A NEW $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-INVARIANT OF DESSINS D'ENFANTS

RAVI JAGADEESAN

Abstract. We study the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the category of Belyi functions (finite, étale covers of $\mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus \{0,1,\infty\}$). We describe a new combinatorial $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-invariant for a certain class of Belyi functions. As a corollary, we obtain that for all $k < 2^{\sqrt{\frac{2}{3}}}$ and all positive integers N, there is an $n \leq N$ such that the set of degree n Belyi functions of a particular rational Nielsen class must split into at least $\Omega\left(k^{\sqrt{N}}\right)$ Galois orbits.

1. Introduction

In his *Esquisse d'un Programme* [6], Grothendieck expressed a program to understand the structure of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. The idea is that there is a faithful, outer action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the tower of profinite mapping class groups (the étale fundamental groups of the moduli spaces $M_{g,n}$ of curves of genus g with n ordered marked points over $\overline{\mathbb{Q}}$). Grothendieck conjectured that the action is "generated" on the dimension 1 moduli spaces with "relations" in dimension 2. The moduli space $M_{0,4}$ is of dimension 1, and is isomorphic to $\mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus \{0,1,\infty\}$, and therefore as part of the program, one wishes to study the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the category of étale covers of $\mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus \{0,1,\infty\}$. Grothendieck's *dessins d'enfants* encode the covers combinatorially, and one can try to understand the faithful action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on them. A first step is to determine a set of invariants, perhaps algebraic, arithmetic, geometric, or topological in nature, that can distinguish distinct $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-orbits of dessins. In this paper, we construct a new invariant for a certain class of dessins and describe it combinatorially.

The key idea is to consider commutative squares of the form

$$\begin{tikzcd}
Y \arrow[d] & X \arrow[l] \arrow[d] \\
\mathbb{P}^1 & \mathbb{P}^1 \arrow[l, "\frac{(z+1)^2}{4z}"']
\end{tikzcd}$$

with X the normalization of the fibered product $Y \times_{\mathbb{P}^1} \mathbb{P}^1$. In certain cases, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-invariants of the left morphism extend to $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-invariants of the right morphism. In particular, by considering the cycle types of the monodromy generators of the left morphism as a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-invariant, we partition the set of possible right morphisms into $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-invariant subsets. We describe this new invariant combinatorially as the *square-root cycle type class*. It provides non-trivial information regarding only the $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-orbits of Belyi functions that have the

Date: December 31, 2013.

same monodromy cycle type over 0 and ∞. However in Theorems 3.4 and 3.5, we prove that our invariant is substantially stronger than the rational Nielsen class (and therefore substantially stronger than the monodromy group and the monodromy cycle type). As a corollary, we obtain that for all $k < 2^{\sqrt{\frac{2}{3}}}$ and all positive integers N, there is an $n \leq N$ such that the set of degree n Belyi functions of a particular rational Nielsen class must split into at least $\Omega\left(k^{\sqrt{N}}\right)$ Galois orbits.

The structure of this paper is as follows. In Section 2, we recall the basic definitions and discuss previous work. In Section 3, we state our main results, and in Section 4, we prove the basic properties of our new invariant. In Section 5, we prove our main theorems and we prove that our invariant is stronger than the rational Nielsen class invariant in certain cases, and in Section In Section 6, we give concluding remarks and state open problems. Elementary computatations are deferred to Appendix A.

Acknowledgements. I would like to thank Akhil Mathew for his incredibly helpful insight and guidance that went into this work. I would also like to thank Prof. Noam Elkies for proposing this project and offering numerous useful observations, such as suggesting that we consider fibered products of curves, suggesting the proof of Theorem 3.3(c), and suggesting that we apply Proposition 5.3. Lastly, I would like to thank the PRIMES program of the MIT Department of Mathematics, where this research was done.

2. Previous Work

Unless otherwise specified, a curve will mean a smooth, irreducible, projective algebraic curve over $\mathbb{C}$, or equivalently a compact Riemann surface. We will denote by $\mathbb{P}^1$ the complex projective line $\mathbb{P}^1_{\mathbb{C}}$. Fix an embedding $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$. Let $\chi : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \widehat{\mathbb{Z}}^\times$ denote the cyclotomic character.

Fundamental groups are topological unless otherwise specified. Fix a generating set x_0, x_1, x_∞ of $\pi_1\left(\mathbb{P}^1 \setminus \{0, 1, \infty\}, \frac{3}{4}\right)$ such that $x_0 x_1 x_\infty = 1$ and in $\mathbb{C} \setminus \{0, 1\}$, the loops have winding numbers of $1, 0, -1$ about 0 and $0, 1, -1$ about 1, respectively. Sending the generators x, y of F_2, the free group on two letters, to x_0, x_1, respectively, yields an isomorphism $F_2 \cong \pi_1\left(\mathbb{P}^1 \setminus \{0, 1, \infty\}, \frac{3}{4}\right)$.

By a *weak action* of a group G on a category $\mathcal{C}$, we mean a group homomorphism from G to the group of equivalences from $\mathcal{C}$ to $\mathcal{C}$, modulo natural isomorphism. Let $\widehat{G}$ denote the profinite completion, G^{ab} the abelianization, and G' the derived subgroup of a group G. Given a pro-finite group G, elements $g_1, g_2 \in G$ and $f \in \widehat{F_2}$, let $f(g_1, g_2)$ denote the image of f under the homomorphism from $\widehat{F_2}$ to G that sends the generators x, y to g_1, g_2, respectively.

Given a partition $\lambda \dashv n$, let the *ramification number* of λ, which we denote by $\mathrm{ram}(\lambda)$, equal $n - k$, where k is the number of parts of λ. We can extend the definition of ram to permutations $\sigma \in S_n$ by defining the ramification number of σ to be the ramification number of the cycle type of σ.

2.1. The action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on profinite fundamental groups.

Let $\overline{p}$ be a geometric point of $\mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus \{0, 1, \infty\}$, let p be the corresponding geometric point of $\mathbb{P}^1_{\mathbb{Q}}$, and let $p_{\mathbb{C}}$ be the base-change of $\overline{p}$ to $\mathbb{C}$. There is an isomorphism between étale fundamental groups and profinite completions of topological fundamental groups [7, Exposé X, Corollaire 1.8]:

$$\pi_1^{\text{ét}}\left(\mathbb{P}^1_{\overline{\mathbb{Q}}}\setminus\{0,1,\infty\},\overline{p}\right)\cong\pi_1^{\text{ét}}\left(\mathbb{P}^1_{\mathbb{C}}\setminus\{0,1,\infty\},p_{\mathbb{C}}\right)\cong\pi_1\left(\mathbb{P}^1_{\mathbb{C}}\setminus\widehat{\{0,1,\infty\}},p_{\mathbb{C}}\right)\cong\widehat{F_2},$$

where the first two isomorphisms are canonical and the last given by fixing generators for $\pi_1(\mathbb{P}^1_{\mathbb{C}},p_{\mathbb{C}})$. Furthermore, there is an exact sequence of étale fundamental groups [7, Exposé IX, Théorème 6.1]

$$1\to\pi_1^{\text{ét}}\left(\mathbb{P}^1_{\overline{\mathbb{Q}}}\setminus\{0,1,\infty\}\right)\to\pi_1^{\text{ét}}\left(\mathbb{P}^1_{\mathbb{Q}}\setminus\{0,1,\infty\}\right)\to\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})\to 1.$$

This induces an outer action

$$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})\to\mathrm{Out}\left(\widehat{F_2}\right). \tag{1}$$

The scheme $\mathbb{P}^1_{\mathbb{Q}}\setminus\{0,1,\infty\}$ can be replaced by any quasi-compact, geometrically connected scheme X over $\mathbb{Q}$ and $\mathbb{P}^1_{\overline{\mathbb{Q}}}\setminus\{0,1,\infty\}$ (resp. $\mathbb{P}^1_{\mathbb{C}}\setminus\{0,1,\infty\}$) by the base-change of X to $\overline{\mathbb{Q}}$ (resp. $\mathbb{C}$), but the choice of $\mathbb{P}^1_{\mathbb{Q}}\setminus\{0,1,\infty\}$ has special properties, such as Theorem 2.1, to be outlined in the next subsection.

2.2. **Belyi functions and dessins d'enfants.**

A *Belyi function* is a finite, étale, connected cover of $\mathbb{P}^1_{\overline{\mathbb{Q}}}\setminus\{0,1,\infty\}$. Due to [7, Exposé X, Corollaire 1.8], we can equivalently view a Belyi function as a finite, étale, connected cover of $\mathbb{P}^1_{\mathbb{C}}\setminus\{0,1,\infty\}$, which is a meromorphic function on a curve X that is unbranched outside $\{0,1,\infty\}$. A *dessin d'enfant* is a bipartite, connected graph G with parts V_0,V_1 together with an embedding $G\hookrightarrow X$ where X is a compact, oriented, topological 2-manifold, whose image is the 1-skeleton of a CW-complex structure on X.

The following data are then equivalent [8, 14]:

(1) an isomorphism class of Belyi functions of degree n;
(2) an isomorphism class of dessin d'enfants with n edges; and
(3) a conjugacy class of transitive representations $(F_2\cong)\,\pi_1(\mathbb{P}^1\setminus\{0,1,\infty\},\frac{3}{4})\to S_n$.

To a Belyi function f, we associate the dessin $f^{-1}([0,1])$ with $V_0=f^{-1}(0)$ and $V_1=f^{-1}(1)$, and the monodromy representation of $h:F_2\cong\pi_1(\mathbb{P}^1\setminus\{0,1,\infty\},\frac{3}{4})\to S_n$. It follows from the Riemann Existence Theorem that one can associate a Belyi function to any dessin or representation $F_2\to S_n$.

There is a natural action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the category of Belyi functions: viewing the category of Belyi functions as the category of étale covers of $\mathbb{P}^1\setminus\{0,1,\infty\}$ and given an automorphism $\sigma\in\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, we can base-change by $\operatorname{Spec}\sigma$. There is an action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the category of representations of $\widehat{F_2}$ on finite sets where $\sigma\in\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts by sending h to $h\circ\alpha(\sigma)$; the image of h is defined only up to isomorphism because $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts canonically only by outer automorphisms. The category of Belyi functions is equivalent to the category of representations of F_2 on finite sets, (where F_2 is identified with $\pi_1\left(\mathbb{P}^1\setminus\{0,1,\infty\},\frac{3}{4}\right)$) which is in turn equivalent to the category of representations of $\widehat{F_2}$ on finite sets and therefore Equation 1 yields a weak action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the category of Belyi functions. The fact that the two actions are equivalent follows from the definition of the exact sequence in Equation 1, and the fact that the group of isomorphism classes of self-equivalences of the category of representations of $\widehat{F_2}$ on finite sets is canonically isomorphic to $\mathrm{Out}\left(\widehat{F_2}\right)$.

A key result regarding the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ follows from following theorem of Belyi.

Theorem 2.1 ([1], Theorem 4)**.** *A curve admits a Belyi function if it is defined over $\overline{\mathbb{Q}}$.*

By considering the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the j-invariants of elliptic curves, it follows the actions of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $\widehat{F_2}$, the category of Belyi functions, and the set of isomorphism classes of dessins are faithful [8].

2.3. $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-Invariants.

The outer action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $\widehat{\mathbb{F}_2}$ yields an injection of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ into the *(profinite) Grothendieck-Teichmüller group* $\widehat{GT}$. In particular, the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ satisfies the following property.

Theorem 2.2 ([4], Proposition 3.2)**.** *Let $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and let $\zeta \in \mathrm{Aut}\left(\widehat{\mathbb{F}_2}\right)$ be a lift of $\alpha(\sigma)$. Then for $i \in \{0, 1, \infty\}$, $\zeta(x_i)$ is conjugate to $x_i^{\chi(\sigma)}$ in $\widehat{\mathbb{F}_2}$, where $\chi : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \widehat{\mathbb{Z}}$ is the cyclotomic character.*

Theorem 2.2 yields $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-invariants of Belyi functions and dessins d'enfants. Fix a Belyi function $f : X \to \mathbb{P}^1$ of degree n. We obtain an associated dessin $\Gamma \subseteq X$ and a monodromy representation $h : \pi_1(\mathbb{P}^1 \setminus \{0, 1, \infty\}, \frac{3}{4}) \to S_n$. Let $\lambda_i \dashv n$ denote the cycle type of $\sigma_i = h(x_i)$ for $i \in \{0, 1, \infty\}$. One can easily verify (from Theorem 2.2 or otherwise) that the cycle type of the monodromy $(\lambda_0, \lambda_1, \lambda_\infty)$ is $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-invariant. In fact, λ_0 is the degree multiset of V_0, λ_1 is the degree multiset of V_1, and λ_∞ is the multiset of half the number of edges bounding each face of Γ [9, p.4].

Another $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-invariant is the *monodromy group*, defined as the image of the monodromy representation h, which is $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-invariant by definition of the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the category of Belyi functions. A third invariant is the *rational Nielsen class*, which is the set of triples

$$\left\{ \left([\sigma_0^\lambda], [\sigma_1^\lambda], [\sigma_\infty^\lambda] \right) \mid \lambda \in \hat{\mathbb{Z}}^\times \right\},$$

where $[u]$ denotes the conjugacy class of u in the monodromy group of f; the $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-invariance of the rational Nielsen class follows immediately from Theorem 2.2. Let $\mathcal{N}(n)$ denote the family of pairs of a group G acting transitively on $[n]$ and a rational Nielsen class in G.

There are other combinatorial invariants, such as the Ellenberg's braid group invariant [4] and Serre's lifting invariant. Zapponi [15] defined an invariant for plane trees (equivalently, Belyi polynomials) that is merely a sign ±1, but that is particularly interesting in that it is not combinatorial.

2.4. Hurwitz existence problem.

We investigate Belyi functions with monodromy of fixed cycle type. Let $\mathcal{B}$ be the set of monodromy cycle types of Belyi functions. Determining $\mathcal{B}$ is an unsolved case of the Hurwitz existence problem, which deals with the possible sequences of monodromy cycle types of étale covers of arbitrary curves over $\mathbb{C}$ with removed points, but is a purely group-theoretic question regarding finite permutation representations of the fundamental groups of Riemann surfaces with points removed.

In the case of $\mathbb{P}^1 \setminus \{0, 1, \infty\}$, the question is: given a finite group G and conjugacy classes c_0, c_1, c_∞, how many triples $(\sigma_0, \sigma_1, \sigma_\infty)$ are there of elements $\sigma_i \in c_i$ such that $\sigma_0\sigma_1\sigma_\infty = 1$? There is a formula for the number of solutions in terms of the characters of G (see, for example, Serre [12, Theorem 7.2.1]), but this is not simple to evaluate in general. Edmonds-Kulkarni-Stong [3] construct a family of elements of $\mathcal{B}$.

Theorem 2.3 ([3], Proposition 5.2)**.** *Let n be a positive integer, and let $\alpha, \beta \dashv n$. Let P be the total number of parts of α, β. A Belyi function with monodromy of cycle type (α, β, n) exists if and only if $P \equiv n+1 \pmod 2$ and $P \leq n+1$.*

Necessity follows immediately from the Riemann-Hurwitz formula, and sufficiency is proven constructively. If one of the partitions is not n, the Riemann-Hurwitz condition on the total number of parts of the three partitions is not in general sufficient.

3. Statements of the main results

3.1. A new $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-invariant for Belyi function with monodromy of cycle type (λ, μ, λ).

Definition 3.1. Let n be a positive integer, $\lambda, \mu \dashv n$, and f a Belyi function with monodromy of cycle type (λ, μ, λ). Suppose that f has monodromy generators $\sigma_0, \sigma_1, \sigma_\infty$, over $0, 1, \infty$, respectively. The *square-root class* of f, denoted by $\mathrm{Sqrt}(f)$, is defined as

$$\mathrm{Sqrt}(f) = \left\{ \left(\sigma_0^{-1}\tau_1^{-1}, \tau_1, \sigma_0\right) \in S_n^3 \mid \tau_1^2 = \sigma_1 \text{ and } \sigma_\infty = \tau_1^{-1}\sigma_0\tau_1 \right\}.$$

Because $\sigma_0, \sigma_1, \sigma_\infty$ are only defined up to simultaneous conjugation in S_n, each element of $\mathrm{Sqrt}(f)$ is only defined up to such conjugation.

Definition 3.2. Let the *square-root cycle type class* of f, denoted by $\mathrm{SqCt}(f)$, be the multiset of triples $(\lambda_0, \lambda_1, \lambda_\infty)$ where λ_i is the cycle type of τ_i for $(\tau_0, \tau_1, \tau_\infty) \in \mathrm{Sqrt}(f)$.

For each positive integer n, the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the set of conjugacy classes of representations of F_2 in S_n induces an action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the power set of the set of such representations. Hence, for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and all Belyi functions f, one can define $\sigma(\mathrm{Sqrt}(f))$. A key property of the square-root class is its $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-equivariance. This yields a key property of the square-root cycle type class, which is that it is $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-invariant, and in certain cases it can distinguish $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-orbits of dessins that are indistiguishable by the monodromy group and the rational Nielsen class. The square-root cycle type class is a purely combinatorial invariant, albeit difficult to compute explicitly. In order to state the final properties of the square-root cycle type class, we define the genus of an element of $\mathrm{SqCt}(f)$; for all $\lambda = (\lambda_0, \lambda_1, \lambda_\infty)$ with $\lambda_i \dashv n$, let

$$g(\lambda) = \frac{\sum_{i \in \{0,1,\infty\}} \mathrm{ram}(\lambda_i)}{2} - n + 1.$$

We can naturally extend g to take arguments that are elements of S_n instead. If σ_i is a permutation of cycle type λ_i for $i \in \{0, 1, \infty\}$, such that $\sigma_0\sigma_1\sigma_\infty = 1$ and the σ_i generate a transitive subgroup of S_n, the Riemann-Hurwitz formula implies that this is simply the genus of the curve X that admits a Belyi function with monodromy of cycle type $(\sigma_0, \sigma_1, \sigma_\infty)$.

Now, we are prepared to state the key facts regarding the square root class and the square-root cycle type class.

Theorem 3.3 (Properties of Sqrt and SqCt)**.** *The function* Sqrt *is* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$*-equivariant and thus the function* SqCt *is* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$*-invariant. Let $f : X \to \mathbb{P}^1$ be a Belyi function and suppose that X has genus g. Then,*

(a) $|\operatorname{SqCt}(f)|$ *is at most the number of non-trivial involutions on X, and in particular, if $g > 1$, then $|\operatorname{SqCt}(f)| \leq 84(g-1)-1$;*
(b) if there exist odd positive integers k, c and a triple $(\mu_0, \mu_1, \mu_\infty) \in \operatorname{SqCt}(f)$ such that μ_1 has c parts of size k and no parts of size $2k$, then $|\operatorname{SqCt}(f)| = 1$;
(c) if $g > 1$, then there exists at most one triple $\lambda = (\lambda_0, \lambda_1, \lambda_\infty) \in \operatorname{SqCt}(f)$ such that $g(\lambda) = 0$.

3.2. **The monodromy cycle type and the rational Nielsen class are imprecise invariants.** For all positive integers n, let

$$\mathrm{Cl}(N) = \max_{n \leq N} \max_{\lambda_1, \lambda_2, \lambda_3 \dashv n} \left(\begin{array}{c} \text{number of } \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})\text{-orbits of Belyi} \\ \text{functions with monodromy of} \\ \text{cycle type } (\lambda_1, \lambda_2, \lambda_3) \end{array} \right).$$

Using the tools of Section 3.3, we derive the following optimized lower bound.

Theorem 3.4. *For all positive integers N, we have*

$$\mathrm{Cl}(N) \geq \frac{1}{16} 2^{\sqrt{\frac{2N}{3}}}.$$

For a positive integer N, let

$$\mathrm{Cl}'(N) = \max_{n \leq N} \max_{c \in \mathcal{N}(n)} \left(\begin{array}{c} \text{number of } \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})\text{-orbits of Belyi} \\ \text{functions with rational Nielsen class } c \end{array} \right).$$

We also prove the following theorem.

Theorem 3.5. *For all $k < 2^{\sqrt{\frac{2}{3}}}$, we have*

$$\mathrm{Cl}'(N) = \Omega\left(k^{\sqrt{N}}\right).$$

The monodromy group of the rational Nielsen class achieving the given inequality can be chosen to be A_n.

Remark 3.6. Theorem 3.4 is not special case of Theorem 3.5, because it provides an explicit constant as well as a base of $2^{\sqrt{\frac{2}{3}}}$ instead a base of arbitrarily close to $2^{\sqrt{\frac{2}{3}}}$.

3.3. **Tools to prove the lower bounds.** In this section, we state the specific consequences of the key properties of the square-root cycle type class used to prove the lower bounds stated in the preceding subsection. First, we describe a coarse analogue of SqCt.

Let n be a positive integer, and let $\lambda, \mu \dashv n$. We define a set $M(\lambda, \mu)$, of which $\operatorname{SqCt}(f)$ will be a subset for all Belyi functions f of monodromy cycle type (λ, μ, λ). First, we define an auxiliary set $M'(\lambda, \mu)$. Suppose that μ has ℓ_i parts of size i for all i, and let $\lambda_0 = n$.

$$M'(\lambda, \mu) = \left\{ \begin{array}{c} (u_0, u_1, \ldots, u_n) \mid \frac{\ell_i}{2} \leq u_i \leq \ell_i \text{ for } i \text{ and } i = 0, u_i = \frac{\ell_i}{2} \\ \text{for non-zero even } i, r + u_0 + u_1 + \cdots + u_n - n \\ \text{is an even integer that is at most } 2, \text{and there exists} \\ \text{an odd positive integer } c \text{ such that } u_c = \ell_c \text{ is odd} \end{array} \right\},$$

where r is the number of parts of λ. Given a $(n+1)-$tuple $u = (u_0, u_1, \ldots, u_n) \in M'(\lambda, \mu)$, we associate partitions $\alpha(u), \beta(u) \dashv n$. The partition $\alpha(u)$ is defined by having $2u_0 - \ell_0$ parts of size 1 and $\ell_0 - u_0$ parts of size 2, and $\beta(u)$ is defined by having $2u_k - \ell_k$ parts of size k for k odd, and $\ell_{\frac{k}{2}} - u_{\frac{k}{2}} + 2u_k - \ell_k$ parts of size k for k even. It is clear that $\alpha, \beta \dashv n$. Let $M(\lambda, \mu) = \{(\alpha(u), \beta(u), \lambda) \mid u \in M'(\lambda, \mu)\}$. The constraints on $M'(\lambda, \mu)$ are chosen so that elements of $M(\lambda, \mu)$ are *consistent* in that the existence of a Belyi function with monodromy cycle types given by any element of $M(\lambda, \mu)$ would not violate the Riemann-Hurwitz formula.

One specific application of part (b) of Theorem 3.3, is the following theorem.

Theorem 3.7 (Main Theorem)**.** *Let n be a positive integer and let $\lambda, \mu \dashv n$. Then, there are at least $|M(\lambda, \mu) \cap \mathcal{B}|$ Gal($\overline{\mathbb{Q}}/\mathbb{Q}$)-orbits of Belyi functions with monodromy of cycle type (λ, μ, λ).*

An existence result for Belyi functions, due to Edmonds-Kulkarni-Stong [3], yields the following corollary.

Corollary 3.8 (n-cycle Theorem)**.** *If $\lambda = n \dashv n$, then $M(\lambda, \mu) \subseteq \mathcal{B}$. Hence, if $\mu \dashv n$, then there are at least $|M'(\lambda, \mu)|$ Gal($\overline{\mathbb{Q}}/\mathbb{Q}$)-orbits of Belyi functions with monodromy of cycle type (n, μ, n).*

In certain cases, the constraint that $\mu_c = \ell_c$ is odd for some odd c in the definition of $M'(\lambda, \mu)$ is restrictive, in that there are λ, μ for which the Main Theorem gives weak bounds on the number of Gal($\overline{\mathbb{Q}}/\mathbb{Q}$)-orbits of Belyi functions with monodromy of cycle type (λ, μ, λ). We prove an alternate form that applies even in those cases, but is weaker in other cases. For example, consider $n = 11$, with $\lambda = 11$ and $\mu = 2222111$. The n-cycle Theorem implies that there are at least 0 Gal($\overline{\mathbb{Q}}/\mathbb{Q}$)-orbits of Belyi functions with monodromy of cycle type (λ, μ, λ); the alternate form will imply that there are at least 2 Gal($\overline{\mathbb{Q}}/\mathbb{Q}$)-orbits.

Once again, let n be a positive integer, and let $\lambda, \mu \dashv n$. Suppose that μ has ℓ_i parts of size i for all i, and let $\lambda_0 = n$. Let

$$M_0'(\lambda, \mu) = \left\{ \begin{array}{l} (u_0, u_1, \ldots, u_n) \mid \frac{\ell_i}{2} \leq u_i \leq \ell_i \text{ for odd } i \text{ and } i = 0, \\ \text{there exists an odd } i \text{ with } u_i \neq \frac{\ell_i}{2}, u_i = \frac{\ell_i}{2} \text{ for} \\ \text{non-zero even } i, \text{ and } r + u_0 + u_1 + \cdots + u_n = n + 2 \end{array} \right\},$$

where r is the number of parts of λ. Define $M_0(\lambda, \mu) = \{(\alpha(u), \beta(u), \lambda) \mid u \in M_0'(\lambda, \mu)\}$. We prove the following analogue of the Main Theorem, which follows from Theorem 3.3(c).

Theorem 3.9 (Main Theorem, Alternate Form)**.** *Let n be a positive integer and let $\lambda, \mu \dashv n$. Suppose that λ has r parts and μ has s parts, and $2r + s < n$. Then, there are at least $|M_0(\lambda, \mu) \cap \mathcal{B}|$; and Gal($\overline{\mathbb{Q}}/\mathbb{Q}$)-orbits of Belyi functions with monodromy of cycle type (λ, μ, λ).*

Similar to the n-cycle Theorem, we obtain the following corollary.

Corollary 3.10 (n-cycle Theorem, Alternate Form)**.** *If $\lambda = n \dashv n$, then $M_i(\lambda, \mu) \subseteq \mathcal{B}$ for $i = 0, 1$. Hence, if $\mu \dashv n$ has less than $n - 2$ parts, then there are at least $|M_0(\lambda, \mu)|$ Gal($\overline{\mathbb{Q}}/\mathbb{Q}$)-orbits of Belyi functions with monodromy of cycle type (n, μ, n).*

4. Proof of Theorem 3.3

Let f and t be affine coordinates centered at 0 on $\mathbb{P}^1_f$ and $\mathbb{P}^1_t$, respectively. Define the morphism $t = \frac{(f+1)^2}{4f} : \mathbb{P}^1_f \to \mathbb{P}^1_t$.

4.1. **Choosing generators of $\pi_1\left(\mathbb{P}^1 \setminus \{0,1,\infty\}, b\right)$.** We need to deal with monodromy representations induced by different base-points and different identifications of F_2 with the $\pi_1\left(\mathbb{P}^1 \setminus \{0,1,\infty\}, b\right)$. To this end, we prove the following proposition.

Proposition 4.1. *Let $b_1, b_2 \in \mathbb{P}^1 \setminus \{0,1,\infty\}$, let p be a path from b_1 to b_2 in $\mathbb{P}^1 \setminus \{0,1,\infty\}$ and let p^* denote the induced isomorphism from $\pi_1\left(\mathbb{P}^1 \setminus \{0,1,\infty\}, b_2\right)$ to $\pi_1\left(\mathbb{P}^1 \setminus \{0,1,\infty\}, b_1\right)$. Let*

$$i_1, i_2 : F_2 \to \pi_1\left(\mathbb{P}^1 \setminus \{0,1,\infty\}, b_1\right), \pi_1\left(\mathbb{P}^1 \setminus \{0,1,\infty\}, b_2\right)$$

be isomorphisms such that $i_1(x), i_2(x)$ (resp. $i_1(y), i_2(y)$) have winding numbers 1 and 0 (resp. 0 and 1) about 0 and 1, respectively. Then, $i_1^{-1} \circ p^* \circ i_2$ is an inner automorphism of F_2. In particular, if $f : X \to \mathbb{P}^1$ is Belyi function of degree n, then the monodromy representations of F_2 associated to f induced by the identifications i_1, i_2 are isomorphic.

The key tool we use is the fact that the natural map

$$\operatorname{Out}(F_2) \to \operatorname{Aut}\left({F_2}^{ab}\right) (\cong GL_2(\mathbb{Z})) \tag{2}$$

is an isomorphism (see [13, §0.1]).

Proof. Because $\mathbb{P}^1 \setminus \{0,1,\infty\}$ is path-connected, it suffices to prove that if i_1, i_2 are isomorphisms from F_2 to $\pi_1\left(\mathbb{P}^1 \setminus \{0,1,\infty\}, b\right)$ such that $i_1(x), i_2(x)$ (resp. $i_1(y), i_2(y)$) have winding numbers 1 and 0 (resp. 0 and 1) about 0 and 1, respectively, then $i_1^{-1} \circ i_2$ is an inner automorphism of F_2. By the constraint on winding numbers, the automorphism $i_1^{-1} \circ i_2$ descends to the identity on ${F_2}^{ab} \cong \mathbb{Z}^2$, and the conclusion follows by Equation 2. □

In particular, the outer action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $\widehat{F_2}$ in Equation 1 is independent of the choice of (geometric) base-point and isomorphism of F_2 with $\pi_1\left(\mathbb{P}^1 \setminus \{0,1,\infty\}, b\right)$. In the remainder of this paper, we often suppress base-points and identifications of F_2 or $\widehat{F_2}$ with the appropriate fundamental groups when discussing monodromy representations and the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

4.2. **Proof that** Sqrt **is $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-equivariant.** Let $b_f = \frac{1-\sqrt{-3}}{2}$ be the basepoint of $\mathbb{P}^1_f \setminus \{-1,0,1,\infty\}$, and let $b_t = t(b_f) = \frac{3}{4}$ be the corresponding basepoint of $\mathbb{P}^1_t \setminus \{0,1,\infty\}$. Let $b'_f = \frac{1+\sqrt{-3}}{2}$ be the element of the fiber of t over b_t other than b_f. Fix a generating set $y_{-1}, y_0, y_1, y_\infty$ for $\pi_1(\mathbb{P}^1_f \setminus \{-1,0,1,\infty\}, b_f)$ as in Figure 1, and a generating set x_0, x_1, x_∞ for $\pi_1(\mathbb{P}^1_t \setminus \{0,1,\infty\}, b_t)$ as in Figure 2. It is clear that $y_{-1}y_0y_1y_\infty = 1$ and $x_0x_1x_\infty = 1$. Let ℓ be the shown path from b_f to b'_f in

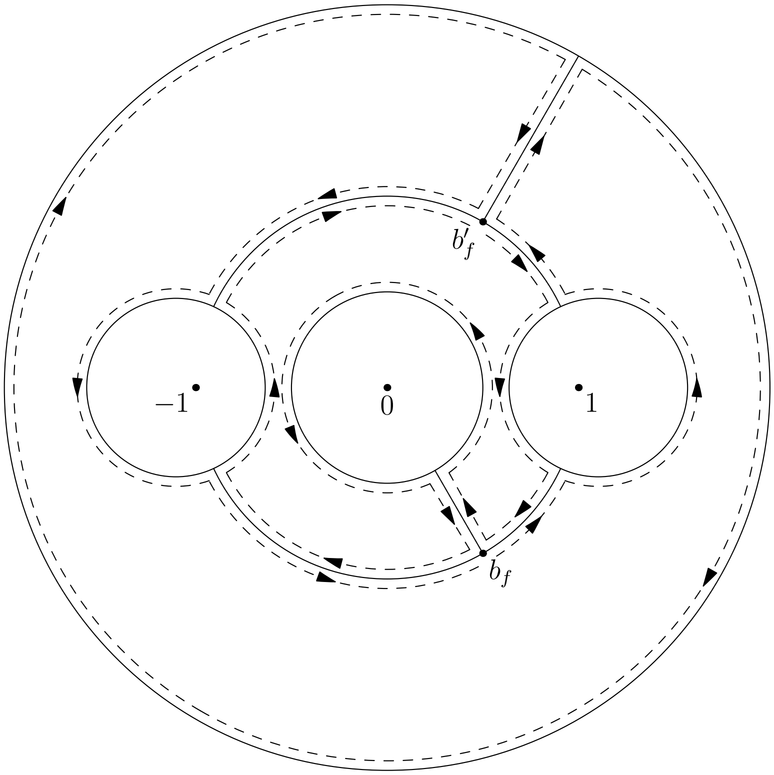

FIGURE 1. Let x_{-1} be the shown loop that traces the path from b_f to b'_f that intersects $[-1,0]$, followed by the path from b'_f to b_f that intersects $(-\infty,0]$, and let x_1 be defined similarly about 1. Let x_0 be the shown loop based at b_f that winds counterclockwise around 0, and let ℓ be the shown path from b_f to b'_f that intersects $[1,\infty)$.

$\mathbb{P}^1_f \setminus \{-1,0,1,\infty\}$. Then, one can easily verify the following relations:

$$\begin{aligned} t_* y_0 &= x_\infty \\ t_* y_{-1} &= x_0^2 \\ t_* y_1 &= x_1^2 \\ t_* \ell &= x_1, \end{aligned}$$

where the equalities are in the fundamental groupoid of $\mathbb{P}^1 \setminus \{0,1,\infty\}$. Let β be the lift of x_∞ to b'_f, and let $y_\infty = \ell^{-1}\beta\ell$, so that $t_* y_\infty = x_1^{-1} x_\infty x_1$ in the fundamental groupoid of $\mathbb{P}^1 \setminus \{0,1,\infty\}$.

Let n be a positive integer, and let $g : X \to \mathbb{P}^1_t$ be a Belyi function of degree n defined on an algebraic curve X. Let X' be the normalization of $X \times_{\mathbb{P}^1_t} \mathbb{P}^1_f$, and let $f : X' \to \mathbb{P}^1_f$ be the projection. The curve X' may not be irreducible.

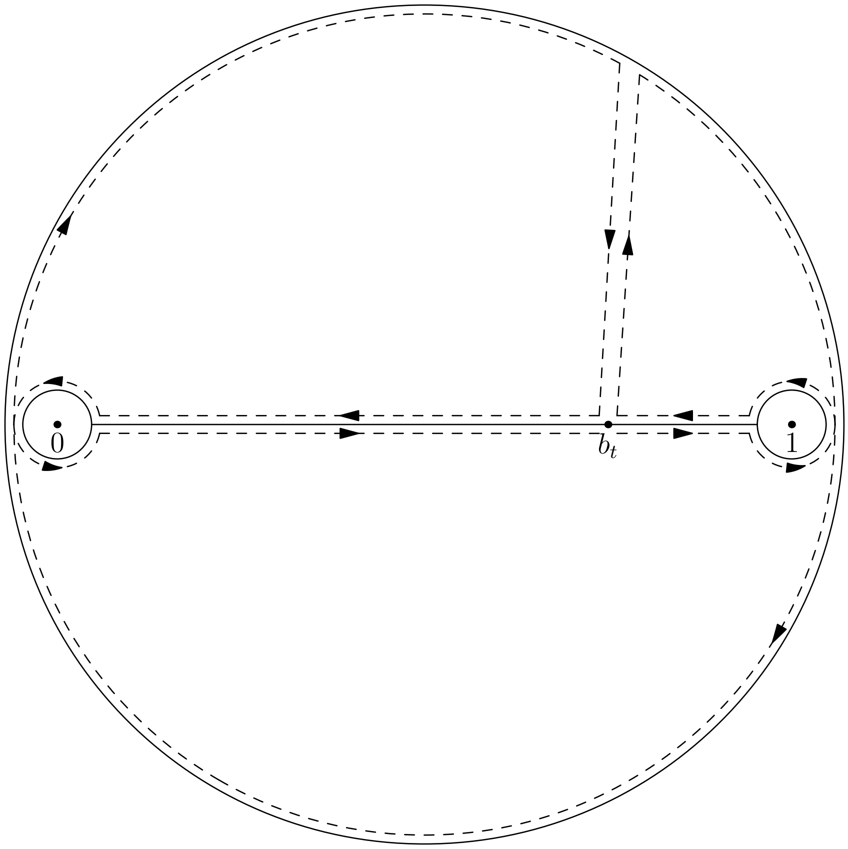

Figure 2. Let y_0 be the shown loop based at b_t that winds counterclockwise around 0, and similarly for y_1 about 1. Let y_∞ be the shown loop based at b_t that traces the outer circle.

Definition 4.2. We write $f = \Sigma(g)$, so that Σ defines a function from the set of isomorphism classes of Belyi functions to the set of isomorphism classes of morphisms of curves $X' \to \mathbb{P}^1$, where X' is not necessarily irreducible.

$$\begin{tikzcd}
X \arrow[d, "g"'] & X' \arrow[l, "\alpha"'] \arrow[d, "f"] \\
\mathbb{P}^1_t & \mathbb{P}^1_f \arrow[l, "t=\frac{(f+1)^2}{4f}"]
\end{tikzcd}$$

The projection $\alpha : X' \to X$ induces a bijection between the fibers $g^{-1}(b_t)$ and $(g')^{-1}(b_f)$. We order the fiber $g^{-1}(b_t)$, which gives an order on $(g')^{-1}(b_f)$ via the restriction of α. Using these orders, we can define the monodromy of f and g as fixed representations (not isomorphism classes of representations) of $\pi_1(\mathbb{P}^1_f \setminus \{-1, 0, 1, \infty\}, b_f)$ and $\pi_1(\mathbb{P}^1_t \setminus \{0, 1, \infty\}, b_t)$ on $[n]$. Let $p_k \in S_n$ be the image of x_k under the representation of $\pi_1(\mathbb{P}^1_t \setminus \{0, 1, \infty\}, b_t)$ for $k \in \{0, 1, \infty\}$, and let σ_k be the image of y_k under the monodromy representation of $\pi_1(\mathbb{P}^1_f \setminus \{-1,0,1,\infty\}, b_f)$ for $k \in \{-1,0,1,\infty\}$.

For all Belyi functions g, the fact that $\Sigma(g)$ is étale outside $\{-1,0,1,\infty\}$ follows from the fact that étaleness is preserved under base-change. The following proposition is immediate by lifting loops.

Proposition 4.3. *Let $g : X \to \mathbb{P}^1$ be a Belyi function, with monodromy generators $\tau_0, \tau_1, \tau_\infty$. Then, $\Sigma(g)$ is unbranched outside $\{-1,0,1,\infty\}$. Let $\sigma_{-1}, \sigma_0, \sigma_1, \sigma_\infty$ be the monodromy of the function $\Sigma(g)$ over $-1, 0, 1, \infty$, respectively (the permutations are defined up to simultaneous conjugation in S_n because we fixed loops of winding number 1 about each branch point in both $\mathbb{P}^1_t$ and $\mathbb{P}^1_f$). Then, we have $\sigma_0 = \tau_\infty$, $\sigma_1 = \tau_1^2$, $\sigma_{-1} = \tau_0^2$, and $\sigma_\infty = \tau_1^{-1}\tau_\infty\tau_1$.*

We are now ready to link the constructions of this subsection to the square-root class.

Definition 4.4. Let $f : X \to \mathbb{P}^1$ be a Belyi function. Define

$$\mathrm{Sqrt}'(f) = \{g \mid \Sigma(g) \cong f\},$$

and call $\mathrm{Sqrt}'(f)$ the *fibered product square-root class of f*.

Theorem 4.5. *(a) The function Sqrt' is $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-equivariant.*
(b) Let n be a positive integer, and let $f : X \to \mathbb{P}^1$ be a Belyi function of degree n. Then, $\mathrm{Sqrt}(f)$ is the set of monodromy triples of elements of $\mathrm{Sqrt}'(f)$.
In particular, the function Sqrt is $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-equivariant.

Proof. We begin by proving part (a). We treat Belyi functions as finite étale covers of $\mathbb{P}^1_{\overline{\mathbb{Q}}} \setminus \{0,1,\infty\}$. The fact that Σ is $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-equivariant then follows from the fact that F_σ preserves fibered products and normalizations.

Part (b) follows immediately from Proposition 4.3. □

4.3. **Proof of Part (a).** Let $f : X \to \mathbb{P}^1$ be a Belyi function. The key to the proof of this part is to construct an injection from $\mathrm{Sqrt}'(f)$ to the set of involutions on X. The remainder of the statement follows from Hurwitz's Automorphism Theorem.

Proof of Theorem 3.3(a). Let $Inv(X)$ denote the set of non-trivial involutions on X. We construct an injection $i : \mathrm{Sqrt}'(f) \to Inv(X)$. Let $g \in \mathrm{Sqrt}'(f)$, so that we have a diagram

$$\begin{tikzcd} Y & X \arrow[l, "\alpha"'] \arrow[d, "f"] \\ \mathbb{P}^1_t \arrow[from=1-1, d, "g"'] & \mathbb{P}^1_f, \arrow[l, "t=\frac{(f+1)^2}{4f}"] \end{tikzcd} \tag{3}$$

with X the normalization of the fibered product $Y \times_{\mathbb{P}^1_t} \mathbb{P}^1_f$. The bottom morphism is of degree 2, and the vertical morphisms are of degree n, which implies that the top morphism α is also of degree 2. There is an involution $\iota : X \to X$, which is the unique deck transformation for the restriction of α to its unramified locus. Let $i(g) = \iota$. Note that $\alpha : X \to Y$ is the quotient of X by ι, so that ι determines α up to composition by an automorphism of Y.

To prove that i is injective, it suffices to prove that α, f, and the bottom morphism uniquely determine g. This is obvious, because α is surjective and diagram 3 is required to commute. Therefore, $|\operatorname{Sqrt}'(f)| \leq |Inv(X)|$, and the fact that $|\operatorname{Sqrt}(f)| \leq |Inv(X)|$ follows by Theorem 4.5(b). □

4.4. **Proof of Part (b).** We transfer to representations of F_2 to analyze the fibered product square-root class. Fix a generating set $F_2 = \langle x, y\rangle$ and a positive integer n. For all positive integers k, let $[k]$ denote the set $\{1, 2, \ldots, k\}$. Let T_r be the set of conjugacy classes of transitive representations $m : F_2 \to S_n$ such that there exists an odd positive integer c such that $m(y)$ contains an odd number of cycles of length c and no cycle of length $2c$. Let ξ denote the representation of F_2 on S_2 with $\xi(x) = (1)(2)$ and $\xi(y) = (1\,2)$.

Proposition 4.6. *Let n be a positive integer. Let $m \in T_r$ be a transitive representation $m : F_2 \to S_n$, and let m' be a representation $m' : F_2 \to S_n$.*

(a) The representation $m \times \xi$ is transitive.
(b) If $m \times \xi \cong m' \times \xi$, then $m \cong m'$.

Proof. Suppose that m, m' satisfy the conditions of the proposition. Let $m_\xi = m\times\xi$ and let $m'_\xi = m \times \xi$.

First, we prove part (a). Let $(a, b), (a', b') \in [n] \times [2]$, and we will prove that there exists a word $w \in F_2$ such that $m_\xi(w)(a, b) = (a', b')$. By definition, the permutation $m(y) \in S_n$ must have an odd cycle in its cycle decomposition. Suppose that $(p_1\, p_2 \cdots p_k)$ be a cycle in $m(y)$ with k odd. Let $w_0, w_1 \in F_2$ be such that $m(w_0)(a) = p_1$ and $m(w_1)(p_1) = a'$; because m is transitive, such w_0, w_1 exist. If $\xi(w_1w_0)(b) = b'$, then we can take $w = w_1w_0$ because $m(w_1w_0)(a) = a'$. Hence, we can assume that $\xi(w_1w_0) \neq b'$. Let $w = w_1y^kw_0$. Because k is odd, $\xi(w)(b) = b'$, and it is easy to see that $m(w)(a) = a'$. It follows that m'_ξ is transitive.

We now prove part (b). It follows from part (a) that m' is also transitive. There is an automorphism α of $[n] \times [2]$ such that $\alpha \circ (m \times \xi) = m' \times \xi$. Let G be the kernel of ξ; it is a normal subgroup of index 2 in F_2. Note that the m-action (resp. m'-action) of G on $[n] \times [2]$ fixes the second coordinate. Because m_ξ and m'_ξ are transitive representations, the group $F_2/G \cong (\mathbb{Z}/2\mathbb{Z})^+$ acts transitively on the set of m_ξ-orbits (resp. m'_ξ-orbits) of G in $[n] \times [2]$. In particular, there are at most 2 m_ξ-orbits (resp. m'_ξ) orbits of G, so that $m_\xi(x)$ and $m_\xi(y^2)$ generate a subgroup of $S_{[n]\times[2]}$ that acts on $[n]\times[2]$ with two orbits, $[n]\times\{1\}$ and $[n]\times\{2\}$, and similarly for m'. The action of α must preserve these orbits. Therefore, the second coordinate of $\alpha(i, j)$ must be j for all i, j. Furthermore, G acts transitively on $[n] \times \{1\}$.

Suppose that $m(y)$ contains $2k + 1$ of cycles of length c and no cycle of length $2c$. Then, $m_\xi(y)$ contains $2k + 1$ cycles of length $2c$. Therefore, $m'_\xi(y)$ must also contain $2k + 1$ cycles of length $2c$. Suppose that $m'(y)$ contains a cycles of length c and b cycles of length $2c$. Then, $m'_\xi(y)$ contains $a + 2b$ cycles of length $2c$, from which it follows that a is odd and thus $a \geq 1$. Let ζ' be a cycle of length c in m'_ξ and $\tau' = \zeta' \times \xi(y)$ the corresponding cycle of length $2c$ in m'_ξ. Let $\tau = \alpha^{-1} \circ \tau' \circ \alpha$ be the corresponding cycle of length $2c$ in m_ξ. Because $m(y)$ does not contain any cycle of length $2c$, we must have $\tau = \zeta \times \xi(y)$ for some cycle ζ of length c in $m(y)$.

Without loss of generality, we assume that 1 is not fixed by ζ, and we may also assume that the second coordinate of $\alpha(1, 1)$ is 1. Let $\alpha(1, 1) = (\beta(1), 1)$. Then, we have $\tau^c(1,1) = (1,2)$ and $\tau^c(1,2) = (1,1)$, and similarly that $\tau'^c(\beta(1),1) = (\beta(1),2)$ and $\tau'^c(\beta(1),2) = (\beta(1),1)$.

It suffices to prove that there is a permutation $\beta \in S_n$ such that $\alpha(i,j) = (\beta(i),j)$, as this would imply that the representations m and m' differ only by conjugation by an element of S_n. Fix i and let $g \in G$ be such that $m_\xi(g)(1,1) = (i,1)$. We must have $m(g)(i) = 1$, from which it follows that $m_\xi(g)(1,2) = (i,2)$. We have

$$m_\xi(g) \circ \tau^c(i,1) = (i,2).$$

It is clear that

$$m'_\xi(g)(\beta(i),1) = \alpha \circ m_\xi(g) \circ \alpha^{-1} = (\beta(1),1).$$

Thus, we have $m'(g)(\beta(i)) = \beta(1)$ from which it follows that $m'_\xi(\beta(i),2) = (\beta(1),2)$. However, we have

$$\begin{aligned}\alpha(i,2) &= \alpha \circ m_\xi(g) \circ \tau^c \circ m_\xi(g)^{-1}(i,1) \\ &= \left(\alpha \circ m_\xi(g) \circ \alpha^{-1}\right) \circ \left(\alpha \circ \tau^c \circ \alpha^{-1}\right)(\alpha(1,1)) \\ &= m'_\xi(g) \circ \tau'^c(\beta(1),1) = m'_\xi(g)(\beta(1),2) = (\beta(i),2),\end{aligned}$$

as desired. The proposition follows. □

Fix the isomorphism $\langle x,y\rangle = F_2 \cong \pi_1(\mathbb{P}^1 \setminus \{0,1,\infty\}, \frac{3}{4})$ with $x \mapsto x_\infty$ and $y \mapsto x_1$. Taking monodromy representations gives a bijection $K = K_n$ between the set of isomorphism classes of degree n Belyi functions and the set of transitive representations $m : F_2 \to S_n$. An important auxiliary proposition that we use in the proof of Theorem 3.3 as well as the proof of the Main Theorem is the following.

Proposition 4.7. *Fix a positive integer n. For all Belyi functions g of degree n, $K(\Sigma(g) \circ t) = K(g) \times \xi$, where $t = \frac{(f+1)^2}{4f}$.*

Proof. Let $\mathcal{C}$ be the category of étale covers of $\mathbb{P}^1 \setminus \{0,1,\infty\}$. The function K is the object function of a contravariant functor from $\mathcal{C}$ to $\mathbf{FinSet}^{F_2}$, the category of representations of F_2 on the category of finite sets. It is well-known that K is in fact an equivalence of categories. In particular, K preserves products. But, $\Sigma(g) = g \times t$ (in $\mathcal{C}$), and the conclusion follows. □

Proof of Theorem 3.3(b). Let $f : X \to \mathbb{P}^1$ be a Belyi function of odd degree n, let $(\tau_0, \tau_1, \tau_\infty) \in \operatorname{Sqrt}(f)$, and let $\mu \dashv n$ be the cycle type of τ_1. Suppose that k, c are odd positive integers such that μ has c parts of size k and no parts of size $2k$. Let m be the representation of F_2 on S_n that sends x to τ_0 and y to τ_1. By Proposition 4.6, if a representation $m' : F_2 \to S_n$ satisfies $m \times \xi \cong m' \times \xi$, then in fact $m \cong m'$.

Suppose that $\tau' = (\tau'_0, \tau'_1, \tau'_\infty) \in \operatorname{Sqrt}(f)$ and $m' : F_2 \to S_n$ is the corresponding representation. It follows from Theorem 4.5(b) and Proposition 4.7 that $m' \times \xi \cong K(f \circ t) \cong m \times \xi$, which implies that $m \cong m'$. Therefore, $(\tau'_0, \tau'_1, \tau'_\infty)$ is conjugate to $(\tau_0, \tau_1, \tau_\infty)$. Since the choice of τ' was arbitrary, $|\operatorname{Sqrt}(f)| = 1$ and the result follows. □

4.5. **Proof of Part (c).** Let n be an odd positive integer, and let $\lambda, \mu \dashv n$. We use the fact that a hyperelliptic curve admits a unique involution with a genus 0 quotient in the proof of Theorem 3.3(a). Equivalently, we replace Proposition 4.6 in the proof of Theorem 3.3(b) with the fact about hyperelliptic curves.

Proof of Theorem 3.3(c). Let T_0 denote the set of isomorphism classes of Belyi functions of that $\mathbb{P}^1$ admits. Note that $g(\lambda_0, \lambda_1, \lambda_\infty)$ is the genus of a curve that admits a Belyi function with monodromy cycle type $(\lambda_0, \lambda_1, \lambda_\infty)$, if such a curve exists. Therefore, by Theorem 4.5(b), it suffices to prove that the restriction of Σ to T_0 is injective.

Consider two commutative squares

$$\begin{tikzcd}
\mathbb{P}^1_z \arrow[d, "g"'] & X \arrow[l, "\alpha"'] \arrow[d, "f"] & \text{and} & \mathbb{P}^1_z \arrow[d, "g'"'] & X \arrow[l, "\alpha'"'] \arrow[d, "f"] \\
\mathbb{P}^1_t & \mathbb{P}^1_f \arrow[l, "t=\frac{(f+1)^2}{4f}"] & & \mathbb{P}^1_t & \mathbb{P}^1_f, \arrow[l, "t=\frac{(f+1)^2}{4f}"]
\end{tikzcd}$$

where in both diagrams X is the normalization of the fibered product $\mathbb{P}^1_z \times_{\mathbb{P}^1_t} \mathbb{P}^1_f$, and the left morphisms are Belyi functions of degree n. Because a hyperelliptic curve of genus at least 2 admits a unique degree 2 function to $\mathbb{P}^1$, there must be an automorphism β of the top left copy of $\mathbb{P}^1$ such that $\alpha' = \beta \circ \alpha$. Hence, we have $g \circ \alpha = t \circ f$ and $(g' \circ \beta) \circ \alpha = t \circ f$. Because α is surjective, this implies that $g = g' \circ \beta$. □

5. Proofs of the Main Theorem and the n-cycle Theorem and lower bounds on $\mathrm{Cl}(n)$, $\mathrm{Cl}'(n)$

5.1. **Proofs of the Main Theorem and the n-cycle Theorem.** Fix a integer n and partitions $\lambda, \mu \dashv n$. For $\alpha, \beta \dashv n$, define $S_{\alpha,\beta}$ to be the set of isomorphism classes of Belyi functions with monodromy of cycle type (α, β, λ). Let

$$S = \bigcup_{(\alpha,\beta,\lambda)\in M(\lambda,\mu)\cap\mathcal{B}} S_{\alpha,\beta} \quad \text{and} \quad S_0 = \bigcup_{(\alpha,\beta,\lambda)\in M_0(\lambda,\mu)\cap\mathcal{B}} S_{\alpha,\beta}.$$

Let $f \in \Sigma(S) \cup \Sigma(S_0)$. Proposition 4.3 implies that f is étale when restricted to the pre-image of $\mathbb{P}^1 \setminus \{0, 1, \infty\}$, and has monodromy of cycle type (λ, μ, λ). By Propositions 4.6(a) and 4.7, the monodromy of f acts transitively on the fiber above the base-point, and it follows that the domain of f is irreducible and f is a Belyi function. The Main Theorem, in its ordinary and alternate forms, follow from Theorem 3.3 parts (b) and (c), respectively.

Proof of the Main Theorem. By Theorem 3.3(b), $|\mathrm{SqCt}(f)| = 1$ for all $f \in \Sigma(S)$. By construction, $\mathrm{SqCt}(f)$ can take any value in $M(\lambda, \mu) \cap \mathcal{B}$ as f ranges over S. Because SqCt is $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-invariant, the theorem follows. □

Proof of the Main Theorem, Alternate Form. By Theorem 3.3(b) and the construction of S_0, $\mathrm{SqCt}(f)$ contains exactly one element $(\lambda_0, \lambda_1, \lambda_\infty)$ such that $g(\lambda_0, \lambda_1, \lambda_\infty) = 0$ for all $f \in \Sigma(S_0)$. Denote this element by $R(f)$. Because SqCt is $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-invariant, so is $R(f)$. By construction of S_0, $R(f)$ can take all values in $M'(\lambda, \mu) \cap \mathcal{B}$ as f ranges over S_0, and the theorem follows. □

By construction, the assertion that $M(\lambda, \mu) \subseteq \mathcal{B}$ would not violate the Riemann-Hurwitz formula. The fact that $M(\lambda, \mu) \subseteq \mathcal{B}$ when $\lambda = n \dashv n$ is immediate by Theorem 2.3, and the n-cycle Theorems follow.

5.2. **Primitive subgroups of S_n.** We need a result on primitive subgroups of S_n, from Dixon-Mortimer [2] but due to Jordan. We also need a result describing permutation groups that contain short length cycles.

Theorem 5.1 ([2], Example 3.3.1)**.** *Let $n \geq 9$, let G be a subgroup of S_n, and suppose that there exists a nonidentity $\sigma \in G$ with at least $n-4$ fixed points. If G does not contain a transposition or a 3-cycle, then G is not primitive.*

Theorem 5.2 ([2], Theorem 3.3E)**.** *Let q be a prime, and let $n > q+2$. If a primitive subgroup G of S_n contains a q-cycle, then G contains A_n.*

The form that we will need is the following proposition, which is immediate from Theorems 5.1 and 5.2.

Proposition 5.3. *Let $p > 7$ be a prime, and let G be a subgroup of S_p that contains a p-cycle and a double transposition. Then G contains A_p.*

Proof. A subgroup of S_p that contains a p-cycle is primitive, and a double transposition in S_p has $p-4$ fixed points. By Theorem 5.1, G contains a 2-cycle or a 3-cycle. In both cases, Theorem 5.2 implies that G contains A_p, as claimed. □

Remark 5.4 (Noam Elkies, private communication). The proposition is false for $p = 5, 7$. For $p = 5$, one can take $G = D_{10}$, and for $p = 7$, one can take $G = PGL_3(\mathbb{Z}/2\mathbb{Z})$.

5.3. **Proofs of Theorems 3.4 and 3.5.** We derive Theorems 3.4 and 3.5 from the Main Theorem and the results quoted in the preceding section. First, we begin with a few computational lemmata, whose proofs are deferred to Appendix A.

Let t and k be positive integers with $k \leq t$. Define

$$f_t(k) = \left\lfloor \frac{4t+2}{2k-1} \right\rfloor.$$

For a positive integer t, define

$$n_0(t) = 2t + 1 + \sum_{i=1}^{t} 2(2k-1) \left\lfloor \frac{4t+2}{2k-1} - 1 \right\rfloor.$$

Lemma 5.5. *For all positive integers t, we have*

$$4t^2 + 12t + 1 < n_0(t) < 6(t+1)^2 - 4.$$

Lemma 5.6. *Let t be a positive integer. Then, we have*

$$\sum_{k=1}^{t} (f(k) - 1) \leq \frac{n_0(t)}{4}.$$

Lemma 5.7. *Let t be a positive integer. Then, we have*

$$\prod_{k=1}^{t} \left\lfloor \frac{4t+2}{2k-1} \right\rfloor > 2^{2t}.$$

Proof of Theorem 3.4. Let t be a positive integer, and let $n = n_0(t)$. We will prove a lower bound on $\mathrm{Cl}(n)$ which will imply the theorem. Let $\lambda = n \dashv n$. Define the partition $\mu \dashv n$ by requiring that u have $2f(k) - 2$ parts of size $2k-1$ for $1 \leq k \leq t$, and 1 part of size $2t+1$.

We claim that

$$|M'(\lambda,\mu)| \geq \prod_{k=1}^{t} f(k). \tag{4}$$

Let S be the set of tuples $(v_0, v_1, \ldots, v_n)$ such that $f(k) - 1 \leq v_{2k-1} \leq 2f(k) - 2$ for all $1 \leq k \leq t$, $v_{2t+1} = 1$, $v_i = 0$ for all $i > 2t+1$ and $i = 2, 4, \ldots, 2t$, and $v_0 = n - r(v)$, where

$$r(v) = \sum_{k=1}^{t} (2f(k) - 2 - v_k).$$

Notice that $v_{2t+1} = 1$, and μ has 1 part of size $2t+1$ and no parts of size $4t+2$. Hence, to prove Equation 4, it suffices to prove that $S \subseteq M'(\lambda,\mu)$. It suffices to prove that $r(v) \leq \frac{n}{2}$. Indeed, we have

$$\frac{r(v)}{2} \leq \sum_{k=1}^{t} (f(k) - 1).$$

Lemma 5.6 implies that $r(v) \leq \frac{n}{2}$ for all t, v.

The n-cycle Theorem implies that $\mathrm{Cl}(n) \geq |M(\lambda,\mu)| \geq \prod_{k=1}^{u} f(k)$. By Lemma 5.7, it follows that $\mathrm{Cl}(n) \geq 2^{2t}$, and Lemma 5.5 implies that

$$\mathrm{Cl}(6(t+1)^2) \geq 2^{2t}$$

for all positive integers t. Fix a positive integer $N \geq 24$. If $6(t+1)^2 \leq N < 6(t+2)^2$, then we have

$$\log_2 \mathrm{Cl}(N) \geq 2t > 2\left(\sqrt{\frac{N}{6}} - 2\right) = \sqrt{\frac{2N}{3}} - 4.$$

It follows that

$$\mathrm{Cl}(N) \geq \frac{1}{16} 2^{\sqrt{\frac{2N}{3}}}.$$

The bound is trivial for $N < 24$, and thus we have established the result for all N. □

Remark 5.8. A simpler construction can establish that $\mathrm{Cl}(N) = \Omega\left(2^{\sqrt{\frac{N}{2}}}\right)$.

Proof of Theorem 3.5. As in the previous proof, let t be a positive integer, and for $1 \leq k \leq t$, let $f(k) = \left\lfloor \frac{4t+2}{2k-1} \right\rfloor$. Let

$$n_1 = 4 + 2t + 1 + \sum_{i=1}^{t} 2(2k-1) \left\lfloor \frac{4t+2}{2k-1} - 1 \right\rfloor.$$

Let n be the smallest prime number that is at least $n_0(t)$. Let $\epsilon(t) = \frac{n}{n_0(t)} - 1$. Because

$$\lim_{t\to\infty} n_0(t) = \infty,$$

the Prime Number Theorem implies that

$$\lim_{t\to\infty} (1 + \epsilon(t)) = \lim_{t\to\infty} \frac{n}{n_0(t)} = 1.$$

It is clear that $n_1 > 2$, which implies that $n \equiv n_1 \pmod 2$. Let $2\alpha + 1 = 2t + 1 + n - n_0$. Let $\lambda = (n) \dashv n$, and let $\mu \dashv n$ be the partition of n with $f(k)$ parts of size $2k-1$ for $1 \leq k \leq t$, two parts of size 2, and one part of size $n - n_0(t)$. By Lemma 5.5, we have $n_1 \leq n_0(t) + 4 < 6(t+1)^2$, which implies that $n < 6(t+1)^2(1 + \epsilon(t))$.

We claim that

$$|M(\lambda,\mu)\cap\mathcal{B}|\geq\prod_{k=1}^{t}f(k). \tag{5}$$

Let S be the set of tuples $(v_0,v_1,\ldots,v_n)$ such that $f(k)-1\leq v_{2k+1}\leq 2f(k)-2$ for all $1\leq k\leq t$, $v_{n-n_0(t)}=1$, $v_0=n-r(v)$ where

$$r(v)=1+\sum_{k=1}^{t}(2f(k)-2-v_k),$$

and $v_i=0$ for all other i. It follows from Lemma 5.6 that $r(v)\leq\frac{n}{2}$ for all v,t, which implies that $S\subseteq M'(\lambda,\mu)$. Notice that $v_{n-n_0(t)}=1$, and μ has 1 part of size $n-n_0(t)$ and no parts of size $2n-2n_0(t)$. Equation 5 follows.

Let f be a Belyi function with monodromy of cycle type (λ,μ,λ) and monodromy generators $\sigma_0,\sigma_1,\sigma_\infty$ over $0,1,\infty$, respectively. By definition, the permutation $\sigma_1^{(2t-1)!!}$ is a double transposition. Because

$$n\geq n_1=n_0(t)+4\geq n_0(1)+4=9,$$

Proposition 5.3 implies that the monodromy group G, which is generated by σ_0 and σ_1, contains A_n. The fact that σ_0 and σ_1 are even implies that $G=A_n$. There are two conjugacy classes of n-cycles in A_n, so that σ_0 and σ_∞ can be in the same conjugacy class or in different conjugacy classes. Because σ_0 and σ_1 are only defined up to conjugation in S_n, the case of both monodromy generators being in one conjugacy class lies in the same rational Nielsen class as the case of both monodromy generators being in the other rational Nielsen class. Furthermore, the S_n-conjugacy class of permutations of cycle type λ forms a single A_n-conjugacy class. Thus, there are at most two possible rational Nielsen classes of Belyi functions with monodromy of cycle type (λ,μ,λ).

By the n-cycle Theorem, there are at least $|M(\lambda,\mu)|\geq\prod_{k=1}^{t}f(k)$ Belyi functions with monodromy of cycle type (λ,μ,λ). The previous paragraph and Lemma 5.7 then yield that

$$\mathrm{Cl}'(6(t+1)^2(1+\epsilon(t)))\geq\frac{1}{2}\prod_{k=1}^{t}f(k)>2^{2t-1}$$

for all positive integers t.

We now let t vary. Fix a constant $k<2^{\sqrt{\frac{2}{3}}}$. Let T be a positive integer such that

$$1+\epsilon(t)<\frac{2}{3\left(\log_2 k\right)^2}$$

for all $t>T$; such a T exists because $\lim_{t\to\infty}\epsilon(t)=0$. Let $P=n_0(T)(1+\epsilon(T))$, and let $N\geq P$. There exist an integer $t\geq T$ such that

$$n_0(t+1)(1+\epsilon(t+1))\leq N<n_0(t+2)(1+\epsilon(t+2)).$$

Then, by Lemma 5.6, we have that $N<6(t+2)^2(1+\epsilon(t+2))$. It follows that

$$t>\sqrt{\frac{N}{6(1+\epsilon(t+2))}}-2.$$

The fact that Cl' is non-decreasing implies that

$$\log_2 \mathrm{Cl}'(N) \geq 2t - 1 > \sqrt{\frac{2N}{3(1+\epsilon(t+2))}} - 5 > \sqrt{N} \log_2 k - 5.$$

The theorem follows. □

6. Concluding remarks and open problems

6.1. **Generalizing the square-root class.** Let $t : \mathbb{P}^1_f \to \mathbb{P}^1_t$ be a morphism of curves satisfying $t(\{0,1,\infty\}) \subseteq \{0,1,\infty\}$. Given a Belyi function $f : X \to \mathbb{P}^1$, we can form the *generalized square-root class* of f, defined by

$$\mathrm{Sqrt}_t(f) = \{\text{Belyi functions } g : X' \to \mathbb{P}^1 \mid g \times_{\mathbb{P}^1_t} t \cong f\}.$$

It is clear that if t is defined over a number field K, then the function $\mathrm{Sqrt}_t(f)$ is $\mathrm{Gal}\left(\overline{\mathbb{Q}}/K\right)$-equivariant. We recover the ordinary square-root class for the choice of $t = \frac{(f+1)^2}{4f}$, so that the square-root class induces the generalized square-root class in a similar fashion to the manner in which the cartographic group induces Wood's Belyi-extending map invariant [14].

However, if t is of degree greater than 1, then $\mathrm{Sqrt}_t(f)$ will be empty for most Belyi functions f, and therefore we do not recover a very general invariant. In our case, where $t = \frac{(f+1)^2}{4f}$, the monodromy cycle types of f above 0 and ∞ must be the same in order for $\mathrm{Sqrt}(f)$ to be nonempty. We give an example that suggests that one may be able to reformulate the invariant in a manner that is applicable more generally.

6.2. **Example: Belyi functions with monodromy of cycle type $(n, (2g+1)11\cdots1, n)$.** We apply the Main Theorem to the case of Belyi functions with monodromy of cycle type $(n, (2g+1)11\cdots1, n)$. An explicit count of $M(n, (2g+1)11\cdots)$ and an application of the n-cycle Theorem yield the following result.

Proposition 6.1. *Let g be a positive integer and let $n \geq 4g+1$ be an odd positive integer. Then, there are at least $\left\lfloor \left(\frac{g}{2}+1\right)^2 \right\rfloor$ $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-orbits classes of Belyi maps of type $(n, (2g+1)11\cdots1, n)$.*

In the case of $g = 1$ and $n = 5, 7, 9$, we constructed the Belyi functions and explicitly verified the following conjecture, which suggests that the square-root cycle type class can be adapted to an invariant that describes the combinatorial action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the group of principal divisors.

Conjecture 6.2. *Let n be an odd positive integer, X an algebraic curve, and $f : X \to \mathbb{P}^1$ a Belyi function with monodromy of cycle type $(n, 311\cdots1, n)$. Let P and O be the locations of the ramifications of order $n-1$ on X, and let T be the location of the ramification of order 2. Then, $\mathrm{SqCt}(f) = \{(22\cdots2111, 322\cdots2, n)\}$ if and only if*

$$(T) \sim \frac{n+1}{2}(P) - \frac{n-1}{2}(O)$$

as divisors on X.

References

[1] G. V. Belyĭ. On Galois extensions of a maximal cyclotomic field. *Mathematics of the USSR-Izvestiya*, 14(2):247, 1980.

[2] J. D. Dixon and B. Mortimer. *Permutation Groups.* Number 163 in Graduate Texts in Mathematics. Springer-Verlag, 1996.

[3] A. L. Edmonds, R. S. Kulkarni, and R. E. Stong. Realizability of branched coverings of surfaces. *Transactions of the American Mathematical Society*, 282(2):773–790, 1984.

[4] J. S. Ellenberg. Galois invariants of dessins d'enfants. In Fried and Ihara [5], pages 27–42.

[5] M. Fried and Y. Ihara, editors. *Arithmetic Fundamental Groups and Noncommutative Algebra*, number 70 in Proceedings of Symposia in Pure Mathematics, 2002.

[6] A. Grothendieck. Esquisse d'un programme. In Schneps and Lochak [11], pages 5–48.

[7] A. Grothendieck. *Revêtements Étales et Groupe Fondemental: Seminaire de Geometrie Algebrique du Bois Marie 1960/61 (SGA 1).* Number 224 in Lecture Notes in Mathematics. Springer-Verlag, 1971.

[8] L. Schneps. Dessins d'enfants on the Riemann sphere. In Schneps [10], pages 47–77.

[9] L. Schneps. Dessins d'enfants: The theory of cellular maps on Riemann surfaces. In Schneps [10], pages 1–15.

[10] L. Schneps, editor. *The Grothendieck Theory of Dessins d'Enfants*, number 200 in London Mathematical Society Lecture Notes Series. Cambridge University Press, 1994.

[11] L. Schneps and P. Lochak, editors. *Geometric Galois Actions I: Around Grothendieck's Esquisse d'un Programme*, number 242 in London Mathematical Society Lecture Notes Series. Cambridge University Press, 1997.

[12] J.-P. Serre. *Topics in Galois Theory.* Number 1 in International Research Notices in Mathematics. A. K. Peters, 2008.

[13] K. Vogtmann. Automorphisms of free groups and outer space. *Geometriae Dedicata*, 94(1):1–31, 2002.

[14] M. M. Wood. Belyi-extending maps and the Galois action on dessins denfants. *Publications of the Research Institute for Mathematical Sciences*, 42(3):721–737, 2006.

[15] L. Zapponi. Fleurs, arbres et cellules: un invariant Galoisien pour une famille d'arbres. *Compositio Mathematica*, 122(2):113–133, 2000.

Appendix A. Proofs of Lemmata 5.5, 5.6, and 5.7

Proof of Lemma 5.5. We have

$$\begin{aligned} n &\le 2t+1+\sum_{k=1}^{t} 2(2k-1)\left(\frac{4t+2}{2k-1}-1\right) = 2t+1+2\sum_{k=1}^{t}(4t+3-2k) \\ &= 2t+1+t(6t+6) = 6t^2+12t+1 < 6(t+1)^2 \end{aligned}$$

and

$$\begin{aligned} n &> 2t+1+\sum_{k=1}^{t} 2(2k-1)\left(\frac{4t+2}{2k-1}-2\right) = 6t^2+12t+1-\sum_{k=1}^{t}2(2k-1) \\ &= 4t^2+12t+1. \end{aligned}$$

□

Proof of Lemma 5.6. We have

$$\sum_{k=1}^{t}(f(k)-1) \le \sum_{k=1}^{t}\left(\frac{4t+1}{2k-1}-1\right) = -t+(4t+1)\sum_{k=1}^{t}\frac{1}{2k-1}.$$

Applying the bound

$$\log(m+1) \le \sum_{k=1}^{m}\frac{1}{k} \le \log m + 1,$$

which holds for all positive integers m, we have

$$\sum_{k=1}^{t}(f(k)-1) \leq -t + (4t+1)\left(\log(2t-1) + 1 - \frac{\log(t)}{2}\right).$$

Therefore, we have

$$2\sum_{k=1}^{t}(f(k)-1) \leq 6t + 2 + (4t+1)\log(4t).$$

It follows that $2\sum_{k=1}^{t}(f(k)-1) \leq 2t^2 + 6t + \frac{1}{2} \leq \frac{n_0(t)}{2}$ for $t \geq 8$, where the second inequality is by Lemma 5.5. We can easily verify the lemma for $t \leq 7$, and the lemma follows. □

Proof of Lemma 5.7. Fix t, and let M denote the left-hand side. We have

$$M > \prod_{k=1}^{t}\left(\frac{4t+2}{2k-1} - 1\right) = \frac{\prod_{k=1}^{t}(4t+3-2k)}{\prod_{k=1}^{t}(2k-1)}.$$

Recall that

$$(2m-1)!! = \prod_{k=1}^{m}(2k-1) = \frac{(2m)!}{2^m(m!)}.$$

Returning to M, we have

$$\begin{aligned} M &> \frac{(4t+1)!!}{(2t+1)!!(2t-1)!!} = \frac{(4t+2)!2^{t+1}2^t}{(2t+2)!(2t)!2^{2t+1}} = \frac{(4t+2)!2^{t+1}(t+1)!2^t t!}{(2t+1)!(2t+2)!(2t)!2^{2t+1}} \\ &= \frac{(4t+2)!(t+1)!t!}{(2t+1)!(2t+2)!(2t)!} = \frac{\binom{4t+2}{2t+1}}{2\binom{2t}{t}}. \end{aligned}$$

We now apply Stirling's formula with error bounds, which is the well-known inequality

$$e^{\frac{1}{12m+1}} < \frac{m!}{\sqrt{2\pi m}\left(\frac{m}{e}\right)^m} < e^{\frac{1}{12m}}.$$

It follows that

$$e^{\frac{1}{24m+1} - \frac{1}{6m}} < \frac{\binom{2m}{m}\sqrt{\pi m}}{2^m} < e^{\frac{1}{24m} - \frac{2}{12m+1}}.$$

In particular, we have

$$\frac{-1}{6m} < \log\frac{\binom{2m}{m}\sqrt{\pi m}}{2^{2m}} < 0.$$

Applying this bound to M, we have

$$M > 2^{2t}\sqrt{2}e^{\frac{-1}{12t+6}} > 2^{2t}.$$

□

Phillips Exeter Academy, 20 Main St, Exeter, NH 03833
E-mail address: ravi.jagadeesan@gmail.com