MONODROMY GROUPS OF INDECOMPOSABLE COVERINGS OF BOUNDED GENUS

DANNY NEFTIN AND MICHAEL E. ZIEVE

ABSTRACT. Determining the possibilities for the key invariants associated to a covering of complex curves $f\colon X \to \mathbb{P}^1$ is a fundamental question with applications to various areas of math. For each nonnegative integer g we classify the ramification types and monodromy groups of indecomposable coverings $f\colon X \to \mathbb{P}^1$ where X has genus g, under the hypothesis that $n := \deg(f)$ is sufficiently large and the monodromy group is not A_n or S_n. This proves conjectures of Guralnick–Shareshian.

1. INTRODUCTION

The classification of monodromy groups. Since the work of Riemann and Hurwitz, it has been known that many properties of a branched covering $f\colon X \to Y$ of complex curves are determined by the values of certain fundamental invariants of the covering. This has led to much effort in studying the possibilities for the values of these invariants. The most important invariant of f is its *monodromy group* $\mathrm{Mon}(f)$, namely the Galois group of the Galois closure of the function field extension $\mathbb{C}(X)/\mathbb{C}(Y)$, viewed as a group of permutations of $\mathrm{Hom}_{\mathbb{C}(Y)}(\mathbb{C}(X), \overline{\mathbb{C}(Y)})$. Equivalently, writing B for the branch locus of f and choosing a base point $P_0 \in Y(\mathbb{C}) \setminus B$, the group $\mathrm{Mon}(f)$ is isomorphic as a permutation group to the image of the fundamental group of $Y \setminus B$ under the monodromy representation $\pi_1(Y \setminus B, P_0) \to \mathrm{Sym}(f^{-1}(P_0))$. In many respects, all degree-n coverings with monodromy group A_n or S_n behave similarly to random degree-n coverings, so that it is of particular interest to describe the coverings with different monodromy groups. Our main result achieves this goal by describing all coverings $f\colon X \to Y$ whose monodromy group is neither $A_{\deg(f)}$ nor $S_{\deg(f)}$ nor a member of a finite list of groups which depends only on the genus of X. In particular, for any value of the genus of X we determine all exceptional coverings of sufficiently large degree. The main source of such exceptional coverings is *decomposable* coverings, namely the coverings $f\colon X \to Y$ which can be written as the composition $f = f_1 \circ f_2$ of coverings $f_2\colon X \to Z$ and $f_1\colon Z \to X$ which both have degree at least 2. We determine the exceptional *indecomposable* coverings in the sense that we determine

We thank Thao Do and Robert Guralnick for helpful discussions, Ted Chinburg for noting the relationship to root discriminants, and Arielle Leitner for her comments on this manuscript. The first author is grateful for the support of the Israel Science Foundation grant No. 577/15, and the NSF for support under a Mathematical Sciences Postdoctoral Fellowship. The second author thanks the NSF for support grant DMS-1162181. We also thank the United States-Israel Binational Science Foundation (BSF) for its support under Grant No. 2014173.

all occurring possibilities for their key invariants, namely the monodromy group and the *ramification type* of the covering. Here the ramification type of a covering $f\colon X \to Y$ with branch locus B is the multiset $\{E_f(P) : P \in B\}$, where $E_f(P)$ is the multiset of ramification indices (i.e., local multiplicities) of f at the points in $f^{-1}(P)$. As we will demonstrate, knowledge of the monodromy group and ramification type of a covering provides sufficient information to answer a wide assortment of questions about the covering.

In the case of indecomposable polynomials, the classificaiton of monodromy groups [15, 32] is used in: (1) the determination of pairs of rational polynomials f, g of coprime degrees such that the intersection $f(\mathbb{Q})\cap g(\mathbb{Q})$ is infinite by Avanzi–Zannier [3]; (2) in proving Ritt's theorem on the possible decompositions of $f \in \mathbb{C}[x]$ as a composition of indecomposable polynomials, see [35]; (3) in the characterization of varieties invariant by coordinatewise actions of univariate polynomials, by Medvedev–Scanlon [30]; and (4) determining for which prime degree polynomials $f(t, x) \in \mathbb{Z}[t, x]$, there are infinitely many integers $a \in \mathbb{Z}$ such that $f(a, x) \in \mathbb{Z}[X]$ is reducible, by Müller [33]; and in many other applications.

The first steps towards classifying monodromy groups and ramification of indecomposable coverings were for groups with trivial two point stabilizer, which include solvable primitive groups of prime degree. In the latter case, Chisini [10] and Ritt [41] determine the ramification of prime degree rational maps $f : \mathbb{P}^1 \to \mathbb{P}^1$. Moreover, Ritt shows that there are no coverings $f : X \to \mathbb{P}^1$ with genus $g > 0$ and sufficiently large degree in comparison to g, that is, for every $g > 0$, there exists a constant $N_g > 0$ such that every covering $f : X \to \mathbb{P}^1$ of prime degree and genus g has degree at most N_g. The results of Chisini and Ritt were then generalized by Zariski [46, 47] to coverings whose monodromy group has a trivial two point stabilizer.

Subsequently, there has been a major progress towards determining the ramification and monodromy groups of indecomposable coverings $f : X \to \mathbb{P}^1$ with sufficiently large degree in comparison to the genus g. Notably, if n is sufficiently large in comparison to g, it was shown that for every covering $f : X \to \mathbb{P}^1$ of degree n, genus g and simple monodromy group G, the group G is either cyclic or alternating. This is achieved by the combined efforts of Liebeck–Saxl [26], Liebeck–Shalev [27] and Frohardt–Magaard [17], following the work of Guralnick–Thompson [23], Aschbacher [1] and others including [42, 19, 37, 38, 21, 28, 20].

Together with the above work, this paper and its companion [36] give a complete list of the possible monodromy groups and ramification in sufficiently large degree.

Theorem 1.1. *Fix a nonnegative integer g. There exists a constant N_g such that every indecomposable covering $f : X \to \mathbb{P}^1$ of genus $g_X = g$ and degree $n \geq N_g$ satisfies one of the following:*

1. $\mathrm{Mon}(f) = A_n$ *or* S_n*;*
2. $\mathrm{Mon}(f) = A_\ell$ *or* S_ℓ *with* $n = \ell(\ell-1)/2$*, and* $g_X = 0$*. Moreover, the ramification type of f is given in Table 4.2.*
3. $A_\ell^2 \leq \mathrm{Mon}(f) \leq S_\ell^2 \rtimes C_2$*, where C_2 permutes the two copies of S_ℓ,* $n = \ell^2$ *and* $g_X \leq 1$*. Moreover, the ramification type of f is given in* [36, Table 3.1]*.*
4. $\mathrm{Mon}(f) \leq C_p^i \rtimes C_k$*,* $n = p^i$*, and* $g_X \leq g_{\tilde{X}} \leq 1$*, where p is prime, $i \leq 2$, and $k \leq 6$. Moreover, the ramification type of f is given in Table 9.1.*

Note that case (1) in Theorem 1.1 is the general case which includes all coverings whose ramification type does not appear in cases (2)–(4). In particular, this theorem proves [22, Conjecture 1.0.1] of the pioneering work by Guralnick–Shareshian, which first conjectures the possible monodromy groups of indecomposable coverings $f : X \to \mathbb{P}^1$ of sufficiently large degree compared to $g = g_X$. The ramification types appearing in case (4) already appear in Zariski's work and are completely determined in Proposition 9.5. Up to composition with linear fractionals, the rational maps corresponding to these ramification types are X^n, the Chebyshev polynomials, and composition factors of Lattés maps (the maps induced on x-coordinates by isogenies of elliptic curves). Moreover, the ramification types in cases (2) and (3), arise from ramification types similar to those in case (4).

We note that the theorem also holds (much more simply) for coverings of $Y \ncong \mathbb{P}^1$, that is, there is a constant N_g such that for every indecomposable covering $f : X \to Y$ of degree $n \geq N_g$ and $g_X \leq g$, one has $g_Y = 1$, and $\mathrm{Mon}(f) \cong A_n, S_n$, or C_n for prime n, with known ramification in the latter case, see [21, Proposition 2.3].

Theorem 1.1 is expected to play a key role in many applications. This includes (1) the determination of pairs of coverings $f : X \to Z$, $g : Y \to Z$ with f indecomposable of sufficiently large degree such that the fiber product of f and g is reducible, extending the results for polynomials by Davenport–Lewis–Schinzel, Feit, Fried, Cassou-Noguès–Couveignes [8]; (2) a description of the set of reducible values in Hilbert's irreducibility theorem: given an absolutely irreducible $f(t, x) \in \mathbb{Q}[t, x]$ with alternating or symmetric monodromy group whose ramification is not in an explicit list of exceptions, the set $\{a \in \mathbb{Q} \colon f(a, x) \in \mathbb{Q}[x] \text{ is reducible}\}$ is contained in the union of $\{b \in \mathbb{Q} \colon f(b, x) \in \mathbb{Q}[x] \text{ has a root}\}$ with a finite set, cf. [31]; and (3) the sufficiently large indecomposable case of the Carney–Hortsch–Zieve conjecture [9], namely, every indecomposable rational map viewed as a mapping $f : \mathbb{Q} \to \mathbb{Q}$ is at most 2-to-1 over all but finitely many values. These applications will be further developed in subsequent manuscripts.

The growth of the constant N_g with g in Theorem 1.1 can be estimated by combining the above results with further results communicated to us by Guralnick, see Remark 3.2. Namely, these show that there exists a positive constant a_0 such that Theorem 1.1 holds for coverings of genus g and degree at least $N_g := a_0 g^2$. These asymptotic results are expected to be applicable to the study of number fields K with bounded root discriminant [39], or more generally global fields, due to the close relationship between the root discriminant and the genus of a global field of positive characteristic [44, Section 3.5]. Namely, results over number fields analogues to the above, should describe the possibilities for the Galois group $G = \mathrm{Gal}(\Omega/\mathbb{Q})$, where Ω is the Galois closure of an extension $K/\mathbb{Q}$ with bounded root discriminant and no nontrivial intermediate extension. The hope here is to shed light on the possibilities for base fields K over which one can construct large or even infinite unramiified extensions.

Main result. One of the most difficult cases in the classification of monodromy groups, is the case where $t = 1$ and G is alternating or symmetric. This case is treated in the following theorem. Note that for a Galois covering $\tilde{f} : \tilde{X} \to \mathbb{P}^1$ with monodromy group $G \in \{A_\ell, S_\ell\}$, and a maximal subgroup $H \leq G$, the covering $\tilde{f}$ induces a natural indecomposable

covering $\tilde{X}/H \to \mathbb{P}^1$. Since every indecomposable covering $f : X \to \mathbb{P}^1$ with alternating or symmetric monodromy is isomorphic to a natural projection $\tilde{X}/H \to \mathbb{P}^1$ induced by some $\tilde{f}$ and H as above, Theorem 1.1 reduces, in this case, to finding all pairs $\tilde{f}, H$ such that $g_{\tilde{X}/H}$ is bounded.

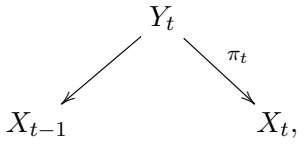
Theorem 1.2. *There exist constants $a, N > 0$ such that for every Galois covering $\tilde{f} : \tilde{X} \to \mathbb{P}^1$ with monodromy group $G = A_\ell$ or S_ℓ, with $\ell \geq N$, and every maximal subgroup H of G such that $H \neq A_\ell$, one of the following conditions holds:*

(1) *H is the group of elements of G fixing some prescribed point in $\{1, 2, \dots, \ell\}$.*
(2) *H is the group of elements of G preserving some prescribed two-element subset of $\{1, 2, \dots, \ell\}$, and the ramification type of the natural projection $\tilde{X}/H \to \mathbb{P}^1$ is given in Table 4.2. In all of these cases $g_{\tilde{X}/H} = 0$.*
(3) *$g_{\tilde{X}/H} > a\ell$.*

Note that case (1) corresponds to the generic case (1) in Theorem 1.1 and case (2) also corresponds to case (2) in Theorem 1.1. In particular, this theorem proves [22, Conjecture 1.0.4][1] of Guralnick–Shareshian for sufficiently large ℓ. In [22] (resp., [6]), Theorem 1.2 is proven for all coverings $\tilde{f}$ with at least five (resp., four) branch points[2], relying on the classification of finite simple groups or more specifically on the classification of 3-homogenous groups. However, as communicated to us by Shareshian, the method of [22] and [6] could not be carried over to the most difficult case where $\tilde{f}$ has three branch points. The fixed point ratio method which was used in the case of almost simple groups different from A_ℓ or S_ℓ, also does not apply in this case.

About the proof. The proof of Theorem 1.2 does not rely on the classification of finite simple groups. Instead we use a result which goes back to Jordan [24], whose proof is simplified by Babai–Seress [4]. Namely, there exists a constant $c_1 > 0$ such that every group $G \leq S_\ell$ which is t-transitive for all $t \leq c_1(\log \ell)^2/\log\log \ell$ must be $G = A_\ell$ or S_ℓ. Let X_t be the quotient $\tilde{X}/\overline{H}_t$ by a stabilizer $\overline{H}_t$ of a set of cardinality t. We combine Jordan's theorem with a character theoretic results of Guralnick–Shareshian [22] and Livingstone–Wagner [29], to reduce the problem to proving that the difference $g_{X_t} - g_{X_{t-1}}$ is large for every $2 \leq t \leq k$, where $k = \lceil c_1(\log \ell)^2/\log\log \ell \rceil$. This is in contrast to [22], where $g_{X_t} - g_{X_{t-1}}$ is shown to be large for $t = 2$ and 3, and the classification of 3-homogenous groups (and hence the classification of finite simple groups) is applied.

We note that there is no natural projection from X_t to X_{t-1} but there is a correspondence



[1] The ramification types in Conjecture 1.0.4 were conjectured using computer software.
[2] See Remark 4.2 for the required adjustments to the lists of ramification types in [22] and [6].

where $\pi_t : Y_t \to X_t$ is the natural projection from the quotient $Y_t := \tilde{X}/H_t$ by a t-point stabilizer H_t. The difficulty in showing that $g_{X_t} - g_{X_{t-1}}$ is large lies in bounding the difference $g_{Y_t} - t!g_{X_t}$ (or equivalently the Riemann–Hurwitz contribution R_{π_t} of π_t) which becomes an extremely complicated expression when described group theoretically. In Sections 5 and 6, we bound the main term of this expression in order to prove the claim when g_{Y_1} is sufficiently large. This method allows us to assume g_{Y_1} is bounded, but breaks down completely when g_{Y_1} is small.

To overcome the difficulty of estimating R_{π_t}, we use two main innovative tools. First, we use Castelnuovo's inequality which, as oppose to previous arguments, is of completely geometric origin. For simplicity, let us consider here the case $t = 2$. In this case, Castelnuovo's inequality allows us to bound g_{Y_2} in terms of g_{X_2} and g_{Y_1}, see Section 8, amounting to a linear bound $g_{Y_2} < c\ell - d$, for some constants $c, d > 0$.

The second innovative tool amounts to the claim that a linear bound on g_{Y_2} forces the ramification of the natural projection $h : Y_1 \to \mathbb{P}^1$ to be similar to that of a Galois extension, that is, all but a bounded number of preimages in $h^{-1}(P)$ have the same ramification index under h for each point P of $\mathbb{P}^1$. The latter argument appears in Section 7 and is based on an idea from Do–Zieve [12].

The final steps of the proof are determining which ramification data for h that are similar to those of Galois extensions make the difference $g_{X_2} - g_{X_1}$ small. The list of such ramification data is quite large, and we use an explicit version of the translation method, Lemma 9.1, in order to show that many of these ramification data do not correspond to an indecomposable covering h. This shows that the ramification of h appears in Table 4.1.

In Appendix A, we show that in fact all of the ramification data appearing in Table 4.1 and hence also those in Table 4.2 correspond to ramification types of rational maps $\mathbb{P}^1 \to \mathbb{P}^1$.

2. Preliminaries and notation

2.1. **Monodromy and ramification.** Fix an algebraically closed field $\mathbb{K}$ of characteristic 0. A nonconstant morphism $h : Y_1 \to Y$ of (smooth projective) curves over $\mathbb{K}$ is called *a covering*. A covering $\tilde{h} : \tilde{Y}_1 \to Y$ is called *the Galois closure of* h if it is a minimal Galois covering which factors as $\tilde{h} = h \circ h_0$, for some covering $h_0 : \tilde{Y}_1 \to Y_1$. The *monodromy group* $G = \mathrm{Mon}(h)$ of h is then defined to be the automorphism group $\mathrm{Aut}(\tilde{h})$. Note that G is a permutation group of degree $\deg h$ via its action on the set $S := H\backslash G$, where $H := \mathrm{Mon}(h_0)$. All group actions are right actions. Permutation multiplication is left to right, e.g. $(1,2)(1,3) = (1,2,3)$. All facts stated in this section are derived from a basic reference on function fields, e.g. [44], via the correspondence between function fields and curves [18, Section 7.1].

For every subgroup $H \leq G$, the covering $\tilde{h}$ induces a covering $\tilde{Y}_1/H \to Y$ which we call the natural projection. If $\tilde{h} = h \circ h_0$ as above then h_0 is Galois, and h is equivalent to the natural projection $\tilde{Y}_1/H \to Y$ for $H = \mathrm{Aut}(h_0)$, that is, there is an isomorphism $\mu : \tilde{Y}_1/H \to Y_1$ such that $h \circ \mu$ is the natural projection $\tilde{Y}_1/H \to Y$.

The subgroup I consisting of all elements $\sigma \in G$ such that $\tilde{Q}^\sigma = \tilde{Q}$ is called *the decomposition subgroup* of $\tilde{Q}$. It coincides with the *inertia subgroup* of $\tilde{Q}$ since $\mathbb{K}$ is algebraically closed. Since G acts transitively on $\tilde{h}^{-1}(P)$ and the stabilizer of $\tilde{Q}$ is I, the action of G on $\tilde{h}^{-1}(P)$ is equivalent to its action on $I\backslash G$, and in particular all decomposition subgroups of points in $\tilde{h}^{-1}(P)$ are conjugate (as point stabilizers). Since $\mathbb{K}$ is of characteristic 0, $\tilde{h}$ is tamely ramified, and hence all inertia subgroups are cyclic. A generator of an inertia subgroup of a place in $\tilde{h}^{-1}(P)$ is called a *branch cycle* over P.

The following is a well known description of the points in $h^{-1}(P)$ using $\mathrm{Mon}(h)$. Let $I\backslash G/H$ denote the double coset space $IxH, x \in G$, and let $e_h(Q)$ denote the *ramification index* of a point Q of Y_1 under h.

Lemma 2.1. *Let $h : Y_1 \to Y$ be a covering and $\tilde{h} : \tilde{Y}_1 \to Y$ a Galois covering that factors as $\tilde{h} = h \circ h_0$. Let $G := \mathrm{Mon}(h)$ and $H := \mathrm{Mon}(h_0)$. Fix points P of Y and $\tilde{Q} \in \tilde{h}^{-1}(P)$, and let I be the decomposition subgroup of $\tilde{Q}$. Then there is a natural bijection $\psi_{H,\tilde{Q}} : h^{-1}(P) \to I\backslash G/H$ such that $e_h(Q) = |\psi_{H,\tilde{Q}}(Q)|/|H|$ for all $Q \in h^{-1}(P)$.*

Proof. As noted earlier there is an isomorphism $\phi_{\tilde{Q}} : \tilde{h}^{-1}(P) \to I\backslash G$ of G-sets such that $\phi_{\tilde{Q}}(\tilde{Q}^\sigma) = I\sigma$ for all $\sigma \in G$. Let $Q \in h^{-1}(P)$ and choose $\sigma \in G$ such that $\tilde{Q}^\sigma \in h_0^{-1}(Q)$. Since $h_0^{-1}(Q)$ coincides with the orbit of H on $\tilde{Q}^\sigma$, one has $\tilde{Q}^\tau \in h_0^{-1}(Q)$ if and only if $I\sigma H = I\tau H$. Thus $\phi(h_0^{-1}(Q))$ is the orbit of H on $I\sigma$, that is, the double coset $I\sigma H$. Thus $\psi_{H,\tilde{Q}}(Q) := \phi_{\tilde{Q}}(\tilde{Q}^\sigma) = I\sigma H$ is well defined as it is independent of the choice of σ, and gives a one to one correspondence. It also follows that the cardinality of the orbit $h_0^{-1}(Q)$ equals the cardinality of the orbit of H on $I\backslash G$ which is $|I\sigma H|/|I|$. Since $e_h(Q) = e_{\tilde{h}}(\tilde{Q}^\sigma)/e_{h_0}(\tilde{Q}^\sigma)$, since $e_{\tilde{h}}(\tilde{Q}^\sigma) = |I|$ as $\tilde{h}$ is Galois, and since $e_{h_0}(\tilde{Q}^\sigma) = |H|/|h_0^{-1}(Q)|$ as h_0 is Galois, we have

$$e_h(Q) = \frac{e_{\tilde{h}}(\tilde{Q}^\sigma)}{e_{h_0}(\tilde{Q}^\sigma)} = \frac{|I|}{|H|/|h_0^{-1}(Q)|} = \frac{|I\sigma H|}{|H|}. \qquad \square$$

Moreover, note that if $h = h_2 \circ h_1$ so that $\tilde{h} = h_2 \circ h_1 \circ h_0$, and $H \le H_2 \le G$ is a point stabilizer of h_2 so that H_2 is the monodromy group of $h_1 \circ h_0$, then the bijection $\psi_{H,\tilde{Q}}$ induces the bijection $\psi_{H_2,\tilde{Q}}$. Indeed by definition $\psi_{H_2,\tilde{Q}}(h_1(Q)) = I\sigma H_2$ whenever $\psi_{H,\tilde{Q}}(Q) = I\sigma H$, for all $Q \in h^{-1}(P)$.

The *ramification type* of P under h is the multiset $E_h(P) := [e_h(Q_1), \dots, e_h(Q_r)]$, where $Q_1, \dots, Q_r$ are the preimages in $h^{-1}(P)$. Denote by $\mathrm{Orb}_S(U)$ the set of orbits on S of the group generated by a subset $U \subseteq G$. Then Lemma 2.1 implies that $E_h(P)$ equals the multiset of lengths of orbits in $\mathrm{Orb}_S(x)$, where x is a branch cycle over P and $S = H\backslash G$. The *ramification type* of h is then defined to be the multiset $\{E_h(P) \neq [1^\ell] \colon P \in Y(\mathbb{K})\}$.

The Riemann–Hurwitz formula $2(g_{Y_1} - \ell g_Y + \ell - 1) = \sum_{P \in Y(\mathbb{K})} R_h(P)$ describes the *genus* g_{Y_1} in terms of g_Y and the contributions $R_h(P)$, where

$$R_h(P) := \sum_{r \in E_h(P)} (r-1) = \ell - |\mathrm{Orb}_S(x)|.$$

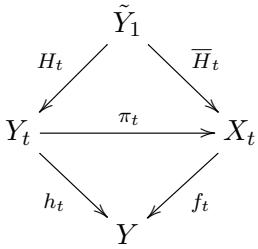
For a set T of points in Y we denote by $R_h(T)$ the sum $\sum_{P\in T} R_h(P)$. We note that if $\hat{h} = h \circ \pi$ for a covering π of degree m, then $R_{\hat{h}}(P)$ satisfies the chain rule:

$$\begin{aligned} R_{\hat{h}}(P) &= \sum_{\hat{Q}\in\hat{h}^{-1}(P)} (e_{\hat{h}}(\hat{Q}) - 1) = \sum_{\hat{Q}\in\hat{h}^{-1}(P)} \Big(e_\pi(\hat{Q}) - 1 + e_\pi(\hat{Q}) \left(e_h(\pi(\hat{Q})) - 1 \right) \Big) \\ &= \sum_{Q\in h^{-1}(P)} \left(R_\pi(Q) \; + \; (e_h(Q) - 1) \cdot \sum_{\hat{Q}\in\pi^{-1}(Q)} e_\pi(\hat{Q}) \right) \\ &= R_\pi(h^{-1}(P)) + mR_h(P). \end{aligned} \tag{2.1}$$

A *ramification data* of degree ℓ is a finite multiset $\{A_1, \dots, A_r\}$ of partitions of ℓ, so that $\ell = \sum_{\alpha\in A_i} \alpha$ for each i. A ramification data $A_1, \dots, A_r$ is said to be of *genus* g if $2(g+\ell-1) = \sum_{i=1}^r (\ell - |A_i|)$. It is not known which ramification data arise as ramification types of coverings. We write $E_h(P) = [e_1, \dots, e_r, e^*]$ to denote that $E_h(P)$ is the union of the multiset $[e_1, \dots, e_r]$ with a (possibly empty) multiset consisting of copies of e.

2.2. **Setup.** We use the following basic setup throughout the paper. Let $h : Y_1 \to Y$ be a covering of degree ℓ with monodromy group $G = \mathrm{Mon}(h)$ acting on a set $S = H\backslash G$ such that $G \cong A_\ell$ or S_ℓ as permutation groups. Let $\tilde{h}_1 : \tilde{Y}_1 \to Y$ be the Galois closure of h.

Enumerating the elements in S by $\{1, \dots, \ell\}$, we let H_t be the pointwise stabilizer of $1, \dots, t$, and $\overline{H}_t$ the setwise stabilizer of $\{1, \dots, t\}$, so that the action of G on $\overline{H}_t\backslash G$ (resp., $H_t\backslash G$) is equivalent to its action on the set $\overline{S}^{(t)}$ (resp., $S^{(t)}$) of t-element subsets (resp., ordered t-tuples of pairwise distinct elements) in S for $t \le \ell$. Henceforth we write t-set to mean t-element subset. Let $\pi_t : Y_t \to X_t$, $h_t : Y_t \to Y$, $f_t : X_t \to X_0$ be the natural projections from $Y_t := \tilde{Y}_1/H_t$, and $X_t := \tilde{Y}_1/\overline{H}_t$, so that $\mathrm{Mon}(f_t)$ (resp., $\mathrm{Mon}(h_t)$) is G with its action on $\overline{S}^{(t)}$ (resp., $S^{(t)}$) for $t \le \ell$. The following diagram is commuative:



Note that the original covering h is equivalent to the covering h_1.

3. Reduction to genera of set stabilizers

In this section we derive Theorem 1.2 from the following theorem, and then prove Theorem 1.1. This section follows [22]. We use Setup 2.2: for a degree ℓ covering $h : Y_1 \to Y$ with monodromy group G acting on a set S, let X_t be the quotient by the stabilizer $\overline{H}_t \le G$ of a subset of S of cardinality t, for every integer $0 \le t \le \ell/2$.

Theorem 3.1. *There exist constants $c, d > 0$ such that for every covering $h : Y_1 \to Y$ of degree ℓ and monodromy group $G \in \{A_\ell, S_\ell\}$, one has*

$$g_{X_t} - g_{X_{t-1}} > (c\ell - dt^{15}) \frac{\binom{\ell}{t}}{\binom{\ell}{2}}$$

for all integers $2 \le t \le \ell/2$ if the ramification type of h does not appear in Table 4.1, and for all integers $3 \le t \le \ell/2$ otherwise.

Note that the proof also gives $g_{Y_1} = 0$ if the ramification of h appears in Table 4.1.

Proof of Theorem 1.2 assuming Theorem 3.1. Let log denote the natural logarithm. Let $c_1 := 8 \log 2$ be the constant given in [4]. Thus by setting $M_\ell := \lceil c_1 (\log \ell)^2 / \log\log \ell \rceil$, every M_ℓ-transitive subgroup of S_ℓ contains A_ℓ.

Let c and d be the constants from Theorem 3.1. Put $a := c/2$ and note that as M_ℓ is subpolynomial in ℓ, there exists a constant $N_{c,d}$ such that $a\ell > dt^{15}$ for every $2 \le t \le M_\ell$ and $\ell \ge N_{c,d}$. Put $N := \max\{183, N_{c,d}\}$.

Let $f : X \to Y$ be an indecomposable covering with monodromy group $G = A_\ell$ or S_ℓ, with $\ell \ge N$, and $g_Y = 0$. Let $H \le G$ be the monodromy group of the natural projection $\tilde{X} \to X$ from the Galois closure $\tilde{X}$ of f. Let Y_1 be the quotient of $\tilde{X}$ by the point stabilizer $H_1 \le G$ in the natural action on $\{1, \dots, \ell\}$, and $h : Y_1 \to Y$ the natural projection which has monodromy group G, equipped with an action on the set $S = H_1 \backslash G$ of cardinality ℓ. As a subgroup of S_ℓ, the group H has a natural action on the set $\overline{S}^{(t)}$ of all subsets of S of cardinality t, for $t = 0, \dots, \ell$. Put $|\mathrm{Orb}_{\overline{S}^{(0)}}(H)| = 1$.

As $\ell \ge 5$, [22, Lemma 2.0.13] gives

$$g_X \ge \sum_{1 \le t \le \lfloor \ell/2 \rfloor} \Big(|\mathrm{Orb}_{\overline{S}^{(t)}}(H)| - |\mathrm{Orb}_{\overline{S}^{(t-1)}}(H)| \Big) \cdot \big(g_{X_t} - g_{X_{t-1}} \big). \tag{3.1}$$

Moreover, $|\mathrm{Orb}_{\overline{S}^{(t)}}(H)| \ge |\mathrm{Orb}_{\overline{S}^{(t-1)}}(H)|$ and $g_{X_t} \ge g_{X_{t-1}}$ for $1 \le t \le \lfloor \ell/2 \rfloor$, by the Livingstone–Wagner theorem [29, Theorem 1], and Guralnick–Shareshian [22, Lemma 2.0.12][3], respectively, where the latter uses the assumption $g_Y = 0$.

Combining this with the assumptions $|\mathrm{Orb}_{\overline{S}^{(0)}}(H)| = 1$, $\ell \ge 5$, and that H does not contain A_ℓ, (3.1) gives

$$g_X \ge (|\mathrm{Orb}_{\overline{S}^{(t)}}(H)| - |\mathrm{Orb}_{\overline{S}^{(t-1)}}(H)|)(g_{X_t} - g_{X_{t-1}}) \tag{3.2}$$

for $1 \le t \le \lfloor \ell/2 \rfloor$. The proof splits into cases according to types of actions of H on S.
Case 1: H acts intransitively on S. Then H must be the stabilizer of a t-set for some $2 \le t \le \ell/2$: for, since H permutes each of its orbits, H is contained in the stabilizer (in G) of each orbit. Since H is intransitive, there are at least two such orbits, so at least one of them has size at most $\ell/2$, and the stabilizer of any orbit is a proper subgroup of G. Since f is indecomposable, H is maximal, and hence equals the stabilizer of each of its orbits, and in particular equals the stabilizer of an orbit which has size $t \le \ell/2$.

[3]The inequality $g_{X_k} \ge g_{X_{k-1}}$ holds more generally for every k-transitive subgroup $G \le S_\ell$, as an immediate consequence of [34, Theorem 4.34] and [33, Lemma 4.15].

If $t = 2, 3$, the theorem follows from Theorem 3.1 as then either

$$g_{X_t} > (c\ell - dt^{15}) > (c\ell - a\ell) = a\ell, \tag{3.3}$$

or $t = 2$ and the ramification of h appears in Table 4.1. If $4 \le t \le \lfloor \ell/2 \rfloor$, then as above $g_X = g_{X_t} \ge g_{X_3}$, and the claim follows from (3.3) with $t = 3$. As noted in Section 4, $g_{\tilde{X}/H} = 0$ if $t = 2$ and the ramification of h appears in Table 4.1.

Case 2: H acts transitively on S. By Theorem 3.1, as $a\ell > dt^{15}$ we have

$$g_{X_t} - g_{X_{t-1}} \ge (c\ell - dt^{15}) \frac{\binom{\ell}{t}}{\binom{\ell}{2}} > (c\ell - a\ell) \frac{\binom{\ell}{t}}{\binom{\ell}{2}} \ge a\ell, \tag{3.4}$$

for $\ell \ge N_{c,d}$, and $2 < t \le M_\ell$, and also for $t = 2$ if the ramification of h does not appear in Table 4.1. Thus the claim follows from (3.2) if $|\mathrm{Orb}_{\overline{S}^{(t)}}(H)| > |\mathrm{Orb}_{\overline{S}^{(t-1)}}(H)|$ for some $t \in \{2, 3, \dots, M_\ell\}$. Since in addition $|\mathrm{Orb}_{\overline{S}^{(1)}}(H)| = 1$ as H is transitive, henceforth assume

$$\begin{array}{l} |\mathrm{Orb}_{\overline{S}^{(t)}}(H)| = |\mathrm{Orb}_{\overline{S}^{(2)}}(H)| \text{ for all } 2 \le t \le M_\ell, \text{ and either} \\ |\mathrm{Orb}_{\overline{S}^{(2)}}(H)| = 1 \text{ or the ramification type of } h \text{ appears in Table 4.1.} \end{array} \tag{3.5}$$

Case 2a: H is imprimitive. Then H must be the stabilizer in G of a partition into t parts of size ℓ/t, where $1 < t < \ell$: for, H preserves some such partition, and the stabilizer of such a partition is a proper subgroup of G, so since H is a maximal subgroup it must equal this stabilizer.

Note that $|\mathrm{Orb}_{\overline{S}^{(2)}}(H)| = 2$: for, H acts doubly transitively on the set of parts of the partition, and also acts doubly transitively on the elements in a given part, so the two orbits are [two points in the same part] or [two points in different parts].

Also $|\mathrm{Orb}_{\overline{S}^{(3)}}(H)| = 3$ if $2 < t < \ell/2$: for, H acts as S_t on the set of parts, and also acts as $(S_{\ell/t})^{t-1}$ on any prescribed $(t-1)$-parts. So the orbits are [three points in different parts], [two in one part and one in another], [three points in one part].

Similarly, if $t = 2$ or $\ell/2$ we have $|\mathrm{Orb}_{\overline{S}^{(4)}}(H)| = 3$: for, if $t = 2$ the orbits are [four points in one part], [three points in one part and one in the other], [two points in both parts], and if $t = \ell/2$ the orbits are [four points in different parts], [two points in one part, and two in other two parts], [two points in two parts].

We get that $|\mathrm{Orb}_{\overline{S}^{(3)}}(H)| > |\mathrm{Orb}_{\overline{S}^{(2)}}(H)|$ if $2 < t < \ell/2$ and $|\mathrm{Orb}_{\overline{S}^{(4)}}(H)| > |\mathrm{Orb}_{\overline{S}^{(2)}}(H)|$ if $t = 2$ or $\ell/2$, contradicting (3.5).

Case 2b: H is primitive. In this case the condition $|\mathrm{Orb}_{\overline{S}^{(3)}}(H)| = |\mathrm{Orb}_{\overline{S}^{(2)}}(H)|$ implies that $|\mathrm{Orb}_{\overline{S}^{(2)}}(H)| = 1$, by [7, Proposition on p.165]. Hence $|\mathrm{Orb}_{\overline{S}^{(t)}}(H)| = 1$ by (3.5) for all $1 \le t \le M_\ell$. By [29, Theorem 2], this condition implies that H is M_ℓ-transitive. By [4] every M_ℓ-transitive group H is A_ℓ or S_ℓ, contradicting the assumption $H \ne A_\ell, S_\ell$. □

Proof of Theorem 1.1. Let G denote the monodromy group of f and $n = \deg f$. Since f is indecomposable, G is primitive. The Aschbacher–O'Nan–Scott theorem [23] divides primitive groups G according to the interaction of their 1-point stabilizer $H \le G$, and a minimal normal subgroup Q of G. Let L be a minimal normal subgroup of Q, and $L_1 = L, L_2, ..., L_t$ the conjugates of L in G. Then one of the following holds:

(A) $|L|$ is prime;
(B) G has more than one minimal normal subgroup;
(C) Q is the unique minimal normal subgroup of G, and $Q = L_1 \times L_2 \times \cdots \times L_t$, where L is simple nonabelian and either
(C1) $H \cap Q = 1$; or
(C2) $H \cap Q \neq 1$ but $H \cap L = 1$; or
(C3) $H \cap Q = H_1 \times \cdots \times H_t$, where $H_i = H \cap L_i \neq 1$ for $1 \leq i \leq t$.

In case (A), Neubauer's proof of [37, Theorems 1.4-1.6], which refines Guralnick–Thompson [23, Theorem A], shows that for sufficiently large n, either $g_X > n/1024$ or $g_X = 0$ and G is of derived length at most 2. In the latter cases, [23, Proposition 3.8] combined with the formula for the genus of a Galois closure (Remark 9.3) show that in these case the genus of the Galois closure $\tilde{f} : \tilde{Y}_1 \to Y_1$ is $g_{\tilde{Y}_1} \leq 1$. Proposition 9.5 gives all possible ramification types for indecomposable h and its corresponding monodromy groups G, in case $g_{\tilde{Y}_1} \leq 1$. In Case (B), Shih [42] shows that $g_X > 0$, and Guralnick noted [19, Pg. 353] that the same methods yield $g_X > cn - d$ for some constants $c, d > 0$. In case (C1) the result follows directly from the proof of Guralnick–Thompson [23, Theorem C1], which gives $g_X > n/2000$. The case (C2) is covered by Aschbacher [1] which proves $g_X > n/336$ when n is larger than a constant.

Henceforth assume G is as in case (C3). For $t > 8$, the theorem follows from Guralnick–Neubauer [21, Corollary 8.7], which shows that $g_X > (1/1250)n^{1-1/t}$. Consider the case $t = 1$, so that $L \leq G \leq \mathrm{Aut}(L)$ for a finite simple group L, and first assume L is non-alternating. By assuming n is sufficiently large, we may assume L is of Lie type. Let q be the cardinality of the field over which L is defined. Letting $\mathrm{fpr}(G)$ denote the maximal ratio $|\{\text{fixed points of } x\}|/n$ over all $x \in G \setminus \{1\}$, Guralnick [19, Theorem 1] shows that for any $0 < \varepsilon < 1/85$, there exists a constant $c_\varepsilon > 0$ such that if $\mathrm{fpr}(G) < \varepsilon$ then $g_X > c_\varepsilon n$. Assuming $q \geq 23$, Liebeck–Saxl [26, Theorem 1] show that $\mathrm{fpr}(G) \leq 4/(3q)$ if $L \neq \mathrm{PSL}_2(q)$, and that $\mathrm{fpr}(G) < (\sqrt{q} + 1 + (2/\sqrt{q}))/(q+1)$ if $L = \mathrm{PSL}_2(q)$. Pick $0 < \varepsilon < 1/85$ such that $4/(3q) < \varepsilon$ for $q > 113$ and $(\sqrt{q} + 1 + (2/\sqrt{q}))/(q+1) < \varepsilon$ for $q > (86)^2$, so that $\mathrm{fpr}(G) < \varepsilon$ for such q. If the action of G is not a subspace action, then Liebeck–Shalev [27, Theorem 1.1], extending [28], show that $\mathrm{fpr}(G) < \varepsilon$ for sufficiently large n. If the action of G is a subspace action, then Frohardt–Magaard [17, Proposition 5.1] show that there exists a constant N_q, depending only on q, such that $g_X > n/2000$ for $n \geq N_q$. Thus, letting $\tilde{c}_\varepsilon := \min\{c_\varepsilon, 1/2000\}$, one has $g_X > \tilde{c}_\varepsilon n$ for sufficiently large n, by the combination of [19] and [26] if $q > 113$ for $L \neq \mathrm{PSL}_2(q)$ and $q > (86)^2$ for $L = \mathrm{PSL}_2(q)$, and by the combination of [27] and [17] otherwise.

Finally, the proof in case (C3) is completed for $t = 1$ by Theorem 1.2 which covers the cases where L is alternating, and for $t > 1$ (and in particular for $2 < t \leq 8$) by [36, Theorem 1.1] which gives positive constants c_t, d_t, depending only on t, such that either $t = 2$ and the ramification of f appears in [36, Table 3], or $g_X > c_t n^{1-1/t} - d_t$. □

The classification of finite simple groups is used in cases (B), (C1), (C2), and the case (C3) with $t = 1$. It seems plausible that a classification free proof will be given in all cases but (C3) with $t = 1$, that is, for all but almost simple monodromy groups.

Remark 3.2. We note that in Theorem 1.1, it is expected that one can choose $N_g = a_0(g^2+1)$ for some absolute constant $a_0 > 0$. More specifically, there exist positive constants a_1, b_1 for which the following holds.

For every indecomposable coverings of genus g, degree n, monodromy group G, either one of the cases (1)-(4) in Theorem 1.1 holds or $n < N_g$, where $N_g = a_1(g^2+1)$ if G is alternating or symmetric, or of type (C3) with $t \geq 2$, and $N_g = b_1(g+1)$ otherwise. Thus, one can choose $a_0 := \max\{a_1, b_1\}$.

If G is not alternating, symmetric, or of type (C3) with $t \geq 2$, this follows directly from the proof of Theorem 1.1. We sketch the proof in the remaining cases. First assume that G is of type (C3) with $t \geq 2$. By [36] and [21], there exist constants $a_2 > 0$ and $0 < a_3 < 1$ such that for every indecomposable genus g covering of degree $n > a_2$ with such monodromy group, either $g > a_3 n^{1-1/t}$ or case (3) of Theorem 1.1 holds. Here, a_3 is picked as the minimum over $1/1250$, and the constants $c_k/2$, $2 \leq k \leq 8$ from [36, Theorem 1.1]. Equivalently, either $n < \max\{a_2, (g/a_3)^{t/(t-1)}\}$ or case (3) of Theorem 1.1 holds. As $t \geq 2$, the assertion holds in this case for $N_g \geq a_4(g^2+1)$ where $a_4 := \max\{a_2, 1/a_3\}$.

Now assume that $G = A_\ell$ or S_ℓ. Frohardt, Guralnick, Hoffman and Magaard [16] have proved that there exists a constant $a_5 > 0$ such that $n < a_5 g$ for every indecomposable covering with monodromy group G and point stabilizer $H \leq G$ which acts transitively in the usual action of G on $\{1, \ldots, \ell\}$. Henceforth assume H is nontransitive. As H is maximal in G and is nontransitive, H is the stabilizer of a t-set in G for $t \geq 1$. As Theorem 1.1 holds trivially in the case $t = 1$, we assume $t \geq 2$. Let $\tilde{X}$ denote the Galois closure of f, and X_k its quotient by the stabilizer of a k-subset. In this case, apply the same argument as in the proof of [22, Theorem 1.3.1], and replace the use of [22, Theorem 4.0.30] which asserts that $g_{X_2} - g_{X_1}$ is large under the assumption that f has at least 5 branch points, with Theorem 3.1 for $t = 2$ which does not make this assumption, to obtain the following. There exists positive constants a_6, a_7 such that for every indecomposable covering with alternating or symmetric monodromy, and degree $n > a_7$, either $g < a_6 n/\ell$ or the ramification type of the natural projection $h : \tilde{X}/(G \cap S_{\ell-1}) \to \mathbb{P}^1$ appears in Table 4.1.

Consider the case where the ramification of h appears in Table 4.1, so that the number B of branch points of h is at most 5. Note that since in this case Theorem 3.1 holds trivially for $t = 2$, we can assume $t \geq 3$. Since $g_{X_3} > (c\ell - 3^{15}d)\binom{\ell}{3}/\binom{\ell}{2}$ by Theorem 3.1 for $t = 3$, [22, Lemma 2.0.6 and Lemma 9.0.6] give

$$\frac{g}{n} > \frac{c\ell - 3^{15}d}{\binom{\ell}{2}} - \frac{6}{\ell(\ell-1)(\ell-2)} - \frac{3B}{2(\ell-1)(\ell-3)}.$$

As $B \leq 5$, this implies the existence of positive constants a_8, a_9 such that $g > a_8 n/\ell$ for every indecomposable covering with such monodromy with $t \geq 3$, and degree $n > a_9$, for which the ramification type of h appears in Table 4.1.

Picking $a_{10} := \min\{a_6, a_8\}$ and $a_{11} := \max\{a_7, a_9\}$, it follows that when $n > a_{11}$, either $g > a_{10} n/\ell$ or case (2) of Theorem 1.1 holds. It is well known that $n = \binom{\ell}{t} \geq (\ell/t)^t$ or

equivalently $\ell \le tn^{1/t}$. Thus the inequality $g > a_{10}n/\ell$ holds when $g > a_{10}n^{1-1/t}/t$ or equivalently when $n < (tg/a_{10})^{t/(t-1)}$. As $t \ge 2$, the assertion follows for coverings with alternating or symmetric monodromy when $N_g \ge a_{12}(g^2+1)$ where $a_{12} := \max\{2/a_{10}, 1/a_5, a_{11}\}$. Thus the entire assertion holds with $a_1 := \max\{a_4, a_{12}\}$.

4. The ramification types in Theorems 1.1, 1.2, and 3.1

In this section we complete the statements of Theorems 1.1, 1.2, and 3.1 by presenting the ramification types excluded in the statement of Theorem 3.1, as well as the ramification types from case (2) of Theorems 1.1 and 1.2. Specifically, in Table 4.1 we present the ramification types of some degree-ℓ coverings $h : \mathbb{P}^1 \to \mathbb{P}^1$ having monodromy group A_ℓ or S_ℓ, and in Table 4.2 we present the ramification types of the degree-$\ell(\ell-1)/2$ coverings $f : X \to \mathbb{P}^1$ obtained from the coverings in Table 4.1 by means of the action of A_ℓ or S_ℓ on the set of two-element subsets of $\{1, 2, \dots, \ell\}$. Crucially, the ramification types in Table 4.1 have the property that the induced degree-$\ell(\ell-1)/2$ covering $f : X \to \mathbb{P}^1$ has X being of genus zero. We emphasize that each ramification type listed in Tables 4.1 and 4.2 actually occurs for some indecomposable rational function with monodromy group A_ℓ or S_ℓ. We will prove this in Proposition A.1 for the types in Table 4.1, and in this section we will indicate how this fact implies the corresponding fact for each ramification type in Table 4.2.

The ramification types for the coverings $f : X_2 \to \mathbb{P}^1$ in Table 4.2 are obtained from those of $h : Y_1 \to \mathbb{P}^1$ in Table 4.1 using the following process. As in Setup 2.2, $h : Y_1 \to \mathbb{P}^1$ is a degree ℓ covering with monodromy group $G \in \{A_\ell, S_\ell\}$ acting on an ℓ-element set S, and with Galois closure $\tilde{X} \to \mathbb{P}^1$, and $f : X_2 \to \mathbb{P}^1$ is the natural projection from the quotient $X_2 := \tilde{X}/\overline{H}_2$ of $\tilde{X}$ by the stabilizer $\overline{H}_2$ of a 2-set in S, so that $\mathrm{Mon}(f) = G$ in its action on the set $\overline{S}^{(2)}$ of 2-sets in S.

Let P be a point of $\mathbb{P}^1$ and $x \in G$ a branch cycle for h over P. As in Section 2.2, the ramification type $E_h(P)$ (resp., $E_f(P)$) equals the multiset of orbit cardinalities $\{|o| : o \in \mathrm{Orb}_S(x)\}$ (resp., $\{|o| : o \in \mathrm{Orb}_{\overline{S}^{(2)}}(x)\}$). The orbit cardinalities of x on $\overline{S}^{(2)}$ are deduced from those on S by means of the following lemma:

Lemma 4.1. *Let $R_1, R_2 \subseteq S$ be orbits of $x \in S_\ell$ having cardinalities r_1, r_2, respectively. Let T be the set of unordered pairs $\{a, b\}$ of distinct elements a, b with $a \in R_1$ and $b \in R_2$. Then the orbits of the action of x on T consist of*

1. *(r_1, r_2) orbits of cardinality $\mathrm{lcm}(r_1, r_2)$ if $R_1 \ne R_2$;*
2. *$(r_1 - 1)/2$ orbits of cardinality r_1 if $R_1 = R_2$ and r_1 is odd;*
3. *one orbit of cardinality $r_1/2$, and $r_1/2 - 1$ orbits of cardinality r_1 if $R_1 = R_2$ and r_1 is even.*

Proof. Let $a \in R_1$ and $b \in R_2$. The orbit of every element $\{c, d\} \in T$ under the action of x is of cardinality $\mathrm{lcm}(r_1, r_2)$ unless $R_1 = R_2$, r_1 is even, and a is the image of b under the action of $x^{r_1/2}$. Since there are $r_1 r_2$ (resp., $r_1(r_1-1)/2$) elements in T if $R_1 \ne R_2$ (resp., $R_1 = R_2$), there are $r_1 r_2/\mathrm{lcm}(r_1, r_2) = (r_1, r_2)$ (resp., $(r_1-1)/2$) such orbits if $R_1 \ne R_2$

TABLE 4.1. Ramification types for some coverings $h : \mathbb{P}^1 \to \mathbb{P}^1$ of degree $\ell \geq 13$ and monodromy group A_ℓ or S_ℓ. Here $a \in \{1, \dots, \ell - 1\}$ is odd, $(a, \ell) = 1$, and in each type ℓ satisfies the necessary congruence conditions to make all exponents integral. The third column refers to the corresponding ramification type in [22].

$I1.1$	$[\ell], [a, \ell - a], \left[1^{\ell-2}, 2\right]$	
$I2.1$	$[\ell], [1^3, 2^{(\ell-3)/2}], [1, 2^{(\ell-1)/2}], \left[1^{\ell-2}, 2\right]$	[22, Proposition 3.0.24(e)]
$I2.2$	$[\ell], [1^2, 2^{(\ell-2)/2}]$ twice, $\left[1^{\ell-2}, 2\right]$	[22, Proposition 3.0.24(c)]
$I2.3$	$[\ell], \left[1^3, 2^{(\ell-3)/2}\right], [2^{(\ell-3)/2}, 3]$	[22, Proposition 3.0.25(b)]
$I2.4$	$[\ell], \left[1^2, 2^{(\ell-2)/2}\right], [1, 2^{(\ell-4)/2}, 3]$	[22, Proposition 3.0.25(d)]
$I2.5$	$[\ell], \left[1, 2^{(\ell-1)/2}\right], [1^2, 2^{(\ell-5)/2}, 3]$	[22, Proposition 3.0.25(f)]
$I2.6$	$[\ell], \left[1^3, 2^{(\ell-3)/2}\right], [1, 2^{(\ell-5)/2}, 4]$	[22, Proposition 3.0.25(a)]
$I2.7$	$[\ell], \left[1^2, 2^{(\ell-2)/2}\right], [1^2, 2^{(\ell-6)/2}, 4]$	[22, Proposition 3.0.25(c)]
$I2.8$	$[\ell], \left[1, 2^{(\ell-1)/2}\right], [1^3, 2^{(\ell-7)/2}, 4]$	[22, Proposition 3.0.25(e)]
$I2.9$	$[a, \ell - a], [1^2, 2^{(\ell-2)/2}], [2^{\ell/2}], \left[1^{\ell-2}, 2\right]$	[22, Proposition 3.0.24(d)]
$I2.10$	$[a, \ell - a], [1, 2^{(\ell-1)/2}]$ twice, $\left[1^{\ell-2}, 2\right]$	[22, Proposition 3.0.24(f)]
$I2.11$	$[a, \ell - a], \left[2^{\ell/2}\right], [1^2, 2^{(\ell-6)/2}, 4]$	[22, Proposition 3.0.27(c)]
$I2.12$	$[a, \ell - a], \left[1, 2^{(\ell-1)/2}\right], [1, 2^{(\ell-5)/2}, 4]$	[22, Proposition 3.0.27(a)]
$I2.13$	$[a, \ell - a], \left[1^2, 2^{(\ell-2)/2}\right], [2^{(\ell-4)/2}, 4]$	[22, Proposition 3.0.28(c)]
$I2.14$	$[a, \ell - a], \left[1, 2^{(\ell-1)/2}\right], [2^{(\ell-3)/2}, 3]$	[22, Proposition 3.0.27(b)]
$I2.15$	$[a, \ell - a], \left[2^{\ell/2}\right], [1, 2^{(\ell-4)/2}, 3]$	[22, Proposition 3.0.27(d)]
$F1.1$	$\left[1^{\ell-2}, 2\right], [2^{\ell/2}], [1^2, 2^{(\ell-2)/2}]$ thrice	[22, Proposition 3.0.24(a)]
$F1.2$	$\left[1^{\ell-2}, 2\right], [1^3, 2^{(\ell-3)/2}], [1, 2^{(\ell-1)/2}]$ thrice	[22, Proposition 3.0.24(b)]
$F1.3$	$\left[1^3, 2^{(\ell-3)/2}\right], [2^{(\ell-3)/2}, 3], [1, 2^{(\ell-1)/2}]$ twice	[22, Proposition 3.0.26(b)]
$F1.4$	$\left[2^{\ell/2}\right], [1, 2^{(\ell-4)/2}, 3], [1^2, 2^{(\ell-2)/2}]$ twice	[22, Proposition 3.0.26(d)]
$F1.5$	$\left[1^2, 2^{(\ell-5)/2}, 3\right], [1, 2^{(\ell-1)/2}]$ thrice	[22, Proposition 3.0.26(f)]
$F1.6$	$\left[1^3, 2^{(\ell-3)/2}\right], [1, 2^{(\ell-5)/2}, 4], [1, 2^{(\ell-1)/2}]$ twice	[22, Proposition 3.0.26(a)]
$F1.7$	$\left[2^{\ell/2}\right], [1^2, 2^{(\ell-6)/2}, 4], [1^2, 2^{(\ell-2)/2}]$ twice	[22, Proposition 3.0.26(c)]
$F1.8$	$\left[1^3, 2^{(\ell-7)/2}, 4\right], [1, 2^{(\ell-1)/2}]$ thrice	[22, Proposition 3.0.26(e)]
$F1.9$	$\left[2^{(\ell-4)/2}, 4\right], [1^2, 2^{(\ell-2)/2}]$ thrice;	
$F3.1$	$\left[1^2, 2^{(\ell-2)/2}\right], [1, 3, 4^{(\ell-4)/4}], [4^{\ell/4}]$	[22, Conjecture 3.0.29(a)]
$F3.2$	$\left[1, 2^{(\ell-1)/2}\right], [1, 4^{(\ell-1)/4}], [2, 3, 4^{(\ell-5)/4}]$	[22, Conjecture 3.0.29(b)]
$F3.3$	$\left[1, 2^{(\ell-1)/2}\right], [1, 2, 4^{(\ell-3)/4}], [3, 4^{(\ell-3)/4}]$	[22, Conjecture 3.0.29(c)]
$F4.1$	$\left[1^2, 2^{(\ell-2)/2}\right], [1, 2, 3^{(\ell-3)/3}], [6^{\ell/6}]$	[22, Conjecture 3.0.29(d)]
$F4.2$	$\left[1^2, 2^{(\ell-2)/2}\right], [2, 3^{(\ell-2)/3}], [2, 6^{(\ell-2)/6}]$	
$F4.3$	$\left[1, 2^{(\ell-1)/2}\right], [1, 3^{(\ell-1)/3}], [3, 4, 6^{(\ell-7)/6}]$	[22, Conjecture 3.0.29(e)]
$F4.4$	$\left[1, 2^{(\ell-1)/2}\right], [1, 2, 3^{(\ell-3)/3}], [3, 6^{(\ell-3)/6}]$	[22, Conjecture 3.0.29(h)]
$F4.5$	$\left[1^2, 2^{(\ell-2)/2}\right], [1, 3^{(\ell-1)/3}], [4, 6^{(\ell-4)/6}]$	[22, Conjecture 3.0.29(i)]
$F4.6$	$\left[1, 2^{(\ell-1)/2}\right], [2, 3^{(\ell-2)/3}], [2, 3, 6^{(\ell-5)/6}]$	[22, Conjecture 3.0.29(j)]

TABLE 4.2. Ramification types for some coverings $f : \mathbb{P}^1 \to \mathbb{P}^1$ of degree $n = \ell(\ell-1)/2$, $\ell \geq 13$, and monodromy group A_ℓ or S_ℓ. Here a is an odd number in $\{1, \dots, \ell-1\}$, $(a, \ell) = 1$, and ℓ satisfies the necessary congruence conditions to make exponents integral. The notation k^* means that the rest of the entries in the multiset equal k.

$I1.1a$	$[\ell^*], [a(\ell-a), a^{(a-1)/2}, \frac{\ell-a}{2}, (\ell-a)^*], [2^{\ell-2}, 1^*]$
$I1.1b$	$[\frac{\ell}{2}, \ell^*], [a(\ell-a), a^{(a-1)/2}, (\ell-a)^*], [2^{\ell-2}, 1^*]$
$I2.1$	$[\ell^*], [1^{(\ell+3)/2}, 2^*], [1^{(\ell-1)/2}, 2^*], [2^{\ell-2}, 1^*]$
$I2.2$	$[\frac{\ell}{2}, \ell^*], [1^{\ell/2}, 2^*]$ twice, $[2^{\ell-2}, 1^*]$
$I2.3$	$[\ell^*], [1^{(\ell+3)/2}, 2^*], [3, 1^{(\ell-3)/2}, 6^{(\ell-3)/2}, 2^*]$
$I2.4$	$[\frac{\ell}{2}, \ell^*], [1^{\ell/2}, 2^*], [3^2, 1^{(\ell-4)/2}, 6^{(\ell-4)/2}, 2^*]$
$I2.5$	$[\ell^*], [1^{(\ell-1)/2}, 2^*], [3^3, 1^{(\ell-3)/2}, 6^{(\ell-5)/2}, 2^*]$
$I2.6$	$[\ell^*], [1^{(\ell+3)/2}, 2^*], [1^{(\ell-5)/2}, 4^{\ell-3}, 2^*]$
$I2.7$	$[\frac{\ell}{2}, \ell^*], [1^{\ell/2}, 2^*], [1^{(\ell-4)/2}, 4^{\ell-3}, 2^*]$
$I2.8$	$[\ell^*], [1^{(\ell-1)/2}, 2^*], [1^{(\ell-1)/2}, 4^{\ell-3}, 2^*]$
$I2.9$	$[a(\ell-a), a^{(a-1)/2}, (\ell-a)^*], [1^{\ell/2}, 2^*]$ twice, $[2^{\ell-2}, 1^*]$
$I2.10$	$[a(\ell-a), a^{(a-1)/2}, \frac{\ell-a}{2}, (\ell-a)^*], [1^{(\ell-1)/2}, 2^*]$ twice, $[2^{\ell-2}, 1^*]$
$I2.11$	$[a(\ell-a), a^{(a-1)/2}, (\ell-a)^*], [1^{\ell/2}, 2^*], [1^{(\ell-4)/2}, 4^{\ell-3}, 2^*]$
$I2.12$	$[a(\ell-a), a^{(a-1)/2}, \frac{\ell-a}{2}, (\ell-a)^*], [1^{(\ell-1)/2}, 2^*], [1^{(\ell-5)/2}, 4^{\ell-3}, 2^*]$
$I2.14$	$[a(\ell-a), a^{(a-1)/2}, \frac{\ell-a}{2}, (\ell-a)^*], [1^{(\ell-1)/2}, 2^*], [3, 1^{(\ell-3)/2}, 6^{(\ell-3)/2}, 2^*]$
$I2.15$	$[a(\ell-a), a^{(a-1)/2}, (\ell-a)^*], [1^{\ell/2}, 2^*], [3^2, 1^{(\ell-4)/2}, 6^{(\ell-4)/2}, 2^*]$
$F1.1$	$[2^{\ell-2}, 1^*], [1^{\ell/2}, 2^*]$ four times
$F1.2$	$[2^{\ell-2}, 1^*], [1^{(\ell+3)/2}, 2^*], [1^{(\ell-1)/2}, 2^*]$ thrice
$F1.3$	$[1^{(\ell+3)/2}, 2^*], [3, 1^{(\ell-3)/2}, 6^{(\ell-3)/2}, 2^*], [1^{(\ell-1)/2}, 2^*]$ twice
$F1.4$	$[1^{\ell/2}, 2^*]$ thrice, $[3^2, 1^{(\ell-4)/2}, 6^{(\ell-4)/2}, 2^*]$
$F1.5$	$[3^3, 1^{(\ell-3)/2}, 6^{(\ell-5)/2}, 2^*], [1^{(\ell-1)/2}, 2^*]$ thrice
$F1.6$	$[1^{(\ell+3)/2}, 2^*], [1^{(\ell-5)/2}, 4^{\ell-3}, 2^*], [1^{(\ell-1)/2}, 2^*]$ twice
$F1.7$	$[1^{\ell/2}, 2^*], [1^{(\ell-4)/2}, 4^{\ell-3}, 2^*], [1^{\ell/2}, 2^*]$ twice
$F1.8$	$[1^{(\ell-1)/2}, 4^{\ell-3}, 2^*], [1^{(\ell-1)/2}, 2^*]$ thrice
$F3.1$	$[1^{\ell/2}, 2^*], [3^2, 2^{(\ell-4)/4}, 12^{(\ell-4)/4}, 4^*], [2^{\ell/4}, 4^*]$
$F3.2$	$[1^{(\ell-1)/2}, 2^*], [2^{(\ell-1)/4}, 4^*], [1, 3, 6, 2^{(\ell-5)/4}, 12^{(\ell-5)/4}, 4^*]$
$F3.3$	$[1^{(\ell-1)/2}, 2^*], [1, 2^{(\ell+1)/4}, 4^*], [3, 2^{(\ell-3)/4}, 12^{(\ell-3)/4}, 4^*]$
$F4.1$	$[1^{\ell/2}, 2^*], [1, 2, 6^{(\ell-3)/3}, 3^*], [3^{\ell/6}, 6^*]$
$F4.2$	$[1^{\ell/2}, 2^*], [1, 6^{(\ell-2)/3}, 3^*], [1, 3^{(\ell-2)/6}, 6^*]$
$F4.3$	$[1^{(\ell-1)/2}, 2^*], [3^*], [2, 4, 3^{(\ell-1)/6}, 12^{(\ell-4)/3}, 6^*]$
$F4.4$	$[1^{(\ell-1)/2}, 2^*], [1, 2, 6^{(\ell-3)/3}, 3^*], [3^{(\ell+3)/6}, 6^*]$
$F4.5$	$[1^{\ell/2}, 2^*], [3^*], [2, 4, 3^{(\ell-4)/6}, 12^{(\ell-4)/3}, 6^*]$
$F4.6$	$[1^{(\ell-1)/2}, 2^*], [1, 6^{(\ell-2)/3}, 3^*], [1, 3^{(\ell+1)/6}, 6^*]$

(resp., if $R_1 = R_2$ and r_1 is even), proving (1) and (2). In case (3), all pairs $\{a, a^{x^{r_1/2}}\}$ are in the same orbit of x which has cardinality $r_1/2$. As there are $r_1(r_1-2)/2$ pairs in T which are not of the form $(a, a^{x^{r_1/2}})$, these comprise $r_1/2 - 1$ orbits, proving (3). □

Applying this lemma for each of the ramification types of h in Table 4.1 over each branch point, we obtain the corresponding ramification types for f. As noted after Theorem 3.1, $g_{Y_1} = 0$ for each ramification type in Table 4.1. Hence the formula (6.3) gives $g_{X_2} = 0$ for every $f : X_2 \to \mathbb{P}^1$ whose ramification type appears in Table 4.2.

The ramification types for h are labeled according to the case in the proof of Proposition 10.1 from which they arise. The ramification types for f are labeled as their corresponding ramification type of h with additional subcases if a single ramification type for h has several corresponding types for f, depending on whether ℓ is odd or even.

Remark 4.2. Note that Item I1.1 in Table 4.1 corresponds to the rational function $X^a(X-1)^{\ell-a}$; Item F1.9 does not appear in [22]; Item (g) of [22, Conjecture 3.0.29] is replaced by Item F4.2; Item (f) of [22, Conjecture 3.0.29] does not correspond to a covering with primitive monodromy group by the special case of Lemma 9.9 corresponding to case F1.N4 of Table 9.2. The ramification types F1.7 and F1.9 (resp., I2.11 and I2.13) in Table 4.1 correspond to the same ramification type in Table 4.2, so we do not include an entry for cases F1.9 or I2.13 in Table 4.2.

5. Relating set and point stabilizers

As in Setup 2.2, let $h : Y_1 \to Y$ be a covering of degree ℓ with monodromy group $G \in \{A_\ell, S_\ell\}$ acting on a set $S = \{1, \dots, \ell\}$, let X_t be the quotient by the stabilizer $\overline{H}_t$ of the set $\{1, \dots, t\}$, and Y_t the quotient by the pointwise stabilizer H_t of $\{1, \dots, t\}$.

A key ingredient in proving Theorem 3.1 is bounding the contribution R_{π_t} of the natural projection $\pi_t : Y_t \to X_t$. The following proposition describes the main term of the Riemann–Hurwitz contribution from π_t. This contribution accounts for the extent to which the orbits of branch cycles on t-tuples are longer than their orbits on t-sets. For $t = 2$, such orbits appear whenever the branch cycle has an even length orbit.

For $n \in \mathbb{N} \cup \{0\}$, let $v_p(n)$ be the largest integer such that $p^{v_p(n)} \mid n$.

Proposition 5.1. *There exists a constant $E_0 > 0$ satisfying the following property. Let $t, \ell \in \mathbb{N}$ be integers such that $t \geq 2$ and $\ell > t^2$. Let $h : Y_1 \to Y$ be a covering of degree ℓ with monodromy group $G \in \{A_\ell, S_\ell\}$. Let P be a point of Y and x a branch cycle of h over P. Then*

(1) $R_{\pi_2}(f_2^{-1}(P)) = |\{\text{even } r \in E_h(P)\}|$;
(2)
$$R_{\pi_t}(f_t^{-1}(P)) \leq \binom{t}{2} \sum_{\theta_1, \dots, \theta_{t-1}} \frac{\hat{r}_1 \cdots \hat{r}_{t-1}}{\operatorname{lcm}(r_1, \dots, r_{t-1})} + E_0 t^4 \cdot \frac{(\ell-2)!}{(\ell-t)!}$$
where $r_i := |\theta_i|$, and $\hat{r}_i := r_i - |\{j : j < i, \theta_j = \theta_i\}|$ for $i = 1, \dots, t-1$, and $\theta_1, \dots, \theta_{t-1}$ run through orbits of x with r_1 even and $v_2(r_1) > v_2(r_j)$, for $j = 2, \dots, t-1$.

Proof. **Step I:** *We first express $R_{\pi_t}(f_t^{-1}(P))$ using orbits of x on t-sets and t-tuples.* As in Section 2.2, let $h_t : Y_t \to Y$ and $f_t : X_t \to Y$ denote the natural projections, so that their monodromy act on the set $S^{(t)}$ of t-tuples of pairwise distinct elements of S and on the set $\overline{S}^{(t)}$ of t-subsets of S, respectively.

Let $O_1, \dots, O_s$ be the orbits of x on $\overline{S}^{(t)}$. For a t-tuple $U \in S^{(t)}$, denote by $\overline{U} \in \overline{S}^{(t)}$ its underlying t-set, and by r_U the length of its orbit. For given $i \in \{1, \dots, s\}$, we claim that the length r_U is independent of the choice of a t-tuple $U \in S^{(t)}$ for which $\overline{U} \in O_i$. Given a t-set $\overline{V} \in O_i$, the element $x^{|O_i|}$ defines a permutation on the elements of $\overline{V}$. Let e_i be the order of this permutation. The orbit of every t-tuple $V \in S^{(t)}$ with underlying set $\overline{V}$ is then of length $r_V = e_i \cdot |O_i|$. Since the orbit of every t-tuple $U \in S^{(t)}$ with $\overline{U} \in O_i$ contains such a tuple V, we have $r_U = r_V = e_i \cdot |O_i|$, proving the claim.

Since every t-subset $\overline{U}$ in O_i has $t!$ tuples in $S^{(t)}$ with underlying set $\overline{U}$, the number of t-tuples in $S^{(t)}$ with underlying set in O_i is $t! \cdot |O_i|$, for $i = 1, \dots, s$. By the above claim, the action of x on such tuples breaks into equal length orbits O_i^j, $j = 1, \dots, s_i$, where $s_i := t!|O_i|/|O_i^1|$, for $1 \le i \le s$. Thus the Riemann–Hurwitz contributions are

$$R_{f_t}(P) = \sum_{i=1}^{s} (|O_i| - 1) \quad \text{and} \quad R_{h_t}(P) = \sum_{i=1}^{s} \sum_{j=1}^{s_i} (|O_i^j| - 1).$$

Since $s_i = t!|O_i|/|O_i^1|$ and $|O_i^j| = |O_i^1|$, it follows that:

$$R_{f_t}(P) = \sum_{i=1}^{s} (|O_i| - 1) = \sum_{i=1}^{s} \frac{1}{s_i} \sum_{j=1}^{s_i} (|O_i| - 1) = \frac{1}{t!} \sum_{i=1}^{s} \sum_{j=1}^{s_i} \Big(|O_i^j| - \frac{|O_i^j|}{|O_i|} \Big).$$

Since $R_{h_t}(P) = t! R_{f_t}(P) + R_{\pi_t}(f_t^{-1}(P))$ by the chain rule (2.1), we get

$$R_{\pi_t}(f_t^{-1}(P)) = R_{h_t}(P) - t! R_{f_t}(P) = \sum_{i=1}^{s} \sum_{j=1}^{s_i} \Big(\frac{|O_i^j|}{|O_i|} - 1 \Big). \tag{5.1}$$

Step II: *To bound $R_{\pi_t}(f_t^{-1}(P))$ using (5.1), we bound the number of pairs (i, j) for which $|O_i^j|/|O_i|$ is divisible by a given power q of a prime p.* Let $U := [u_1, \dots, u_t] \in S^{(t)}$ be a tuple in O_i^j. If $q \,|\, (|O_i^j|/|O_i|)$, then $|O_i|$ divides (r_U/q) and hence $x^{r_U/q}$ defines a permutation of order q on $\overline{U}$. As q is a prime power this implies that q and U satisfy the condition

$(Cyc)_{q,U}$ There exist $v_1, \dots, v_q \in \overline{U}$ that form a cycle under the action of $x^{r_U/q}$.

We next bound the total number of tuples $U \in S^{(t)}$ satisfying $(Cyc)_{q,U}$ for a given q. Note that if $v_1, \dots, v_q$ is a cycle of $x^{r_U/q}$, then it is also a cycle of $x^{r_1/q}$ where r_1 is the length of the orbit of v_1. Thus, a choice of v_1 determines $v_2, \dots, v_q$ as the images of v_1 under $x^{r_1/q}$. Thus, there are at most ℓ choices for the first entry v_1 and these determine $v_2, \dots, v_q$; there are $t!/(t-q)!$ choices for the positions of $v_1, \dots, v_q$ in U; and $(\ell-q)!/(\ell-t)!$ choices for the rest of the entries in U. Hence in total the number of tuples $U \in S^{(t)}$ satisfying $(Cyc)_{q,U}$

is at most $\frac{t!}{(t-q)!}\ell\frac{(\ell-q)!}{(\ell-t)!}$. Since the orbit of each such U is of length at least q, we have

$$|\{(i,j): q \text{ divides } |O_i^j|/|O_i|\}| \leq \frac{1}{q}\frac{t!}{(t-q)!}\ell\frac{(\ell-q)!}{(\ell-t)!}. \tag{5.2}$$

Step III: *We now apply* (5.2) *to estimate* (5.1). Note that every integer $e > 1$ is bounded by $e \leq q!$ where q is the largest prime power dividing e, since at worst every integer $1 < u < q$ is a prime power dividing e. Hence, each summand $|O_i^j|/|O_i| - 1$ in (5.1) is bounded by $q! - 1$ where q is the largest power dividing $|O_i^j|/|O_i|$. Combining this bound with (5.2) for each $q > 2$, we get the following estimate of (5.1):

$$R_{\pi_t}(f_t^{-1}(P)) \leq |\{(i,j): \frac{|O_i^j|}{|O_i|} = 2\}| + \sum_q \left(\frac{1}{q}\frac{t!}{(t-q)!}\ell\frac{(\ell-q)!}{(\ell-t)!}(q!-1)\right) \tag{5.3}$$

where q runs over all prime powers between 3 and t. Since $3 \leq q \leq t$ and $\ell > t^2$, a routine calculation shows that the summands in (5.3) are strictly decreasing as functions of q. Hence each of the summands corresponding to prime powers between 3 and t is bounded by the summand at $q = 3$ which is at most $E_1 t^3 \frac{(\ell-2)!}{(\ell-t)!}$, for some contant $E_1 > 0$. Since there are less than t prime powers between 3 and t, (5.3) gives

$$R_{\pi_t}(f_t^{-1}(P)) < |\{(i,j): \frac{|O_i^j|}{|O_i|} = 2\}| + E_1 t^4 \frac{(\ell-2)!}{(\ell-t)!}. \tag{5.4}$$

Step IV: *We use a similar argument in order to bound the number of pairs* (i,j) *with* $|O_i^j|/|O_i| = 2$. Note that for a tuple $U = [u_1, \ldots, u_t] \in S^{(t)}$ in an orbit O_i^j with $|O_i^j|/|O_i| = 2$, the element $x^{r_U/2}$ is a permutation of order 2 on $\overline{U}$. We divide such tuples U into two types according to whether $x^{r_U/2}$ acts on $\overline{U}$ as a transposition. If $x^{r_U/q}$ does not act as a transposition then U satisfies:

($\overline{Trans}$)$_{2,U}$ There exist $u_1, u_2, v_1, v_2 \in \overline{U}$, such that u_1, u_2 and v_1, v_2 are pairwise disjoint length 2 cycles of $x^{r_U/2}$.

We next bound the number of tuples U satisfying ($\overline{Trans}$)$_{2,U}$. As in Step II, if u_1, u_2 is a cycle of $x^{r_U/2}$, then it is also a cycle of $x^{r_1/2}$, where r_1 is the length of the orbit of u_1 under x. Hence, a choice of u_1 (resp., v_1) determines u_2 (resp., v_2), as its image under $x^{r_1/2}$. It follows that there are ℓ choices for u_1, which then determine u_2; $\ell - 2$ choices for v_1 which then determine v_2; $t!/(t-4)!$ choices for the positions for u_1, u_2, v_1, v_2 in U; and $\ell!/(\ell-4)!$ choice for the rest of the entries in U. Hence in total the number of tuples $U \in S^{(t)}$ satisfying ($\overline{Trans}$)$_{2,U}$ is at most:

$$\frac{t!}{(t-4)!}\ell(\ell-2)\frac{(\ell-4)!}{(\ell-t)!} < E_2 t^4 \frac{(\ell-2)!}{(\ell-t)!}, \text{ for some constant } E_2 > 0. \tag{5.5}$$

We next count the number of tuples $U \in S^{(t)}$ satisfying:

($Trans$)$_{2,U}$ $x^{r_U/2}$ acts on $\overline{U}$ as a transposition (u_1, u_t), for some $u_1, u_t \in \overline{U}$.

As the number of tuples U satisfying $(Trans)_{2,U}$ with given positions of u_1, u_t in U, is independent of the choice of these positions, it suffices to count the number of tuple $U = [u_1, \dots, u_t] \in S^{(t)}$ such that $x^{r_U/2}$ acts on $\overline{U}$ as the transposition (u_1, u_t).

Letting θ_i be an orbit of x and $r_i = |\theta_i|$ for $i = 1, \dots, t$, a tuple $U = [u_1, \dots, u_t] \in S^{(t)}$ with $u_i \in \theta_i$, $i = 1, \dots, t$, has an orbit of length $r_U = \operatorname{lcm}(r_1, \dots, r_t)$. For such a tuple U, the element $x^{r_U/2}$ acts on $\overline{U}$ as the transposition (u_1, u_t) if and only if $\theta_1 = \theta_t$, and $v_2(r_1) = v_2(r_U) > 0$, and $v_2(r_i) < v_2(r_U)$ for all $1 < i < t$.

Fix orbits $\theta_1, \dots, \theta_{t-1}$ satisfying the latter constraints, that is, $v_2(r_1) = v_2(r) > 0$ and $v_2(r_i) < v_2(r_1)$, $i = 2, \dots, t-1$, where $r_i := |\theta_i|$ and $r := \operatorname{lcm}(r_1, \dots, r_{t-1})$. We count the number of tuples $U = [u_1, \dots, u_t] \in S^{(t)}$ with $u_i \in \theta_i$, $i = 1, \dots, t-1$, and $u_t = u_1^{x^{r/2}}$. Since there are $\hat{r}_1 := r_1$ choices for $u_1 \in \theta_1$, and $\hat{r}_i := r_i - |\{j : j < i, \theta_j = \theta_i\}|$ choices for $u_i \in \theta_i$, for each $i = 2, \dots, t-1$, the number of such tuples U is $\hat{r}_1 \hat{r}_2 \cdots \hat{r}_{t-1}$.

In total we get that the number of tuples $U \in S^{(t)}$ satisfying $(Trans)_{2,U}$ is

$$\frac{t(t-1)}{2} \sum_{\theta_1, \dots, \theta_{t-1}} \frac{\hat{r}_1 \cdots \hat{r}_{t-1}}{\operatorname{lcm}(r_1, \dots, r_{t-1})}, \tag{5.6}$$

where $r_i = |\theta_i|$, and $\hat{r}_i = r_i - |\{j : j < i, \theta_j = \theta_i\}|$, and $\theta_1, \dots \theta_{t-1}$ run through orbits of x with even r_1 and $v_2(r_1) > v_2(r_i)$, for $i = 2, \dots, t-1$. Plugging the bound (5.5) on tuples $U \in S^{(t)}$ satisfying $(\overline{Trans})_{2,U}$ and the count (5.6) of orbits of tuples $U \in S^{(t)}$ satisfying $(Trans)_{2,U}$ into (5.4) proves part (2) with $E_0 := E_1 + E_2$.

Step V: *The case* $t = 2$. For $t = 2$, there are no 2-tuples $U \in S^{(2)}$ satisfying $(Cyc)_{q,U}$ with $q > 2$, nor tuples satisfying $(\overline{Trans})_{2,U}$. Moreover, the number of orbits O_i^j consisting of tuples $U \in S^{(2)}$ that satisfy $(Trans)_{2,U}$ equals the number of even length orbits of x by (5.6). In total, evaluating (5.1) when $t = 2$, then gives

$$\begin{aligned} R_{\pi_t}(f_t^{-1}(P)) &= |\{(i,j) : \frac{|O_i^j|}{|O_i|} = 2\}| = |\{(i,j) : (Trans)_{2,U} \text{ holds for every } U \in O_i^j\}| \\ &= |\{\text{even length orbits of } x\}|. \end{aligned}$$

□

Remark 5.2. By Proposition 5.1, if the ramification type of h appears in Table 4.1 and is different from $[\ell], [a, \ell - a], [2, 1^{\ell-2}]$, then the sum of the contributions $R_{\pi_2}(f_2^{-1}(P))$ over all points P of Y is at least $(2\ell - 5)/3$, as this is the minimal number of even entries among the ramification types in Table 4.1 with $\ell \geq 13$.

The proof of Theorem 3.1 uses the following proposition to cancel out the main term of $R_{\pi_t}(f_t^{-1}(P))$ in Proposition 5.1 with the Riemann–Hurwitz contribution of the natural projection $h_1^{t-1} : Y_{t-1} \to Y_1$ for $t \geq 2$.

Proposition 5.3. *Let $h : Y_1 \to Y$ be a degree ℓ covering with monodromy group $G \in \{A_\ell, S_\ell\}$ acting on S. Let $3 \leq t \leq \ell/2$ be an integer, P a point of Y, and x a branch cycle over P. Then*

$$\sum_{(\theta_1, \dots, \theta_{t-1}) \in O_h(P)} \frac{\hat{r}_1 \cdots \hat{r}_{t-1}}{\operatorname{lcm}(r_1, \dots, r_{t-1})} \leq R_{h_1^{t-1}}(h^{-1}(P)),$$

where $r_i := |\theta_i|$, *and* $\hat{r}_i := r_i - |\{j : j < i, \theta_j = \theta_i\}|$, $i = 1, \dots, t-1$, *and* $O_h(P)$ *consists of tuples* $(\theta_1, \dots, \theta_{t-1}) \in \mathrm{Orb}_S(x)^{t-1}$ *such that* $v_2(r_1) > v_2(r_j)$ *for* $j = 2, \dots, t-1$.

The proof relies on the following lemma.

Lemma 5.4. *Let* $h : Y_1 \to Y$ *be a degree* ℓ *covering with monodromy group* $G \in \{A_\ell, S_\ell\}$ *acting on* S. *Let* $t \geq 2$, *and* P *be a point of* Y, *and* $x \in G$ *a branch cycle over* P. *Then*

$$R_{h_1^{t-1}}(h^{-1}(P)) = \sum_{(\theta_1,\dots,\theta_{t-1}) \in \mathrm{Orb}_S(x)^{t-1}} \frac{\hat{r}_1 \cdots \hat{r}_{t-1}}{\mathrm{lcm}(r_1, \dots, r_{t-1})} \Big(\frac{\mathrm{lcm}(r_1, \dots, r_{t-1})}{r_1} - 1 \Big),$$

where $r_i := |\theta_i|$ *and* $\hat{r}_i := r_i - |\{j : j < i, \theta_j = \theta_i\}|$ *for* $i = 1, \dots, t-1$.

Proof. As in Setup 2.2, the monodromy group of the natural projection $h_{t-1} : Y_{t-1} \to Y$ is G with its action on the set $S^{(t-1)}$ of $(t-1)$-tuples of distinct elements from S. Hence h_{t-1} is of degree $\ell!/(\ell - (t-1))!$ and h_1^{t-1} is of degree $(\ell-1)!/(\ell-(t-1))!$.

By the chain rule (2.1), one has $R_{h_1^{t-1}}(h^{-1}(P)) = R_{h_{t-1}}(P) - \frac{(\ell-1)!}{(\ell-(t-1))!} R_h(P)$. Since $R_{h_{t-1}}(P) = \frac{\ell!}{(\ell-(t-1))!} - |\mathrm{Orb}_{S^{(t-1)}}(x)|$ and $R_h(P) = \ell - |\mathrm{Orb}_S(x)|$, this gives

$$R_{h_1^{t-1}}(h^{-1}(P)) = \frac{(\ell-1)!}{(\ell-(t-1))!} |\mathrm{Orb}_S(x)| - |\mathrm{Orb}_{S^{(t-1)}}(x)|. \tag{5.7}$$

Letting $p : \mathrm{Orb}_{S^{(t-1)}}(x) \to \mathrm{Orb}_S(x)$ denote the projection onto the first coordinate, we partition $\mathrm{Orb}_{S^{(t-1)}}(x)$ as the union of the fibers of p. Hence (5.7) yields:

$$R_{h_1^{t-1}}(h^{-1}(P)) = \sum_{\theta \in \mathrm{Orb}_S(x)} \Big(\frac{(\ell-1)!}{(\ell-(t-1))!} - |p^{-1}(\theta)| \Big). \tag{5.8}$$

Given $\theta \in \mathrm{Orb}_S(x)$, we note that the total number of tuples $U = [u_1, \dots, u_{t-1}] \in S^{(t-1)}$ contained in orbits in $p^{-1}(\theta)$ is $|\theta| \cdot \frac{(\ell-1)!}{(\ell-(t-1))!}$: for, there are $|\theta|$ choices for u_1, and $(\ell-1)!/(\ell-(t-1))!$ choices for the rest of the entries. It follows that

$$\sum_{\hat{\theta} \in p^{-1}(\theta)} |\hat{\theta}| = |\theta| \cdot \frac{(\ell-1)!}{(\ell-(t-1))!}.$$

Hence (5.8) amounts to:

$$R_{h_1^{t-1}}(h^{-1}(P)) = \sum_{\theta \in \mathrm{Orb}_S(x)} \sum_{\hat{\theta} \in p^{-1}(\theta)} \Big(\frac{|\hat{\theta}|}{|\theta|} - 1 \Big). \tag{5.9}$$

For orbits $\theta_1, \dots, \theta_{t-1}$ denote $r_i := |\theta_i|$, and $\hat{r}_i := r_i - |\{j : j < i, \theta_j = \theta_i\}|$ for $i = 1, \dots, t-1$. Let $U(\theta_1, \dots, \theta_{t-1})$ be the set of orbits of x on $(\theta_1 \times \cdots \times \theta_{t-1}) \cap S^{(t-1)}$, so that $p^{-1}(\theta)$ partitions into the sets $U(\theta_1, \dots, \theta_{t-1})$ where $\theta_2, \dots, \theta_{t-1}$ run through orbits of x, and $\theta_1 = \theta$. For fixed $\theta_1, \dots, \theta_{t-1}$, the number of tuples in orbits in $U(\theta_1, \dots, \theta_{t-1})$ is

$\hat{r}_1 \cdots \hat{r}_{t-1}$, and the length of each orbit $\hat{\theta} \in U(\theta_1, \dots, \theta_{t-1})$ is $\mathrm{lcm}(r_1, \dots, r_{t-1})$, so that the number of orbits in $U(\theta_1, \dots, \theta_{t-1})$ is $\hat{r}_1 \cdots \hat{r}_{t-1}/\mathrm{lcm}(r_1, \dots, r_{t-1})$. Hence (5.9) yields:

$$\begin{aligned} R_{h_1^{t-1}}(h^{-1}(P)) &= \sum_{\theta_1,\theta_2,\dots,\theta_{t-1} \in \mathrm{Orb}_S(x)} \sum_{\hat{\theta} \in U(\theta_1,\dots,\theta_{t-1})} \left(\frac{|\hat{\theta}|}{|\theta_1|} - 1 \right) \\ &= \sum_{\theta_1,\dots,\theta_{t-1} \in \mathrm{Orb}_S(x)} \frac{\hat{r}_1 \cdots \hat{r}_{t-1}}{\mathrm{lcm}(r_1, \dots, r_{t-1})} \left(\frac{\mathrm{lcm}(r_1, \dots, r_{t-1})}{r_1} - 1 \right). \end{aligned}$$ □

Proof of Proposition 5.3. For a tuple $(\theta_1, \dots, \theta_{t-1})$, denote $r_i := |\theta_i|$ and let $\hat{r}_i$ denote $r_i - |\{j : j < i, \theta_j = \theta_i\}|$, for $i = 1, \dots, t-1$. Let $\overline{O}_h(P)$ be the set of all $(\theta_1, \dots, \theta_{t-1}) \in O_h(P)$ such that $r_j \mid r_1$ for $j = 2, \dots, t-1$. As $t \geq 3$, we can define a map $\phi : \overline{O}_h(P) \to \mathrm{Orb}_S(x)^{t-1}$ which swaps the first and i-th entry of $(\theta_1, \dots, \theta_{t-1}) \in \overline{O}_h(P)$, where $2 \leq i \leq t-1$ is the smallest index for which $r_i = \min_{2 \leq j \leq t-1}(r_j)$. Note that since $v_2(r_1) > v_2(r_j)$ for all $j = 2, \dots, t-1$ and $(\theta_1, \dots, \theta_{t-1}) \in O_h(P)$, the image $\phi(\overline{O}_h(P))$ is disjoint from $O_h(P)$.

Restricting the sum in Lemma 5.4 to the set $\phi(\overline{O}_h(P)) \cup O_h(P) \setminus \overline{O}_h(P)$ we get

(5.10)
$$R_{h_1^{t-1}}(h^{-1}(P)) \geq \sum_{(\theta_1,\dots,\theta_{t-1}) \in \phi(\overline{O}_h(P)) \cup O_h(P) \setminus \overline{O}_h(P)} \frac{\hat{r}_1 \cdots \hat{r}_{t-1}}{\mathrm{lcm}(r_1, \dots, r_t)} \left(\frac{\mathrm{lcm}(r_1, \dots, r_{t-1})}{r_1} - 1 \right).$$

By the definitions of $\overline{O}_h(P)$ and ϕ, we have $\mathrm{lcm}(r_1, \dots, r_{t-1})/r_1 \geq 2$ for every tuple $(\theta_1, \dots, \theta_{t-1})$ in $\phi(\overline{O}_h(P))$ or in $O_h(P) \setminus \overline{O}_h(P)$. Hence (5.10) gives

$$R_{h_1^{t-1}}(h^{-1}(P)) \geq \sum_{(\theta_1,\dots,\theta_{t-1}) \in \phi(\overline{O}_h(P)) \cup O_h(P) \setminus \overline{O}_h(P)} \frac{\hat{r}_1 \cdots \hat{r}_{t-1}}{\mathrm{lcm}(r_1, \dots, r_t)}. \tag{5.11}$$

Noting that the product $\hat{r}_1 \cdots \hat{r}_{t-1}$ and $\mathrm{lcm}(r_1, \dots, r_{t-1})$ are preserved by ϕ, we deduce that the right hand side of (5.11) equals $\sum_{(\theta_1,\dots,\theta_{t-1}) \in O_h(P)} \frac{\hat{r}_1 \cdots \hat{r}_{t-1}}{\mathrm{lcm}(r_1,\dots,r_{t-1})}$. □

6. Theorem 3.1 when g_{Y_1} is bounded from below

The following lemma and proposition prove Theorem 3.1 for coverings $h : Y_1 \to Y$ for which g_{Y_1} is large in comparison to t. We use Setup 2.2, so that X_t (resp., Y_t) is the quotient by the stabilizer of a t-set (resp., t-tuple of distinct elements).

Proposition 6.1. *There exist positive constants c_2, d_2, β such that for every covering $h : Y_1 \to Y$ of degree ℓ, with monodromy group A_ℓ or S_ℓ, and genus $g_{Y_1} \geq \beta t^4$ (resp., $g_{Y_1} \geq 2$), one has*

$$g_{X_t} - g_{X_{t-1}} > (c_2 \ell - d_2 t^8) \frac{\binom{\ell}{t}}{\binom{\ell}{2}}, \quad \text{for } t \geq 3 \text{ (resp., } t = 2).$$

Furthermore for $t \geq 3$, one can set $c_2 = 2$.

Remark 6.2. As in the setup of Proposition 6.1, let π_t, h_{t-1} and h_{t-1}^t be the natural projections $Y_t \to X_t$, $Y_{t-1} \to Y$, and $Y_t \to Y_{t-1}$, respectively. The proof relies on the following formula

$$\begin{aligned} 2t!(g_{X_t} - g_{X_{t-1}}) &= 2(\ell - 2t + 1)(g_{Y_{t-1}} - 1) \\ &+ \sum_{P \in Y(\mathbb{K})} \left(R_{h_{t-1}^t}({h_{t-1}}^{-1}(P)) + tR_{\pi_{t-1}}({f_{t-1}}^{-1}(P)) - R_{\pi_t}(f_t^{-1}(P)) \right) \end{aligned} \tag{6.1}$$

and its immediate consequence

$$2t!(g_{X_t} - g_{X_{t-1}}) \geq 2(\ell - 2t + 1)(g_{Y_{t-1}} - 1) - \sum_{P \in Y(\mathbb{K})} R_{\pi_t}(f_t^{-1}(P)). \tag{6.2}$$

Indeed, (6.1) follows from the Riemann–Hurwitz formula for the natural projections h_{t-1}^t, π_t, and π_{t-1}:

$$\begin{aligned} 2(g_{Y_t} - 1) =& 2(\ell - t + 1)(g_{Y_{t-1}} - 1) + \sum_{P \in Y(\mathbb{K})} R_{h_{t-1}^t}({h_{t-1}}^{-1}(P)) \\ 2t(g_{Y_{t-1}} - 1) =& 2t!(g_{X_{t-1}} - 1) + t \sum_{P \in Y(\mathbb{K})} R_{\pi_{t-1}}({f_{t-1}}^{-1}(P)), \text{ and} \\ 2(g_{Y_t} - 1) =& 2t!(g_{X_t} - 1) + \sum_{P \in Y(\mathbb{K})} R_{\pi_t}(f_t^{-1}(P)), \end{aligned}$$

by subtracting the first and second equalities from the third.

In particular for $t = 2$ and $\ell \geq 5$, as π_1 is the identity map, $R_{\pi_2}(f_2^{-1}(P))$ is the number of even $r \in E_h(P)$ by Proposition 5.1, and as $R_{h_1^2}(h^{-1}(P)) = \sum_{r_1, r_2 \in E_h(P)} \Big(r_1 - (r_1, r_2) \Big)$ by Lemma 5.4, the equality (6.1) amounts to

$$4(g_{X_2} - g_{X_1}) = 2(\ell - 3)(g_{Y_1} - 1) + \sum_{P \in Y(\mathbb{K})} \Big(-|\{\text{even } r \in E_h(P)\}| + \sum_{r_1, r_2 \in E_h(P)} \big(r_1 - (r_1, r_2) \big) \Big). \tag{6.3}$$

The proof of Proposition 6.1 for $t = 2$ relies on the following estimate of the latter sum:

Lemma 6.3. *Let $1 \leq r_1 \leq \ldots \leq r_u \leq \ell$ be integers whose sum is ℓ.*

(1) *If the quantity*

$$\mu_r := -|\{\text{even } r_i \colon 1 \leq i \leq u\}| + \sum_{1 \leq i,j \leq u} \big(r_i - (r_i, r_j) \big)$$

is negative then $r_1 = \cdots = r_u = \ell/u$ and ℓ/u is even;

(2) *If $\sum_{i,j \leq u} \big(r_i - (r_i, r_j) \big) \leq \ell/2u$ then $r_1 = \cdots = r_u = \ell/u$.*

Proof. Let $S_i := \sum_{j=1}^u \big(r_i - (r_i, r_j) \big)$ for $i = 1, \ldots, u$, and let s be the greatest common divisor of $r_1, \ldots, r_u$. Since r_u (resp. r_1) is maximal (resp., minimal) among the r_i's, if $r_u \neq s$, then $r_u > \ell/u > r_1$ and $S_u \geq r_u - (r_u, r_1) \geq r_u - r_u/2 = r_u/2 > \ell/2u$, proving (2).

If no r_i equals s then $S_i \geq 1$ for each i, so that μ_r is nonnegative. Now assume there is an i for which r_i divides all r_j's (so that $r_i = s$). If all the r_i's equal one another then

obviously μ_r is 0 if s is odd, and $-\ell/s$ if s is even. If there are k values i for which $r_i = s$ (with $0 < k < \ell/s$), then if $r_j \neq s$ we get $S_j \geq k(r_j - s)$, so since $\sum_{j:r_j \neq s} r_j = (\ell - ks)$ it follows that $\sum_j S_j \geq k(\ell - ks) - ks \cdot |\{j : r_j \neq s\}|$. Since in addition $u - k = |\{j : r_j \neq s\}| \leq (\ell - ks)/2s$, we get

$$\begin{aligned}\mu_r \geq \sum_j (S_j - 1) &\geq k(\ell - ks) - ks(u - k) - \Big(k + (u - k)\Big) \\ &\geq k(\ell - ks) - k - (ks + 1)\frac{\ell - ks}{2s}.\end{aligned}$$

For fixed s and ℓ, this is a quadratic polynomial in k with leading coefficient $-s/2$, so on any interval it is minimized only at an endpoint. In particular, as $1 \leq k \leq \ell/s - 2$ the function is minimized only when k is either 1 or $\ell/s - 2$, where its values are $(\ell - s - 1)/2 - \ell/(2s)$ and $\ell - 2s - \ell/s + 1$. If we now fix ℓ and vary s, then these values are minimized only when s is either as small or as big as possible; for $s = 1$ the values are -1, for $s = \ell/3$ they are $\ell/3 - 2$; note that for $s = \ell/2$, we have $r_1 = r_2 = \ell/2$. Since the sum of the $S_j - 1$'s is an integer, it follows that it is nonnegative unless $s = 1$ and the sum equals -1, but in that case some r_i is odd so the sum we want is again nonnegative. □

We separate the proof according to whether $t = 2$ or $t > 2$. For $t = 2$ we use Lemma 6.3 to bound R_{π_2} while for $t > 2$ we use the bound from Proposition 5.3. In both cases the proof splits to cases according to the number of branch points.

Proof of Proposition 6.1 for $t = 2$. For $t = 2$ we assume $g_{X_1} \geq 2$. We will show $4(g_{X_2} - g_{X_1}) \geq \ell/2 - 6$. Since the claim is trivial if $\ell/2 < 6$, we may assume $\ell \geq 12$. By equality (6.3) of Remark 6.2 and Lemma 6.3 we have

$$4(g_{X_2} - g_{X_1}) \geq 2(\ell - 3)(g_{Y_1} - 1) - \sum_{B_s} \frac{\ell}{s_P} \geq 2(\ell - 3)(g_{Y_1} - 1) - \frac{B\ell}{2} \tag{6.4}$$

where B_s is the set of branch points P such that $E_h(P) = [s_P^{n/s_P}]$ with s_P even, and $B := |B_s|$. Since Riemann–Hurwitz for h gives

$$2(g_{Y_1} - 1) \geq 2\ell(g_Y - 1) + \sum_{P \in B_s} \Big(\ell - \frac{\ell}{s_P}\Big) \geq -2\ell + \frac{B\ell}{2}, \tag{6.5}$$

we have

$$\begin{aligned}4(g_{X_2} - g_{X_1}) \geq 2(\ell - 3)(g_{Y_1} - 1) - \frac{B\ell}{2} &\geq (\ell - 3)\Big(-2\ell + \frac{B\ell}{2}\Big) - \frac{B\ell}{2} \\ &= \ell\Big(6 - 2\ell + \frac{B(\ell - 4)}{2}\Big).\end{aligned}$$

If $B \geq 5$ then the right hand side is at least $\ell^2/2 - 4\ell > \ell/4 - 6$. If $B \leq 3$ then (6.4) yields

$$4(g_{X_2} - g_{X_1}) \geq 2(\ell - 3)(g_{Y_1} - 1) - 3\ell/2,$$

and since $g_{Y_1} = g_{X_1} \geq 2$ we get $4(g_{X_2} - g_{X_1}) \geq \frac{\ell}{4} - 6$. The only remaining case is $B = 4$. In this case, the expression $2(\ell - 3)(g_{Y_1} - 1) - \sum_{P \in B_s} \ell/s_P$ in (6.4) is bigger than $\ell/4 - 6$

if $g_{Y_1} = g_{X_1} \geq 3$ or if $s_P \geq 4$ for some $P \in B_s$. Thus, we may assume that $g_{Y_1} = g_{X_1} = 2$ and there are four branch points of type $[2^{\ell/2}]$. The only ramification types which satisfy these conditions and Riemann–Hurwitz for $h : X_1 \to Y$ are

$$[2^{\ell/2}]^4, [1^{\ell-4}, 2^2]; \quad \text{or} \quad [2^{\ell/2}]^4, [1^{\ell-3}, 3]; \quad \text{or} \quad [2^{\ell/2}]^4, [1^{\ell-2}, 2], [1^{\ell-2}, 2].$$

By equality (6.3), in all three cases one has $4(g_{X_2} - g_{X_1}) > \ell/4 - 6$ for $\ell \geq 12$. □

Proof of Proposition 6.1 for $t \geq 3$. Let E_0 be the constant from Proposition 5.1. Note that we will pick $c_2 = 2$ and let $d_2 \geq \max\{4E_0, 1\}$ be a constant which will be determined by the proof. Since it suffices to prove the proposition when $2\ell - d_2 t^8 \geq 0$, we can assume $\ell \geq d_2 t^8/2 \geq \max\{t^8/2, 2E_0 t^4 + 1\}$. By (6.2), we have

$$2t!(g_{X_t} - g_{X_{t-1}}) \geq 2(\ell - 2t + 1)(g_{Y_{t-1}} - 1) - \sum_{P \in Y(\mathbb{K})} R_{\pi_t}(f_t^{-1}(P)).$$

Combining this inequality with the Riemann–Hurwitz formula for the natural projection $h_1^{t-1} : Y_{t-1} \to Y_1$ gives

$$\begin{aligned} 2t!(g_{X_t} - g_{X_{t-1}}) &\geq 2(\ell - 2t + 1)\frac{(\ell-1)!}{(\ell-t+1)!}(g_{Y_1} - 1) \\ &\quad + \sum_{P \in Y(\mathbb{K})} \Big((\ell - 2t + 1) R_{h_1^{t-1}}(h^{-1}(P)) - R_{\pi_t}(f_t^{-1}(P)) \Big). \end{aligned} \tag{6.6}$$

To show that the right hand side is positive and large we will cancel out the contribution $R_{\pi_t}(f_t^{-1}(P))$ using the former two terms. As $\ell \geq t^2$, we may apply Proposition 5.1, and Proposition 5.3, to obtain $R_{\pi_t}(f_t^{-1}(P)) \leq \binom{t}{2} R_{h_1^{t-1}}(h^{-1}(P)) + E_0 t^4 \frac{(\ell-2)!}{(\ell-t)!}$, for every point P of Y. Hence (6.6) gives

$$\begin{aligned} 2t!(g_{X_t} - g_{X_{t-1}}) &\geq 2(1-\varepsilon)\frac{(\ell-1)!}{(\ell-t)!}(g_{Y_1} - 1) - E_0 B t^4 \frac{(\ell-2)!}{(\ell-t)!} \\ &\quad + \sum_{P \in Y(\mathbb{K})} \left(\ell - 2t + 1 - \binom{t}{2} \right) R_{h_1^{t-1}}(h^{-1}(P)) \end{aligned} \tag{6.7}$$

where B denotes the number of branch points of h and $\varepsilon := t/(\ell - t + 1)$. Since $\ell \geq t^8/2$, we have $\ell - 2t + 1 > \binom{t}{2}$ and hence (6.7) gives

$$2t!(g_{X_t} - g_{X_{t-1}}) \geq 2(1-\varepsilon)\frac{(\ell-1)!}{(\ell-t)!}(g_{Y_1} - 1) - E_0 B t^4 \frac{(\ell-2)!}{(\ell-t)!}. \tag{6.8}$$

To cancel out the term $E_0 B t^4 (\ell-2)!/(\ell-t)!$, we divide the argument into two cases according to how large B is. First assume $B \leq 2\ell + C$, where $C := 2(E_0 t^4 + 1)/(1-\varepsilon)$. Set $\beta := 2E_0 + 1$. Note that as $\ell > 3t$, one has $\varepsilon < 1/2$ and hence $C/2 < 2E_0 t^4 + 3 < \beta t^4$. Assuming $g_{Y_1} \geq \beta t^4$, since $\beta t^4 > C/2$, since $B \leq 2\ell + C$ and $C(1-\varepsilon) = 2(1 + E_0 t^4)$, (6.8)

gives

$$\begin{aligned} 2t!(g_{X_t}-g_{X_{t-1}}) &\geq 2\frac{(\ell-1)!}{(\ell-t)!}(1-\varepsilon)\frac{C}{2}-E_0(2\ell+C)t^4\frac{(\ell-2)!}{(\ell-t)!} \\ &= 2\frac{(\ell-1)!}{(\ell-t)!}(E_0t^4+1)-E_0(2\ell+C)t^4\frac{(\ell-2)!}{(\ell-t)!} \\ &= \frac{(\ell-2)!}{(\ell-t)!}\Big(2\ell-2-2E_0t^4-E_0Ct^4\Big) > (2\ell-\gamma_1 t^8)\frac{(\ell-2)!}{(\ell-t)!} \end{aligned} \tag{6.9}$$

for some absolute constant $\gamma_1>0$.

Henceforth assume $B\geq 2\ell+C$. Since $2(g_{Y_1}-1)\geq -2\ell+B$ by the Riemann–Hurwitz formula for h, (6.8) gives

$$\begin{aligned} 2t!(g_{X_t}-g_{X_{t-1}}) \geq& \frac{(\ell-2)!}{(\ell-t)!}\Big((1-\varepsilon)(-2\ell+B)(\ell-1)-E_0Bt^4\Big) \\ =& \frac{(\ell-2)!}{(\ell-t)!}\Big(B\big((1-\varepsilon)(\ell-1)-E_0t^4\big)-2\ell(1-\varepsilon)(\ell-1)\Big). \end{aligned} \tag{6.10}$$

Since $B\geq 2\ell+C$, and $(1-\varepsilon)(\ell-1)>(\ell-1)/2>E_0t^4$, (6.10) gives

$$\begin{aligned} 2t!(g_{X_t}-g_{X_{t-1}}) \geq& \frac{(\ell-2)!}{(\ell-t)!}\Big((2\ell+C)\big((1-\varepsilon)(\ell-1)-E_0t^4\big)-2\ell(1-\varepsilon)(\ell-1)\Big) \\ =& \frac{(\ell-2)!}{(\ell-t)!}\Big(-2E_0t^4\ell+C(1-\varepsilon)(\ell-1)-CE_0t^4\Big) \end{aligned}$$

Since $C(1-\varepsilon)=2(1+E_0t^4)$, we get

$$2t!(g_{X_t}-g_{X_{t-1}}) \geq \frac{(\ell-2)!}{(\ell-t)!}\Big(2\ell-2-2E_0t^4-E_0Ct^4\Big) > (2\ell-\gamma_2 t^8)\frac{(\ell-2)!}{(\ell-t)!} \tag{6.11}$$

for some absolute constant $\gamma_2>0$. The result follows with $d_2:=\max\{\gamma_1,\gamma_2,1,4E_0\}$ from (6.9) and (6.11). □

7. Almost Galois ramification

In this section we prove severe restrictions on the ramification of a degree-ℓ covering $h:Y_1\to Y$ with monodromy group in $\{A_\ell,S_\ell\}$ for which the induced curve Y_2 has genus at most a constant multiple of ℓ. The argument in this section is based on the method introduced in [12].

We first show that the ramification indices over every point behave similarly to ramification in Galois extensions. More precisely, for every point P of Y, either (1) all but a bounded number of bounded elements in $E_h(P)$ equal a common value, or (2) $E_h(P)$ contains only a small number of small values. We use Setup 2.2.

Proposition 7.1. *There exists a constant λ_1 satisfying the following property. Let $\alpha>0$ be an integer, and $h:Y_1\to Y$ a covering of degree $\ell\geq\lambda_1\alpha^2$ with monodromy group $G\in\{A_\ell,S_\ell\}$, such that the quotient Y_2 of the Galois closure of h by a two point stabilizer of G satisfies $g_{Y_2}\leq\alpha\ell$. Then any point P of Y satisfies one of the following:*

(1) *there is some k with $1 \le k \le 6$ such that the number of h-preimages of P with ramification index k is at least $\ell/k - 2(\alpha+1)(k+1)$;*
(2) *for each k with $1 \le k \le 6$, the number of h-preimages of P with ramification index k is at most $4(\alpha+1)$.*

Proof. We pick λ_1 such that $\lambda_1\alpha^2 \ge 156(\alpha+1)(4\alpha+5)$. Suppose that (2) does not hold, so that there is an integer $k \le 6$ for which $E_h(P)$ contains more than $4(\alpha+1)$ copies of k. Let k be the smallest such integer. We will show that $E_h(P)$ contains at least $\ell/k - 2(\alpha+1)(k+1)$ copies of k, so that (1) holds. Let $h_1^2 : Y_2 \to Y_1$ be the natural projection. Combining Lemma 5.4 with the Riemann–Hurwitz formula for h_1^2 yields

$$\begin{aligned}\sum_{r_1,r_2\in E_h(P)} \big(r_1 - (r_1,r_2)\big) &= R_{h_1^2}(h^{-1}(P)) \le \sum_{Q\in Y(\mathbb{K})} R_{h_1^2}(h^{-1}(Q)) \\ &= 2\big(g_{Y_2} - 1 - (\ell-1)(g_{Y_1}-1)\big) \le 2\big(\alpha\ell - 1 + (\ell-1)\big) < 2(\alpha+1)\ell,\end{aligned} \tag{7.1}$$

where the second inequality holds because $g_{Y_2} \le \alpha\ell$ and $g_{Y_1} \ge 0$. Let m be the number of copies of k in $E_h(P)$, and let R be the sum of the elements in $E_h(P)$ which are less than k. By minimality of k, for each $k_0 < k$ there are at most $4(\alpha+1)$ copies of k_0 in $E_h(P)$, so that

$$R \le \sum_{k_0=1}^{k-1} 4(\alpha+1)k_0 = 2(\alpha+1)(k^2-k).$$

Restricting the left side of (7.1) to pairs (r_1, r_2) with $r_1 > r_2 = k$ yields

$$m \sum_{\substack{r\in E_h(P)\\ r>k}} (r - (r,k)) < 2(\alpha+1)\ell.$$

For any integer $r > k$, the value (r,k) is a proper divisor of r and hence is at most $r/2$, so that $r - (r,k) \ge r/2$ and thus

$$m\frac{\ell - km - R}{2} = m \sum_{\substack{r\in E_h(P)\\ r>k}} \frac{r}{2} \le m \sum_{\substack{r\in E_h(P)\\ r>k}} \big(r - (r,k)\big) < 2(\alpha+1)\ell.$$

Putting $d := 2(\alpha+1)(k^2-k)$ and $s := (\ell - d)/k$, we deduce that

$$km(s-m) = m(\ell - km - d) \le m(\ell - km - R) < 4(\alpha+1)\ell. \tag{7.2}$$

Let u be the unique element of $\{m, s-m\}$ such that $u \le s/2$. The hypothesis $\ell \ge \lambda_1\alpha^2 \ge 156(\alpha+1)(4\alpha+5)$ implies that $s > \max(\ell/(2k), 16(\alpha+1))$, so that $s - u \ge s/2 > \ell/(4k) > 0$ and thus by (7.2) we have

$$u < \frac{4(\alpha+1)\ell}{k(s-u)} < 16(\alpha+1) < s,$$

whence

$$ku < \frac{4(\alpha+1)\ell}{s-u} < \frac{4(\alpha+1)\ell}{s - 16(\alpha+1)} = \frac{4(\alpha+1)\ell k}{\ell - d - 16(\alpha+1)k}. \tag{7.3}$$

The hypothesis $\ell \geq \lambda_1 \alpha^2 \geq 156(\alpha+1)(4\alpha+5)$ implies that the right side of (7.3) is at most $(4\alpha+5)k$, so that $u < 4\alpha+5$. The definition of k implies that $m > 4(\alpha+1)$, so since $u \in \{m, s-m\}$ it follows that $u = s-m$. As in addition $u \leq 4(\alpha+1)$, one has

$$m \geq s-4(\alpha+1) = \frac{\ell-d}{k} - 4(\alpha+1) = \frac{\ell - 2(\alpha+1)(k^2-k)}{k} - 4(\alpha+1) = \frac{\ell}{k} - 2(\alpha+1)(k+1).$$

This shows that (1) holds, which completes the proof. □

Definition 7.2. Let α, ℓ be positive integers such that $\ell \geq \lambda_1 \alpha^2$, and let P be a point of Y. If there is any integer k with $1 \leq k \leq 6$ for which $E_h(P)$ contains at least $\ell/k - 2(\alpha+1)(k+1)$ copies of k then we define $m_h(P)$ to be the least such integer k. If there is no such integer k, and case (2) of Proposition 7.1 holds, then we define $m_h(P)$ to be ∞.

We define the *error* $\varepsilon_h(P)$ to be $2(\alpha+1)(m_h(P)+1)m_h(P)$ if $m_h(P) < \infty$ and $4(\alpha+1)\sum_{k=1}^{6} k = 84(\alpha+1)$ if $m_h(P) = \infty$; thus if $m_h(P) < \infty$ then $\varepsilon_h(P)$ is an upper bound on the sum of the elements of $E_h(P)$ different from $m_h(P)$, while if $m_h(P) = \infty$ then $\varepsilon_h(P)$ is an upper bound on the sum of the elements of $E_h(P)$ which are at most 6.

Corollary 7.3. *There exists a constant $\lambda_2 > 0$ satisfying the following property. Let $\alpha > 0$ be an integer, and $h : Y_1 \to Y$ a covering of degree $\ell \geq \lambda_2 \alpha^3$ and monodromy group A_ℓ or S_ℓ, such that $g_{Y_2} \leq \alpha\ell$. Let M_h denote the multiset of $m_h(P)$'s which are bigger than 1 (with P varying over all points of Y). Then $g_Y \leq 1$, and M_h is the empty set if $g_Y = 1$, and M_h is one of the following if $g_Y = 0$:*

- ∞, ∞
- $\infty, 2, 2$
- $3, 3, 3$
- $2, 3, 6$
- $2, 4, 4$
- $2, 2, 2, 2$.

Moreover, $g_{Y_1} \leq \alpha+1$, there are at most $2(\alpha+1)$ points P for which $m_h(P) = 1$, and the sum of the quantities $R_h(P)$ over all such points is at most $8(\alpha+1)^2$. There exists also an absolute constant $\nu > 0$ such that the number of preimages in Y_1 of each point P with $m_h(P) = \infty$ is at most $\nu\alpha^2$.

Proof. Let $h_1^2 : Y_2 \to Y_1$ the natural projection. By the Riemann–Hurwitz formula for h_1^2 and Lemma 5.4, we have

(7.4)

$$2(\alpha\ell+\ell-2) \geq 2(g_{Y_2} - \ell g_{Y_1} + \ell - 4) = \sum_{P \in Y(\mathbb{K})} R_{h_1^2}(h^{-1}(P)) = \sum_{P \in Y(\mathbb{K})} \sum_{r_1, r_2 \in E_h(P)} \big(r_1 - (r_1, r_2)\big).$$

For $\ell \geq \lambda_1\alpha^2$, Proposition 7.1 implies that if $m_h(P) = 1$ then

$$\begin{aligned}|R_{h_1^2}(h^{-1}(P)) - \ell R_h(P)| &= |\sum_{r_1,r_2\in E_h(P)} \big(r_1 - (r_1,r_2)\big) - \ell \sum_{r\in E_h(P)} (r-1)| \\ &\leq |\sum_{r_1,r_2\in E_h(P)\colon\, r_1,r_2>1} (r_1-(r_1,r_2)) - (\varepsilon_h(P)-1)\sum_{r\in E_h(P)}(r-1)| \\ &\leq \varepsilon_h(P)(\varepsilon_h(P)-1) < \delta\alpha^2\end{aligned}$$

for some absolute constant $\delta > 0$. In particular, $R_{h_1^2}(h^{-1}(P)) \geq \ell - \delta\alpha^2$ if P ramifies under h. Hence for $\ell \geq (2\alpha+3)\delta\alpha^2$, it follows from (7.4) that there are at most $2(\alpha+1)$ points P of Y which ramify under h and have $m_h(P) = 1$. By definition, for every point P with $m_h(P) = 1$, we have $R_h(P) \leq 4(\alpha+1)$, so the sum of this quantity over all such points P is at most $8(\alpha+1)^2$.

The Riemann–Hurwitz formula for h_1^2 implies that

$$g_{Y_1} - 1 \leq (g_{Y_2}-1)/(\ell-1) < \alpha+1,$$

for $\ell > \alpha - 2$. Thus, the Riemann–Hurwitz formula for h gives $\ell(g_Y-1) < g_{Y_1} - 1 < \alpha+1$, forcing $g_Y \leq 1$ for $\ell \geq \alpha+1$. Hence in total, the Riemann–Hurwitz formula for h gives

(7.5)
$$\begin{aligned}\Big|\sum_{P\colon\, m_h(P)>1} \big(\ell - |h^{-1}(P)|\big) - 2\ell(1-g_Y)\Big| &= \Big|2(g_{Y_1}-1) - \sum_{P\colon\, m_h(P)=1} R_h(P)\Big| \\ &< \max\{2(\alpha+1), 8(\alpha+1)^2+2\} = 8(\alpha+1)^2+2.\end{aligned}$$

If $m_h(P) < \infty$ then by definition $E_h(P)$ contains at least $\ell/m_h(P) - 2(\alpha+1)(m_h(P)+1)$ entries equal to $m_h(P)$, and hence $|E_h(P)|$ is at most $2(\alpha+1)(m_h(P)+1)(m_h(P)-1)$ and at least $\ell/m_h(P) - 2(\alpha+1)(m_h(P)+1)+1$. Thus, it is $\ell/m_h(P)$ up to a bounded constant depending on α:

$$\Big||E_h(P)| - \frac{\ell}{m_h(P)}\Big| < \max\big\{2(\alpha+1)(m_h(P)+1)+1, 2(\alpha+1)(m_h(P)+1)(m_h(P)-1)\big\}.$$

If $m_h(P) = \infty$, then this number of points is at least $\ell/7 - \varepsilon_h(P)$. Thus if $g_Y = 1$, there exists a constant $\lambda_3 > 0$ such that the condition (7.5) for $\ell \geq \lambda_3\alpha^2$ implies that $m_h(P) = 1$ for all points P of Y, as desired. If $g_Y = 0$, there exists a constant λ_4, such that the only ways to add up numbers of the form $\ell(1-1/m_h(P))$ (with $2 \leq m_h(P) \leq 6$) and numbers in the interval $[6\ell/7, \ell]$ for $\ell \geq \lambda_4\alpha^2$, and get a sum that differs from 2ℓ by a bounded constant depending only on α, are the familiar ones, namely $\ell+\ell$, $\ell+\ell/2+\ell/2$, $2\ell/3+2\ell/3+2\ell/3$, $\ell/2+2\ell/3+5\ell/6$, $\ell/2+3\ell/4+3\ell/4$, and $\ell/2+\ell/2+\ell/2+\ell/2$. Thus by picking the constant λ_2 so that

$$\lambda_2\alpha^3 \geq \max\{\lambda_1\alpha^2, (2\alpha+3)\delta\alpha^2, \alpha+1, \lambda_3\alpha^2, \lambda_4\alpha^2\},$$

we have shown that all but the last assertion of Corollary 7.3 hold for $\ell \geq \lambda_2\alpha^3$.

Finally, suppose that the values $m_h(P)$ bigger than 1 are $\infty, 2, 2$ so that $g_Y = 0$. Then (7.5) implies that the number of points of Y_1 lying over the point P with $m_h(P) = \infty$ is at most $\nu_1\alpha^2$ for some absolute constant $\nu_1 > 0$. Likewise if the $m_h(P)$'s bigger than 1 are

∞, ∞ then (7.5) implies that the number of preimages over both points P with $m_h(P) > 1$ is at most $\nu_2\alpha^2$ for some absolute constant $\nu_2 > 0$. Thus, the last assertion of Corollary 7.3 holds with $\nu := \max\{\nu_1, \nu_2\}$. □

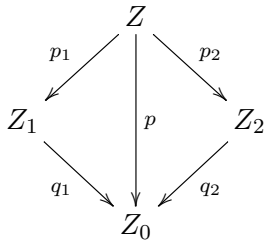
Definition 7.4. We say that a degree ℓ covering $h : Y_1 \to Y$ with monodromy group A_ℓ or S_ℓ has 2-point genus bound $\alpha\ell$ if $\ell \geq \lambda_2\alpha^3$, and $g_{Y_2} \leq \alpha\ell$. Corollary 7.3 then gives the possibilities for the values $m_h(P)$ for points P of Y.

The constants λ_2 and ν can be improved, at the cost of a lengthier proof and larger errors $\varepsilon_h(P)$.

8. Castelnuovo's inequality

We shall use Castelnuovo's inequality to prove that a covering has a 2-point genus bound, and hence ramification of almost Galois type.

Recall [44, Theorem 3.11.3] that given two coverings $q_i : Z_i \to Z_0$, for $i = 1, 2$, Casetlnuovo's inequality bounds the genus of a *minimal covering* $p : Z \to Z_0$ *which factors through* q_1 *and* q_2 [4], that is, a covering which factors as $p = p_i \circ q_i$ for coverings $p_i : Z \to Z_i$, $i = 1, 2$, such that p_1 and p_2 do not have a common factorization $p_i = p_i' \circ w$, $i = 1, 2$, with $\deg w > 1$.



Namely, it gives $g_Z \leq n_1 g_{Z_1} + n_2 g_{Z_2} + (n_1 - 1)(n_2 - 1)$, where $n_i := \deg p_i$, $i = 1, 2$.

We use the notation of Setup 2.2, so that the quotient by a stabilizer of a t-set (resp., t-tuple of distinct elements) is denoted by X_t (resp., Y_t).

Proposition 8.1. *Let $h : Y_1 \to Y$ be a covering of degree ℓ with monodromy group $G = A_\ell$ or S_ℓ. Let $2 \leq t \leq \ell/2$ be an integer, and $\alpha > 0$ a constant such that $g_{X_t} - g_{X_{t-1}} < \frac{\alpha}{\ell}\binom{\ell}{t}$. Then*

$$g_{Y_2} < \begin{cases} g_{Y_1}(\ell+1) + (\alpha+1)(\ell-1) & \text{if } t = 2 \\ \frac{1}{1-\varepsilon}\Big((t-1)g_{Y_1} + \binom{t}{2} + \alpha\Big)\ell & \text{if } t > 2, \end{cases}$$

where $\varepsilon := t/(\ell - t + 1)$.

Proof. As in Setup 2.2, let G act on a set $S = \{1, \dots, \ell\}$. Let $X_t^{(i)}$ denote the quotient of the Galois closure $\tilde{Y}_1$ by the subgroup $H_{i,t} \leq G$ of elements that fix $\{1, \dots, i\}$ pointwise, and stabilize $\{1, \dots, t\}$. In particular, $X_t^{(t-1)}$ is a t-point stabilizer and $X_t^{(0)}$ is a t-set

[4] Note that the curve Z can always be identified with an irreducible component of the (normalization) of the fiber product of q_1 and q_2.

stabilizer. Set $Y_t := X_t^{(t-1)}$ and $X_t := X_t^{(0)}$. Let $Y_{\{i\}}$ denote the quotient by the stabilizer $H_{\{i\}}$ of the element i, for $i \le t$.

Since G is t-transitive, $[H_{i-1,t} : H_{i,t}] = t-i+1$ and $[H_{\{i\}} : H_{i,t}] = \frac{(\ell-1)!}{(\ell-t)!(t-i)!}$ for $i \le t$. Since $H_{i-1,t} \cap H_{\{i\}} = H_{i,t}$ for $i = 1, \dots, t-1$, Castelnuovo's inequality gives

$$\begin{aligned} g_{X_t^{(i)}} &\le \frac{(\ell-1)!}{(\ell-t)!(t-i)!} g_{Y_{\{i\}}} + (t-i+1) g_{X_t^{(i-1)}} + \Big(\frac{(\ell-1)!}{(\ell-t)!(t-i)!} - 1 \Big)(t-i) \\ &< \frac{(\ell-1)!}{(\ell-t)!(t-i)!} g_{Y_{\{i\}}} + (t-i+1) g_{X_t^{(i-1)}} + \frac{(\ell-1)!}{(\ell-t)!(t-i-1)!}. \end{aligned} \tag{8.1}$$

For $t = 2$ and $i = 1$, as $X_1 = Y_1$ and $g_{X_2} - g_{X_1} \le \alpha(\ell-1)/2$, the first inequality in (8.1) gives

$$\begin{aligned} g_{Y_2} &\le (\ell-1) g_{Y_1} + 2 g_{X_2} + \ell - 2 = (\ell+1) g_{Y_1} + 2(g_{X_2} - g_{X_1}) + \ell - 2 \\ &< (\ell+1) g_{Y_1} + (\alpha+1)(\ell-1) - 1, \end{aligned}$$

as desired.

Hencefore we assume $t \ge 3$. Applying (8.1) iteratively for $i = t-1, \dots, 1$, using the fact that $g_{Y_{\{i\}}} = g_{Y_1}$ since G is transitive, we get

$$\begin{aligned} g_{Y_t} = g_{X_t^{(t-1)}} &< \frac{(\ell-1)!}{(\ell-t)!} g_{Y_1} + 2 g_{X_t^{(t-2)}} + \frac{(\ell-1)!}{(\ell-t)!} \\ &< 2\frac{(\ell-1)!}{(\ell-t)!} g_{Y_1} + 3! g_{X_t^{(t-3)}} + (1+2)\frac{(\ell-1)!}{(\ell-t)!} \\ &\vdots \\ &< (t-1)\frac{(\ell-1)!}{(\ell-t)!} g_{Y_1} + t! g_{X_t^{(0)}} + (1+\cdots+t-1)\frac{(\ell-1)!}{(\ell-t)!} \\ &= \frac{(\ell-1)!}{(\ell-t)!}\left((t-1) g_{Y_1} + \binom{t}{2} \right) + t! g_{X_t}. \end{aligned} \tag{8.2}$$

Since $t!(g_{X_t} - g_{X_{t-1}}) < \alpha \frac{(\ell-1)!}{(\ell-t)!}$, the inequality (8.2) yields

$$g_{Y_t} < \frac{(\ell-1)!}{(\ell-t)!}\left((t-1) g_{Y_1} + \binom{t}{2} + \alpha \right) + t! g_{X_{t-1}}. \tag{8.3}$$

By the Riemann–Hurwitz formula for the natural projections $\pi_{t-1} : Y_{t-1} \to X_{t-1}$ and $Y_t \to Y_{t-1}$, one has $(t-1)! \cdot (g_{X_{t-1}} - 1) \le g_{Y_{t-1}} - 1$ and $(\ell - t + 1)(g_{Y_{t-1}} - 1) \le g_{Y_t} - 1$. Hence (8.3) gives

$$(\ell-t+1)(g_{Y_{t-1}} - 1) \le g_{Y_t} - 1 < \frac{(\ell-1)!}{(\ell-t)!}\left((t-1) g_{Y_1} + \binom{t}{2} + \alpha \right) + t(g_{Y_{t-1}} - 1) + t! - 1,$$

or equivalently

$$(\ell - 2t + 1)(g_{Y_{t-1}} - 1) < \frac{(\ell-1)!}{(\ell-t)!}\left((t-1) g_{Y_1} + \binom{t}{2} + \alpha \right) + t! - 1. \tag{8.4}$$

Since $g_{Y_{t-1}} - 1 \geq \frac{(\ell-2)!}{(\ell-t+1)!}(g_{Y_2} - 1)$ by the Riemann–Hurwitz formula for the natural projection $Y_{t-1} \to Y_2$, (8.4) gives

$$g_{Y_2} \leq \frac{(\ell-t+1)!}{(\ell-2)!}(g_{Y_{t-1}} - 1) + 1 < \frac{1}{1-\varepsilon}\left((t-1)g_{Y_1} + \binom{t}{2} + \alpha\right)(\ell-1) + v, \tag{8.5}$$

where $v := \frac{(t!-1)(\ell-t)!}{(1-\varepsilon)(\ell-2)!}$. For $t \geq 3$ and $\ell \geq 2t$, a straight forward check shows that the right hand side of (8.5) is bounded by $\big((t-1)g_{Y_1} + \binom{t}{2} + \alpha\big)\ell/(1-\varepsilon)$, as desired. □

9. Ramification data of indecomposable coverings

The final step of the proof of Theorem 3.1 is determining whether there exists a covering with a given ramification data, also known as the Hurwitz problem. In this section, we provide conditions under which a given ramification data does not correspond to an indecomposable covering. The following lemma is an explicit version of the "translation" process in Guralnick–Shareshian [22, Proposition 2.0.16 and Corollary 2.0.17].

Lemma 9.1. *Let p be a rational prime and $h : \mathbb{P}^1 \to \mathbb{P}^1$ a covering whose monodromy group is noncyclic, nondihedral, and is not A_4. Let P_1, P_2, P_3 be points of $\mathbb{P}^1$. Then h is decomposable if at least one of the following conditions holds:*

1. *All entries in $E_h(P_1)$ and $E_h(P_2)$ are divisible by p;*
2. *All entries in $E_h(P_1)$ are divisible by p, and there is a total of exactly two odd entries in $E_h(P_2)$ and $E_h(P_3)$;*
3. *All entries of $E_h(P_1)$ are even and there is a total of exactly two entries coprime to 3 in $E_h(P_2)$ and $E_h(P_3)$.*

The proof uses the following version of Abhyankar's lemma. As in Section 8, we consider a minimal covering that factors through two given coverings.

Lemma 9.2. *Let $q_i : Z_i \to Z_0$, for $i = 1, 2$ be two coverings, and $p : Z \to Z_0$ a minimal covering that factors through q_1 and q_2, say as $p = p_i \circ q_i$, for $i = 1, 2$. Let Q_i be a point of Z_i, $i = 1, 2$ such that $q_1(Q_1) = q_2(Q_2)$. Then*

1. *for every point Q of Z such that $p_1(Q) = Q_1$ and $p_2(Q) = Q_2$, one has*
$$e_p(Q) = \operatorname{lcm}(e_{q_1}(Q_1), e_{q_2}(Q_2)) \text{ and } e_{p_2}(Q) = \frac{e_{q_1}(Q_1)}{\big(e_{q_1}(Q_1), e_{q_2}(Q_2)\big)}.$$
2. *If furthermore $\deg p = \deg q_1 \cdot \deg q_2$ then the number of points Q such that $p_1(Q) = Q_1$ and $p_2(Q) = Q_2$ is $\big(e_{q_1}(Q_1), e_{q_2}(Q_2)\big)$.*

Proof. Set $P := q_1(Q_1) = q_2(Q_2)$. Let $\tilde{p} : \tilde{Z} \to Z_0$ be a Galois closure of p and G its monodromy group. Writing $\tilde{p} = q_1 \circ u_1 = q_2 \circ u_2 = p \circ v$, we let $H_i \leq G$ be the monodromy group of u_i, $i = 1, 2$. Since p is minimal, the monodromy group of v is $H_1 \cap H_2$. Let $x \in G$ be a branch cycle of $\tilde{p}$ over P. By Section 2.1, there is a one to one correspondence between points Q of Z and orbits θ in $\mathrm{Orb}_{(H_1 \cap H_2)\backslash G}(x)$ such that $e_p(Q) = |\theta|$. Moreover as in Section 2.1, the image $p_i(Q)$ corresponds to the restriction of θ to an orbit in $\mathrm{Orb}_{H_i\backslash G}(x)$

for $i = 1, 2$. Let $\theta_i \in \mathrm{Orb}_{H_i \backslash G}(x)$ be the orbit corresponding to Q_i and $r_i := |\theta_i| = e_{q_i}(Q_i)$ for $i = 1, 2$.

Note that the natural map $\iota : (H_1 \cap H_2)\backslash G \to (H_1\backslash G) \times (H_2\backslash G)$ of G-sets is an injection. Identifying $(H_1 \cap H_2)\backslash G$ with its image, the orbit of any pair in $\theta_1 \times \theta_2$ has length $\mathrm{lcm}(r_1, r_2)$. Thus by the above correspondence, $e_p(Q) = |\theta| = \mathrm{lcm}(r_1, r_2)$ for every point Q of Z with $p_i(Q) = Q_i$, $i = 1, 2$, and hence

$$e_{p_2}(Q) = \frac{e_p(Q)}{e_{q_2}(Q_2)} = \frac{\mathrm{lcm}(r_1, r_2)}{r_2} = \frac{r_1}{(r_1, r_2)},$$

giving (1). If $\deg p = \deg q_1 \cdot \deg q_2$, then ι is surjective and hence the number of orbits is the number $r_1 r_2$ of pairs in $\theta_1 \times \theta_2$ divided by the length $\mathrm{lcm}(r_1, r_2)$ of each orbit, and hence is (r_1, r_2), giving (2). □

Remark 9.3. Let $h : Y_1 \to \mathbb{P}^1$ be a covering with Galois closure $\tilde{h} : \tilde{Y}_1 \to \mathbb{P}^1$. Then Lemma 9.2.(1) applied iteratively shows that $e_{\tilde{h}}(P)$ is the least common multiple of all entries in $E_h(P)$ for every point P in $\mathbb{P}^1$. Indeed, each such entry and hence their least common multiple divide $e_{\tilde{h}}(P)$. On the other hand, letting $G = \mathrm{Mon}(h)$ and H_1 a point stabilizer, $\tilde{h}$ is the minimal Galois covering which factors through the natural projections $h^\sigma : \tilde{Y}_1/H_1^\sigma \to \mathbb{P}^1$, $\sigma \in G$. Thus, Lemma 9.2.(1) implies that $e_{\tilde{h}}(P)$ is the least common multiple of $e_{h^\sigma}(Q_\sigma)$, $\sigma \in G$ for some points $Q_\sigma \in \tilde{Y}_1/H_1^\sigma$. As h^σ, $\sigma \in G$ are isomorphic coverings, $E_{h^\sigma}(P) = E_h(P)$ for $\sigma \in G$, and hence $e_{\tilde{h}}(P)$ is also the least common multiple of entries from $E_h(P)$.

To ensure the assumption of Lemma 9.2.(2) is satisfied, we shall use:

Lemma 9.4. *Let $q_i : Z_i \to Z_0$, $i = 1, 2$ be coverings with no common factorization $q_i = u \circ q_i'$, $i = 1, 2$ with $\deg u > 1$. If q_1 is Galois then the degree of a minimal covering p that factors through q_1 and q_2 is $\deg q_1 \cdot \deg q_2$.*

Proof. Let $\tilde{p} : \tilde{Z} \to Z_0$, u_1, u_2, v, G, H_1, and H_2 be as in the proof of Lemma 9.2. The minimality of p shows that monodromy group of v is $H_1 \cap H_2$. Since q_1 and q_2 have no common factorization, we have $G = \langle H_1, H_2 \rangle$. Since q_1 is Galois, H_1 is normal in G, and hence $G = H_1 H_2$. It follows that the natural map $(H_1 \cap H_2)\backslash G \to (H_1\backslash G) \times (H_2\backslash G)$ is an isomorphism, and hence $\deg p = [G : H_1 \cap H_2] = [G : H_1] \cdot [G : H_2] = \deg q_1 \cdot \deg q_2$. □

Proof of Lemma 9.1. Consider a Galois covering $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ such that in cases (1), (2), and (3), respectively, we have

(1) $E_\phi(P_j) = [p]$ for $j = 1, 2$, and $\mathrm{Mon}(\phi) \cong C_p$;
(2) $E_\phi(P_1) = [p^2]$, $E_\phi(P_j) = [2^p]$ for $j = 2, 3$, and $\mathrm{Mon}(\phi) \cong D_{2p}$;
(3) $E_\phi(P_1) = [2^6]$, $E_\phi(P_j) = [3^4]$ for $j = 2, 3$, and $\mathrm{Mon}(\phi) \cong A_4$.

Note that in each of the cases (1), (2), and (3), there exists a covering ϕ' with the described ramification type and monodromy, namely, X^p, $X^p + X^{-p}$, and $(X^4 + 8X)^3/(X^3 - 1)^3$, respectively. The covering ϕ is then obtained by composing ϕ with a linear fractional which sends the branch points of ϕ' to P_1, P_2, P_3.

Since h is indecomposable, either $\phi = h \circ \psi$ for some covering ψ, or h and ϕ have no common factor $\phi = w \circ \phi'$, $h = w \circ h'$, with $\deg w > 1$. The latter case contradicts the assumption that the monodromy group of h is noncyclic, nondihedral, and is not A_4.

Hencefore we assume ϕ and h have no common factor w as above. Let $p : Z \to \mathbb{P}^1$ be a minimal covering which factors through ϕ and h, say $p = \phi \circ \eta = h \circ \pi$. Then $\deg p = \deg \phi \cdot \deg h$ by Lemma 9.4. Hence, we may apply Lemma 9.2.(2) to compute the ramification of π in cases (1), (2), and (3), respectively, giving

(1) $R_\pi(h^{-1}(P_j)) = (p-1) \cdot |\{r \in E_h(P_j) : p \nmid r\}|$ for $j = 1, 2$;
(2) $R_\pi(h^{-1}(P_1)) = 2(p-1) \cdot |\{r \in E_h(P_1) : p \nmid r\}|$ and
$$R_\pi(h^{-1}(P_j)) = p \cdot |\{r \in E_h(P_j) : 2 \nmid r\}| \quad \text{for } j = 2, 3;$$
(3) $R_\pi(h^{-1}(P_1)) = 6 \cdot |\{r \in E_h(P) : 2 \nmid r\}|$ and
$$R_\pi(h^{-1}(P_j)) = 8 \cdot |\{r \in E_h(P_j) : 3 \nmid r\}| \quad \text{for } j = 2, 3.$$

Since $g_Z \geq 0$, Riemann–Hurwitz for π yields

$$\sum_{j=1}^{3} R_\pi(h^{-1}(P_j)) = \sum_{P \in \mathbb{P}^1(\mathbb{K})} R_\pi(h^{-1}(P)) \geq 2 \deg \pi - 2 = 2 \deg \phi - 2. \tag{9.1}$$

In case (1), (9.1) shows that the total number of coprime to p entries in $E_h(P_1)$ and $E_h(P_2)$ is at least two, contradicting (1).

In case (2), (9.1) gives

$$2(p-1) \cdot |\{r \in E_h(P_1) : p \nmid r\}| + p \cdot |\{\text{odd } r \in E_h(P_j), j = 2, 3\}| \geq 4p - 2. \tag{9.2}$$

By case (1), there exists at least one odd entry in $E_h(P_2)$ or in $E_h(P_3)$. Since $\sum_{r \in E_h(P_2)} r = \sum_{r \in E_h(P_3)} r \bmod 2$, there is an even number of such odd entries. Hence (9.2) shows that either there is an entry in $E_h(P)$ that is coprime to p, or the total number of odd entries in $E_h(P_2)$ and $E_h(P_3)$ is at least four, contradicting (2).

In case (3), (9.1) gives

$$6 \cdot |\{\text{odd } r \in E_h(P_1)\}| + 8 \cdot |\{r \in E_h(P_j) : j = 2, 3, \ r \text{ coprime to } 3\}| \geq 22. \tag{9.3}$$

By part (1) there exists at least one entry in $E_h(P_2)$ or $E_h(P_3)$ that is coprime to 3. Since $\sum_{r \in E_h(P_2)} r \equiv \sum_{r \in E_h(P_3)} r \pmod 3$, the number of such coprime entries is at least 2. Hence (9.3) shows either that there is an odd entry in $E_h(P_1)$, or the total number of coprime to 3 entries in $E_h(P_2)$ and $E_h(P_3)$ is at least three, contradicting (3). □

The following proposition gives the list of ramification types in case (4) of Theorem 1.1, and is then used to restrict ramification types of indecomposable polynomials.

Proposition 9.5. *Let $h : Y_1 \to \mathbb{P}^1$ be an indecompsable covering with Galois closure of genus 0 or 1. Then the ramification type and monodromy group of h appear in Table 9.1.*

Lemma 9.6. *Let Z be a curve of genus 1 and let O be a point of Z. Then the automorphism group $\mathrm{Aut}(Z)$ is the semidirect product $T \rtimes A^\times$, where T is the group of translations by points on the elliptic curve (Z, O), and $A^\times$ is the group of automorphisms of Z fixing O.*

TABLE 9.1. Ramification types of indecomposable coverings $h : Y_1 \to \mathbb{P}^1$ of degree ℓ and Galois closure $\tilde{h} : \tilde{Y}_1 \to \mathbb{P}^1$ of genus $g_{\tilde{Y}_1} \leq 1$. In each case, we assume ℓ satisfies the necessary congruence conditions to make all exponents integral. In all cases p denotes a prime.

	Ramification types for h	$g_{\tilde{Y}_1}$	$\mathrm{Mon}(h)$
$(A1)$	$[\ell], [\ell]$	0	C_ℓ, ℓ *prime*
$(A2)$	$[1, 2^{(\ell-1)/2}], [1, 2^{(\ell-1)/2}], [\ell]$	0	$D_{2\ell}, \ell$ *prime*
$(A3)$	$[1^2, 2^4], [1, 3^3], [5^2]$	0	A_5
$(A4)$	$[1^2, 2^2], [3^2], [1, 5]$	0	A_5
$(A5)$	$[1, 2^2], [1^2, 3], [5]$	0	A_5
$(A6)$	$[1^2, 2], [1, 3], [4]$	0	S_4
$(A7)$	$[2^2], [1, 3], [1, 3]$	0	A_4
$(E1)$	$[1, 2^{(\ell-1)/2}]$ *four times*	1	$D_{2\ell}, \ell$ *prime*
$(E2)$	$[1, 3^{(\ell-1)/3}], [1, 3^{(\ell-1)/3}], [1, 3^{(\ell-1)/3}]$	1	$C_\ell \rtimes C_3, \ell$ *prime*
$(E3)$	$[1, 3^{(\ell-1)/3}], [1, 3^{(\ell-1)/3}], [1, 3^{(\ell-1)/3}]$	1	$(C_p)^2 \rtimes C_3, \ell = p^2$, $p \equiv 2$ *mod* 3
$(E4)$	$[1, 2^{(\ell-1)/2}], [1, 4^{(\ell-1)/4}], [1, 4^{(\ell-1)/4}]$	1	$C_\ell \rtimes C_4, \ell$ *prime*
$(E5)$	$[1, 2^{(\ell-1)/2}], [1, 4^{(\ell-1)/4}], [1, 4^{(\ell-1)/4}]$	1	$(C_p)^2 \rtimes C_4, \ell = p^2$, $p \equiv 3$ *mod* 4
$(E6)$	$[1, 2^{(\ell-1)/2}], [1, 3^{(\ell-1)/3}], [1, 6^{(\ell-1)/6}]$	1	$C_\ell \rtimes C_6, \ell$ *prime*
$(E7)$	$[1, 2^{(\ell-1)/2}], [1, 3^{(\ell-1)/3}], [1, 6^{(\ell-1)/6}]$	1	$(C_p)^2 \rtimes C_6, \ell = p^2$, $p \equiv 5$ *mod* 6
$(Q1)$	$[2], [2], [2], [2]$	1	C_2
$(Q2)$	$[3], [3], [3]$	1	C_3

Proof. Considering the group structure $(Z, +, O)$ on Z, the claim follows since every automorphism $f : Z \to Z$ can be written as a composition $\sigma_{f(O)} \circ g$, where $\sigma_{f(O)} \in T$ is the translation map $P \mapsto P + f(O)$ and $g := \sigma_{f(O)}^{-1} \circ f$ is an automorphism fixing O. □

Remark 9.7. (1) The normal subgroup T is independent of the choice of base point O, namely it is the subgroup consisting of all fixed point free automorphisms of Z.

(2) The endomorphism ring $A := \mathrm{End}(Z)$ is isomorphic either to $\mathbb{Z}$ or to an order in an imaginary quadratic field, so that the multiplicative group $A^\times$ is the group μ_v of v-th roots of unity for some $v \in \{2, 4, 6\}$, cf. [43, Section III.9 and III.10] and [43, Example III.4.4]. Moreover, up to isomorphism there is a unique elliptic curve Z for which $A^\times \cong \mu_v$, for $v = 4, 6$. The cardinality of the kernel of an endomorphism $\eta \in A$ equals the norm of its corresponding element in $\mathbb{Z}$ or in the imaginary quadratic field.

(3) For a finite subgroup $H \leq \mathrm{Aut}(Z)$, the quotient Z/H is of genus 1 if and only if $H \leq T$, and is of genus 0 otherwise.

(4) Every covering $h : Y_1 \to Y$ of genus 1 curves is Galois with abelian monodromy group [43, Theorem 4.10(c)].

Proof of Proposition 9.5. Let $G = \mathrm{Mon}(h)$ and $H_1 \leq G$ a point stabilizer, so that H_1 is maximal in G. Let $\tilde{h} : \tilde{Y}_1 \to \mathbb{P}^1$ be the Galois closure of h, and $n := \deg \tilde{h}$. At first assume $g_{\tilde{Y}_1} = 0$. The ramification and mondromy groups of genus 0 Galois coverings $\tilde{h} : \tilde{Y}_1 \to \mathbb{P}^1$ is well-known as a consequence of Klein's classification of finite subgroups of $\mathrm{Aut}(\mathbb{P}^1) \cong \mathrm{PGL}_2(\mathbb{K})$. Namely, it is one of $[n], [n]$ with $G \cong C_n$; $[n/2, n/2], [2^{n/2}], [2^{n/2}]$ with $G \cong D_{2n}$; $[2^6], [3^4], [3^4]$ with $G \cong A_4$; $[2^{12}], [3^8], [4^6]$ with $G \cong S_4$; and $[2^{30}], [3^{20}], [5^{12}]$ with $G \cong A_5$. As H_1 is maximal and does not contain a normal subgroup of G, we have $n = \ell$ is prime and $H_1 = 1$ if $G \cong C_\ell$; and $n = 2\ell$ with ℓ an odd prime, and H_1 is generated by a reflection if $G \cong D_{2\ell}$; and $H_1 \cong A_3$ if $G \cong A_4$; and $H_1 \cong S_3$ if $G \cong S_4$; and $H_1 \cong A_4$, or D_{10}, or S_3 if $G \cong A_5$. By Abhyankar's lemma 9.3, $e_{\tilde{h}}(P)$ is the least common multiple of entries in $E_h(P)$, for every point P of $\mathbb{P}^1$. For each possibility of G and H_1, the latter constraint and the Riemann–Hurwitz formula force the ramification of h to be one of types A in Table 9.1.

Henceforth assume $g_{\tilde{Y}_1} = 1$. Let $T \lhd \mathrm{Aut}(\tilde{Y}_1)$ be the abelian normal subgroup from Lemma 9.6, and let $N := G \cap T$, so that $N \lhd G$. First consider the case where $g_{Y_1} = 1$, in which case Remark 9.7.(3) implies that $H_1 \subseteq N$ and that N is a proper subgroup of G. As H_1 is maximal, we have $H_1 = N$. Hence the natural projection $\phi : \tilde{Y}_1/N \to \mathbb{P}^1$ factors through h. Since ϕ is Galois as $N \lhd G$, and $\tilde{h}$ is the Galois closure of h, it follows that $N = 1$. It follows that the natural map $G \to \mathrm{Aut}(\tilde{Y}_1)/T$ is injective, and hence that $G \cong \mu_v$ for $v \in \{2, 3, 4, 6\}$ by Remark 9.7.(2). In particular h is Galois. As h is indecomposable, we get $G \cong C_2$ or C_3. By the Riemann–Hurwitz formula for h, its ramification is (Q1) or (Q2) in Table 9.1.

Henceforth assume $g_{Y_1} = 0$. Remark 9.7 then implies that H_1 is not contained in N. As H_1 is maximal, this gives $G = N \cdot H_1$. Let $\psi : \tilde{Y}_1/(H_1 \cap N) \to \mathbb{P}^1$ be the natural projection. Since $H_1 \cap N \lhd H_1$ as $N \lhd G$, and since $H_1 \cap N \lhd N$ as N is abelian, we have $H_1 \cap N \lhd N \cdot H_1 = G$, so that ψ is Galois. Since ψ factors through h, and $\tilde{h}$ is the Galois closure of h, it follows that $H_1 \cap N = 1$, and hence $G = N \cdot H_1 = N \rtimes H_1$.

We next describe H_1 and N using the decomposition in Lemma 9.6. As N consists of the fixed point free automorphisms in G by Remark 9.7.(1), it follows that a generator of H_1 and hence H_1 has a fixed point O in $\tilde{Y}_1$, so that $(\tilde{Y}_1, O)$ is an elliptic curve, and H_1 is a subgroup of the group $A^\times$ of automorphisms fixing O. Let $Z_1 := \tilde{Y}_1/N$, let $\eta : \tilde{Y}_1 \to Z_1$ be the natural projection, and set $O' = \eta(O)$. Then (Z_1, O') is an elliptic curve by Remark 9.7.(3), and η is an isogeny.

(9.4)
$$\begin{array}{ccc} \tilde{Y}_1 & \xrightarrow{\eta} & Z_1 \\ {\scriptstyle \rho_1}\downarrow & & \downarrow{\scriptstyle \rho_2} \\ Y_1 & \xrightarrow[h]{} & \mathbb{P}^1 \end{array}$$

By Remark 9.7.(2), we can identify the endomorphism ring $A := \mathrm{End}(\tilde{Y}_1)$ either with $\mathbb{Z}$ or with an order in an imaginary quadratic field, so that the subgroup H_1 of $A^\times$ identifies with a multiplicative subgroup of v-th roots of unity μ_v for $v \in \{2, 3, 4, 6\}$. Let B be the

subring $\mathbb{Z}[\mu_v]$ of A. Since H_1 is maximal, there are no nontrivial intermediate subgroups between H_1 and $N \rtimes H_1$, and hence no nontrivial proper subgroups of N that are invariant under conjugation by H_1. In particular, N is p-torsion for some prime p. Thus, the action of H_1 gives N the structure of an irreducible p-torsion B-module.

First consider the case where p is coprime to $v = |H_1|$. Let $[-1] \in A^\times$ be the map $P^{[-1]} = -P$, and $\sigma_Q \in T$ the translation $P^\sigma_Q = P + Q$ for $P, Q \in \tilde{Y}_1$. If $v = 2$, then $H_1 = \mu_2 = \langle [-1] \rangle$, and $\sigma_P^{[-1]} = [-1] \circ \sigma_P \circ [-1] = \sigma_{-P}$ for $\sigma_P \in N$. As N is an irreducible $\mathbb{Z}$-module, in this case $|N| = p$, so that $G = N \rtimes H_1 \cong D_{2p}$.

For $v = 3$, since N is an irreducible p-torsion B-module, we have

- $N \cong B/pB$ as a B-module if $p \equiv 2 \bmod 3$, so that $N \cong C_p^2$ as an abelian group;
- $N \cong B/\pi B$ as a B-module if $p \equiv 1 \bmod 3$, where π is an irreducible element in B of norm p, so that $N \cong C_p$ as an abelian group.

Similarly, one obtains a description of the B-module N for $v = 6$ and 4, according to whether the ideal (p) is prime or not in B, giving the groups G in cases E of Table 9.1.

Next assume p divides $v = |H_1|$, so that $p = 2$ or 3. If $p = 2$ and v is even, then $[-1] \in H_1$ as it fixes O, and $\sigma_P^{[-1]} = \sigma_{-P} = \sigma_P$ for every point P in N. Hence $[-1]$ is in the center of G, so that the natural projection $\tilde{Y}_1/[-1] \to \mathbb{P}^1$ is Galois, and factors through h as $[-1] \in H_1$, contradicting the choice of $\tilde{h}$ as the Galois closure of h. Assume $p = 3$ and $3 \,|\, v$. Since an element of order 3 fixes a nontrivial subgroup of $T[3]$ (in any action), and every subgroup of $T[3]$ is invariant under conjugation by $[-1]$, the B-module $T[3]$ is reducible. Since $N \leq T[3]$ is irreducible, $N \cong C_3$ as an abelian group. As an element of order 3 acts trivially on C_3, we get that $\mu_3 \leq H_1$ is in the center of G. It follows that the natural projection $\tilde{Y}_1/\mu_3 \to \mathbb{P}^1$ is Galois, and factors through h, contradicting the choice of $\tilde{h}$ as the Galois closure of h.

Henceforth we may assume p is coprime to v. We next determine the ramification types in each possibility for H_1. If $v = 2$, then the ramification points of the natural projection $\rho_1 : \tilde{Y}_1 \to Y_1$ (resp., $\rho_2 : Z_1 \to \mathbb{P}^1$) are the fixed points of the involution $[-1] \in H_1$ (resp., $[-1] \in \mathrm{Aut}(Z_1)$), that is, the four 2-torsion points of $\tilde{Y}_1$ (resp., Z_1). Since η is of odd degree it is injective on 2-torsion points and hence maps the ramification points of ρ_1 to the ramification points of ρ_2. Since η is unramified, the multiplicativity of ramification indices in (9.4) implies that $e_h(\rho_1(Q)) = e_{\rho_2}(\eta(Q))/e_{\rho_1}(Q)$ for every point Q of $\tilde{Y}_1$. As ρ_1 and ρ_2 both have four ramification points, and $\deg h$ is odd as p is odd, this forces the ramification of h to be type (E1).

If $v > 2$, we identify $\tilde{Y}_1$ with the unique elliptic curve E whose automorphism group contains μ_v, cf. Remark 9.7.(2). Note that as H_1 preserves $\ker \eta$, it also acts on Z_1 by $\eta(P)^\sigma := \eta(P^\sigma)$ for $\sigma \in H_1$, $P \in \tilde{Y}_1$. Since this action is faithful, and preserves O', the automorphism group of the elliptic curve Z_1 also contains μ_v, and hence we also identify Z_1 with E. As H_1 preserves the fibers of $h \circ \rho_1$, it also preserves the fibers of ρ_2. As in addition $\deg \rho_1 = \deg \rho_2$, the map ρ_2 is also the quotient map by the same subgroup μ_v of automorphisms of E.

TABLE 9.2. Ramification data that does not correspond to a covering with monodromy group A_ℓ or S_ℓ.

$F1.N1$	$[1^2, 2^{(\ell-2)/2}], [2^{\ell/2}]$ *thrice*, $[2, 1^{\ell-2}]$;
$F1.N2$	$[1, 3, 2^{(\ell-4)/2}], [2^{\ell/2}]$ *thrice*;
$F1.N3$	$[1^2, 4, 2^{(\ell-6)/2}], [2^{\ell/2}]$ *thrice*;
$F1.N4$	$[4, 2^{(\ell-4)/2}], [1^2, 2^{(\ell-2)/2}], [2^{\ell/2}]$ *twice*;
$F4.N1$	$[2^{\ell/2}], [2, 3^{(\ell-2)/3}], [1^2, 6^{(\ell-2)/6}]$;
$I2.N1$	$[\ell], [4, 2^{(\ell-4)/2}], [2^{\ell/2}]$;
$I2.N2$	$[\ell], [2^{\ell/2}], [2^{\ell/2}], [2, 1^{\ell-2}]$.

A point Q of E is then a ramification point of order e under ρ_1 if and only if e is the maximal integer for which Q is fixed by an e-th root of unity z in A. Computing $|\ker(1-z)|$ for $z \in \mu_v$ via Remark 9.7.(2), we get that the ramification of ρ_i is $[3], [3], [3]$ if $v = 3$, and $[2^2], [4], [4]$ if $v = 4$, and $[2^3], [3^2], [6]$ if $v = 6$, for $i = 1, 2$. In particular, $|\ker(1-z)|$ is of order prime to ℓ, and hence the map η maps this kernel injectively to itself. In particular, if Q is a ramification point of ρ_1, then $\eta(Q)$ is a ramification point of ρ_2 with $e_{\rho_1}(Q) = e_{\rho_2}(\eta(Q))$. Since in addition $e_h(\rho_1(Q)) = e_{\rho_2}(\eta(Q))/e_{\rho_1}(Q)$ as η is unramified for every point Q of $\tilde{Y}_1$, the ramification type of h is forced to be one of the types (E2)-(E7) in Table 9.1.

□

Corollary 9.8. *Let $h : Y_1 \to \mathbb{P}^1$ be an indecomposable covering with branch points $P_1, \dots, P_r$. If the multiset $\{\mathrm{lcm}(E_h(P_i)) : i = 1, \dots, r\}$ is one of $\{2, 2, 2, 2\}$, $\{3, 3, 3\}$, $\{2, 4, 4\}$, $\{2, 3, 6\}$, then the monodromy group of h is solvable.*

Proof. Let $\tilde{h} : \tilde{Y}_1 \to \mathbb{P}^1$ be the Galois closure of h. By Abhyankar lemma 9.3, $e_{\tilde{h}}(P)$ is the least common multiple of the entries in $E_h(P)$ for every point P. Thus, the Riemann–Hurwitz formula for $\tilde{h}$ gives $g_{\tilde{Y}_1} = 1$. Thus, $\mathrm{Mon}(h)$ is solvable by Proposition 9.5. □

Lemmas 9.1 and 9.5 suffice to rule out all ramification data we shall encounter with the exception of the ones appearing in the following lemma.

Lemma 9.9. *There is no degree ℓ covering with monodromy group A_ℓ or S_ℓ whose ramification type appears in Table 9.2.*

The proof of Lemma 9.9 is given in Section 11.

10. PROOF OF THEOREM 3.1

We start by deriving Theorem 3.1 from the following propositions which deal with the case of ramification of almost Galois type. The propositions are separated according to the cases $t = 2$ and $t \geq 3$. We use the notation of Setup 2.2, so that for a covering $h : Y_1 \to Y$,

the quotient by the stabilizer of a t-set (resp., t-tuple of distinct elements) is denoted by X_t (resp., Y_t).

Proposition 10.1. *For every integer $\alpha > 0$, there exist constants $c_{2,\alpha}, d_{2,\alpha} > 0$ satisfying the following property. For every covering $h : Y_1 \to Y$ of degree ℓ with monodromy group A_ℓ or S_ℓ, and 2-point genus bound $\alpha\ell$, either $g_{X_2} - g_{X_1} > c_{2,\alpha}\ell - d_{2,\alpha}$ or $g_{Y_1} = 0$ and the ramification type of h appears in Table 4.1.*

Proposition 10.2. *There exists an absolute constant $c_4 > 0$, and for every integer $\beta_1 > 0$ a constant $d_{4,\beta_1} > 0$ satisfying the following property. Let $k \geq 2$ and $t \geq 3$ be integers. If $h : Y_1 \to Y$ is a covering of degree $\ell \geq 2t$ with monodromy group A_ℓ or S_ℓ, and 2-point genus bound $\alpha\ell$ for $\alpha = \beta_1 t^k$, then*

$$g_{X_t} - g_{X_{t-1}} > (c_4\ell - d_{4,\beta_1} t^{2(k+1)}) \frac{\binom{\ell}{t}}{\binom{\ell}{2}}.$$

Proof of Theorem 3.1. Let β, c_2, d_2 be the constants from Proposition 6.1, let c_3, d_3 be the constants from Proposition 8.1, and let λ_2 be the constant from Corollary 7.3. Set $\beta_1 := \lceil \beta/(1 - 10^{-6}) \rceil + 1$.

We shall define constants $c, d > 0$ such that for every degree ℓ covering $h : Y_1 \to Y$ with monodromy group A_ℓ or S_ℓ and integer $2 \leq t \leq \ell/2$ satisfying

$$g_{X_t} - g_{X_{t-1}} \leq (c\ell - dt^{15}) \frac{\binom{\ell}{t}}{\binom{\ell}{2}}, \tag{10.1}$$

one has $t = 2$ and the ramification of h is in Table 4.1.

We pick $0 < c \leq \min\{1/2, c_2, c_3, c_{2,3}, c_{2,\beta_1}, c_4\}$, and let $d \geq \max\{1, d_2, d_3, d_{2,3}, d_{4,\beta_1}\}$ be sufficiently large so that $dt^{15}/c \geq \max\{3^3\lambda_2, \lambda_2(\beta_1 t^5)^3\}$ for every $2 \leq t \leq \ell/2$. Since $c \leq c_2$ and $d \geq d_2$, the theorem follows from Proposition 6.1 if $g_{Y_1} \geq 2$ and $t = 2$, or if $g_{Y_1} \geq \beta t^4$ and $t > 2$. Hencefore assume that $g_{Y_1} \leq \beta t^4$ if $t > 2$, and $g_{Y_1} \leq 1$ if $t = 2$. We may also assume that $c\ell - dt^{15} \geq 0$ and hence that $\ell \geq dt^{15}/c \geq \max\{2t^{15}, 3^3\lambda_2, \lambda_2(\beta_1 t^5)^3\}$. As $c \leq 1/2$ and $d \geq 1$ we have:

$$g_{X_t} - g_{X_{t-1}} \leq (c\ell - dt^{15}) \frac{\binom{\ell}{t}}{\binom{\ell}{2}} < \frac{1}{\ell}\binom{\ell}{t}.$$

Thus, Proposition 8.1 with $\alpha = 1$ gives

$$\begin{aligned} &g_{Y_2} < g_{Y_1}(\ell + 1) + 2(\ell - 1) \quad \text{for } t = 2, \text{ and} \\ &g_{Y_2} < \frac{1}{1 - \varepsilon}\left((t-1)g_{Y_1} + \binom{t}{2} + 1\right)\ell \quad \text{for } t \geq 3, \end{aligned} \tag{10.2}$$

where $\varepsilon := t/(\ell - t + 1)$. Since $\ell \geq 2t^{15}$, we have $\varepsilon < 10^{-6}$ for $t \geq 3$. Thus, the bound $g_{Y_1} \leq \beta t^4$ and (10.2) give $g_{Y_2} < \beta_1 t^5 \ell$ for $t \geq 3$. Since $g_{Y_1} \leq 1$ for $t = 2$, in this case (10.2) gives $g_{Y_2} < 3\ell$. Since in addition $\ell \geq \lambda_2 \alpha^3$ for $\alpha = 3$ if $t = 2$, and for $\alpha = \beta_1 t^5$ if $t \geq 3$, we deduce that h has 2-point genus bound $\alpha\ell$. Since $c \leq \min\{c_{2,3}, c_{4,\beta_1}\}$ and $d \geq \max\{d_{2,3}, d_{4,\beta_1}\}$, the theorem follows from Proposition 10.1 with $\alpha = 3$ and Proposition 10.2 with $\alpha = \beta t^k$ and $k = 5$. □

The proof of Proposition 10.1 relies on the following estimates of the contributions $R_{h_1^2}(P)$, $P \in Y(\mathbb{K})$, for the natural projection $h_1^2 : Y_2 \to Y_1$. For fixed $\alpha > 0$, we write $A = B + O_\alpha(1)$ for expressions A, B to denote that there exists a constant c_α depending only on α such that $|A - B| \le c_\alpha$ for all values of A, B. Let ν be the constant from Corollary 7.3.

Lemma 10.3. *Fix $\alpha > 0$. Let $h : Y_1 \to Y$ be a degree ℓ cover with monodromy group A_ℓ or S_ℓ and 2-point genus bound $\alpha\ell$. Let P be a point of Y, and $m := m_h(P)$. If $m < \infty$, then $R_{h_1^2}(P) = S_h(P) + O_\alpha(1)$, where $S_h(P)$ is*

$$\begin{aligned}
&\ell R_h(P) && \text{if } m = 1;\\
&\ell\Big(\frac{\ell}{2} - |E_h(P)| + |\{r \in E_h(P) : 2 \nmid r\}|\Big) && \text{if } m = 2;\\
&\ell\Big(\frac{\ell}{3} - |E_h(P)| + \frac{4}{3}|\{r \in E_h(P) : 3 \nmid r\}|\Big) && \text{if } m = 3;\\
&\ell\Big(\frac{\ell}{4} - |E_h(P)| + |\{r \in E_h(P) : r \equiv 2 \pmod 4\}| + \frac{3}{2}|\{r \in E_h(P) : 2 \nmid r\}|\Big) && \text{if } m = 4;\\
&\ell\Big(\frac{\ell}{6} - |E_h(P)| + |\{r \in E_h(P) : r \equiv 3 \pmod 6\}| + \frac{4}{3}|\{r \in E_h(P) : r \equiv \pm 2 \pmod 6\}|\\
&\quad + \frac{5}{3}|\{r \in E_h(P) : r \equiv \pm 1 \pmod 6\}|\Big) && \text{if } m = 6.
\end{aligned}$$

If $m = \infty$, then either $E_h(P) = [\ell/u, \dots, \ell/u]$ (in which case $R_{h_1^2}(P) = 0$) or $R_{h_1^2}(P)$ is at least $\ell/(2\nu\alpha^2)$.

Proof. First consider the case $m < \infty$. Since $\mathrm{Mon}(h) = A_\ell$ or S_ℓ, and since the sum of the entries of h different from m is at most $\varepsilon_h(P) = O_\alpha(1)$, Lemma 5.4 gives

$$\begin{aligned}
R_{h_1^2}(P) &= \sum_{r_1, r_2 \in E_h(P), r_1 \ne m} \big(r_1 - (r_1, r_2)\big) + \sum_{r_1, r_2 \in E_h(P), r_1 = m} \big(m - (m, r_2)\big)\\
&= \frac{\ell}{m}\Big(\sum_{r_1 \in E_h(P)} \big(r_1 - (r_1, m)\big) + \sum_{r_2 \in E_{h_1}(P)} \big(m - (m, r_2)\big)\Big) + O_\alpha(1)\\
&= \frac{\ell}{m} \sum_{r \in E_h(P)} \big(r + m - 2(r, m)\big) + O_\alpha(1).
\end{aligned}$$

Evaluating the latter sum for each of the possibilities for a finite m gives the desired estimates for $R_{h_1^2}(P)$.

Let $u := |E_h(P)|$. If $m = \infty$ and $E_h(P) \ne [\ell/u, \dots, \ell/u]$, then Lemma 6.3.(2) implies that $R_{h_1^2}(P) \ge \ell/(2u)$. The claim follows in this case since $u \le \nu\alpha^2$ by Corollary 7.3. □

Proof of Proposition 10.1. As in Lemma 10.3, write $A = B + O_\alpha(1)$ (resp., $A \ge B + O_\alpha(1)$) to denote that $|A - B|$ is bounded (resp. $A - B$ is bounded from below) by a constant depending only on α.

We divide the proof into cases according to the possible multisets

$$M_h := \{m_h(P) > 1 : P \in Y(\mathbb{K})\}.$$

By Corollary 7.3, the set M_h is one of the following: (I1) $\{\infty,\infty\}$; (I2) $\{\infty,2,2\}$; (F1) $\{2,2,2,2\}$; (F2) $\{3,3,3\}$; (F3) $\{2,4,4\}$; (F4) $\{2,3,6\}$; or (F5) $\emptyset$. Moreover, the corollary implies $g_{Y_1} \le \alpha+1$, and also that $g_Y = 0$ in all cases but (F5) where $g_Y = 1$.

It suffices to prove that for some constants $c_{2,\alpha}, d_{2,\alpha} > 0$, either $g_{X_2} > c_{2,\alpha}\ell - d_{2,\alpha}$ or the ramification of h appears in Table 4.1. In each case we add a constraint on $c_{2,\alpha}$ and $d_{2,\alpha}$, and determine the ramification types of h for which $g_X \le c_{2,\alpha}\ell - d_{2,\alpha}$. The proposition then follows by taking $c_{2,\alpha}$ and $d_{2,\alpha}$ which satisfy the constraints in each case. Since it suffices to prove the proposition when $c_{2,\alpha}\ell - d_{2,\alpha} \ge 0$, by requiring $d_{2,\alpha}/c_\alpha > \nu^2\alpha^4$ we may assume $\ell > \nu^2\alpha^4$.

Case I1: Assume $m_h(P_1) = m_h(P_2) = \infty$ for two points P_1, P_2 of Y, and $m_h(P) = 1$ for any other point P of Y.

Let $u = u_{P_1} := |E_h(P_1)|$ and $v = v_{P_2} := |E_h(P_2)|$. Note that u and v are both less than the bound $\nu\alpha^2$ from Corollary 7.3. By (6.3) with $g_Y = 0$ and $g_{Y_1} = O_\alpha(1)$, and by Lemma 10.3, one has

(10.3)

$$\begin{aligned} 4(g_{X_2}-1) &= 2\ell(g_{Y_1}-1) + \ell \sum_{P\neq P_1,P_2} R_h(P) + \sum_{j=1}^{2} \sum_{r_1,r_2\in E_h(P_j)} \big(r_1 - (r_1,r_2)\big) + O_\alpha(1) \\ &\ge \ell\Big(2(g_{Y_1}-1) + \sum_{P\neq P_1,P_2} R_h(P) + \epsilon_h\Big) + O_\alpha(1), \end{aligned}$$

for $\epsilon_h = 1/(2\nu\alpha^2)$ whenever $E_h(P_1) \neq [\ell/u,\dots,\ell/u]$ or $E_h(P_2) \neq [\ell/v,\dots,\ell/v]$, and for $\epsilon_h = 0$ otherwise. On the other hand, the Riemann–Hurwitz formula for h gives

$$\sum_{P\neq P_1,P_2} R_h(P) = 2(g_{Y_1}-1) + u + v. \tag{10.4}$$

Substituting the latter into (10.3) gives

$$4g_{X_2} \ge 4\ell(g_{Y_1}-1) + (u+v+\epsilon_h)\ell - B_\alpha, \tag{10.5}$$

for some constant B_α depending only on α. Multiplying the latter inequality by $2\nu\alpha^2$, we get that all summands are integers, except perhaps $2\nu\alpha^2 B_\alpha$. Thus choosing $d_{2,\alpha}$ to be larger than $2\nu\alpha^2 B_\alpha$, and $c_{2,\alpha} < 1/(8\nu\alpha^2)$, the condition $g_{X_2} \le c_{2,\alpha}\ell - d_{2,\alpha}$ and (10.5) force $0 \ge 4(g_{Y_1}-1) + u + v + \epsilon_h$, or equivalently $u+v \le 4(1-g_{Y_1}) - \epsilon_h$.

It follows that $g_{Y_1} = 0$. Moreover, if $u+v = 4$ then $\varepsilon_h = 0$ and hence $E_h(P_1) = [\ell/u,\dots,\ell/u]$, and $E_h(P_2) = [\ell/v,\dots,\ell/v]$. In this case, since $\ell > \nu^2\alpha^4 \ge uv$ the number $\ell/(uv)$ is greater than 1 and divides the greatest commond divisor of all entries of $E_h(P_1)$ and $E_h(P_2)$, contradicting the indecomposability of h by Lemma 9.1.(1). Hence $u+v \le 3$. If $u = v = 1$ then $E_h(P_1) = E_h(P_2) = [\ell]$, contradicting the indecomposability of h by Lemma 9.1.(1). We may therefore assume without loss of generality that $u = 1$ and $v = 2$. Then (10.4) gives $\sum_{P\neq P_1,P_2} R_h(P) = 1$, showing that h has a single branch point

Q different from P_1, P_2, and moreover $E_h(Q) = [2, 1, \dots, 1]$. Put $E_h(P_2) = [a, \ell - a]$. Since h is indecomposable, Lemma 9.1.(1) shows that $(a, \ell) = 1$. Thus, the ramification type of h corresponding to P_1, P_2, Q is $[\ell], [a, \ell - a], [2, 1, \dots, 1]$, with $(a, \ell) = 1$, corresponding to type $I1.1$ in Table 4.1.

Case I2: Assume that $m_h(P_0) = \infty, m_h(P_1) = m_h(P_2) = 2$ for points P_0, P_1, P_2 of Y, and $m_h(P) = 1$ for all other points P of Y. Denote $u = u_{P_0} := |E_h(P_0)|$ and $O := |\{r \in E_h(P_i) : r \text{ is odd}, i = 1, 2\}|$. Note that O is even. By (6.3) and Lemma 10.3 one has

$$\begin{aligned} 4g_{X_2} = 2\ell(g_{Y_1} - 1) + \sum_{r_1, r_2 \in E_h(P_0)} \big(r_1 - (r_1, r_2)\big) + \ell \sum_{P \neq P_1, P_2} R_h(P) \\ + \ell \sum_{i=1}^{2} \Big(-\frac{1}{2} + \frac{\ell}{2} - |E_h(P_i)| + |\{\text{odd } r \in E_h(P_i)\}| \Big) + O_\alpha(1). \end{aligned} \tag{10.6}$$

On the other hand the Riemann–Hurwitz formula for h gives

$$2(g_{Y_1} - 1) + u = \sum_{P \neq P_1, P_2} R_h(P) + \sum_{i=1}^{2} \Big(\frac{\ell}{2} - |E_h(P_i)| \Big). \tag{10.7}$$

Substituting (10.7) into (10.6) and applying Lemma 10.3 we get

$$\begin{aligned} 4g_{X_2} &= 4\ell(g_{Y_1} - 1) + \sum_{r_1, r_2 \in E_h(P_0)} \big(r_1 - (r_1, r_2)\big) + (u - 1)\ell + O\ell + O_\alpha(1) \\ &\geq 4\ell(g_{Y_1} - 1) + \epsilon_h \ell + (u - 1)\ell + O\ell + O_\alpha(1), \end{aligned} \tag{10.8}$$

for $\epsilon_h = 1/(2\nu\alpha^2)$ whenever $E_h(P_0) \neq [\ell/u, \dots, \ell/u]$ and for $\epsilon_h = 0$ otherwise. Thus, by taking $d_{2,\alpha}$ to be sufficiently large and $0 < c_{2,\alpha} < 1/(8\nu\alpha^2)$, the assumption $g_{X_2} \leq c_{2,\alpha}\ell - d_{2,\alpha}$ and (10.8) force

$$4(1 - g_{Y_1}) + 1 - \epsilon_h \geq u + O. \tag{10.9}$$

Hence $g_{Y_1} \leq 1$. First consider the case $g_{Y_1} = 1$ in which (10.9) gives $u = 1$, $\epsilon_h = 0$, and $O = 0$. The only ramification type of h satisfying the latter constraints and (10.7) are types I2.N1, I2.N2 in Table 9.2. These do not correspond to any covering by Lemma 9.9.

Now assume $g_{Y_1} = 0$. In this case (10.9) gives $u + O \leq 5 - \epsilon_h$. Since h is indecomposable, Lemma 9.1.(1) shows that at least one of $E_h(P_i)$, $i = 1, 2$, contains an odd number. Since the sum of entries of $E_h(P_1)$ has the same parity as that of $E_h(P_2)$, the number O is even, and hence $O \geq 2$. It follows from (10.9) that $u \leq 3$.

If $u = 1$, then $E_h(P_0) = [\ell]$, and hence $\varepsilon_h = 0$, and (10.8) and (10.9) become equalities. It follows that $O = 4$. Moreover, if ℓ is even $E_h(P_i), i = 1, 2$ do not consist of even entries, by Lemma 9.1. The ramification types of h satisfying these constraints and (10.7) correspond, over P_0, P_1, P_2 and possibly another branch point Q, to types I2.1-I2.8 in Table 4.1.

If $u = 2$, since O is even and nontrivial by Lemma 9.1.(1), by (10.9) we have $O = 2$. Write $E_h(P_0) = [a, \ell - a]$ and let $d := (a, \ell)$. If $d > 1$, Lemma 9.1.(2) applied with a prime p dividing d contradicts the indecomposability of h. Thus $d = (a, \ell) = 1$. The only

ramification types of h which satisfy these constraints and (10.7) are types I2.9-I2.15 in Table 4.1 corresponding to the points P_0, P_1, P_2 and possibly another point Q.

It remains to treat the case $u = 3$. In this case (10.9) is necessarily an equality with $O = 2$ and $\epsilon_h = 0$, forcing $E_h(P_0) = [\ell/3, \ell/3, \ell/3]$. Since $\ell > 3$, Lemma 9.1.(2) applied with a prime dividing $\ell/3$ contradicts the indecomposability of h.

Case F1: Assume $m_h(P_i) = 2$ for four points $P_i, i = 1, 2, 3, 4$ of Y, and $m_h(P) = 1$ for all other points of Y. Then (6.3) and Lemma 10.3 give

$$\begin{aligned} 4(g_{X_2} - 1) = 2\ell(g_{Y_1} - 1) + \ell\Big(-2 + \sum_{j=1}^{4}\Big(\frac{\ell}{2} - |E_h(P_j)| + |\{\text{odd } r \in E_h(P_j)\}|\Big)\Big) \\ + \ell \sum_{P \neq P_1,\dots,P_4} R_h(P) + O_\alpha(1). \end{aligned} \tag{10.10}$$

On the other hand the Riemann–Hurwitz formula for h gives

$$2(g_{Y_1} - 1) = \sum_{j=1}^{2}\Big(\frac{\ell}{2} - |E_h(P_j)|\Big) + \sum_{P \neq P_1,\dots,P_4} R_h(P).$$

Substituting the latter equality into the former gives

$$4(g_{X_2} - 1) = 4\ell(g_{Y_1} - 1) + \ell\Big(-2 + \sum_{j=1}^{4}|\{\text{odd } r \in E_h(P_j)\}|\Big) + O_\alpha(1).$$

Hence for sufficiently large $d_{2,\alpha}$ and $c_{2,\alpha} < 1/4$, the latter equality and the assumption $g_{X_2} \leq c_{2,\alpha}\ell - d_{2,\alpha}$ force

$$|\{\text{odd } r \in E_h(P_j), j = 1, \dots, 4\}| = 4(1 - g_{Y_1}) + 2. \tag{10.11}$$

Hence $g_{Y_1} \leq 1$. If $g_{Y_1} = 1$, there are exactly two odd entries among $E_h(P_j)$, for $j = 1, \dots, 4$. The only possible ramification types of h which satisfy these constraints and the Riemann–Hurwitz formula for h are types F1.N1-F1.N4 in Table 9.2. These ramification types do not correspond to any covering by Lemma 9.9.

Assume $g_{Y_1} = 0$, in which case there is a total of 6 odd entries in $E_h(P_j)$, for $j = 1, \dots, 4$, by (10.11). Since h is indecomposable, $E_h(P_j)$ can have no odd entries for at most one point among $P_1, \dots, P_4$, by Lemma 9.1.(1). The ramification types of h satisfying these constraints and the Riemann–Hurwitz formula for h are types F1.1-F1.9 in Table 4.1.

Case F2: Assume $m_h(P_j) = 3, j = 1, 2, 3$ for three points P_1, P_2, P_3 of Y, and $m_h(P) = 1$ for all other points P of Y. By (6.3) and Lemma 10.3 one has

$$\begin{aligned} 4(g_{X_2} - 1) =& 2\ell(g_{Y_1} - 1) + \ell\sum_{j=1}^{3}\Big(\frac{\ell}{3} - |E_h(P_j)| + \frac{4}{3}|\{r \in E_h(P_j) : 3 \nmid r\}|\Big) \\ &+ \ell \sum_{P \neq P_1,P_2,P_3} R_h(P) + O_\alpha(1). \end{aligned} \tag{10.12}$$

The Riemann–Hurwitz formula for h gives

$$-2=\sum_{j=1}^{3}\Big(\frac{\ell}{3}-|E_h(P_j)|\Big)+\sum_{P\neq P_1,P_2,P_3}R_h(P).$$

Substituting the latter equality into (10.12) gives:

$$4(g_{X_2}-1)=4\ell(g_{Y_1}-1)+\frac{4\ell}{3}\sum_{j=1}^{3}|\{r\in E_h(P_j)\colon 3\nmid r\}|+O_\alpha(1).$$

When $d_{2,\alpha}$ is sufficiently large and $c_{2,\alpha}<1/4$, this equality and the assumption $g_{X_2}\le c_{2,\alpha}\ell-d_{2,\alpha}$ force

$$4(1-g_{Y_1})=\frac{4}{3}\sum_{j=1}^{3}|\{r\in E_h(P_j)\colon 3\nmid r\}|. \tag{10.13}$$

In particular $g_{Y_1}\le 1$, and if $g_{Y_1}=1$ then the ramification type of h is $[3^{\ell/3}]$ thrice, contradicting $\mathrm{Mon}(h)=A_\ell$ or S_ℓ by Corollary 9.8. Assume $g_{Y_1}=0$. Then (10.13) shows that there are a total of three coprime to 3 entries in $E_h(P_j)$, for $j=1,2,3$. Since h is indecomposable, at most one point has all indices divisible by 3 by Lemma 9.1.(1). The only ramification types satisfying these constraint and the Riemann–Hurwitz formula for h is $[1,3^{(n-1)/3}]$ thrice, contradicting $\mathrm{Mon}(h)=A_\ell$ or S_ℓ, by Lemma 9.8.

Case F3: Assume $m_h(P_0)=2$, $m_h(P_1)=m_h(P_2)=4$ for points P_0,P_1,P_2 of Y, and $m_h(P)=1$ for all other points P of Y. By (6.3) and Lemma 10.3 one has

$$\begin{aligned}4g_{X_2}=2\ell(g_{Y_1}-1)+\ell\big(\frac{\ell}{2}-|E_h(P_0)|+|\{\text{odd } r\in E_h(P_0)\}|-\frac{1}{2}\big)+\ell\sum_{P\neq P_0,P_1,P_2}R_h(P)\\ +\ell\sum_{i=1}^{2}\Big(-\frac{1}{2}+\frac{\ell}{4}-|E_h(P_i)|+|\{r\in E_h(P_i)\colon r\equiv 2 \pmod 4\}|\\ +\frac{3}{2}|\{\text{odd } r\in E_h(P_i)\}|\Big)+O_\alpha(1).\end{aligned} \tag{10.14}$$

The Riemann–Hurwitz formula for h gives

$$2(g_{Y_1}-1)=\Big(\frac{\ell}{2}-|E_h(P_0)|\Big)+\sum_{P\neq P_0,P_1,P_2}R_h(P)+\sum_{i=1}^{2}\Big(\frac{\ell}{4}-|E_h(P_i)|\Big).$$

Substituting the latter into (10.14) gives

$$\begin{aligned}4g_{X_2}=&4\ell(g_{Y_1}-1)+\ell|\{\text{odd } r\in E_h(P_0)\}|+\ell\sum_{i=1}^{2}\Big(|\{r\in E_h(P_i)\colon r\equiv 2 \pmod 4\}|\\ &+\frac{3}{2}|\{\text{odd } r\in E_h(P_i),i=1,2\}|\Big)-\ell+O_\alpha(1).\end{aligned} \tag{10.15}$$

Note that since the total number of odd entries in $E_h(P_i), i=1,2$ is even, the sum on the right hand side of the above equality is an integer. Hence for sufficiently large $d_{2,\alpha}$ and for $c_{2,\alpha}<1/4$ we get

$$\begin{aligned} 5-4g_{Y_1} = &|\{\text{odd } r\in E_h(P_0)\}|+|\{r\in E_h(P_i)\colon r\equiv 2 \pmod 4, i=1,2\}| \\ &+\frac{3}{2}|\{\text{odd } r\in E_h(P_i), i=1,2\}|. \end{aligned} \tag{10.16}$$

Hence $g_{Y_1}\le 1$. If $g_{Y_1}=1$, there is no ramification type of h which satisfies (10.16) and the Riemann–Hurwitz formula for h. Assume $g_{Y_1}=0$. Note that since h is indecomposable, Lemma 9.1.(1) implies that the total number of odds in $E_h(P_i), i=1,2$, is at least two (recall it is even). Moreover, if ℓ is even then there are at least four odd numbers in $E_h(P_0), E_h(P_1), E_h(P_2)$ (since at least two of these contain at least two odd numbers). The only ramification types of h which satisfy these constraints and the Riemann–Hurwitz formula for h are types F3.1-F3.3 over the points P_0, P_1, P_2.

Case F4: Assume $m_h(P_1)=2, m_h(P_2)=3, m_h(P_3)=6$ for points P_1, P_2, P_3 of Y and that $m_h(P)=1$ for all other points of Y. By (6.3) and Lemma 10.3 one has

$$\begin{aligned} 4g_{X_2} = &2\ell(g_{Y_1}-1)+\ell\Big(-\frac{1}{2}+\frac{\ell}{2}-|E_h(P_1)|+|\{\text{odd } r\in E_h(P_1)\}|\Big) \\ &+\ell\sum_{P\neq P_1,P_2,P_3} R_h(P)+\ell\Big(\frac{\ell}{3}-|E_h(P_2)|+\frac{4}{3}|\{r\in E_h(P_2)\colon 3\nmid r\}|\Big) \\ &+\ell\Big(-\frac{1}{6}+\frac{\ell}{6}-|E_h(P_3)|+|\{r\in E_h(P_3)\colon r\equiv 3 \pmod 6\}| \\ &\quad+\frac{4}{3}|\{r\in E_h(P_3)\colon r\equiv \pm 2 \pmod 6\}| \\ &\quad+\frac{5}{3}|\{r\in E_h(P_3)\colon r\equiv \pm 1 \pmod 6\}|\Big)+O_\alpha(1). \end{aligned} \tag{10.17}$$

The Riemann–Hurwitz formula for h gives

$$2(g_{Y_1}-1)=\Big(\frac{\ell}{2}-|E_h(P_1)|\Big)+\sum_{P\neq P_1,P_2,P_3} R_h(P)+\Big(\frac{\ell}{3}-|E_h(P_2)|\Big)+\Big(\frac{\ell}{6}-|E_h(P_3)|\Big).$$

Substituting the latter into (10.17) we get

$$\begin{aligned} 4g_{X_2} = &4\ell(g_{Y_1}-1)-2\ell/3+\ell\Big(|\{\text{odd } r\in E_h(P_1)\}|+\frac{4}{3}|\{r\in E_h(P_2)\colon (r,3)=1\}| \\ &+|\{r\in E_h(P_3)\colon r\equiv 3 \pmod 6\}|+\frac{4}{3}|\{r\in E_h(P_3)\colon r\equiv \pm 2 \pmod 6\}| \\ &+\frac{5}{3}|\{r\in E_h(P_3)\colon r\equiv \pm 1 \pmod 6\}|\Big)+O_\alpha(1). \end{aligned} \tag{10.18}$$

Note that the right hand side is a third of an integer. Hence for sufficiently large $d_{2,\alpha}$ and for $c_{2,\alpha} < 1/12$, (10.18) and the assumption $g_{X_2} \le c_{2,\alpha}\ell - d_{2,\alpha}$ force

$$\begin{aligned}\frac{14}{3} - 4g_{Y_1} = |\{\text{odd } r \in E_h(P_1)\}| + \frac{4}{3}|\{r \in E_h(P_i) : (r,3) = 1\}| \\ + |\{r \in E_h(P_3) : r \equiv 3 \pmod 6\}| \\ + \frac{4}{3}|\{r \in E_h(P_3) : r \equiv \pm 2 \pmod 6\}| \\ + \frac{5}{3}|\{r \in E_h(P_3) : r \equiv \pm 1 \pmod 6\}|.\end{aligned} \tag{10.19}$$

If $g_{Y_1} = 1$, there is no ramification type of h which satisfies (10.19) and the Riemann–Hurwitz formula for h. Assume $g_{Y_1} = 0$. Note that since h is indecomposable, Lemma 9.1.(1) implies that there are odd entries in at least one of $E_h(P_1), E_h(P_3)$ and there are coprime to 3 entries in at least one of $E_h(P_2), E_h(P_3)$. The only ramification types of h over P_1, P_2, P_3 which satisfy these restrictions and the Riemann–Hurwitz formula for h are types F4.1–F4.6 and the following:

$[2^{n/2}]$	$[3^{n/3}]$	$[1^2, 4, 6^{(n-6)/6}]$
$[1^2, 2^{(n-2)/2}]$	$[3^{n/3}]$	$[2, 4, 6^{(n-6)/6}]$
$[1, 2^{(n-1)/2}]$	$[3^{n/3}]$	$[2, 3, 4, 6^{(n-9)/6}]$
$[2^{n/2}]$	$[1, 2, 3^{(n-3)/3}]$	$[3^2, 6^{(n-6)/6}]$
$[2^{n/2}]$	$[1, 3^{(n-1)/3}]$	$[3^2, 4, 6^{(n-10)/6}]$
$[2^{n/2}]$	$[2, 3^{(n-2)/3}]$	$[2, 3^2, 6^{(n-8)/6}]$
$[2^{n/2}]$	$[3^{n/3}]$	$[2, 3^2, 4, 6^{(n-12)/6}]$
$[2^{n/2}]$	$[2, 3^{(n-2)/3}]$	$[1^2, 6^{(n-2)/6}]$

(10.20)

The first three types in (10.20) do not occur as a ramification type of a covering by Lemma 9.1.(2), the next four do not occur by Lemma 9.1.(3), and the last is type F4.N1 which does not appear by Lemma 9.9.

Case F5: Assume $m_h(P) = 1$ for all points P of Y, and that $g_Y = 1$. Then (6.3) and Lemma 10.3 give

$$4(g_{X_2} - 1) = 2\ell(g_{Y_1} - 1) + \ell \sum_{P \ne P_1,\dots,P_4} R_h(P) + O_\alpha(1). \tag{10.21}$$

Hence for sufficiently large $d_{2,\alpha}$ and $c_{2,\alpha} < 1/4$, (10.21) and the assumption $g_{X_2} \le c_{2,\alpha}\ell - d_{2,\alpha}$ force $2(1 - g_{Y_1}) = \sum_{P \in Y(\mathbb{K})} R_h(P)$. On the other hand the Riemann–Hurwitz formula for h gives $2(g_{Y_1} - 1) = \sum_{P \in Y(\mathbb{K})} R_h(P)$. These two equalities force $g_{Y_1} = 1$ and h is unramified, contradicting the assumption that $\mathrm{Mon}(h) = A_\ell$ or S_ℓ, by Remark 9.7.(4). □

The proof for $t \ge 3$ relies on the following bound on the Riemann–Hurwitz contribution $R_{\pi_t}(f_t^{-1}(P))$, where $\pi_t : Y_t \to X_t$ and $f_t : X_t \to Y$ are the natural projections. Let E_0 (resp. ν) be the constant from Proposition 5.1 (resp. Corollary 7.3).

Lemma 10.4. *Let $h : Y_1 \to Y$ be a degree ℓ covering with monodromy group A_ℓ or S_ℓ and 2-point genus bound $\alpha\ell$. Let $3 \le t \le \ell/2$ an integer. Assume P is a point of Y with error $\varepsilon_h(P) < \ell/2 - 1$. Then*

$$R_{\pi_t}(f_t^{-1}(P)) < \begin{cases} \left((\varepsilon_h(P) + \frac{1}{2})\binom{t}{2} + E_0 t^4\right)\frac{(\ell-2)!}{(\ell-t)!} & \text{if } m_h(P) < \infty \\ \left(\nu\alpha^2\binom{t}{2} + E_0 t^4\right)\frac{(\ell-2)!}{(\ell-t)!} & \text{if } m_h(P) = \infty. \end{cases}$$

Proof. Let $m := m_h(P)$. We estimate the main term of Proposition 5.1.(2). Let $\mathrm{Mon}(h)$ act on the set S. Let $x \in \mathrm{Mon}(h)$ be a branch cycle over P, and let

$$M_h := \sum_{(\theta_1,\dots,\theta_{t-1})\in O_{t-1}} \frac{\hat r_1 \cdots \hat r_{t-1}}{\mathrm{lcm}(r_1,\dots,r_{t-1})},$$

where $r_i := |\theta_i|$, and $\hat r_i$ is r_i minus the number of $j < i$ with $\theta_j = \theta_i$ for $i = 1,\dots,t-1$, and O_{t-1} is the set of tuples $(\theta_1,\dots,\theta_{t-1})$ of orbits of x such that r_1 is even and $v_2(r_1) > v_2(r_k)$ for $k > 1$. Note that since $\mathrm{lcm}(r_1,\dots,r_{t-1}) \ge r_1 = \hat r_1$, we have

$$\begin{aligned} M_h &\le \sum_{(\theta_1,\theta_2,\dots,\theta_{t-1})\in O_{t-1}} \hat r_2 \cdots \hat r_{t-1} \\ &= \sum_{\substack{(\theta_1,\dots,\theta_{t-1})\in O_{t-1} \\ r_1 \ne m}} \hat r_2 \cdots \hat r_{t-1} + \sum_{\substack{(\theta_1,\dots,\theta_{t-1})\in O_{t-1} \\ r_1 = m}} \hat r_2 \cdots \hat r_{t-1}. \end{aligned} \tag{10.22}$$

We bound each of the summands on the right hand side, noting that the last sum is zero if $m = \infty$.

Fix $2 \le k \le t-1$ and orbits $\theta_1,\dots,\theta_{k-1}$, and let U_{θ_1} be the set of orbits θ of x such that $v_2(|\theta|) < v_2(r_1)$. We claim that the sum $\sum_{\theta_k \in U_{\theta_1}} \hat r_k$ is bounded by $\ell - k$ if $r_1 \ne m$, and by $\varepsilon_h(P) - (k-2)$ if $r_1 = m$. Indeed, note that the sum $\sum_{\theta_k\in U_k} r_k$ is at most $\ell - r_1$, and at most $\varepsilon_h(P)$ if further $r_1 = m$. Since in addition $r_1 \ge 2$, and $\sum_{\theta_k\in U_{\theta_1}} |\{1 < j < k : \theta_j = \theta_k\}| = k-2$, we get

$$\begin{aligned} \sum_{\theta_k\in U_{\theta_1}} \hat r_k &= \sum_{\theta_k\in U_{\theta_1}} r_k - \sum_{\theta_k\in U_{\theta_1}} |\{1 < j < k : \theta_j = \theta_k\}| \\ &\le \begin{cases} \varepsilon_h(P) - (k-2) & \text{if } r_1 = m \\ \ell - 2 - (k-2) & \text{otherwise,} \end{cases} \end{aligned}$$

proving the claim.

Applying the claim for $k = t-1, t-2, \dots, 2$, we get

$$\begin{aligned} \sum_{(\theta_1,\dots,\theta_{t-1})\in O_{t-1}, r_1\ne m} \hat r_2 \cdots \hat r_{t-1} &\le (\ell - t + 1) \sum_{(\theta_1,\dots,\theta_{t-2})\in O_{t-2}, r_1\ne m} \hat r_2 \cdots \hat r_{t-2} \\ &\le \cdots \le \sum_{\theta_1\in O_1, r_1\ne m} \frac{(\ell-2)!}{(\ell-t)!} = \tilde N_h \frac{(\ell-2)!}{(\ell-t)!}, \end{aligned}$$

where $\tilde{N}_h$ is the number of even entries in $E_h(P)$ that are different from m. Similarly if $r_1 = m < \infty$, applying the claim for $k = t-1, \dots, 2$ gives

$$\sum_{(\theta_1,\dots,\theta_{t-1})\in O_{t-1}, r_1=m} \hat{r}_2 \cdots \hat{r}_{t-1} \le \sum_{\theta_1 \in O_1, r_1=m} \frac{\varepsilon_h(P)!}{(\varepsilon_h(P)-(t-2))!} \le \frac{\ell}{m} \frac{\varepsilon_h(P)!}{(\varepsilon_h(P)-(t-2))!},$$

where $(\varepsilon_h(P)-t+2)!$ is defined to be 1 if $\varepsilon_h(P) \le t-2$. Note that in case $r_1 = m$, we have $m \ge 2$ since r_1 is even. In total, estimating each of summands in (10.22), we get

$$M_h < \begin{cases} \tilde{N}_h \frac{(\ell-2)!}{(\ell-t)!} + \frac{\ell}{2} \frac{\varepsilon_h(P)!}{(\varepsilon_h(P)-t+2)!} & \text{if } m < \infty \\ \tilde{N}_h \frac{(\ell-2)!}{(\ell-t)!} & \text{if } m = \infty. \end{cases}$$

Since $t \ge 3$, and $\varepsilon_h(P) + 1 < \ell/2$, a straightforward check shows that $\ell \frac{\varepsilon_h(P)!}{(\varepsilon_h(P)-t+2)!} < (\varepsilon_h(P)+1)\frac{(\ell-2)!}{(\ell-t)!}$. Note that $\tilde{N}_h \le \varepsilon_h(P)/2$ if m is finite, and $\tilde{N}_h \le \nu\alpha^2$ if $m = \infty$, by Corollary 7.3. In total we get $M_h < (\varepsilon_h(P)+1/2)\frac{(\ell-2)!}{(\ell-t)!}$ if m is finite, and $M_h < \nu\alpha^2 \frac{(\ell-2)!}{(\ell-t)!}$ if $m = \infty$. Thus Proposition 5.1 gives

$$R_{\pi_t}(f_t^{-1}(P)) < \binom{t}{2} M_h + E_0 t^4 \frac{(\ell-2)!}{(\ell-t)!} < \begin{cases} ((\varepsilon_h(P)+\frac{1}{2})\binom{t}{2} + E_0 t^4)\frac{(\ell-2)!}{(\ell-t)!} & \text{if } m < \infty \\ (\nu\alpha^2\binom{t}{2} + E_0 t^4)\frac{(\ell-2)!}{(\ell-t)!} & \text{if } m = \infty. \end{cases} \quad \square$$

Proof of Proposition 10.2. Denote $R_{\pi_t} := \sum_{P\in Y(\mathbb{K})} R_{\pi_t}(f_t^{-1}(P))$. By inequality (6.2) of Remark 6.2, and the Riemann–Hurwitz formula the natural projection $Y_{t-1} \to Y_2$, we get:

$$\begin{aligned} 2t!(g_{X_t} - g_{X_{t-1}}) &\ge 2(\ell - 2t + 1)(g_{Y_{t-1}} - 1) - R_{\pi_t} \\ &\ge 2(1-\varepsilon)\frac{(\ell-2)!}{(\ell-t)!}(g_{Y_2} - 1) - R_{\pi_t}, \end{aligned} \tag{10.23}$$

where $\varepsilon := t/(\ell - t + 1)$. We show that R_{π_t} is bounded by a constant times $t^{2k+2}\frac{(\ell-2)!}{(\ell-t)!}$ while the first term on the right hand side is at least a linear factor in ℓ times $\frac{(\ell-2)!}{(\ell-t)!}$.

Step I: *Bounding R_{π_t} using Lemma 10.4.* Let $\varepsilon_h(P)$ denote the error over a point P of Y, and let $\nu\alpha^2$ denote the bound on $|h^{-1}(P)|$ from Corollary 7.3 in case $m_h(P) = \infty$. By Lemma 10.4, $R_{\pi_t}(f_t^{-1}(P))$ is at most $((\varepsilon_h(P)+1/2)\binom{t}{2} + E_0 t^4))\frac{(\ell-2)!}{(\ell-t)!}$ if $m_h(P) < \infty$ and at most $(\nu\alpha^2\binom{t}{2} + E_0 t^4)\frac{(\ell-2)!}{(\ell-t)!}$ if $m_h(P) = \infty$. By definition, $\varepsilon_h(P) + 1/2 < 84(\alpha + 3/2)$ for every point P of Y. Moreover by Corollary 7.3, there are at most four branch points P with $m_h(P) > 1$, at most $2(\alpha+1)$ with $m_h(P) = 1$, and at most two with $m_h(P) = \infty$.

In total we have the following bound on R_{π_t}

$$\begin{aligned} R_{\pi_t} &= \sum_{P\in Y(\mathbb{K})\colon\, m_h(P)<\infty} R_{\pi_t}(f_t^{-1}(P)) + \sum_{P\in Y(\mathbb{K}), m_h(P)=\infty} R_{\pi_t}(f_t^{-1}(P)) \\ &< \left(\sum_{P\in Y(\mathbb{K})\colon\, m_h(P)<\infty} \left(\binom{t}{2}(\varepsilon_h(P)+1/2)+E_0t^4\right) + 2\left(\nu\alpha^2\binom{t}{2}+E_0t^4\right)\right)\frac{(\ell-2)!}{(\ell-t)!} \\ &< \left((2\alpha+6)\left(84(\alpha+3/2)\binom{t}{2}+E_0t^4\right)+2\nu\alpha^2\binom{t}{2}+2E_0t^4\right)\frac{(\ell-2)!}{(\ell-t)!}. \end{aligned}$$

As $\alpha=\beta_1 t^k$ for $k\geq 2$, this gives $R_{\pi_t}\leq d_{5,\beta_1}t^{2k+2}(\ell-2)!/(\ell-t)!$ for some constant $d_{5,\beta_1}>0$ depending only on β_1.

Step II: *Bounding g_{Y_2} from below and estimating* (10.23). We next claim similarly to the proof of Theorem 3.1 that if the ramification type of h is not $[\ell],[a,\ell-a],[2,1^{\ell-2}]$ then $g_{Y_2}>2c'\ell-2d'-1$, for constants $c'\leq\min\{1/3,c_2,c_{2,3}\}$ and $d'\geq\max\{2,d,2^8d_2,d_{2,3}\}$ such that $d'/c'\geq 3^3\lambda_2$.

First consider coverings h whose ramification type does not appear in Table 4.1. It suffices to prove the claim when $c'\ell-d'\geq 0$, and hence when $\ell\geq d'/c'\geq\max\{6,3^3\lambda_2\}$. If $g_{Y_1}\leq 1$ then $g_{Y_2}<3\ell$ by Proposition 8.1. Since in addition $\ell\geq 3^3\lambda_2$ and the ramification type of h is not in Table 4.1, Proposition 10.1 with $\alpha=3$ implies that

$$g_{X_2}\geq g_{X_2}-g_{X_1}>c_{2,3}\ell-d_{2,3}\geq c'\ell-d'.$$

If $g_{Y_1}>1$, then $g_{X_2}\geq g_{X_2}-g_{X_1}>c_2\ell-2^8d_2\geq c'\ell-d'$ by Proposition 6.1. Thus, in combination with the Riemann–Hurwitz formula for π_2, we have

$$g_{Y_2}-1\geq 2(g_{X_2}-1)>2(c'\ell-d'-1),$$

proving the claim when the ramification of h is not in Table 4.1.

If the ramification type of h does appear in Table 4.1 but is not $[\ell],[a,\ell-a],[2,1^{\ell-2}]$, then $R_{\pi_2}=\sum_{P\in Y(\mathbb{K})}R_{\pi_2}(f_2^{-1}(P))$ is at least $(2\ell-5)/3$ by Remark 5.2. Since in addition $c'\leq 1/3$ and $d'\geq 2$, the Riemann–Hurwitz formula for π_2 gives

$$g_{Y_2}-1\geq 2(g_{X_2}-1)+R_{\pi_2}\geq -2+\frac{2\ell-5}{3}>2(c'\ell-d'-1),$$

completing the proof of the claim.

Set $c_4:=\min\{(99/25)c',1\}$ and let $d_{4,\beta_1}\geq 1$ be sufficiently large so that

$$d_{4,\beta_1}t^{2k+2}\geq(99/25)(d'+1)+d_{5,\beta_1}t^{2k+2} \tag{10.24}$$

and $d_{4,\beta_1}t^6\geq(3E_0+1)t^4+8$ for all $t\geq 3$. Since the claim is trivial when $c_4\ell-d_{4,\beta_1}t^{2k+2}<0$, we may assume $\ell\geq d_{4,\beta_1}t^{2k+2}/c_4\geq t^{2k+2}$.

Since $g_{Y_2}-1>2(c'\ell-d'-1)$ and $R_{\pi_t}\leq d_{5,\beta_1}t^{2k+2}(\ell-2)!/(\ell-t)!$ by Step II, (10.23) gives

$$2t!(g_{X_t}-g_{X_{t-1}})>\frac{(\ell-2)!}{(\ell-t)!}\left(4(1-\varepsilon)(c'\ell-d'-1)-d_{5,\beta_1}t^{2k+2}\right) \tag{10.25}$$

As $t \geq 3$ and $k \geq 2$, we have $\ell \geq t^6$, so that $\varepsilon < 1/100$ and $4(1-\varepsilon)c' > 25/99c' > c_4$. Thus (10.25) gives

$$2t!(g_{X_t} - g_{X_{t-1}}) > \frac{(\ell-2)!}{(\ell-t)!}\Big(c_4\ell - 4(1-\varepsilon)(d'+1) - d_{5,\beta_1}t^{2k+2}\Big).$$

The right hand side is at least $(c_4\ell - d_{4,\beta_1}t^{2k+2})\frac{(\ell-2)!}{(\ell-t)!}$ by (10.24). This completes the proof when the ramification type of h is not $[\ell], [a, \ell-a], [2, 1^{\ell-2}]$.

Step III: *The case where h has ramification type $[\ell], [a, \ell-a], [2, 1^{\ell-2}]$.* Let P_1, P_2, P_3 be the branch points with ramification $[\ell], [a, \ell-a], [2, 1^{\ell-2}]$, respectively. In this case, applying the Riemann–Hurwitz formula to the natural projections $Y_2 \to Y_1$ and $Y_3 \to Y_2$ gives $g_{Y_2} = 0$, and

$$2(g_{Y_3} - 1) = (\ell-5)(\ell-2) + 2(a-1)(\ell-a-1) \geq (\ell-5)(\ell-2). \tag{10.26}$$

On the other hand, computing the bounds on R_{π_t} via Proposition 5.1 give

$$\begin{aligned}
R_{\pi_t}(f_t^{-1}(P_1)) &< \left(\binom{t}{2}\delta_\ell + E_0t^4\right)\frac{(\ell-2)!}{(\ell-t)!}\\
R_{\pi_t}(f_t^{-1}(P_2)) &< \left(\binom{t}{2}(1-\delta_\ell) + E_0t^4\right)\frac{(\ell-2)!}{(\ell-t)!}\\
R_{\pi_t}(f_t^{-1}(P_3)) &< \left(E_0t^4 + \binom{t}{2}\cdot\frac{1}{\ell-2}\right)\frac{(\ell-2)!}{(\ell-t)!},
\end{aligned}$$

where $\delta_\ell = 1$ if ℓ is even and 0 otherwise. Note that as $\ell \geq t^6 \geq 3^6$, in total we have $R_{\pi_t} < (3E_0+1)t^4(\ell-2)!/(\ell-t)!$. Thus for $t = 3$, in combination with (10.26), the Riemann–Hurwitz formula for π_3 gives

$$\begin{aligned}
12(g_{X_3} - 1) &= 12(g_{Y_3} - 1) - \sum_{P\in Y(\mathbb{K})} R_{\pi_3}(f_3^{-1}(P))\\
&> (\ell-2)(\ell-5) - (3E_0+1)t^4(\ell-2) > (c_4\ell - d_{4,\beta_1}t^{2k+2})(\ell-2).
\end{aligned}$$

As $g_{X_2} = 0$, this gives $12(g_{X_3} - g_{X_2}) > (c_4\ell - d_{4,\beta_1}t^{2k+2})(\ell-2)$ as desired. Henceforth assume $t \geq 4$. By (6.2) and Riemann–Hurwitz for the natural projection $Y_{t-1} \to Y_3$, we have

$$2t!(g_{X_t} - g_{X_{t-1}}) \geq 2\frac{\ell-5}{\ell-2}(g_{Y_{t-1}} - 1) - R_{\pi_t} \geq 2\frac{\ell-5}{\ell-2}\cdot\frac{(\ell-3)!}{(\ell-t)!}(g_{Y_3} - 1) - R_{\pi_t}. \tag{10.27}$$

Since $R_{\pi_t} < (3E_0+1)t^4(\ell-2)!/(\ell-t)!$ and $k \geq 2$, (10.26) and (10.27) give

$$\begin{aligned}
2t!(g_{X_t} - g_{X_{t-1}}) &\geq 2\frac{\ell-5}{\ell-2}\cdot\frac{(\ell-3)!}{(\ell-t)!}(g_{Y_3} - 1) - R_{\pi_t}\\
&> \frac{(\ell-2)!}{(\ell-t)!}\left(\frac{(\ell-5)^2}{\ell-2} - (3E_0+1)t^4\right)\\
&> (\ell - (3E_0+1)t^4 - 8)\frac{(\ell-2)!}{(\ell-t)!} > (c_4\ell - d_{4,\beta_1}t^{2k+2})\frac{(\ell-2)!}{(\ell-t)!}.
\end{aligned}$$

□

11. Nonoccurring ramification data

It remains to prove that the ramification data in Table 9.2 do not correspond to an indecomposable covering (Lemma 9.9). We shall use the following lemma of Guralnick–Shareshian [22, Lemma 2.0.12]. We follow the notation of Setup 2.2. Permutation multiplication is left to right, that is, $(1,2)(1,3) = (1,2,3)$.

Lemma 11.1. *Let $h : Y_1 \to Y$ be a degree ℓ covering with monodromy group $G \in \{A_\ell, S_\ell\}$, and X_k the quotient by a k-set stabilizer. Then $g_{X_k} \le g_{X_{k+1}}$ for all $1 \le k < \ell/2$.*

Remark 11.2. Let G be a primitive subgroup of S_ℓ which does not contain A_ℓ. Classical results of Jordan [13, Theorem 3.3.E and Example 3.3.1] imply that G does not contain a p-cycle for any prime $p < \ell - 2$, and also that if $\ell \ge 9$ then G does not contain a product of two disjoint 2-cycles.

Proof of Lemma 9.9. Assume on the contrary that there exists an indecomposable degree ℓ covering $h : Y_1 \to \mathbb{P}^1$ whose ramification type is in Table 9.2, and let $G \le S_\ell$ be its (primitive) monodromy group. By Riemann's existence theorem there exists a product 1 tuple $a, b, c, d \in G$ that generates G, and whose cycle structures correspond to the given ramification data. We divide the argument into cases according to the types in Table 9.2.
Cases F1.N1-F1.N4: Since G is primitive (as h is indecomposable) and contains a 2-cycle in case F1.N1, a 3-cycle in case F1.N2, and an element of cycle structure $[2^2, 1^{\ell-4}]$ in cases F1.N3, F1.N4, G contains A_ℓ if $\ell \ge 9$ by Remark 11.2. Riemann–Hurwitz for h implies that $g_{X_1} = g_{Y_1} = 1$ in all cases F1.N1-F1.N4. However, in each case we get $g_{X_2} = 0$ by Remark 6.2, equality (6.3). As $G \supseteq A_\ell$, this contradicts $g_{X_2} \ge g_{X_1}$ by Lemma 11.1.
Case F4.N1: Let P_1, P_2, P_3 be the branch points of h corresponding to $[2^{\ell/2}]$, $[2, 3^{(\ell-2)/3}]$, $[1^2, 6^{(\ell-2)/6}]$, respectively. Let $\alpha : \mathbb{P}^1 \to \mathbb{P}^1$ be a Galois degree 3 covering totally ramified over P_2 and P_3, and unramified anywhere else. Consider a minimal covering $p : Z \to \mathbb{P}^1$ which factors through h and α, say as $p = h \circ h' = \alpha \circ \alpha'$.

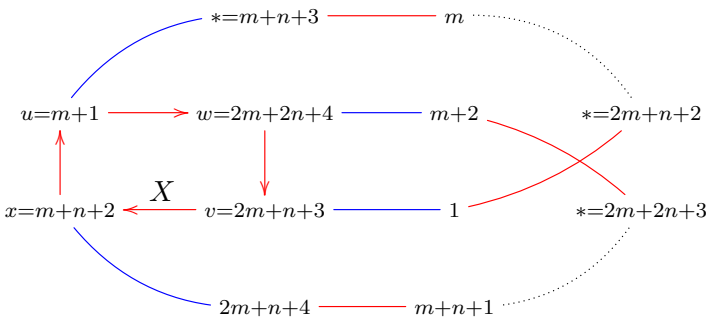
We first claim that α' is a degree ℓ covering with monodromy group S_ℓ and ramification $[2^{\ell/2}]^3, [1^2, 2^{\ell/2-1}], [2, 1^{\ell-2}]$. Let $p \circ \tilde{p} : \tilde{Z} \to \mathbb{P}^1$ be the Galois closure of p. Since G is a primitive subgroup of S_ℓ containing the 2-cycle y^3, we have $G = S_\ell$ by Remark 11.2. Since G and $\mathrm{Mon}(\alpha) = C_3$ have no common nontrivial quotient, we have $\mathrm{Mon}(p \circ \tilde{p}) \cong S_\ell \times C_3$, $\mathrm{Mon}(\alpha' \circ \tilde{p}) = S_\ell$, and h and α have no common factorization $\alpha = w \circ \tilde{\alpha}$, $h = w \circ \tilde{h}$, with $\deg w > 1$. In particular, $\deg p = \deg \alpha \cdot \deg h$ by Lemma 9.4 and the ramification type of α' is $[2^{\ell/2}]^3, [1^2, 2^{\ell/2-1}], [2, 1^{\ell-2}]$ by Lemma 9.2.(2). Since $\mathrm{Mon}(\alpha' \circ \tilde{p}) = S_\ell$, and $\deg \alpha' = \ell$, $\alpha' \circ \tilde{p}$ is the Galois closure of α', completing the proof of the claim.

Letting Z_2 be the quotient of $\tilde{Z}$ by a stabilizer of a 2-set in $\mathrm{Mon}(\alpha') = S_\ell$, we get that $g_Z = 1$ and $g_{Z_2} = 0$ by Remark 6.2, equality (6.3), contradicting $g_{Z_2} \ge g_Z$ by Lemma 11.1.
Case I2.N1 Without loss of generality assume c has cycle structure $[2^{\ell/2}]$, and b has structure $[4, 2^{\ell/2-2}]$, so that bc is an ℓ-cycle. View the letters $1, 2, \ldots, \ell$ as vertices in a directed bicolored graph, with red edges representing b and blue edges representing c. Since edges corresponding to a transposition go both way we denote them by an undirected edge.

Each of the four vertices in the 4-cycle X of b meets an edge of c, and if the other vertex of that edge is not in X then it meets an edge of b whose other vertex is not in X, and so

on, where eventually we have an edge of c whose other vertex is in X. So from each vertex in X we get a path of edges colored $cbcbcb\dots bc$ in which the first and last vertices are in X (and are distinct) but no intermediate vertex is in X.

First suppose that one such path connects two adejacent vertices $u, v \in X$ where $u^b = v$; then bc maps u to [all vertices in the uv path occurring after c's] to u, so bc is not an ℓ-cycle. Thus the two paths connect the two pairs of non-adjacent vertices in X, say u, v and w, x, where the path connecting u and v contains m edges from b and $m+1$ edges from c (for some $m \geq 0$), and likewise the path connecting w and x contains n edges from b and $n+1$ edges from c (for some $n \geq 0$), and where X is (u, w, v, x). Here $\ell = 2m + 2n + 4$.



Now label the vertices so that bc is $(1, 2, \dots, \ell)$, starting by putting $w^{bc} = 1$. Then the path from v to u is $v, 1, *, 2, *, 3, *, \dots, m, *, u$ where the $*$ represent as-yet-unlabelled vertices. Thus u gets label $m + 1$, and the path from w to x is

$$w, m + 2, *, m + 3, *, \dots, m + n + 1, *, x$$

so that x gets label $m + n + 2$, and the path from u to v is

$$m + 1, m + n + 3, m, m + n + 4, m - 1, m + n + 5, \dots, 2, 2m + n + 2, 1, v$$

so that v gets label $2m + n + 3$, and the path from x to w is

$$m + n + 2, 2m + n + 4, m + n + 1, 2m + n + 5, \dots, m + 3, 2m + 2n + 3, m + 2, w$$

so that w gets label $2m + 2n + 4$.

Thus c is the product of transpositions $(i, 3m + 2n + 6 - i)$, for $m + 2 \leq i \leq m + n + 2$, and $(i, 2m + n + 4 - i)$ for $1 \leq i \leq m + 1$, and b is the product of the transpositions $(i, 3m + 2n + 5 - i)$ for $m + 2 \leq i \leq m + n + 1$, and $(i, 2m + n + 3 - i)$ for $1 \leq i \leq m$, and the 4-cycle $(m + 1, 2m + 2n + 4, 2m + n + 3, m + n + 2)$.

The $(\ell/2)$-th power of the ℓ-cycle bc is the product of $(i, \ell/2 + i)$, for $1 \leq i \leq \ell/2$. For $1 \leq i \leq m + 1$, we have $2m + n + 4 - 1 \geq m + n + 2 + i \geq 2m + n + 4 - (m + 1)$ so that c maps $\{i, \ell/2 + i\}$ to $\{2m + n + 4 - i, 2m + n + 4 - \ell/2 - i\}$. For $m + 2 \leq i \leq m + n + 2$, we have

$$3m + 2n + 6 - (m + 2) \geq m + n + 2 + i \geq 3m + 2n + 6 - (m + n + 2)$$

so that c maps $\{i, \ell/2+i\}$ to $\{3m+2n+6-i, 3m+2n+6-\ell/2-i\}$. Therefore both bc and c preserve the partition $\{i, \ell/2+i\}$, $1 \le i \le \ell/2$, so also $\langle b, c\rangle$ preserves this partition, whence $\langle b, c\rangle$ is not primitive.

Case I2.N2 Without loss of generality assume b and c have cycle structure $[2^{\ell/2}]$, and d is a 2-cycle (u, v) such that dcb is an ℓ-cycle. Then each vertex of d is an endpoint of a unique b-edge and a unique c-edge, and each b-or-c-edge emanating from a vertex of d gives rise to a path of alternating b-and-c-edges which ends in one of the vertices of d. If each such path ends at the same vertex of d at which it starts, then dcb maps $u \mapsto v^{cb} \mapsto v^{cbcb} \mapsto \ldots \mapsto v \mapsto u^{cb} \mapsto u^{cbcb} \mapsto \ldots \mapsto u$ so that dcb is not an ℓ-cycle, as it does not cover all vertices in the alternating b-and-c paths from u to v and from v to u. Hence there are two paths from u to v consisting of b-and-c-edges, one starting with b and one starting with c. If the path starting with c ends in b then dcb maps $v \to u^{cb} \to u^{cbcb} \to \ldots \to v$, so dcb is not an ℓ-cycle. Thus the path starting with c ends in c; say it consists of m b-edges and $m+1$ c-edges. Then the path starting with b ends in b; say it consists of $n+1$ b-edges and n c-edges. Here $\ell = 2m+2n+2$.

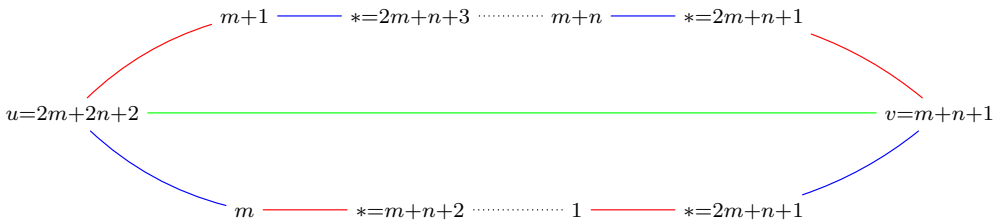
Now label the vertices so that dcb is $(1, 2, \ldots, \ell)$, starting by putting $v^{cb} = 1$. Then the path from v to u which starts with c is $v, *, 1, *, 2, *, 3, *, \ldots, *, m, u$ where the $*$ represent as-yet-unlabelled vertices. Thus the path from u to v which starts with b is $u, m+1, *, m+2, *, \ldots, m+n, *, v$ where v gets label $m+n+1$. Then the path from u to v which starts with c is

$$u, m, m+n+2, m-1, m+n+3, \ldots, 1, 2m+n+1, v = m+n+1$$

so the path from v to u which starts with b is

$$m+n+1, 2m+n+2, m+n, 2m+n+3, \ldots, m+1, u = 2m+2n+2 = \ell.$$

Thus c is the product of $(m+n+1, 2m+n+1)$, $(m, 2m+2n+2)$, $(i, 2m+n+1-i)$ for $1 \le i \le m-1$, and $(i, 3m+2n+2-i)$ for $m+1 \le i \le m+n$; b is the product of $(i, 2m+n+2-i)$ for $1 \le i \le m$, and $(i, 3m+2n+3-i)$ for $m+1 \le i \le m+n+1$; and d is $(\ell/2, \ell)$.



The $\ell/2$-th power of the ℓ-cycle dcb is the product of $(i, \ell/2+i)$ over all $1 \le i \le \ell/2$. Plainly d preserves the partition $\{i, \ell/2+i\}$, $1 \le i \le \ell/2$. For every $1 \le i \le m$ we have $2m+n+2-1 \ge \ell/2+i \ge 2m+n+2-m$, so that b maps $\{i, n/2+i\}$ to $\{2m+n+2-i, 2m+n+2-\ell/2-i\}$. For $m+1 \le i \le m+n+1$ we have $3m+2n+3-(m+1) \ge \ell/2+i \ge 3m+2n+3-(m+n+1)$, so that b maps $\{i, \ell/2+i\}$ to

$\{3m+2n+3-i, 3m+2n+3-\ell/2-i\}$. Therefore the partition $\{i, \ell/2+i\}$, $1 \le i \le \ell/2$ is preserved by b, d and dcb, so also by $\langle b, c, d\rangle$, whence $\langle b, c, d\rangle$ is not primitive. □

Appendix A. Existence of coverings with ramification as in Table 4.1

We use Riemann's existence theorem to show:

Proposition A.1. *Each ramification data in Table 4.1 is the ramification type of a degree ℓ covering $h : \mathbb{P}^1 \to \mathbb{P}^1$ with $\mathrm{Mon}(h) \cong A_\ell$ or S_ℓ.*

Proof. The branch cycles in types I1, I2, and types F1.1-F1.8 were proven to occur in Propositions 3.0.24–3.0.28 of [22]. It remains to treat the cases F1.9 and the cases in F3 and F4. For each of these ramification data, we write a product 1 tuple $x_1, \dots, x_r \in S_\ell$ of elements whose cycle structures correspond to the ramification type, and show that that the group $G := \langle x_1, \dots, x_r\rangle$ contains A_ℓ. This prove the proposition by Riemann's existence theorem. Each element in a product 1 relation is written within parenthesis.
Case F1.9: Write the product 1 relation as $x_1x_2 = x_4x_3$ where $x_3^2 = x_4^2 = 1$:

$$\begin{aligned}&\left((1,4)(3,5)\prod_{i=3}^{\ell/2-1}(2i,2i+1)\right)\cdot\left((1,2,3,4)\prod_{i=2}^{\ell/2-1}(2i+1,2i+2)\right)\\&=(4,2,3,6,8,10,\dots,\ell-2,\ell,\ell-1,\ell-3,\ell-5,\dots,7,5)\\&=\left(\prod_{i=2}^{\ell/2-1}(2i+1,2i+2)\right)\cdot\left((2,3)(4,6)\prod_{i=1}^{\ell/2-2}(2i+1,2i+4)\right).\end{aligned}$$

The subgroup $G = \langle x_1, x_2, x_3, x_4\rangle \le S_\ell$ is transitive and contains an $(\ell-1)$-cycle, hence doubly transitive and in particular primitive. But $x_2^2 \in G$ has cycle structure $[2^2, 1^{\ell-4}]$, so G contains A_ℓ if $\ell > 8$ by Remark 11.2.
Case F3.1: For $\ell = 4k$, $k \ge 2$, write the relation as $x_1x_2 = x_3$ where $x_3^2 = 1$:

$$\begin{aligned}&\left((2,1,4,5)(4k-2,4k-5,4k,4k-1)\prod_{i=1}^{k-2}(4i+2,4i-1,4i+4,4i+5)\right)\\&\cdot\left((1)(2,3,4)\prod_{i=1}^{k-1}(4i+1,4i+2,4i+3,4i+4)\right)\\&=\left((2,1)(4k-1)(4k)\prod_{i=1}^{k-1}(4i,4i+2)(4i+1,4i-1)\right).\end{aligned}$$

Consider a block which contains 2 and has size at least 2. Since $x_2^4 = (2,3,4)$, if this block contains a point outside $\{2,3,4\}$ then that point (and hence the whole block) is fixed by $(2,3,4)$; and if the block contains either 3 or 4 then the block must be fixed by $(2,3,4)$. In any case, the block is fixed by $(2,3,4)$, so it contains 3 and 4. Thus the block is fixed by x_2 (and not just by x_1^4), and by x_1^2. Since $\langle x_2, x_1^2\rangle \le S_\ell$ is transitive the block is $\{1, 2, \dots, \ell\}$. So G is primitive and contains a 3-cycle, so it contains A_ℓ by Remark 11.2. Note that

$G = S_\ell$, as x_3 has cycle structure $[1^2, 2^{2k-1}]$. A similar argument applies in **cases F3.2 and F3.3**. In case F3.2 with $\ell = 4k+5$, $k \geq 1$, we write the relation $x_1x_2 = x_3$ as

$$\Big((1)(4,5,4k+5,4k+4)(4k-2,4k-1,4k+2,4k+3)\prod_{i=1}^{k-1}(4i-2,4i-1,4i+4,4i+5)\Big)$$
$$\cdot\Big((1,2,3)(4k+4,4k+5)\prod_{i=1}^{k}(4i,4i+1,4i+2,4i+3)\Big)$$
$$=\Big((1,2)(5,4k+4)(4k-1,4k+3)(4k,4k+2)(4k+5)\prod_{i=1}^{k-1}(4i-1,4i+5)(4i,4i+2)\Big).$$

and in case F3.3 with $\ell = 4k+3$, $k \geq 1$, we write it as[5]

$$\Big((1,4,5)(4k-2,4k-1,4k+2,4k+3)\prod_{i=1}^{k-1}(4i-2,4i-1,4i+4,4i+5)\Big)$$
$$\cdot\Big((1)(2,3)\prod_{i=1}^{k}(4i,4i+1,4i+2,4i+3)\Big)$$
$$=\Big((1,5)(2)(4k-1,4k+3)(4k,4k+2)\prod_{i=1}^{k-1}(4i-1,4i+5)(4i,4i+2)\Big).$$

Case F4.3: For $\ell = 6k+7$, $k \geq 1$, write $x_1x_2 = x_3$, where $x_3^2 = 1$:

$$\Big((1,6k+7,6k+5)(2,6k+4,6)(6k-3,6k-1,6k+1)(6k-2,6k+3,6k+2)$$
$$(6k+6)\prod_{i=1}^{k-1}(6i-3,6i-1,6i+1)(6i+2,6i-2,6i+6)\Big)$$
$$\cdot\Big((6k+1,6k+2,6k+3)(6k+4,6k+5,6k+6,6k+7)$$
$$\prod_{i=0}^{k-1}(6i+1,6i+2,6i+3,6i+4,6i+5,6i+6)\Big)$$
$$=\Big((1,6k+4)(2,6k+5)(6k+3)(6k+6,6k+7)$$
$$\prod_{i=1}^{k}(6i-3,6i)(6i-2,6i+1)(6i-1,6i+2)\Big).$$

[5]Note that when applying the argument from case F3.1 to case F3.3, one uses the 3-cycle x_1^4 to replace the role of the 3-cycle x_2^4 in case F3.1.

Consider a block which contains $6k+4$ and has size at least 2. Since x_2^6 equals $(6k+4,6k+6)(6k+5,6k+7)$, if the block does not contain $6k+6$ then the block is not fixed by x_2^6 and hence does not contain any elements fixed by x_2^6, so the block is contained in $\{6k+4,6k+5,6k+7\}$ (and must have size 2 since it is not fixed by x_2^6). But then the block is fixed by x_2, so it contains $6k+6$, contradiction. Thus the block contains $6k+6$, so it is fixed by x_1 and x_2^2. Since $\langle x_2^2, x_1\rangle \le S_\ell$ is transitive the block is $\{1,2,\dots,\ell\}$. So G is primitive and contains an element of cycle structure $[2^2, 1^{\ell-4}]$, hence G contains A_ℓ for $\ell \ge 9$ by Remark 11.2. A similar argument applies in **case F4.5**[6]. Here $\ell = 6k+4$, $k \ge 1$, and the relation $x_1x_2 = x_3$ is written as

$$\begin{aligned}&\Big((1,6,2)(3,5,7)(6k-2,6k+4,6k+2)(6k+3)\\&\qquad\prod_{i=2}^{k}(6i-4,6i-8,6i)(6i-3,6i-1,6i+1)\Big)\\&\cdot\Big((6k+1,6k+2,6k+3,6k+4)\prod_{i=0}^{k-1}(6i+1,6i+2,6i+3,6i+4,6i+5,6i+6)\Big)\\&=\Big((1)(2)(6k+3,6k+4)\prod_{i=1}^{k}(6i-3,6i)(6i-2,6i+1)(6i-1,6i+2)\Big).\end{aligned}$$

Case F4.6: For $\ell = 6k+5$, $k \ge 1$, write the relation as $x_1x_2 = x_3$, where $x_3^2 = 1$:

$$\begin{aligned}&\Big((1,6k+5)(2,6k+4,6)(6k-3,6k-1,6k+1)(6k+2,6k-2,6k+3)\\&\qquad\prod_{i=1}^{k-1}(6i-3,6i-1,6i+1)(6i+2,6i-2,6i+6)\Big)\\&\cdot\Big((6k+1,6k+2,6k+3)(6k+4,6k+5)\prod_{i=0}^{k-1}(6i+1,6i+2,6i+3,6i+4,6i+5,6i+6)\Big)\\&=\Big((1,6k+4)(2,6k+5)(6k+3)\prod_{i=1}^{k}(6i-3,6i)(6i-2,6i+1)(6i-1,6i+2)\Big).\end{aligned}$$

Consider a block which contains 1 and has size at least 2. Since $x_1^3 = (1,6k+5)$, it must fix the block so the block contains $6k+5$ and hence is fixed by x_2. Also x_2^2 fixes $6k+5$ and hence fixes the block. Since $\langle x_2^2, x_1\rangle \le S_\ell$ is transitive, the block is $\{1,\dots,\ell\}$. So G is primitive and contains a 2-cycle, hence $G = S_\ell$ by Remark 11.2. A similar argument applies in **cases F4.1, F4.2, and F4.4**. In case F4.1 with $\ell = 6k$, $k \ge 1$, write the relation

[6]When applying the argument from case F4.3 to case F4.5, one uses x_2^2 to replace the role of the element x_2^6 in case F4.3

$x_1x_2 = x_3$ as

$$\Big((1)(2,6)(6k-1,6k-2,6k-3)\prod_{i=1}^{k-1}(6i-3,6i-1,6i+1)(6i+2,6i-2,6i+6)\Big)$$
$$\cdot\Big(\prod_{i=0}^{k-1}(6i+1,6i+2,6i+3,6i+4,6i+5,6i+6)\Big)$$
$$=\Big((6k-2)(6k-1)(1,2)(6k-3,6k)\prod_{i=1}^{k-1}(6i-3,6i)(6i-2,6i+1)(6i-1,6i+2)\Big).$$

In case F4.2 with $\ell = 6k+2$, $k \geq 1$, we write this relation as

$$\Big((1,6k+1)(2,6k+2,6)(6k-1,6k-2,6k-3)$$
$$\cdot\prod_{i=1}^{k-1}(6i-3,6i-1,6i+1)(6i+2,6i-2,6i+6)\Big)$$
$$\Big((6k+1,6k+2)\prod_{i=0}^{k-1}(6i+1,6i+2,6i+3,6i+4,6i+5,6i+6)\Big)$$
$$=\Big((1,6k+2)(2,6k+1)(6k,6k-3)(6k-1)(6k-2)$$
$$\prod_{i=1}^{k-1}(6i-3,6i)(6i-2,6i+1)(6i-1,6i+2)\Big).$$

In case F4.4 with $\ell = 6k+3$, $k \geq 1$, we write this relation as

$$\Big((1)(2,6)(6k-2,6k+3,6k+2)(6k-3,6k-1,6k+1)$$
$$\prod_{i=1}^{k-1}(6i-3,6i-1,6i+1)(6i+2,6i-2,6i+6)\Big)$$
$$\cdot\Big((6k+1,6k+2,6k+3)\prod_{i=0}^{k-1}(6i+1,6i+2,6i+3,6i+4,6i+5,6i+6)\Big)$$
$$=\Big((1,2)(6k+3)\prod_{i=1}^{k}(6i-3,6i)(6i-2,6i+1)(6i-1,6i+2)\Big).$$

□

References

[1] M. Aschbacher, On conjectures of Guralnick and Thompson. J. Algebra 135 (1990), 277–343. 2, 10
[2] M. Aschbacher, L. Scott, Maximal subgroups of finite groups. J. Algebra 92 (1985), 44–80.

[3] R. Avanzi, U. Zannier, Genus one curves defined by separated variable polynomials and a polynomial Pell equation. Acta Arith. 99 (2001), 227–256. 2
[4] L. Babai and Á. Seress, On the degree of transitivity of permutation groups: a short proof. J. Comb. Theory Ser. A 45 (1987), 310–315. 4, 8, 9
[5] Y. Bilu, R. Tichy, The Diophantine equation f(x)=g(y). Acta Arith. 95 (2000), 261–288.
[6] R. Brieler, Symmetric and alternating groups as monodromy groups of Riemann surfaces: The case of four branch points. Ph.D. thesis (2009). 4
[7] P. Cameron, P. Neumann, J. Saxl, An interchange property in finite permutation groups. Bull. London Math. Soc. 11 (1979), 161–169. 9
[8] P. Cassou-Noguès, J. Couveignes, Factorizations explicites de $g(y) - h(z)$, Acta Arith. 87 (1999), 291–317. 3
[9] A. Carney, R. Hortsch, M. Zieve, Near-injectivity of polynomial mappings on number fields. Preprint. 3
[10] O. Chisini, Sulla risolubilita‘ per radicali delle equazioni contenenti linearmente un parametro, Rend. Reale Instituto Lombardo di Sci. e Let. 68 (1915), 382–402. 2
[11] P. Dèbes, M. D. Fried, Integral specialization of families of rational functions. Pacific J. Math., 190 (1999), 45–85.
[12] T. Do, M. Zieve, On a question of Lyubich and Minsky on laminations in complex dynamics. 5, 24
[13] J. D. Dixon, B. Mortimer, Permutation Groups. Springer GTM 163 (1996). 49
[14] F. Dorey, G. Whaples, Prime and composite polynomials. J. Algebra 28 (1974), 88–101.
[15] W. Feit, Some consequences of the classification of finite simple groups. The Santa Cruz conference on finite groups. Proc. Sympos. Pure Math., vol. 37, AMS, Providence, Rhode Island (1980), 175–181. 2
[16] D. Frohardt, R. Guralnick, C. Hoffman and K. Magaard, Monodromy groups of coverings of curves, in preparation. 11
[17] D. Frohardt, K. Magaard, Composition factors of monodromy groups. Ann. Math. 154 (2001), 327–345. 2, 10
[18] W. Fulton, Algebraic Curves: An Introduction to Algebraic Geometry. Advanced Book Classics. Addison-Wesley Publishing Company, Advanced Book Program, Redwood City, CA, 1989. 5
[19] R. Guralnick, The genus of a permutation group. Groups, Combinatorics and Geometry (eds: M.W. Liebeck and J. Saxl), London Math. Soc. Lecture Note Series 165 (1992), 351–363. 2, 10
[20] R. Guralnick, K. Magaard, On the minimal degree of a primitive permutation group. J. Algebra 207 (1998), 127–145. 2
[21] R. Guralnick, M. Neubauer, Monodromy groups of branched coverings: the generic case. Contemporary Mathematics 186 (1995), 325–352. 2, 3, 10, 11
[22] R. Guralnick, J. Shareshian, Symmetric and Alternating Groups as Monodromy Groups of Riemann Surfaces I: Generic Covers and Covers with Many Branch Points. Appendix by R. Guralnick and R. Stafford. Mem. Amer. Math. Soc. 189 (2007). 3, 4, 7, 8, 11, 13, 15, 30, 49, 52
[23] R. Guralnick, J. Thompson, Finite groups of genus zero. J. Algebra 131 (1990), 303–341. 2, 9, 10
[24] C. Jordan, Nouvelles recherches sur la limite de transitivité des groupes qui ne contiennent pas le groupe alternité, J. Math. 1 (1895), 35–60. 4
[25] W. M. Kantor, k-Homogeneous groups. Math. Z. 124 (1972), 261–265.
[26] M. Liebeck, J. Saxl, Minimal degrees of primitive permutation groups, with an application to monodromy groups of covers of Riemann surfaces. Proc. London Math. Soc. 63 (1991), 266–314. 2, 10
[27] M. Liebeck, A. Shalev, Simple groups, permutation groups, and probability. J. Amer. Math. Soc. 12 (1999), 497–520. 2, 10
[28] M. Liebeck, P. Wayman, On the genus of a finite classical group. Bull. London Math. Soc. 29 (1997), 159–164. 2, 10
[29] D. Livingstone, A. Wagner, Transitivity of finite permutation groups on unordered sets. Math. Z., 90 (1965), 393–403. 4, 8, 9

[30] A. Medvedev, T. Scanlon, Invariant varieties for polynomial dynamical systems. Ann. of Math. 179 (2014), 81–177. 2
[31] T. Monderer, D. Neftin, Symmetric Galois groups under specialization, Preprint. Arxiv:2003.11324. 3
[32] P. Müller, Primitive monodromy groups of polynomials. Recent developments in the inverse Galois problem, Contemp. Maths. 186, 385–401, Amer. Math. Soc., 1995. 2
[33] P. Müller, Finiteness results for Hilbert's irreducibility theorem. Annales de l'institut Fourier, 52 (2002), 983–1015. 2, 8
[34] P. Müller, Darstellungstheorie endlicher Gruppen. Class notes. 8
[35] P. Müller, M. Zieve. On Ritt's polynomial decomposition theorems, Preprint, arXiv:0807.3578. 2
[36] D. Neftin, M. Zieve, Monodromy groups of product type. Preprint, version from July 12, 2016. 2, 10, 11
[37] M. G. Neubauer, On monodromy groups of fixed genus. J. Algebra 153 (1992), 215–261. 2, 10
[38] M. G. Neubauer, On primitive monodromy groups of genus zero and one. I. Comm. Algebra 21 (1993), 711–746. 2
[39] A. M. Odlyzko, Bounds for discriminants and related estimates for class numbers, regulators and zeros of zeta functions: a survey of recent results. Sém. Théor. Nombres Bordeaux 2 (1990), 119–141. 3
[40] J. F. Ritt, Prime and composite polynomials, Trans. Amer. Math. Soc. 23 (1922), 51–66.
[41] J. F. Ritt, On algebraic functions which can be expressed in terms of radicals. Trans. AMS 24 (1922), 21–30. 2
[42] T. Shih, A note on groups of genus zero. Comm. Algebra 19 (1991), 2813–2826. 2, 10
[43] J. H. Silverman, The Arithmetic of Elliptic Curves. Graduate Texts in Mathematics, Second Edition. 33
[44] H. Stichtenoth, Algebraic function fields and codes. Universitext. Springer-Verlag, Berlin (1993). 3, 5, 28
[45] H. Völklein, Groups as Galois Groups: An Introduction. Cambridge Studies in Advanced Mathematics, 1996.
[46] O. Zariski, Sulle equazioni algebriche contenenti linearmente un parametro e risolubili per radicali. Atti Accad. Naz. Lincei Rend., Cl. Sci. Fis. Mat. Natur., serie V, 33 (1924), 80–82. 2
[47] O. Zariski, Sopra una classe di equazioni algebriche contenenti linearmente un parametro e risolubili per radicali. Rend. Circolo Mat. Palermo 50 (1926), 196–218. 2

Department of Mathematics, Technion - IIT, Haifa 3200, Israel
Email address: dneftin@tx.technion.ac.il

Department of Mathematics, University of Michigan, Ann Arbor, MI 48109–1043, USA
Email address: zieve@umich.edu