with $c \equiv a \pmod 8$, there is an isomorphism of groups $\phi : \Gamma \to \mathbb{Z}/2^r\mathbb{Z}$ such that*

$$\langle x, y \rangle = \frac{c\phi(x)\phi(y)}{2^r}.$$

Figure 2. Three-banana graph and the subdivided banana $B_{(4,2,3)}$

Theorem 2.7. *The groups $\mathcal{A}_{2^r}, \mathcal{B}_{2^r}, \mathcal{C}_{2^r}, \mathcal{D}_{2^r}, \mathcal{E}_{2^r}, \mathcal{F}_{2^r}$ generate all 2-groups with pairing under orthogonal direct sum.*

3. Odd Groups with Pairing

In this section, we investigate which groups with pairing of odd order occur as the Jacobian of a graph. The decomposition of the Jacobian of a wedge sum as the orthogonal sum of the Jacobians of its components reduces our goal to the following.

Problem. Given a pairing $\langle\cdot,\cdot\rangle$ on the group $\mathbb{Z}/p^r\mathbb{Z}$ with p odd, find a graph G such that $\mathrm{Jac}(G)$ is isomorphic to $\mathbb{Z}/p^r\mathbb{Z}$, such that $\langle\cdot,\cdot\rangle$ is induced by the monodromy pairing.

When $p = 2$, which we consider in Sect. 4, we must also consider the nondecomposable pairings on $\mathbb{Z}/2^r\mathbb{Z} \times \mathbb{Z}/2^r\mathbb{Z}$.

3.1. Subdivided Banana Graphs

We begin with the following construction.

Construction 1. Let $\mathbf{s} = (s_1, \ldots, s_m)$ be a tuple of positive integers. Let B_m denote the so-called "banana graph", which has two vertices and m edges between them. Construct the $\mathbf{s}$-*subdivided banana graph* from B_m by subdividing the ith edge $s_i - 1$ times. We denote this graph by $B_{\mathbf{s}}$, see Fig. 2.

Proposition 3.1. *Fix a prime p and an integer r. Let $\mathbf{s} = (s_1, \ldots, s_m)$ be a tuple of positive integers such that*

$$\sum_{i=1}^{m} \frac{\prod_{j=1}^{m} s_j}{s_i} = p^r,$$

and $\gcd(s_i, p) = 1$ *for all i. Then*

$$\mathrm{Jac}(B_{\mathbf{s}}) \cong (\mathbb{Z}/p^r\mathbb{Z}, \langle\cdot,\cdot\rangle),$$

where $\langle\cdot,\cdot\rangle$ is the pairing on $\mathbb{Z}/p^r\mathbb{Z}$ given by

$$\langle x, y\rangle = \frac{\left(\prod_{i=1}^{m} s_i\right) xy}{p^r}.$$

Proof. We first show that $|\operatorname{Jac}(B_{\mathbf{s}})| = p^r$. Every spanning tree of $B_{\mathbf{s}}$ is obtained by deleting one edge each from all but one of the subdivided edges of B_m. It follows that the number of spanning tees of $B_{\mathbf{s}}$ is as follows:

$$\sum_{i=1}^{m} \frac{\prod_{j=1}^{m} s_j}{s_i} = p^r.$$

We now show that $\operatorname{Jac}(B_{\mathbf{s}})$ is cyclic by exhibiting a generator. Let v and w be the two vertices of $B_{\mathbf{s}}$ of valence m pictured in Fig. 2, and consider the divisor $D = v - w$. Note that the order of D must be a power of p, and let $t \le r$ be the smallest nonnegative integer such that $p^t D$ is equivalent to 0. By definition, there exists a function $f : V(G) \to \mathbb{Z}$ such that $\operatorname{div}(f) = p^t D$.

Orienting the graph, so that the head of each edge points toward w, and for each edge e with head x and tail y, let $b(e) = f(x) - f(y)$. Since $D(v) = 0$ for any $v \in V(G) \setminus \{v, w\}$, we must have $b(e_1) = b(e_2)$ for any two edges in the same subdivided edge of B_m, and we may, therefore, write $b_i = b(e)$ for any edge e in the ith subdivided edge. Observe that $b_i s_i = f(w) - f(v)$ for all i. As $\operatorname{div}(f) = p^t D$, we may conclude that $\sum_{i=0}^{m} b_i = p^t$. Consequently,

$$p^t = \sum_{i=1}^{m} \frac{f(w) - f(v)}{s_i} = \frac{(f(w) - f(v))p^r}{\prod_{i=1}^{m} s_i}.$$

From this, we deduce

$$\prod_{i=1}^{m} s_i = p^{r-t}(f(w) - f(v)).$$

Since $\gcd(s_i, p) = 1$ for all i, this is impossible unless $r = t$, and thus, the group is cyclic, generated by D.

The monodromy pairing on $\operatorname{Jac}(B_{\mathbf{s}})$ is fully determined by the value of $\langle D, D \rangle$. Consider a function $f : V(G) \to \mathbb{Z}$ such that $b_i = \frac{\prod_{j=1}^{m} s_j}{s_i}$. We see that $\operatorname{div}(f) = p^r D$, and hence, $\langle D, D \rangle = \frac{\prod_{i=1}^{m} s_i}{p^r}$. □

Remark 3.2. We have recently become aware that Proposition 3.1 was proven earlier in [10, Section 2]. We, nevertheless, reprove it here, as the argument is simple and the banana graph $B_{\mathbf{s}}$ is central to our later constructions.

The cycle graph C_n and the banana graph B_n are both special cases of the subdivided banana. The following is an immediate corollary.

Corollary 3.3. *For any prime p and integer r:*

$$\operatorname{Jac}(B_{p^r}) \cong (\mathbb{Z}/p^r\mathbb{Z}, \langle \cdot, \cdot \rangle_1)$$
$$\operatorname{Jac}(C_{p^r}) \cong (\mathbb{Z}/p^r\mathbb{Z}, \langle \cdot, \cdot \rangle_{-1}),$$

where $\langle \cdot, \cdot \rangle_1$ and $\langle \cdot, \cdot \rangle_{-1}$ are the pairings on $\mathbb{Z}/p^r\mathbb{Z}$ given by the following:

$$\langle x, y \rangle_1 = \frac{xy}{p^r} \qquad \langle x, y \rangle_{-1} = \frac{(-1)xy}{p^r}.$$

3.2. Results on Quadratic Residues

Observe that the monodromy pairing on $\mathrm{Jac}(B_{p^r})$ is the residue pairing on $\mathbb{Z}/p^r\mathbb{Z}$. To achieve the nonresidue pairing, we will use the subdivided banana graph $B_{\mathbf{s}}$ for an appropriate choice of $\mathbf{s}$. Our approach will rely on quadratic reciprocity, and it will be necessary to consider the cases $p \equiv 1 \pmod 4$ and $p \equiv 3 \pmod 4$ separately.

Proposition 3.4. *For any sufficiently large prime p, there exists a prime quadratic nonresidue $q \equiv 3 \pmod 4$, such that q is less than $2\sqrt{p}$.*

Proof. Let χ_1 be the nontrivial character mod 4 and χ_2 the quadratic character mod p, and let $\mathbb{X}$ be the group of Dirichlet characters generated by χ_1 and χ_2. The group $\mathbb{X}$ has conductor $f = \mathrm{lcm}(4,p) = 4p$ and exponent dividing $n = 2$. Define the form

$$\chi = 1 + \chi_1\chi_2 - \chi_1 - \chi_2.$$

By [13, Theorem 1.4], there exists an odd prime

$$q_2 \ll (4p)^{\frac{1}{4}+\epsilon} f^{\epsilon} \ll 2p^{\frac{1}{4}+2\epsilon},$$

such that $\chi(q_2) \neq 0$. By construction, however, if $\chi(q_2) \neq 0$, then $\chi_1(q_2) = \chi_2(q_2) = -1$. It follows that q_2 is a quadratic nonresidue and $q_2 \equiv 3 \pmod 4$. □

We will also need the following proposition.

Proposition 3.5. *For any sufficiently large prime p and integer $r > 1$, there exist nonresidues $q_1 = 1 \mod 4$ and $q_2 = 3 \mod 4$, with $q_1, q_2 < 2\sqrt{p^r}$.*

Proof. In the previous proof, let χ_1 be the nontrivial character mod 4 and χ_2 the quadratic character mod p. To ask for a prime quadratic nonresidue, $q \equiv 3 \mod 4$ is to ask for a prime q such that $\chi_1(q) = \chi_2(q) = -1$. Consider the abelian field extension K of $\mathbb{Q}$ given by $K = \mathbb{Q}(\sqrt{-1}, \sqrt{\alpha})$, where

$$\alpha = (-1)^{\frac{p-1}{2}} p.$$

The extension K is degree 4 with conductor $4p$. The characters χ_1 and χ_2 are quadratic, and thus, we may apply [13, Theorem 1.7], to obtain an upper bound on the prime q:

$$q \ll 2p^{\frac{1}{2}+\epsilon}.$$

Now, for the $1 \mod 4$ case, we simply replace $\chi_1(q) = \chi_2(q) = -1$ above with the conditions:

$$\chi_1(q) = 1,\ \chi_2(q) = -1.$$

and we apply [13, Theorem 1.7] again. □

Proposition 3.6 (Conditional on GRH). *For any prime $p > 10^9$, there exists a prime quadratic nonresidue $q \equiv 3 \pmod 4$ such that $q < 2\sqrt{p}$.*

Proof Let $\alpha = (-1)^{\frac{p-1}{2}} p$, and let $K = \mathbb{Q}(\sqrt{-1}, \sqrt{\alpha})$. The degree of the extension $K/\mathbb{Q}$ is 4, and the discriminant is $(4p)^2$. By [1, Theorem 5.1], by assuming GRH, there exists a prime quadratic nonresidue $q \equiv 3 \pmod 4$ satisfying

$$q < (8 \log(4p) + 15)^2.$$

The term on the right is smaller than $2\sqrt{p}$ as long as $p > 10^9$. $\square$

Given a prime q that satisfies the bounds above, we will need to find a particular way to write it as a sum of two positive integers, to ensure that $\mathbf{s}$ has the desired properties. Below, we check that such a decomposition exists, and that this decomposition provides the properties that we require.

Lemma 3.7. *Let q be an odd prime and let k be an integer such that $\left(\frac{k}{q}\right) = \left(\frac{-1}{q}\right)$. Then, there exists $0 < a < q$ such that $a(q-a) \equiv k \pmod q$.*

Proof. Consider the set

$$R_q = \left\{ \ell \in \mathbb{F}_q : \left(\frac{\ell}{q}\right) = \left(\frac{-1}{q}\right) \right\},$$

and the map $\phi : \mathbb{F}_q \to \mathbb{F}_q$ given by $\phi(x) = -x^2$. The image of ϕ must be a subset of R_q. For a fixed a, the polynomial $x^2 + a$ has at most two roots in $\mathbb{F}_q$. Since $|R_q| = \frac{q-1}{2}$, ϕ must, therefore, surject onto R_q. Hence, there exists an integer a such that $\phi(a) = k$, and we have $k \equiv -a^2 \equiv a(q-a) \pmod q$, as required. $\square$

Lemma 3.8. *Let p be a sufficiently large prime with $p \equiv 1 \pmod 4$ and let r be an integer. Then, there exists a prime q, with $\left(\frac{q}{p^r}\right) = -1$, and a positive integer $a < q$ such that the quantity*

$$\frac{p^r - a(q-a)}{q}$$

is a positive integer.

Proof. By Proposition 3.5, there exists a nonresidue q with $\left(\frac{-1}{q}\right) = \left(\frac{p^r}{q}\right)$, and $\frac{q^2}{4} < p^r$. By Lemma 3.7, there exists a positive integer $a < q$ such that $p^r \equiv a(q-a) \pmod q$. Therefore, $p^r - a(q-a)$ is positive and divisible by q. $\square$

We now apply Lemma 3.8 to establish the existence of an $\mathbf{s}$ such that $\mathrm{Jac}(B_{\mathbf{s}}) \cong \mathbb{Z}/p^r\mathbb{Z}$ with the nonresidue pairing.

Proposition 3.9. *For any sufficiently large prime p and integer r, there exists $\mathbf{s} = \{s_1, \ldots, s_m\}$ such that*

$$\sum_{i=1}^{m} \frac{\prod_{j=1}^{m} s_j}{s_i} = p^r,$$

$\gcd(p, s_i) = 1$ *for all i, and $\prod_{i=1}^{m} s_i$ is a nonresidue modulo p.*

Proof. First, consider the case that $p \equiv 3 \pmod 4$. Choose $\mathbf{s} = \{1, p^r - 1\}$, and note that $p^r - 1 \equiv -1 \pmod{p^r}$ is a nonresidue modulo p^r.

In the case that $p \equiv 1 \pmod 4$, let q, a be as in Lemma 3.8, and let

$$s_1 = a, \quad s_2 = q - a, \quad s_3 = \frac{p^r - a(q-a)}{q}.$$

Since both a and $q - a$ are smaller than p, they are relatively prime to p, and therefore, the product $a(q-a)$ is relatively prime to p, as well. Now, the quantity $s_1 s_2 s_3$ is a nonresidue mod p^r iff $\dfrac{(-1)(a(q-a))^2}{q}$ is a nonresidue mod p. Since $p \equiv 1 \pmod 4$, -1 is a residue modulo p^r, and hence, the numerator of this expression is also a residue. Therefore, $\left(\frac{s_1 s_2 s_3}{p^r}\right) = \left(\frac{q}{p^r}\right) = -1$, and the result follows. □

3.3. Proof of Theorems 1.1 and 1.2

Proof of Theorem 1.1. By Corollary 3.3, $\mathrm{Jac}(B_{p^r}) \cong \mathbb{Z}/p^r\mathbb{Z}$ with the residue pairing. By Propositions 3.1 and 3.9, for any sufficiently large prime p and integer $r \geq 1$, there exists an $\mathbf{s}$ such that $\mathrm{Jac}(B_{\mathbf{s}}) \cong \mathbb{Z}/p^r\mathbb{Z}$ with the nonresidue pairing. By taking wedge sums of these graphs, we obtain all groups with pairing of odd order. □

Our proof of Theorem 1.2 is aided by the fact that, in certain cases, we can explicitly construct an $\mathbf{s}$ satisfying the conditions required to achieve the nonresidue pairing:

Proposition 3.10. *Let p be an odd prime, not equivalent to $1 \pmod{24}$, and $r \geq 1$ an integer. Then, there exists an $\mathbf{s}$ such that*

$$\sum_{i=1}^{m} \frac{\prod_{j=1}^{m} s_j}{s_i} = p^r,$$

and $\prod_{i=1}^{m} s_i$ is a nonresidue modulo p.

Proof. We consider the following three cases.

(A) When $p \equiv 3 \pmod 4$, as before, we may use $\mathbf{s} = \{1, p^r - 1\}$.

(B) When $p \equiv 5 \pmod 8$, use $\mathbf{s} = \{1, 1, \frac{p^r-1}{2}\}$. Since $p \equiv 1 \pmod 4$, the product $s_1 s_2 s_3$ is a nonresidue modulo p iff 2 is a nonresidue modulo p—which is the case when $p \equiv 5 \pmod 8$.

(C) When $p \equiv 2 \pmod 3$, if $p \equiv 3 \pmod 4$, we are in the first case above. Otherwise, we have $p \equiv 1 \pmod 4$, and 2 is a nonresidue modulo p. Choose $\mathbf{s} = \{1, 1, \frac{p^r-1}{2}\}$ as before.

The only remaining possibility after eliminating these three cases is $p \equiv 1 \pmod{24}$. □

Remark 3.11. Proposition 3.10 shows that we could provide an unconditional proof of Theorem 1.2 if we could show that Proposition 3.6 holds for all primes $p \equiv 1 \pmod{24}$. In fact, computer search has verified that the proposition holds for all such primes smaller than 10^9. The code is available upon request of the authors.

Proof of Theorem 1.2. By Corollary 3.3, $\mathrm{Jac}(B_{p^r}) \cong \mathbb{Z}/p^r\mathbb{Z}$ with the residue pairing. By Propositions 3.1 and 3.10, for any odd prime p not congruent to $1 \pmod{24}$ and integer $r \geq 1$, there exists an $\mathbf{s}$ such that $\mathrm{Jac}(B_{\mathbf{s}}) \cong \mathbb{Z}/p^r\mathbb{Z}$ with the nonresidue pairing. By Propositions 3.6 and 3.9, if we assume GRH, then, for any prime $p > 10^9$ and integer $r \geq 1$, there exists an $\mathbf{s}$ such that $\mathrm{Jac}(B_{\mathbf{s}}) \cong \mathbb{Z}/p^r\mathbb{Z}$ with the nonresidue pairing. Finally, the computer search referenced in Remark 3.11 shows that, for all primes $p \equiv 1 \pmod{24}$, $p < 10^9$, there exists an $\mathbf{s}$ such that $\mathrm{Jac}(B_{\mathbf{s}}) \cong \mathbb{Z}/p^r\mathbb{Z}$ with the nonresidue pairing. Using the wedge sum construction, we may obtain all groups with pairing of odd order, as desired. □

4. 2-Groups with Pairing

We now turn to the task of constructing graphs G for which $\mathrm{Jac}(G) \cong ((\mathbb{Z}/2^r\mathbb{Z})^k, \langle\cdot,\cdot\rangle)$ for given positive integers r and k, and pairing $\langle\cdot,\cdot\rangle$. For each of the nonexceptional pairings on $\mathbb{Z}/2^r\mathbb{Z}$, we find a graph whose Jacobian is isomorphic to $\mathbb{Z}/2^r\mathbb{Z}$ with the given pairing.

4.1. Multicycle Graphs

In addition to the subdivided banana graphs of Sect. 3.1, we will require one more construction.

Construction 2. Let $\mathbf{s} = (s_1, \ldots, s_m)$ be a tuple of positive integers. Construct the $\mathbf{s}$-*multicycle graph* $C_{\mathbf{s}}$ on the vertices $v_1, \ldots, v_m$ by introducing s_i edges between v_i and v_{i+1} (here, i is taken mod m) (see Fig. 3).

Note that the graphs $B_{\mathbf{s}}$ and $C_{\mathbf{s}}$ are planar duals of each other, and thus, by Theorem 2.1, $\mathrm{Jac}(B_{\mathbf{s}}) \cong \mathrm{Jac}(C_{\mathbf{s}})$ as groups, but not necessarily as groups with pairing (see Fig. 4).

We now show that all of the cyclic 2-groups with nonexceptional pairing are realizable as Jacobians of graphs.

Theorem 4.1. *Let* $\Gamma \cong (\mathbb{Z}/2^r\mathbb{Z}, \langle\cdot,\cdot\rangle)$. *Then, there exists a graph* G *such that* $\mathrm{Jac}(G) \cong \Gamma$.

Proof. Observe that, by Corollary 3.3, $\mathrm{Jac}(B_{2^r}) \cong \mathcal{A}_{2^r}$ and $\mathrm{Jac}(C_{2^r}) \cong \mathcal{B}_{2^r}$. It remains to find constructions for graphs providing the groups $\mathcal{C}_{2^r}$ and $\mathcal{D}_{2^r}$.

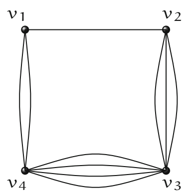

FIGURE 3. $C_{(1,3,4,2)}$ multicycle graph

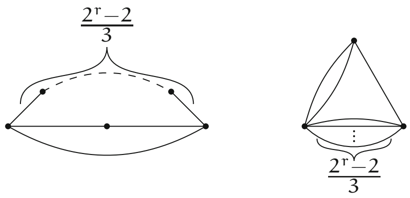

FIGURE 4. Graphs $B_{\mathbf{s}}$ and $C_{\mathbf{s}}$, for $\mathbf{s} = \{1, 2, \frac{2^r-2}{3}\}$

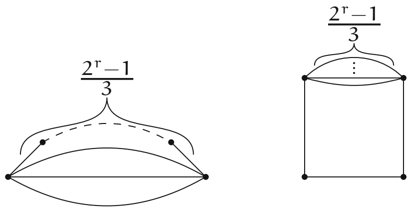

FIGURE 5. Graphs $B_{\mathbf{s}}$ and $C_{\mathbf{s}}$, for $\mathbf{s} = \{1, 1, 1, \frac{2^r-1}{3}\}$

By Lemma 2.6, it suffices to find graphs G_1 and G_2, with $\mathrm{Jac}(G_1) \cong \mathrm{Jac}(G_2) \cong \mathbb{Z}/2^r\mathbb{Z}$, such that for some $D_1 \in \mathrm{Jac}(G_1)$ and $D_2 \in \mathrm{Jac}(G_2)$, we have

$$\langle D_1, D_1 \rangle_1 = \frac{a}{2^r}$$
$$\langle D_2, D_2 \rangle_2 = \frac{b}{2^r},$$

where $a \equiv 3 \pmod 8$ and $b \equiv -3 \pmod 8$.

We consider the cases for even and odd r separately. For odd r, let $\mathbf{s} = \{1, 2, \frac{2^r-2}{3}\}$, and let $G_1 = B_{\mathbf{s}}$, $G_2 = C_{\mathbf{s}}$.

Consider a function $f : V(B_{\mathbf{s}}) \to \mathbb{Z}$, given by the following:

$$\begin{aligned} v_0 &\mapsto 0 \\ v_0' &\mapsto 2 \\ v_{21} &\mapsto 1 \\ v_{3j} &\mapsto 2^n - 4 - j. \end{aligned}$$

If $D_1 = v_{31} - v_0$, then $\mathrm{div}(f) = 2^r D_1$. It follows that $\langle D_1, D_1 \rangle_1 = \frac{f(v_{31})}{2^r} = \frac{2^r-3}{2^r}$, as required.

Now, consider the function $f : V(C_{\mathbf{s}}) \to \mathbb{Z}$ given by

$$v_0 \mapsto 0, \quad v_1 \mapsto 2, \quad v_2 \mapsto 3.$$

If $D_2 = v_2 - v_0$, then $\mathrm{div}(f) = 2^r D_2$, so $\langle D_2, D_2 \rangle_2 = \frac{3}{2^r}$, as desired.

For even r, let $\mathbf{s} = \{1, 1, 1, \frac{2^r-1}{3}\}$, and again, let $G_1 = B_{\mathbf{s}}$ and $G_2 = C_{\mathbf{s}}$ (Fig. 5).

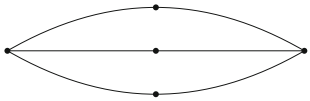

FIGURE 6. Graph $B_{2,2,2}$

For the banana graph, we see from Proposition 3.1 that $\mathrm{Jac}(B_{\mathbf{s}})$ is cyclic of order 2^r, with pairing

$$\langle x, y\rangle = \frac{\frac{2^r-1}{3}xy}{2^r}.$$

For the multicycle graph, consider a function $f\colon V(C_{\mathbf{s}}) \to \mathbb{Z}$, defined by $f(v_i) = i$. If $D_2 = v_3 - v_0$, then $\mathrm{div}(f) = -2^r D_2$, and hence, $\langle D_2, D_2\rangle = \frac{3}{2^r}$, and the result follows. □

4.2. 2-Groups with Exceptional Pairings

Each of the above constructions gives a graph with cyclic Jacobian, giving four of the six generators for 2-groups with pairing. We have a few concrete results concerning the exceptional pairings. However, we make the following observation.

Proposition 4.2. *For any $k \geq 1$, there is no graph G such that $\mathrm{Jac}(G) \cong (\mathcal{E}_2)^k$.*

Proof. This is a result of the characterization of graphs G with $\mathrm{Jac}(G) \cong (\mathbb{Z}/2\mathbb{Z})^{2k}$, given below in Remark 5.4. Since the Jacobian of a cycle always gives rise to the group $\mathcal{A}_2$, any such graph has Jacobian $(A_2)^{2k}$. □

This result, combined with our failure to find *any* graph G that yields the group $\mathcal{E}_{2^r}$, leads us to make the following conjecture:

Conjecture 4.3. *For any $k \geq 1$, there is no graph G such that $\mathrm{Jac}(G) \cong (\mathcal{E}_{2^r})^k$.*

We note, however, that there do exist examples of graphs G such that a *subgroup* $H \subset \mathrm{Jac}(G)$ (with the restricted pairing) is isomorphic to $\mathcal{E}_{2^r}$. For example, $\mathrm{Jac}(B_{2,2,2}) \cong (\mathbb{Z}2\mathbb{Z})^2 \times \mathbb{Z}/3\mathbb{Z}$, and by inspection, we can see that the 2-part with the restricted monodromy pairing is isomorphic to $\mathcal{E}_2$ (Fig 6).

We have even fewer results regarding $\mathcal{F}_{2^r}$. We note that the complete graph K_4 is a graph with Jacobian isomorphic to $\mathcal{F}_4$, but we were unable to find the other examples of graphs that provide this pairing.

5. Jacobians of Simple Graphs

In this section, we consider which groups without a specified pairing occur as Jacobians of simple graphs. If a finite abelian group Γ does not have 2 as an invariant factor, then it is straightforward to construct a simple graph G such that $\mathrm{Jac}(G) \cong \Gamma$, so this question is only interesting for the groups of the form $(\mathbb{Z}/2\mathbb{Z})^k \times H$.

5.1. Preliminaries for Proof of Theorem 1.5

We first observe that any simple graph that has 2 spanning trees must have a third. To see this, consider the union of a spanning tree with a single edge not contained in the spanning tree. This union contains a cycle, and the complement of any edge in this cycle is a spanning tree. Since the graph is simple, however, this cycle must contain at least three edges.

Since the number of spanning trees is equal to the size of the Jacobian, there is no simple graph G with $\mathrm{Jac}(G) \cong \mathbb{Z}/2\mathbb{Z}$.

Many of our arguments focus on the case where the graph G is biconnected. Recall that a graph G is *biconnected* if, for any vertex $v \in V(G)$, the induced subgraph on $V(G)\backslash\{v\}$ is connected. In particular, if G is not biconnected, then, by definition, there is a vertex v such that the induced subgraph on $V(G)\backslash\{v\}$ is not connected. The graph G is, therefore, the wedge sum of the connected components, which implies that $\mathrm{Jac}(G)$ splits as a direct product of Jacobians.

Definition 5.1. Given a graph G, we write $\mu(G)$ for the maximum order of an element of $\mathrm{Jac}(G)$, and $\delta(G)$ for the maximum valency of a vertex in G. When the graph G is clear from context, we will simply write δ and μ.

Lemma 5.2. *For any biconnected graph G, $\delta(G) \leq \mu(G)$. Furthermore, if $\delta(G) = \mu(G)$, then G must be the banana graph B_μ.*

Proof. The statement is immediate if G consists of a single vertex, so we assume that G has at least two vertices. Let v be a vertex in $V(G)$ with valency δ, and let w be a vertex adjacent to v. Consider the divisor $D = v - w$, and let $m < \delta$ be a positive integer. We apply Dhar's burning algorithm to check that mD is w-reduced. From the biconnectivity of G, we deduce that there is a path from w to each of the neighbors of v that does not contain v. Thus, each of the neighbors of v is burned. By definition, $\mathrm{val}(v) > m$, so it is burned, as well. This means that mD cannot be equivalent to 0 as 0 is the unique reduced divisor equivalent to 0. It follows that D has order at least δ.

In the case that $\delta = \mu$, we must have $\delta D \sim 0$. Starting from δD, chip fire v once to obtain a divisor E. Applying the burning algorithm and the biconnectivity condition once more, we see that v, as well as each of its neighbors, must be burned, so that E is w-reduced. E must, therefore, be the zero divisor, which is only possible if the multiplicity of the edge $\{v, w\}$ is δ, i.e., G is a banana graph. □

Recall that the *genus* of a graph G is its first Betti number, given by $g = |E(G)| - |V(G)| + 1$.

Corollary 5.3. *For any biconnected graph G with genus g and $|V(G)| = n$:*

$$n \geq \frac{2g-2}{\mu-2}.$$

Proof. Let e be the total number of edges in G. We have an inequality

$$2e = \sum_{i=1}^{n} \mathrm{val}(v_i) \leq \sum_{i=1}^{n} \delta = n \cdot \delta \leq n \cdot \mu.$$

Since $e = g + n - 1$, we see that $2g - 2 \leq n \cdot (\mu - 2)$. □

We are now ready to prove Theorem 1.5.

Proof of Theorem 1.5. Let G be a simple graph with $\mathrm{Jac}(G) \cong (\mathbb{Z}/2\mathbb{Z})^k$. We may assume that G has no vertices of valence 1, because the graph obtained by contracting the edge adjacent to such a vertex has isomorphic Jacobian. If G is not biconnected, then G decomposes as a wedge sum, and $\mathrm{Jac}(G)$ decomposes as a direct sum of Jacobians, one of which must be isomorphic to $(\mathbb{Z}/2\mathbb{Z})^r$ for some positive integer $r \leq k$. We may, therefore, assume that G is biconnected. By Lemma 5.2, it also has no vertices of valence 3 or greater. It follows that G is a cycle. Since $\mathrm{Jac}(C_n) \cong \mathbb{Z}/n\mathbb{Z}$, we must have $n = 2$, which means that G cannot be simple. □

Remark 5.4. The proof of Theorem 1.5 also gives a complete characterization of graphs G with $\mathrm{Jac}(G) \cong (\mathbb{Z}/2\mathbb{Z})^k$. In general, we can always obtain such a graph by the following procedure. Start with a tree T and choose a subset of k edges of T. Construct a new graph G from T by doubling each edge in this subset (see Fig. 7).

5.2. Preliminaries: Proof of Theorem 1.6

Our next goal is to generalize Theorem 1.5 to graphs whose Jacobian is of the form $(\mathbb{Z}/2\mathbb{Z})^k \times H$. We begin with the following bound on the genus of G.

Proposition 5.5 ([11, Proposition 5.2]). *If G is a graph of genus g and* $\mathrm{Jac}(G) \cong (\mathbb{Z}/2\mathbb{Z})^k \times H$*, then $g \geq k$.*

Applying Corollary 5.3 to this result shows that

$$|V(G)| \geq \frac{2k-2}{\mu - 2}.$$

We require the following result about lengths of paths in G.

Lemma 5.6. *Let G be a biconnected graph, and suppose that there exists a path P with vertices $\{v_1, \ldots, v_\ell\}$ on G such that* $\mathrm{val}(v_i) = 2$ *for all* $1 < i < \ell$*. Then,* $\mathrm{Jac}(G)$ *contains an element of order at least ℓ.*

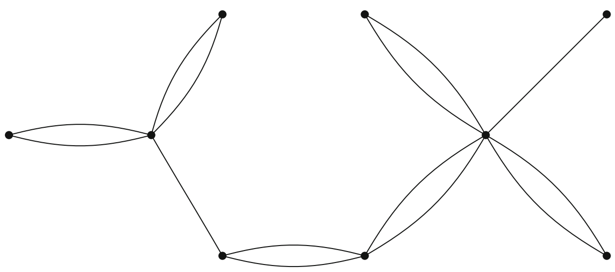

FIGURE 7. Example of a graph G with $\mathrm{Jac}(G) \cong (\mathbb{Z}/2\mathbb{Z})^6$

Proof. Let $m < \ell$, and consider $D = v_2 - v_1$. As G is biconnected, there is a path from v_1 to v_{m+1} that does not contain any of the vertices of P. Dhar's burning algorithm shows that $v_{m+1} - v_1$ is the v_1-reduced divisor equivalent to mD, and hence, $mD \nsim 0$ for $m < \ell$. $\square$

Our approach will now be to establish an upper bound on $|V(G)|$ in terms of μ and $|H|$, and then use this to obtain an upper bound on k.

Proposition 5.7. *For any finite abelian group H, there exists an integer n_H such that, for any biconnected simple graph G with $\mathrm{Jac}(G) \cong (\mathbb{Z}/2\mathbb{Z})^k \times H$, we have $|V(G)| < n_H$.*

Proof. Let $U = \{u \in V(G) : \mathrm{val}(u) > 2\}$. We will first establish a bound on $m = |U|$, and then bound $|V(G)|$ in terms of m.

Fix a vertex $u \in U$, and consider the set of divisors $\mathcal{U} = \{u_i - u | u_i \in U\}$. For any $D_1 \neq D_2 \in \mathcal{U}$, we claim that $2D_1 - 2D_2 = 2u_1 - 2u_2$ is u_2-reduced. Since G is biconnected, there is a path from u_2 to each of the neighbors of u_1 that does not contain u_1. Applying Dhar's burning algorithm, we see that, since $\mathrm{val}(u_2) > 2$, the entire graph will be burned. Therefore, $2D_1 - 2D_2$ is u_2-reduced, and hence, $2D_1 \nsim 2D_2$.

We now define a map

$$\begin{aligned} \varphi\colon\ \mathrm{Jac}(G) &\to \mathrm{Jac}(G) \\ D &\mapsto 2D. \end{aligned}$$

By the above, we have that the restriction of φ to $\mathcal{U}$ is injective. Furthermore, since $|\mathrm{im}(\varphi)| \leq |H|$, we see that $m \leq |H|$.

We now wish to bound $|V(G)|$ in terms of m. To do so, we construct a new graph G' from G, according to the following algorithm.

1. Choose any vertex of G of valency 2. Delete it and draw an edge between its neighbors.
2. Repeat until there are no 2-valent vertices remaining.

Note that even if G is simple, G' need not be. It is clear, however, that G and G' have the same number of vertices with valency greater than 2, and that $\delta(G) = \delta(G')$.

By Lemma 5.2, we must have that $e' = |E(G')|$ is at most $m \cdot \mu$ (since, otherwise, there would necessarily be a vertex of G with valency greater than δ). Each 2-valent vertex of G is uniquely associated with some edge of G'. If there are more than $(e' \cdot \mu)$ divalent vertices in G, then at least μ of them are associated with a single edge of G'. In this case, G would contain a path P of length greater than μ, where each vertex of P has valency 2. This contradicts Lemma 5.6, so we have the following:

$$|V(G)| - m < m\mu^2.$$

If we let $n_H = |H|(1 + \mu^2)$, then $|V(G)| < n_H$ (Fig 8). $\square$

Applying Corollary 5.3 and Proposition 5.5, we see that, for sufficiently large k, we must have $|V(G)| > n_H$. This, in turn, implies that, for sufficiently large k, $(\mathbb{Z}/2\mathbb{Z})^k \times H$ is not the Jacobian of any biconnected simple graph. We will use this fact to show that this result holds generally, for all simple graphs.

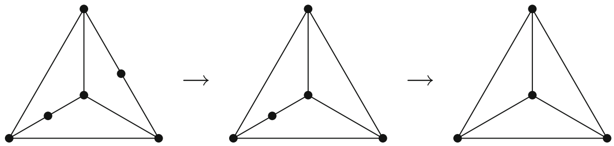

FIGURE 8. Transformation $G \mapsto G'$

Proof of Theorem 1.6. We proceed by induction on $|H|$. When $|H| = 1$ or 2, Theorem 1.5 gives the bound $k_H = 1$. For $|H| \geq 3$, there must exist (by Proposition 5.7) an integer k' such that, if $k > k'$ and $\mathrm{Jac}(G) \cong (\mathbb{Z}/2\mathbb{Z})^k \times H$, then G is not biconnected.

By the inductive hypothesis, for any proper subgroup $H' \subset H$, there exists an integer $k(H')$ such that for all $k > k(H')$, no simple graph G' has $\mathrm{Jac}(G') \cong (\mathbb{Z}/2\mathbb{Z})^k \times H'$. Now, since H is finite, there are finitely many pairs of nontrivial proper subgroups $H_1, H_2 \subset H$ such that $H_1 \times H_2 \cong H$. Define

$$k'' = \max\{k(H_1) + k(H_2) : H_1, H_2 \text{ nontrivial}, H_1 \times H_2 \cong H\}.$$

Now, let $k_H = \max(k', k'')$. We wish to show that, for all $k > k_H$, if $\mathrm{Jac}(G) \cong (\mathbb{Z}/2\mathbb{Z})^k \times H$, then G is not simple. Let G be a graph with this Jacobian, and let $k > k_H$. Since $k > k'$, G is not biconnected, so it must be the wedge sum of two graphs G_1 and G_2. There must then exist integers k_1, k_2 with $k_1 + k_2 = k$ and groups H_1, H_2 with $H_1 \times H_2 \cong H$ such that

$$\mathrm{Jac}(G_1) \cong (\mathbb{Z}/2\mathbb{Z})^{k_1} \times H_1,$$
$$\mathrm{Jac}(G_2) \cong (\mathbb{Z}/2\mathbb{Z})^{k_2} \times H_2.$$

Without loss of generality, we may assume that neither G_1 nor G_2 is a tree, so that $\mathrm{Jac}(G_1)$ and $\mathrm{Jac}(G_2)$ are both nontrivial. If either H_1 or H_2 are trivial, then G_1 (resp. G_2) would have Jacobian isomorphic to $(\mathbb{Z}/2\mathbb{Z})^k$ for $k > 0$, contradicting Theorem 1.5.

Finally, since $k_1 + k_2 = k > k'' \geq k(H_1) + k(H_2)$, we must have that either $k_1 > k(H_1)$ or $k_2 > k(H_2)$. It follows that either G_1 or G_2 is not simple, so G is not simple. $\square$

5.3. Further Queries

Analysis of the proof of Theorem 1.6 suggests that, if $H \cong \mathbb{Z}/p^r\mathbb{Z}$ for some prime p, then $k_H = O(|H|p^3)$. In practice, it seems that much better bounds should hold. For instance, we were unable to find any simple graph G where $\mathrm{Jac}(G) \cong (\mathbb{Z}/2\mathbb{Z})^k \times H$ for any $k > |H|$.

In some cases, it is possible to directly verify that certain groups do not arise as the Jacobian of any simple graph. Recall that a graph is 2-edge-connected if it remains connected after the deletion of any edge. For a given m, while there are infinitely many isomorphism classes of simple graphs with fewer than m spanning trees, at most finitely many of these classes represent 2-edge-connected graphs. This results from the fact that, for any vertex v_0 on a 2-edge-connected graph, any divisor of the form $v - v_0$ is v_0-reduced, and hence, there are at least as many spanning trees on the graph as there are vertices.

By contracting bridges, any graph G may be uniquely associated with a 2-edge-connected graph with isomorphic Jacobian. For a given group H, therefore, it is possible to compute the Jacobian of all 2-edge-connected simple graphs with at most $|H|$ spanning trees, and verify that H does or does not occur.

Computer searches of this nature have led to the following:

Proposition 5.8. *The following groups are not isomorphic to the Jacobian of any simple graph:*

- $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$,
- $(\mathbb{Z}/2\mathbb{Z})^2 \times \mathbb{Z}/4\mathbb{Z}$,
- $\mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/4\mathbb{Z})^2$.

The key fact in the proof of the nonoccurrence of groups with many factors of $\mathbb{Z}/2\mathbb{Z}$ seems to be the requirement that G is biconnected, rather than that G is simple. It has been shown that, asymptotically, the probability that the Jacobian of a random graph is cyclic is relatively high [5]. We expect that the Jacobians of most graphs have a small number of invariant factors. Since random graphs are highly connected, we conjecture the following.

Conjecture 5.9. *For any positive integer n, there exists k_n such that if $k > k_n$, there is no biconnected graph G with* $\mathrm{Jac}(G) \cong (\mathbb{Z}/n\mathbb{Z})^k$.

The conjecture follows from our results for $n = 3$. To see this, observe from Lemma 5.2 that the only biconnected graphs with Jacobian $(\mathbb{Z}/3\mathbb{Z})^k$ are the 3-cycle and the 3-banana. In this case, we have $k_3 = 1$.

Acknowledgements

This project was completed as part of the 2014 Summer Undergraduate Mathematics Research at Yale (SUMRY) program, where the second and third authors were supported as mentors and the first, fourth, and fifth authors were supported as participants. It is a pleasure to thank all involved in the program for creating a vibrant research community. We benefited from conversations with Dan Corey, Andrew Deveau, Jenna Kainic, Nathan Kaplan, Susie Kimport, Dan Mitropolsky, and Anup Rao. We thank Sam Payne for suggesting the problem. We are also especially grateful to Paul Pollack, whose ideas significantly strengthened the results of this paper. Finally, we thank the referees for their careful reading and insightful comments. The authors were supported by NSF grant CAREER DMS-1149054 (PI: Sam Payne).

References

[1] Bach, E., Sorenson, J.: Explicit bounds for primes in residue classes. Math. Comp. 65(216), 1717–1735 (1996)

[2] Baker, M., Norine, S.: Riemann-Roch and Abel-Jacobi theory on a finite graph. Adv. Math. 215(2), 766–788 (2007)

[3] Baker, M., Shokrieh, F.: Chip-firing games, potential theory on graphs, and spanning trees. J. Combin. Theory Ser. A 120(1), 164–182 (2013)

[4] Bosch, S., Lorenzini, D.: Grothendieck's pairing on component groups of Jacobians. Invent. Math. 148(2), 353–396 (2002)

[5] Clancy, J., Kaplan, N., Leake, T., Payne, S., Wood, M.M.: On a Cohen-Lenstra heuristic for Jacobians of random graphs. J. Algebraic Combin. 42(3), 701–723 (2015)

[6] Clancy, J., Leake, T., Payne, S.: A note on Jacobians, Tutte polynomials, and two-variable zeta functions of graphs. Exp. Math. 24(1), 1–7 (2015)

[7] Cori, R., Rossin, D.: On the sandpile group of dual graphs. European J. Combin. 21(4), 447–459 (2000)

[8] Davenport, H.: Multiplicative Number Theory. Third edition. Revised and with a preface by Hugh L. Montgomery. Graduate Texts in Mathematics, Vol. 74. Springer-Verlag, New York (2000)

[9] Dhar, D.: Self-organized critical state of sandpile automaton models. Phys. Rev. Lett. 64(14), 1613–1616 (1990)

[10] Lorenzini, D.: Arithmetical properties of Laplacians of graphs. Linear and Multilinear Algebra 47(4), 281–306 (2000)

[11] Lorenzini, D.J.: Arithmetical graphs. Math. Ann. 285(3), 481–501 (1989)

[12] Miranda, R.: Nondegenerate symmetric bilinear forms on finite abelian 2-groups. Trans. Amer. Math. Soc. 284(2), 535–542 (1984)

[13] Pollack, P.: Prime splitting in abelian number fields and linear combinations of Dirichlet characters. Int. J. Number Theory 10(4), 885–903 (2014)

[14] Shokrieh, F.: The monodromy pairing and discrete logarithm on the Jacobian of finite graphs. J. Math. Cryptol. 4(1), 43–56 (2010)

[15] Wall, C.: Quadratic forms on finite groups, and related topics. Topology 2(4), 281–298 (1963)

[16] Wood, M.: The distribution of sandpile groups of random graphs. J. Amer. Math. Soc. 30(4), 915–958 (2017)

David Jensen
Department of Mathematics
University of Kentucky
Lexington, KY 40506-0027
USA
e-mail: djensen@uky.edu

Louis Gaudet, Nicholas Wawrykow and Theodore Weisman
Department of Mathematics
Yale University
New Haven, CT 06520
USA
e-mail: louis.gaudet@yale.edu

Nicholas Wawrykow
e-mail: nicholas.wawrykow@yale.edu

Theodore Weisman
e-mail: theodore.weisman@yale.edu

Dhruv Ranganathan
Department of Mathematics
Massachusetts Institute of Technology
Cambridge, MA 02139
USA
e-mail: dhruvr@mit.edu

Received: 29 October 2016.