MONODROMY GROUPS OF INDECOMPOSABLE RATIONAL FUNCTIONS

FRANKLYN WANG

Abstract. The most important geometric invariant of a degree-n complex rational function $f(X)$ is its *monodromy group*, which is a set of permutations of n objects. This monodromy group determines several properties of $f(X)$. A fundamental problem is to classify all degree-n rational functions which have special behavior, meaning that their monodromy group G is not one of the two "typical" groups, namely A_n or S_n. Many mathematicians have studied this problem, including Oscar Zariski, John Thompson, Robert Guralnick, and Michael Aschbacher. In this paper we bring this problem near completion by solving it when G is in any of the classes of groups which previously seemed intractable. We introduce new techniques combining methods from algebraic geometry, Galois theory, group theory, representation theory, and combinatorics. The classification of rational functions with special behavior will have many consequences, including far-reaching generalizations of Mazur's theorem on uniform boundedness of rational torsion on elliptic curves and Nevanlinna's theorem on uniqueness of meromorphic functions with prescribed preimages of five points. This improved understanding of rational functions has potential significance in various fields of science and engineering where rational functions arise.

1. Introduction

In many areas of math, a fundamental role is played by *rational functions*, namely ratios between two polynomials. In this paper we consider rational functions with complex coefficients, such as $(\pi X^2 + i)/X$. Our goal is to identify the rational functions which behave differently from "random" rational functions in a certain specific sense.

Many questions about complex rational functions may be answered once one knows two important invariants of the rational function, namely its monodromy group and ramification type. Crucially, there are only finitely many possibilities for the monodromy group and ramification type of a rational function of prescribed degree, even though there are infinitely many possibilities for the rational function itself; thus, these two invariants only contain a small amount of the information contained in the rational function, but in many regards they contain the most important information. To define these invariants, write $\mathbb{C}[X]$ (resp., $\mathbb{C}(X)$) for the sets of polynomials (resp., rational functions) with complex coefficients. Recall that if $p, q \in \mathbb{C}[X]$ have no common roots then the *degree* of the rational function $p(X)/q(X)$ is defined to be the maximum of the degrees of $p(X)$ and $q(X)$. If $f(X) \in \mathbb{C}(X)$ has degree $n > 0$ then the *monodromy group* of $f(X)$ is a certain group of permutations of n objects, which is defined as the image of the monodromy representation of the fundamental group of $S^2 \setminus B$, where B is the set of critical values of $f(X)$. The ramification multiset of $f(X)$ over a point P is the collection $E_f(P)$ of multiplicities under f of all the f-preimages of P; the *ramification type* of $f(X)$ is the collection of all the $E_f(P)$'s as P varies over the points in B. Thus, the ramification type consists of at most $2n-2$ batches of positive integers, where the sum of the integers in each batch is n.

The use of monodromy groups and ramification types to answer questions about rational functions dates back at least to the work of Ritt [22] and Schur [23] in the 1920's. Some examples of results proved by means of these tools are:

(1) If $f, g \in \mathbb{C}[X]$ each have degree at least 2, and there exist $\alpha, \beta \in \mathbb{C}[X]$ for which the orbits $\{\alpha, f(\alpha), f(f(\alpha)), \dots\}$ and $\{\beta, g(\beta), g(g(\beta)), \dots\}$ have infinite intersection, then f and g have a common iterate. [9, 10]

(2) The first general result on center conditions at infinity for Abel differential equations. [5]

(3) Classification of $f, g \in \mathbb{Z}[X]$ for which the equation $f(X) = g(Y)$ has infinitely many integer solutions. [4]

(4) Classification of $f, g \in \mathbb{C}[X]$ for which there exist infinite compact subsets $A, B \subsetneqq \mathbb{C}$ such that $f^{-1}(A) = g^{-1}(B)$. [20]

The reason these results address polynomials rather than rational functions is that rational functions are not sufficiently well understood. The present paper comes close to remedying this situation. We focus on *indecomposable* rational functions, namely rational functions of degree at least 2 which cannot be written as $g(h(X))$ where $g, h \in \mathbb{C}(X)$ each have degree at least 2. These indecomposable rational functions may be viewed as the building blocks of all rational functions, since every rational function of degree at least 2 is the composition of indecomposable rational functions. Moreover, once one understands indecomposable rational functions, one may use an inductive procedure to prove results about arbitrary rational functions. Our main result is as follows.

Theorem 1.1. *If $f(X) \in \mathbb{C}(X)$ is indecomposable of degree n, and G is the monodromy group of $f(X)$, then one of the following holds:*

(1) $G \in \{A_n, S_n\}$
(2) *n is either a prime, a square, or a triangular number $d(d-1)/2$ with d an integer*
(3) $n \leq 455$
(4) *$L \leq G \leq \operatorname{Aut}(L)$ for some nonabelian non-alternating simple group L of bounded size.*

Moreover, we know all possibilities for both the monodromy group and ramification type of $f(X)$ in case neither (1) *nor* (4) *holds.*

A team of group theorists led by Guralnick is currently addressing case (4), and they expect to resolve that case within a year (in the sense of determining the possibilities for the monodromy group and ramification type). Once that is done, we will have a complete list of the possibilities for the monodromy group and ramification type of any indecomposable degree-n rational function whose monodromy group is not A_n or S_n; this will be a powerful tool which should make it possible to prove many results about rational functions. We note that degree-n rational functions with monodromy group A_n or S_n behave like random degree-n rational functions in many regards, so the above result may be interpreted as saying that the non-random rational functions are those which are decomposable or satisfy one of (2)–(4) (but do not satisfy (1)). In addition to rational function analogues of the above-mentioned polynomial results, two other expected consequences of this classification of non-random rational functions are:

(1) For any rational map $f : C \to D$ between curves over $\mathbb{Q}$, the induced map on rational points $C(\mathbb{Q}) \to D(\mathbb{Q})$ is (≤ 32)-to-1 over all but finitely many points.
(2) A classification of solutions to $f \circ p = f \circ q$ with $f \in \mathbb{C}(X)$ and p, q meromorphic on $\mathbb{C}$.

The significance of (1) can be seen from the fact that the case of genus-1 curves is equivalent to Mazur's theorem on uniform boundedness of rational torsion on elliptic curves [17]. The significance of (2) comes from the recent result that, for nonconstant meromorphic p, q on $\mathbb{C}$, there exists f as in (2) if and only if there exist five disjoint nonempty finite sets $T_1, \dots, T_5 \subset \mathbb{C}$ such that, for each i, the collection of p-preimages of T_i (counting multiplicities) equals the collection of q-preimages of T_i (counting multiplicities); when such T_i's exist, f may be chosen to have degree bounded by a function of the sizes of the T_i's. In case each T_i has size 1, this result implies that $p = q$, which is a celebrated result of Nevanlinna's [19]. Thus, these two consequences represent vast generalizations of major results by Mazur and Nevanlinna.

Theorem 1.1 builds on the work of several previous authors. The first progress in this direction was made in the first decades of the 20th century by Chisini [7], Ritt [21], and Zariski [29], who addressed the problem when G is a solvable group; intuitively, the solvability condition means that the group is especially convenient to work with. The bulk of the examples they found had prime degree, and up to changing variables were X^n, Chebyshev polynomials $T_n(X)$, and maps on x-coordinates induced by elliptic curve isogenies. Around 1990, Guralnick and Thompson [13] realized that the improved understanding of finite groups achieved during the 20th century could be applied to this topic. They first noted that, by a theorem of Aschbacher and Scott [3], the monodromy group of an indecomposable rational function must come from one of five classes of groups. Four of these classes were handled almost immediately by Guralnick–Thompson, Aschbacher, and Shih [2, 13, 24], yielding only a few low-degree examples besides the solvable examples known to Zariski. However, as Guralnick and Thompson wrote, "the analysis of case C3 promises to be tough". This case C3 is the fifth Aschbacher–Scott class of groups, and is the focus of the present paper. It consists of those groups G for which there is a nonabelian simple group L contained in S_ℓ such that $L^t \le G \le N \wr S_t := N^t \rtimes S_t$, where N is the normalizer of L in S_ℓ, the action of S_t on N^t is by permuting coordinates, and G is identified with a subgroup of S_{ℓ^t} by permuting t-tuples of elements of $\{1, 2, \dots, \ell\}$. We divide case C3 into three subcases:

(C3.1) $t = 1$ and L is non-alternating
(C3.2) $t = 1$ and L is alternating
(C3.3) $t \ge 2$.

A long series of papers by many authors, culminating in the major papers [8, 15], concluded that an indecomposable rational function of sufficiently large degree cannot have monodromy group as in (C3.1). These papers did not produce a bound on this degree, which is why there is no explicit bound in item (4) of Theorem 1.1. The recent paper [18] resolved cases (C3.2) and (C3.3) in degree at least 10^{3000}; this yielded examples in every such degree which is either square or triangular, and proved three conjectures of Guralnick and Shareshian [12]. Our work resolves (C3.2) and (C3.3) completely, and hence proves Theorem 1.1 by combining some ideas and tools from these previous papers with several new ingredients.

In case (C3.2) the monodromy group must be A_d or S_d when $d > 6$, since $\text{Aut}(A_d) = S_d$. We show:

Theorem 1.2. *If $f(X) \in \mathbb{C}(X)$ is indecomposable of degree n, and the monodromy group G of $f(X)$ is A_d or S_d for some $d \neq n$, then either $n = d(d-1)/2$ or $d \leq 15$, where in either case we know all possibilities for the permutation action of G and the ramification type of $f(X)$.*

In particular, there are cases where $d = 15$, described in Section 7. In Case (C3.3) we show the following result.

Theorem 1.3. *If an indecomposable degree-n rational function $f(X)$ has monodromy group satisfying* (C3.3)*, then either $n = 125$ or $t = 2$, and in either case we know all possibilities for both the monodromy group and ramification type of $f(X)$.*

The remainder of the paper is organized as follows. Section 2 presents notation. Section 3 shows that Theorem 1.2 follows from three auxiliary results. Section 4 proves the hardest of these auxiliary results, contingent on results from Section 5; the proofs of the other auxiliary results are similar but easier. Section 5 presents our methods for determining whether potential ramification types correspond to rational functions. Section 6 outlines the proof of Theorem 1.3. Section 7 gives special examples found in case (C3.2). Section 8 gives our future work and conclusions. Finally, Section 9 is the acknowledgements.

2. Notation and Definitions

We identify the extended complex plane $\mathbb{C}^* := \mathbb{C} \cup \{\infty\}$ as a sphere by "pulling in the sides". Let $f(X) \in \mathbb{C}(X)$ have degree $n > 1$. For any $r \in \mathbb{C}$, the numerator of $f(X) - r$ is a nonzero polynomial which we may factor as $c(X - r_1)^{e_1}(X - r_2)^{e_2} \dots (X - r_u)^{e_u}$, where the r_i's are distinct complex numbers, the e_i's are positive integers, and $c \in \mathbb{C}$ is nonzero. If this numerator has degree n then we define the ramification multiset $E_f(r)$ of $f(X)$ over r to be the collection of integers $[e_1, e_2, \dots, e_u]$. If the numerator does not have degree n then we define $E_f(r)$ to be $[e_1, e_2, \dots, e_u, n - e_1 - e_2 - \dots - e_u]$. We also define $E_f(\infty)$ to be $E_{1/f}(0)$. In each case, $E_f(r)$ is the collection of local multiplicities of the map $f : \mathbb{C}^* \to \mathbb{C}^*$ at all preimages of r. In particular, $E_f(r)$ is a collection of positive integers whose sum is n. Here $E_f(r)$ is a *multiset*, or a set-with-multiplicities, which means that the ordering of the elements of $E_f(r)$ is irrelevant but $E_f(r)$ may contain multiple copies of a single integer.

We use exponents to indicate this number of copies; for example, the multiset $[1,1,1,2]$ is denoted $[1^3,2]$. The *critical values* of $f(X)$ are the points $r \in \mathbb{C}^*$ with $E_f(r) \neq [1^n]$. Finally, the *ramification type* of $f(X)$ is the collection of all multisets $E_f(r)$ with r a critical value.

All but at most two critical values of $f(X)$ have the form $f(s)$ where $f'(s) = 0$, so there are finitely many critical values. Let p be any point in $\mathbb{C}^*$ which is not a critical value of f. Then p has exactly n distinct f-preimages in $\mathbb{C}^*$, say $f^{-1}(p) = \{z_1, z_2, \ldots, z_n\}$. Let τ be a loop in $\mathbb{C}^*$ which starts and ends at p, and does not go through any critical values of $f(X)$. For each z_i, there is a unique path σ_i starting at z_i which maps to τ under f. Since τ starts and ends at p, the ending point of σ_i is some $z_j = z_{\pi(i)}$, where π is a permutation of $[n] := \{1, 2, \ldots, n\}$. The set of π's produced from all such loops τ forms a group G of permutations of $[n]$, called the *monodromy group* of $f(X)$.

The monodromy group G of $f(X)$ is determined by the behavior of f near its critical values, in the following sense. Let x_i be the permutation of $[n]$ induced by a loop based at p which goes around the i-th critical value exactly once in a counterclockwise direction but does not go around any other critical values (that is, x_i is a "local monodromy element"). From basic algebraic topology we know that

- G is generated by $x_1, x_2, \ldots, x_s$.
- The product $x_1 x_2 \ldots x_s = 1$.
- G is a transitive subgroup of S_n, in the sense that for each $i, j \in [n]$ there is at least one element of G which maps $i \mapsto j$.

We will frequently use the Riemann–Hurwitz Formula, which is defined as follows. Let S and S' be compact Riemann surfaces, and let $f : S' \to S$ be a degree-n holomorphic map. If $\mathfrak{g}(S)$ is the genus of S, then $2\mathfrak{g}(S') - 2 = n(2\mathfrak{g}(S) - 2) + \sum_{P \in S}(n - \#f^{-1}(P))$. The Riemann–Hurwitz formula for a function field extension E/F is obtained from this by letting S and S' be the Riemann surfaces defined by F and E, respectively.

3. Proof of Theorem 1.2

In this section we deduce Theorem 1.2 from three auxiliary results that are later proven. A major difficulty in proving Theorem 1.2 is that we must consider every (faithful) primitive permutation representation of A_d and S_d. In this section we reduce Theorem 1.2 to an analysis of three special representations, which correspond to the three auxiliary results mentioned above.

3.1. **Galois Theory.** Let f be a degree-n indecomposable rational function with monodromy group A_d or S_d and $d \neq n$. Let x be a root of $f(X) - t$, where t is transcendental over $\mathbb{C}$. Then let $N = \mathbb{C}(x)$. Let Ω be the Galois closure of $(N/\mathbb{C}(t))$, or the minimal field such that $(\Omega/\mathbb{C}(t))$ is a Galois extension. If $G = \mathrm{Gal}\,(\Omega/\mathbb{C}(t))$, or the Galois group of the extension $\Omega/\mathbb{C}(t)$, then G is the monodromy group of f. We first relate G to $\deg f$ via a natural field extension.

Lemma 3.1. *If $H = \mathrm{Gal}\,(\Omega/N)$, then $\deg f = [G : H]$.*

3.2. **Riemann–Hurwitz Calculations.** Let G_k be a k-set stabilizer of G; that is, all permutations in G for which the subset $\{1, 2, \ldots, k\}$ of $[d]$ is mapped to the subset $\{1, 2, \ldots, k\}$ of $[d]$. Let the local monodromy elements of f be $x_1, x_2, \ldots, x_s$. Now, consider the groups G_k, which are k-set stabilizers of G. By applying the Riemann–Hurwitz formula to the field extensions Ω^{G_k}/Ω^G, we obtain (where $\mathfrak{g}_k$ is the genus of the field Ω^{G_k} for $k \geq 1$)

$$2\mathfrak{g}_k - 2 = -2\binom{d}{k} + \sum_{i=1}^{s}\left(\binom{d}{k} - o_k(x_i)\right), \tag{3.2}$$

where $o_k(x_i)$ is the number of orbits of the group $\langle x_i \rangle$ on the left cosets of G/G_k (which can be represented by the size k sets of elements from $[d]$, $[d]_k$). It can be shown that $o_k(x)$ is invariant under conjugation by elements in G; to this end, let $P_1, P_2, \ldots, P_s$ be the cycle structures of x_i on $G/G_1 = [d]$, and define $o_k(P_i)$ to be $o_k(x_i)$ if x_i is chosen to be a permutation acting on $[d]$ with cycle structure P_i. Let $\mathfrak{o}_k$ be the number of orbits of H on $[d]_k$.

From results of [12] proven with representation theory, we may conclude that:

Corollary 3.3. *Each k with $d/2 \geq k \geq 2$ satisfies either $\mathfrak{g}_k = \mathfrak{g}_{k-1}$ or $\mathfrak{o}_k = \mathfrak{o}_{k-1}$.*

In addition, we have proven two theorems and one lemma which limit the ramification types.

Theorem 3.4. *If $\mathfrak{g}_2 - \mathfrak{g}_1 \leq 0$, then either $d \leq 28$ or the ramification type belongs to $\mathcal{F}$, which will be discussed in Remark 3.5.*

Remark 3.5. *For brevity we will not list $\mathcal{F}$, but we will select representative examples. In this discussion, let $1 \leq a < d$ be an integer such that $\gcd\,(a, d) = 1$. h^k means k instances of the value h. Moreover, for each ramification type in $\mathcal{F}$, $\mathfrak{g}_2 = \mathfrak{g}_1 = 0$.*

- $\{[1^{d-2}, 2], [a, d-a], [d]\}$
- $\{[1^{d-2}, 2], [1^3, 2^{(d-3)/2}], [1, 2^{(d-1)/2}], [d]\}$
- $\{[1^{d-2}, 2], [1^2, 2^{(d-2)/2}], [2^{d/2}], [a, d-a]\}$
- $\{1^{d-2}, 2], [1^3, 2^{(d-3)/2}], [1, 2^{(d-1)/2}], [1, 2^{(d-1)/2}], [1, 2^{(d-1)/2}]\}$
- $\{[1^2, 2^{(d-2)/2}], [1, 3, 4^{(d-4)/4}], [4^{d/4}]\}$
- $\{[1, 2^{(d-1)/2}], [1, 3^{(d-1)/3}], [3, 4, 6^{(d-7)/6}]\}$

Theorem 3.6. *If $d \geq 28$ then $\mathfrak{g}_3 - \mathfrak{g}_2 \geq 1$.*

Lemma 3.7. *Every ramification type in $\mathcal{F}$ has $\mathfrak{g}_4 - \mathfrak{g}_3 \geq 1$.*

3.3. **Proof of Theorem 1.2.** Consider $H = \mathrm{Gal}\,(\Omega/N)$. The indecomposability of f implies that $N/\mathbb{C}(t)$ is a minimal extension, meaning that there are no intermediate fields, so H is a maximal subgroup of $G = A_d$ or $G = S_d$. We claim that if $d > 28$, then H is either a 2-set stabilizer or a 1-set stabilizer. By Lemma 3.1, this will imply our result since $\deg f = [G : H] = d(d-1)/2$ or d. The cases where $d \leq 28$ are easy to treat, and examples are mentioned in Section 5. We use casework, first on whether H acts transitively on $[d]$, and second on whether H acts primitively on $[d]$. A group acts primitively if it preserves no nontrivial partition of $[d]$. First, since $\mathfrak{g}_3 - \mathfrak{g}_2 \geq 1$, Corollary 3.6 implies that $\mathfrak{o}_3 = \mathfrak{o}_2$.

3.3.1. *Case 1: The group H acts intransitively.* In this case, the group H must preserve a set of size k. Therefore, it must also preserve the remaining set of $d-k$ elements. Since H is a maximal subgroup of G, it must arbitrarily permute both the set of size k and the set of size $d-k$, so $H = (S_k \times S_{d-k}) \cap G$. One can see that if $k \geq 3$, then $\mathfrak{o}_2 = 3$ and $\mathfrak{o}_3 = 4$, which is contradiction.

3.3.2. *Case 2: The group H acts transitively.*
Case 2a: The group H acts imprimitively. If H is transitive but imprimitive, it must preserve a partition, of which one block has size k. Due to transitivity, all blocks have size k. By maximality, the permutation action on these blocks is symmetric, so $H = (S_k \wr S_{n/k}) \cap G$. Here, we can see that $\mathfrak{o}_2 = 2$ and that $\mathfrak{o}_3 = 3$ unless $k = 2$ or $k = \frac{d}{2}$, when $\mathfrak{o}_3 = 2$. Therefore, unless $k = 2$ or $k = \frac{d}{2}$, there is a contradiction. Due to the transitivity of H, $2 = \mathfrak{o}_2 \neq \mathfrak{o}_1 = 1$. Therefore, $\mathfrak{g}_2 = \mathfrak{g}_1$ by Corollary 3.3. By Lemma 3.4, the ramification type is in $\mathcal{F}$ and by Lemma 3.7 $\mathfrak{g}_4 - \mathfrak{g}_3 \geq 1$. Thus, by Corollary 3.3 $\mathfrak{o}_4 = \mathfrak{o}_3$, which can be easily disproven; in particular, if $k = 2$ or $k = \frac{n}{2}$, $\mathfrak{o}_4 = 3$.
Case 2b: The group H acts primitively. It was proven in [6] that for a primitive group action, $\mathfrak{o}_3 = \mathfrak{o}_2$ implies that $\mathfrak{o}_3 = 1$, that is, the group H is 3-homogeneous and a maximal subgroup of S_d or A_d. The following folk result severely limits possibilities for H.

Lemma 3.8. *Let H be a 3-homogenous nonalternating maximal subgroup of $G = S_d$ or A_d. Then, one of the following is true:*

(1) $\mathrm{PSL}_2(q) \leq H \leq \mathrm{P\Gamma L}_2(q)$ *and* $d = q+1$.
(2) $H \leq \mathrm{AGL}_k(2)$ *and* $d = 2^k$.
(3) H *is a Mathieu group* M_d*;* $d = 22, 23, 24$ *in these cases.*
(4) $H = M_{11}$ *acting on cosets of* $\mathrm{PSL}_2(11)$ *and* $d = 12$.
(5) $H \leq \mathrm{AGL}_1(q)$ *with* $q = d \in \{8, 32\}$.

Remark 3.9. *Here,* $\mathrm{PSL}_2(q)$*,* $\mathrm{P\Gamma L}_2(q)$*, and* $\mathrm{AGL}_k(2)$ *are the usual groups of linear, semilinear, and affine transformations. More information about these groups is in [16, Section VI.1].*

Of these, cases $3, 4, 5$ are easy to treat, since there are only finitely many possibilities.

Let $E = \{x_1, x_2, \ldots, x_r\}$ be the multiset of local monodromy elements for the rational function $f(X)$. For x in G, let $Cl_G(x)$ be the conjugacy class of x in G, let $o(x)$ be the number of orbits of x on G/H, and let $\mathrm{Fix}(x)$ be the number of fixed points of x on G/H. Then, Riemann–Hurwitz on Ω^H/Ω^G gives

$$-2 = -2[G:H] + \sum_{x \in E}([G:H] - o(x)). \tag{3.10}$$

If $\mathrm{Ord}(x) = k$ is the smallest positive integer that $x^k = 1$, Burnside's Lemma gives

$$o(x) = \frac{1}{\mathrm{Ord}(x)} \sum_{j=1}^{\mathrm{Ord}(x)} \mathrm{Fix}(x^j).$$

The following lemma allows us to bound the number of fixed points of x.

Lemma 3.11. *For $x \in G$ and all $i \in \mathbb{N}$,*

$$\mathrm{Fix}(x) < \frac{|G|}{|Cl_G(x^i)|}$$

Proof. Observe that

$$\begin{aligned}\mathrm{Fix}(x) &= \frac{|\{g \in G, xgH = gH\}|}{|H|} = \frac{|\{g \in G, g^{-1}xg \in H\}|}{|H|} \\ &= \frac{|Cl_G(x) \cap H| \cdot |C_G(x)|}{|H|} < |C_G(x)| \leq |C_G(x^i)| = \frac{|G|}{|Cl_G(x^i)|},\end{aligned}$$

where $C_G(x)$ is the centralizer of x with respect to G. □

The following results ensure that $Cl_G(x^i)$ is relatively large. The first exploits the linear structure of the group H, whereas the second uses results on sizes of conjugacy classes of S_d.

Lemma 3.12. *[12, Lemma 8.0.61] If H satisfies cases 1 or 2 of Lemma 3.8, every non-identity element $x \in H$ fixes at most half the elements in the usual action of G.*

Lemma 3.13. *[12, Corollary 8.0.59] If $d > 5$ and $x \in S_d$ has prime order and has at most $\frac{d}{2}$ fixed points in the usual degree-d action, then*

$$|Cl_{S_d}(x)| \geq \frac{e}{2}\left(\frac{2d}{e}\right)^{d/4}.$$

We now bound $\mathrm{Fix}(x^j)$. If x^j is not conjugate to an element of H, then $\mathrm{Fix}(x^j) = 0$, since $x^j(gH) = gH$ implies $g^{-1}x^jg \in H$. Otherwise, let x^i be a power of x^j which has prime order. Since x^i is conjugate to an element of H, it has at most $d/2$ fixed points by Lemma 3.12.

As $2 \cdot |Cl_G(x^i)| \geq |Cl_{S_d}(x^i)|$,

$$|Cl_G(x^i)| \geq \frac{e}{4}\left(\frac{2d}{e}\right)^{d/4}.$$

Thus, we bound (using Lemma 3.11 and Lemma 3.13)

$$\mathrm{Fix}(x^j) < \frac{|G|}{|Cl_G(x^i)|} < \frac{|G|}{e/4(2d/e)^{d/4}} = [G:H]\frac{|H|}{e/4(2d/e)^{d/4}}$$

We compute that

$$o(x) = \frac{1}{\mathrm{Ord}(x)}\sum_{j=1}^{\mathrm{Ord}(x)} \mathrm{Fix}(x^j) < \frac{[G:H]}{\mathrm{Ord}(x)}\left(1 + \frac{(\mathrm{Ord}(x)-1)|H|}{e/4(2d/e)^{d/4}}\right).$$

Combining this with (3.10), we get

$$\begin{aligned} -2 &= -2[G:H] + \sum_{x\in E}([G:H]-o(x)) \\ &> [G:H]\left(-2 + \sum_{x\in E}\left(1 - \frac{1}{\mathrm{Ord}(x)} - \frac{\mathrm{Ord}(x)-1}{\mathrm{Ord}(x)}\frac{|H|}{e/4(2d/e)^{d/4}}\right)\right) \\ &= [G:H]\left(-2 + \sum_{x\in E}\left(1 - \frac{1}{\mathrm{Ord}(x)}\right)\cdot\left(1 - \frac{|H|}{e/4(2d/e)^{d/4}}\right)\right) \end{aligned}$$

We provide the following bound on $\sum_{x\in E}\left(1 - \frac{1}{\mathrm{Ord}(x)}\right)$:

Lemma 3.14. *If $d > 5$,*

$$\sum_{x\in E}\left(1 - \frac{1}{\mathrm{Ord}(x)}\right) \geq \frac{85}{42}.$$

Proof. Let $\mathfrak{g}$ be the genus of Ω. Then by applying Riemann–Hurwitz to Ω/Ω^G, we have

$$(2\mathfrak{g}-2) = -2|G| + \sum_{x\in E}(|G| - \check{o}(x)),$$

where $\check{o}(x)$ is the number of orbits of x on G. Since $\frac{|G|}{\mathrm{Ord}(x)} = \check{o}(x)$, this equation becomes

$$2 + \frac{2\mathfrak{g}-2}{|G|} = \sum_{x\in E}\left(1 - \frac{1}{\mathrm{Ord}(x)}\right),$$

after division by $|G|$. If $\mathfrak{g} > 1$ our result follows easily by casework. If $\mathfrak{g} \leq 1$, it is known that the group G is solvable or A_5, neither of which are A_d or S_d with $d > 5$. □

It suffices to show $\left(1 - \frac{|H|}{(e/4)(2d/e)^{d/4}}\right) \geq \frac{84}{85}$, or $|H| \leq (1/85)(e/4)(2d/e)^{d/4}$. We prove this for all $d \geq 23$ and treat the remaining cases manually. In case 1 of Lemma 3.8,

$$|H| \leq |\mathrm{P\Gamma L}_2(d-1)| = (d-2)(d-1)(d)\log_p(d-1) \leq d^3\log_2(d)$$

where p is a prime dividing $d-1$. This is smaller than $(1/85)e/4(2d/e)^{d/4}$ whenever $d > 23$. In case 2 of Lemma 3.8,

$$|H| \leq |\mathrm{AGL}_k(2)| = 2^k\prod_{i=0}^{k-1}(2^k - 2^i) < 2^{(k(k+1))} = d^{1+\log_2(d)}.$$

This is smaller than $(1/85)e/4(2d/e)^{d/4}$ for all powers of two higher than 16.

Theorem 3.4 is proven in Section 4, Theorem 3.6 is proven with similar methods to Theorem 3.4, Lemma 3.7 is a direct computation, and we may conclude.

4. Proof of Theorem 3.4

Instead of determining only valid ramification types, we instead determine all collections of multisets $P_1, P_2, \ldots, P_s$ such that $\mathfrak{g}_2 - \mathfrak{g}_1 \leq 0$, and $\mathfrak{g}_2 \geq 0, \mathfrak{g}_1 \geq 0$. We then synthesize which of these collections are ramification types in Section 5. By (3.2) for $k = 1$ and $k = 2$,

$$2\mathfrak{g}_1 - 2 = -2d + \sum_k (d - o_1(P_k)) = -2d + \sum_k (d - |P_k|)$$

and

$$2\mathfrak{g}_2 - 2 = -2\binom{d}{2} + \sum_k \left(\binom{d}{2} - o_2(P_k)\right) \tag{4.1}$$

Define the non-negative function Q_k for a multiset as follows:

$$Q_k = \left(\sum_{\substack{i \in P_k \\ i \text{ even}}} (i-2) + \sum_{\substack{i \in P_k \\ i \text{ odd}}} (i-1) + \sum_{i,j \in P_k} (i - (i,j)) \right).$$

We prove a computational result about this Q_k.

Lemma 4.2.

$$4(\mathfrak{g}_2 - \mathfrak{g}_1) = (2d-8)\mathfrak{g}_1 - (4d-8) + \sum_k Q_k.$$

Proof. We first express $o_2(P_k)$ in terms of P_k. Also, take cycle indices modulo the size of the cycle, and let x_k be a permutation with cycle structure P_k. First, consider sets in $[d]_2$ in which both elements lie in the same cycle of x_k on $[d]$. Write this cycle as $(y_1, y_2, \ldots, y_i)$. The orbit under x_k of the set $\{y_a, y_b\}$ with $a \neq b$ consists of all the sets $\{y_{a+r}, y_{b+r}\}$. If i is odd then there are $\frac{i-1}{2}$ orbits, and if i is even then there are $\frac{i}{2}$ orbits. Summing over all cycles of x_k on $\{1, 2, \ldots, d\}$, the number of orbits of x_k on sets in $[d]_2$ which consist of two elements lying in the same orbit of x_k on $[d]$ is

$$\sum_{\substack{i \in P_k \\ i \text{ odd}}} \frac{i-1}{2} + \sum_{\substack{i \in P_k \\ i \text{ even}}} \frac{i}{2} = \frac{d}{2} - \frac{O_k}{2}$$

where O_k denotes the number of odd elements in P_k. Next, consider sets in $[d]_2$ consisting of elements from two different cycles of x_k on $[d]$. Letting $Y = (y_1, \ldots, y_i)$ and $Z = (z_1, \ldots, z_j)$ be distinct cycles of x_k on $[d]$, then for any y_a and z_b the x_k orbit of $\{y_a, z_b\}$ has size $\operatorname{lcm}(i,j)$, so the number of orbits on the collection of sets in $[d]_2$ having one element in Y and Z is $ij/\operatorname{lcm}(i,j) = \gcd(i,j)$. Thus, the contribution from different cycles of x_k on $[d]$ is

$$\frac{1}{2} \sum_{i,j \in P_k} \gcd(i,j) - \frac{1}{2} \sum_{i \in P_k} \gcd(i,i) = \frac{1}{2} \sum_{i,j \in P_k} \gcd(i,j) - \frac{d}{2}.$$

Adding this to the previous count yields the formula

$$o_2(x_k) = \frac{1}{2} \sum_{i,j \in P_k} \gcd(i,j) - \frac{O_k}{2}.$$

Hence, by (4.1),

$$4\mathfrak{g}_2 - 4 = -2d(d-1) + \sum_k (d(d-1) + O_k - \sum_{i,j \in P_k} \gcd(i,j)).$$

Next we compute

$$\begin{aligned} 4(\mathfrak{g}_2 - 1) - (2d-4)(\mathfrak{g}_1 - 1) = (d-2)(2d - \sum_k (d - |P_k|)) - 2d(d-1) \\ + \sum_k \left(d(d-1) + O_k - \sum_{i,j \in P_k} \gcd(i,j) \right) \\ = -2d + \sum_k \left(\sum_{\substack{i \in P_k \\ i \text{ even}}} (i-2) + \sum_{\substack{i \in P_k \\ i \text{ odd}}} (i-1) + \sum_{i,j \in P_k} (i - (i,j)) \right), \end{aligned}$$

so that

$$4(\mathfrak{g}_2 - \mathfrak{g}_1) = (2d-8)\mathfrak{g}_1 - (4d-8) + \sum_k Q_k. \qquad \square$$

Clearly, we may restrict our attention to cases in which $\mathfrak{g}_1 \leq 2$, or else clearly $\mathfrak{g}_2 - \mathfrak{g}_1 > 0$.

Although the statement and proof of Lemma 4.2 are elementary, this identity (and the definition of Q_k) is a key innovation enabling us to prove Theorem 3.4. Lemma 4.2 is powerful because Q_k is always nonnegative and thus whenever $Q_k > 4d - 8$ for a multiset P_k we can rule it out from being present in a collection of multisets in which $\mathfrak{g}_2 - \mathfrak{g}_1 \leq 0$. For example, we can show none of P_k can be $[1^5, d-5]$, or else $Q_k \geq 6d - 37$.

This intuition is captured in the following lemma.

Lemma 4.3. *Assume that the multiset P has ℓ elements less than or equal to k, and the sum of these elements is R. Then,*

$$\sum_{\substack{i \leq k, j > k \\ i,j \in P}} (j - (i,j)) \geq \ell(d-R)/2.$$

Proof. For $j > k$ but $i \leq k$, then $j - (i,j)$ is at least $\frac{j}{2}$ since (i,j) cannot exceed $j - (i,j)$. Thus,

$$\sum_{\substack{i \leq k, j > k \\ i,j \in P}} (j - (i,j)) \geq \sum_{\substack{i \leq k, j > k \\ i,j \in P}} (j/2) = \ell(d-R)/2. \qquad \square$$

We developed a computer program which first found all multisets P_k that satisfy $Q_k \leq 4d - 4$ with a depth-first search, an algorithm which has the advantages of highly efficient memory management and recursive implementation. For each i, it kept track of the number of appearances of $1, 2, \ldots, i$, represented by $f_1, f_2, \ldots, f_i$. Then, Lemma 4.3 often allowed it to eliminate these as possibilities. Finally, the program put these together to form collections of multisets satisfying our conditions [27]. We found several infinite families (including $\mathcal{F}$) in addition to sporadic cases. We then used various techniques, described in Section 5, to determine which of these collections corresponded to indecomposable rational functions with monodromy group A_d or S_d.

5. Existence of Rational Functions with Specified Ramification Type

5.1. **Conditions for Existence.** The proof of Theorem 1.2 in Section 3 concludes with several batches of multisets, but does not show which of these are actually the ramification type of a rational function. In [18], the elements of the family $\mathcal{F}$ and some other families are treated; however, we need additional methods to handle some of the other batches of multisets arising in our work.

First, we state a consequence of Riemann's Existence Theorem and basic algebraic topology, which provides necessary and sufficient conditions for the existence of an indecomposable rational function with specified local monodromy elements.

Theorem 5.1. *[1, Theorem 15.9.4] For any subgroup G of S_n and any $x_1, x_2, \ldots, x_s \in S_n$, there exists a degree-$n$ indecomposable rational function $f(X)$ with local monodromy elements $x_1, x_2, \ldots, x_s$ and monodromy group G if and only if all of the following hold:*

1. *$x_1, x_2, \ldots, x_s$ generate G;*
2. *$x_1 x_2 \ldots x_s = 1$;*
3. *$2n - 2 = \sum_{i=1}^{s}(n - o(x_s))$;*
4. *G is a primitive subgroup of S_n.*

Since the ramification type gives us the cycle structures of each local monodromy element, we will often have to answer the following question. Given the cycle structures of $x_1, x_2, \ldots, x_s$ on $[d]$, does there exist $x_1, x_2, \ldots, x_s \in S_d$ such that $x_1 x_2 \ldots x_s = 1$ and $x_1, x_2, \ldots, x_s$ generate A_d or S_d?

After we have found these $x_1, x_2, \ldots, x_s$, we will then "lift them" by viewing them as permuting the left cosets G/H, where H is the previously described maximal subgroup of G. This creates a new set of permutations $x_1', x_2', \ldots, x_s'$ in $S_{[G:H]}$. If we verify the numerical condition (condition (3) in Theorem 5.1) for both $x_1, x_2, \ldots, x_s$ and $x_1', x_2', \ldots, x_s'$, then we have a degree-$[G : H]$ rational function with monodromy group $G = S_d$ or A_d, since changing the representation of the elements $x_1, x_2, \ldots, x_s$ does not change the group they generate or their product, verifying conditions (1) and (2). Since H is maximal, the action of G on the cosets G/H is primitive, verifying condition (4).

We present two methods for eliminating collections which do not correspond to rational functions, one based on complex analysis and one based on representation theory.

5.2. **Proving Nonexistence.**

5.2.1. *Using Complex Analysis.* Assume that a ramification type candidate contains multisets P_1 and P_2 of size at least 2, and that there exists an integer g which divides all elements in each of P_1 and P_2. Then, we claim that if for a rational function f, $E_f(p_1) = P_1$ and $E_f(p_2) = P_2$ for points p_1 and p_2, the rational function f is not indecomposable, violating the hypotheses of Theorem 1.2.

Proof. Apply a Möbius transformation to f and the points p_1 and p_2 which takes f to h, p_1 to 0 and p_2 to ∞ such that $E_h(0) = P_1$ and $E_h(\infty) = P_2$. If $h = P/Q$, then this implies P is a g-th power and Q is a g-th power, which means h is the g-th power of a rational function and thus decomposable. □

We used both this result and several more complicated variants, all of which showed that certain candidate ramification types could not occur for indecomposable rational functions.

5.2.2. *Using Representation Theory.* We focus on the product-one condition, which is relatively well understood. We use the following formula, due to Frobenius.

Theorem 5.1. *[14, Theorem A.1.9] Let G be a finite group and let $C_1, C_2, \ldots, C_s$ be conjugacy classes in G. Then the number of product-one tuples $(x_1, x_2, \ldots, x_s)$ with $x_i \in C_i$ is*

$$\frac{|C_1||C_2|\cdots|C_s|}{|G|}\sum_{\chi}\frac{\chi(C_1)\chi(C_2)\cdots\chi(C_s)}{\chi(1)^{s-2}},$$

where the sum is taken over all irreducible complex characters χ of G.

Note that Frobenius's formula does not determine the group generated by the elements x_1, x_2, …, x_s. To work around this, we use enumerative combinatorics. To this end, assume that we calculate the number of product-one tuples $(x_1, x_2, \ldots, x_s)$ where $x_i \in C_i$ as the value v. Then, assume that we have subgroups $G^1, G^2, \ldots, G^k$ of G such that the sum over j of the number of product-one tuples $x_1, x_2, \ldots, x_s \in G^j$ and $x_i \in (C_i \cap G^j)$ is the value v, but for each distinct j, k there are no product-one tuples with each x_i being in $C_i \cap G^j \cap G^k$. Then we would be able to rule out the existence of a product-one tuple $x_1, x_2, \ldots, x_s \in G = A_d$ or S_d which generates G, because all such product one triples generate subgroups of $G^1, G^2, \ldots, G^k$, not G.

For example, consider the ramification type candidate $[1^4, 3^8], [7^4], [2^{14}]$ which satisfies all of our numerical conditions in which $G = A_{28}$ and $H = G_2$, a two-set stabilizer, since $\mathfrak{g}_2 = \mathfrak{g}_1 = 0$. The only way to eliminate this as a ramification type candidate is through the previously described method. First, we determine through Frobenius's formula on A_{28} the number of product-one tuples $x_1, x_2, x_3 \in A_{28}$ with cycle structures $[1^4, 3^8], [7^4], [2^{14}]$. Fixing

x_2 as (1, 2, 3, 4, 5, 6, 7)(8, 9, 10, 11, 12, 13, 14)(15, 16, 17, 18, 19, 20, 21)(22, 23, 24, 25, 26, 27, 28), we find that there are 115248 3-tuples which satisfy $x_1x_2x_3 = 1$ with Frobenius's formula. Applying Frobenius's formula with these conjugacy classes to a group L with order 1092 and a group O with order 1344, we obtained that there were 28812 solutions in which the group generated by x_1, x_2, x_3 was a subgroup of L and 86436 in which the group generated by x_1, x_2, x_3 was a subgroup of O. Applying Frobenius's formula to the maximal subgroups of both L and O gives zero, so there are exactly 115248 product-one triples (x_1, x_2, x_3) in which the group generated is L or O, allowing us to rule out $[1^4, 3^8], [7^4], [2^{14}]$ as a possible ramification type. These counts were done in Magma [28].

6. Outline of Proof of Theorem 1.3

For the sake of simplicity, we give the proof of Theorem 1.3 only in the case of $t = 2$. In this case, f is a degree-ℓ^2 indecomposable rational function with monodromy group G, and G is in Case (C3.3), meaning that it is of *product type*. In particular, this means that we can view G as acting on the set of ordered tuples $(i, j) \in [\ell] \times [\ell]$, where $1 \leq i, j \leq \ell$, and that G acts transitively on this set. G must be a subgroup of $S_\ell \wr S_2 = S_\ell^2 \rtimes S_2$, so we can represent each element of G as (u, v) or $(u, v)\sigma$, where $u, v \in S_\ell$ and the semidirect action acts by $\sigma(a, b) = (b, a)$, where $(a, b) \in [\ell] \times [\ell]$. In addition, this action satisfies $\sigma(u, v)\sigma = (v, u)$. To see this, observe that

$$\sigma(u, v)\sigma(i, j) = \sigma(u, v)(j, i) = \sigma(u(j), v(i)) = (v(i), u(j)) = (v, u)(i, j).$$

Recall that G acts transitively on the set of ℓ^2 letters, since $\deg f = \ell^2$. Let H be the point stabilizer of G, or the group of all elements which fix the tuple $(1, 1)$. Then, the coset space G/H can be represented as $[\ell] \times [\ell]$. Let K be the kernel of the homomorphism from G to S_2, or $G \cap S_\ell^2$. Thus, G/K is a subgroup of S_2, so $[G : K]$ is 1 or 2. The coset space $G/(H \cap K)$ can be represented as (i, j) or $(i, j)\sigma$, where elements in K are in the coset space G/H prescribes and elements not in K in the coset (i, j) of G/H are in the coset $(i, j)\sigma$ of $G/(H \cap K)$.

Lemma 6.1. *K is a normal subgroup of G of index 2.*

Proof. Suppose that $K = G$, or that G is a subgroup of S_ℓ^2. From results of [25, p. 47] we see that since f is indecomposable, G must act primitively on the coset space G/H. If $K = G$, then one can partition the coset space G/H into the ℓ blocks $B_1, B_2, \ldots, B_\ell$, where B_i consists of the elements (i, j) and $j \in [\ell]$. This would imply that G is imprimitive, so $K \neq G$. This implies that σ is in G, so that $[G : K] = 2$, whence K is normal in G. □

We will now show that every element of G is the product of an element from H and K; in other words, $G = HK$. It suffices to show that K acts transitively on the coset space

G/H. Recall that G acts transitively on the coset space G/H. This means that for each $(i,j) \in [\ell] \times [\ell]$, either $(u,v)\sigma(1,1) = (i,j)$ or $(u,v)(1,1) = (i,j)$. If the second case holds, then the result is clear. Otherwise, observe that the first result is still equivalent to the second case, since $\sigma(1,1) = (1,1)$. This shows that the orbit of K on $(1,1)$ is all of (i,j), and we may conclude.

Let K_1 and K_2 be the elements of K which fix the set of the cosets of G/H of the form $(1,i)$ and $(i,1)$, where $i \in [\ell]$, respectively.

We now prove the following results relating the sizes of the aforementioned groups. These will later be used in the Riemann–Hurwitz formula.

Lemma 6.2. *$[G:H] = \ell^2$, $[G:H\cap K] = 2\ell^2$, $[K:K_1] = [K:K_2] = \ell$.*

Proof. The first result follows directly from defining H as the point stabilizer of G. The second follows because $G = HK$ and K is a normal subgroup of G. This means that

$$\frac{|G|^2}{2\ell^2} = |H||K| = |G||H\cap K|,$$

so that $[G:H\cap K] = 2\ell^2$. The final result follows from the transitivity of K on G/H. □

6.1. **Riemann–Hurwitz in various extensions.** Applying the Riemann–Hurwitz genus formula to the extension Ω^H/Ω^G yields

$$-2 = -2[G:H] + \sum_{i=1}^{r}\big([G:H] - o(g_i)\big) = -2\ell^2 + \sum_{i=1}^{r}\big(\ell^2 - o(g_i)\big), \tag{6.3}$$

where $g_1,\dots,g_r$ are elements of G and $o(g_i)$ denotes the number of orbits of the group $\langle g_i\rangle$ on the set G/H of left cosets of H in G. Here the g_i are local monodromy elements associated to the critical values $P_1,\dots,P_r$ of the rational function that corresponds to the field extension Ω^H/Ω^G. Thus we may assume that the product $g_1g_2\dots g_r$ equals 1, and that G is generated by $g_1,g_2,\dots,g_r$.

Writing $\mathfrak{g}$ for the genus of $\Omega^{H\cap K}$, Riemann–Hurwitz for $\Omega^{H\cap K}/\Omega^G$ says

$$2\mathfrak{g} - 2 = -4\ell^2 + \sum_{i=1}^{r}\big(2\ell^2 - \hat{o}(g_i)\big), \tag{6.4}$$

where $\hat{o}(g_i)$ denotes the number of orbits of $\langle g_i\rangle$ on the set $G/(H\cap K)$.

Writing $\mathfrak{g}_0$ for the genus of Ω^K, Riemann–Hurwitz for Ω^K/Ω^G yields

$$2\mathfrak{g}_0 - 2 = -4 + |\{i\colon 1\le i\le r,\ g_i\notin K\}|, \tag{6.5}$$

since g_i acts as a 2-cycle on the cosets G/K if $g_i \notin K$, and g_i acts as the identity otherwise.

Write $\mathfrak{g}_j$ for the genus of Ω^{K_j}. If $g_i \in K$ then write $g_i = (u_i, v_i)$ with $u_i, v_i \in S_\ell$. In this case P_i lies under two points of Ω^K, and the local monodromy elements of these points in Ω/Ω^K are (u_i,v_i) and (v_i,u_i). If $g_i \notin K$ then write $g_i = (u_i,v_i)\sigma$ with $u_i,v_i \in S_\ell$. In this case P_i lies under a single point of Ω^K, and the local monodromy element of this point in Ω/Ω^K is (u_iv_i, v_iu_i). Note that u_iv_i and v_iu_i are conjugate in S_ℓ, and hence have the same orbit lengths. Let I be the set of integers i with $1 \le i \le r$ for which $g_i \in K$, and let J be the set of i's for which $g_i \notin K$. For $i \in I$, let A_i (resp., B_i) be the multiset of orbit-lengths of u_i (resp., v_i) in the usual degree-ℓ action of S_ℓ. For $i \in J$, let C_i be the multiset of orbit-lengths of $u_i v_i$ in the usual degree-ℓ action of S_ℓ. Then Riemann–Hurwitz for Ω^{K_j}/Ω^K yields

$$2\mathfrak{g}_j - 2 = \ell(2\mathfrak{g}_0 - 2) + \sum_{i\in I}\bigl(\ell - |A_i| + \ell - |B_i|\bigr) + \sum_{i\in J}\bigl(\ell - |C_i|\bigr), \tag{6.6}$$

and Riemann–Hurwitz for $\Omega^{H\cap K}/\Omega^{K_2}$ yields

$$\begin{aligned} 2\mathfrak{g} - 2 = \ell(2\mathfrak{g}_2 - 2) &+ \sum_{i\in I}\sum_{\substack{a\in A_i\\ b\in B_i}}\bigl(a - (a,b) + b - (a,b)\bigr) \\ &+ \sum_{i\in J}\sum_{a,b\in C_i}\bigl(a - (a,b)\bigr). \end{aligned} \tag{6.7}$$

6.2. **Bounding the genus of $\Omega^{H\cap K}$.** In this section we prove

Proposition 6.8. $\mathfrak{g} \le 2\ell + 1$.

The proof relies on the following lemma, which relates the actions of elements of G on the coset spaces G/H and $G/(H\cap K)$; we will prove Proposition 6.8 by applying this to the elements g_i, in combination with Riemann–Hurwitz for $\Omega^{H\cap K}/\Omega^G$ and Ω^H/Ω^G.

Lemma 6.9. *Any $g \in K$ satisfies $2o(g) = \hat{o}(g)$. For $g \in G\setminus K$, if we write $g^2 = (w, w')$ with $w, w' \in S_\ell$ then $2o(g) - \hat{o}(g)$ is the number of odd-length orbits of w on $\{1, 2, \dots, \ell\}$, which equals the number of odd-length orbits of w' on $\{1, 2, \dots, \ell\}$, and also equals the number of odd-length orbits of g on G/H.*

Proof. Pick any $g \in K$ and let $\mathcal{O}$ be an orbit of $\langle g\rangle$ on G/H. We may view $\mathcal{O}$ as consisting of pairs (i, j) of elements of $\{1, 2, \dots, \ell\}$, in which case both $\mathcal{O}$ and $\mathcal{O}\sigma := \{(i, j)\sigma \colon (i, j) \in \mathcal{O}\}$ are orbits of $\langle g\rangle$ on $G/(H\cap K)$. Thus $\hat{o}(g) = 2o(g)$.

Henceforth suppose that g is in $G\setminus K$, and write $g = (u, v)\sigma$ with $u, v \in S_\ell$. Here g maps $(i, j) \mapsto (u(j), v(i))\sigma$ and $(i, j)\sigma \mapsto (u(j), v(i))$. It follows that if $\mathcal{O} := (w_1, \dots, w_r)$ is an orbit of $\langle g\rangle$ on G/H then in its action on $G/(H\cap K)$ g maps $w_i \mapsto w_{i+1}\sigma \mapsto w_{i+2}$, where indices are taken mod r. Therefore if r is even then $\mathcal{O}\cup\mathcal{O}\sigma$ is the union of two $\langle g\rangle$-orbits each of length r, while if r is odd then $\mathcal{O}\cup\mathcal{O}\sigma$ is a single $\langle g\rangle$-orbit of length $2r$. Thus $2o(g) - \hat{o}(g)$ is the number of odd-length orbits of g on G/H.

Suppose that the orbit of $(i, j) \in G/H$ under $(u, v)\sigma$ has odd length. Say this length is r. Note that the square of $(u, v)\sigma$ is (uv, vu), since $\sigma(u, v)\sigma = (v, u)$, so that $(u, v)\sigma(u, v)\sigma = (u, v)(v, u) = (uv, vu)$. Hence the orbit of (i, j) under (uv, vu) has length r. This means that r is the least common multiple of the lengths of the uv-orbit of i and the vu-orbit of j. We claim that these two orbits have the same length. The condition that r is also the length of the $(u,v)\sigma$-orbit of $(i,j)\in G/H$ implies that $i=(uv)^{\frac{r-1}{2}}uj$ and $j=v(uv)^{\frac{r-1}{2}}i$. For any $z>0$, if $(uv)^z$ fixes i then

$$(vu)^z j=(vu)^z v(uv)^{\frac{r-1}{2}}i=v(uv)^{z+\frac{r-1}{2}}i=v(uv)^{\frac{r-1}{2}}i=j,$$

so that $(vu)^z$ fixes j; and likewise if $(vu)^z$ fixes j then $(uv)^z$ fixes i. Hence r is the length of the uv-orbit of i. Since $j:=v(uv)^{\frac{r-1}{2}}i$ is uniquely determined by the values of u,v,i, it follows that $2o(g)-\hat{o}(g)$ is the number of odd-length orbits of uv, which equals the number of odd-length orbits of vu. □

Corollary 6.10. *Every $g\in G$ satisfies*

$$\ell^2-o(g)\geq\frac{\ell-1}{2}\bigl(2o(g)-\hat{o}(g)\bigr).$$

Proof. If $g\in K$ then the result follows from Lemma 6.9. Henceforth assume $g\in G\setminus K$. Writing $k:=2o(g)-\hat{o}(g)$, Lemma 6.9 implies that $k\leq\ell$ and also k is the number of odd-length orbits of g on G/H. Hence g has at most ℓ fixed points on G/H, so that $o(g)\leq\ell+\frac{\ell^2-\ell}{2}=\frac{\ell^2+\ell}{2}$, whence

$$\ell^2-o(g)\geq\frac{\ell^2-\ell}{2}\geq k\cdot\frac{\ell-1}{2},$$

which completes the proof of Corollary 6.10. □

Proof of Proposition 6.8. Multiplying both sides of equation (6.3) by 2 and subtracting the resulting equation from (6.4) yields

$$2\mathfrak{g}+2=\sum_{i=1}^{r}\bigl(2o(g_i)-\hat{o}(g_i)\bigr).$$

By Corollary 6.10 and equation (6.3), it follows that

$$2\mathfrak{g}+2=\sum_{i=1}^{r}\bigl(2o(g_i)-\hat{o}(g_i)\bigr)\leq\frac{2}{\ell-1}\sum_{i=1}^{r}\bigl(\ell^2-o(g_i)\bigr)=\frac{2}{\ell-1}\cdot(2\ell^2-2)=4\ell+4,$$

so that $\mathfrak{g}\leq 2\ell+1$. □

6.3. **Restricting the ramification in Ω^{K_j}/Ω^K.** We will now use Proposition 6.8 in order to deduce constraints on the ramification in the extensions Ω^{K_1}/Ω^K. Recall that I and J are finite sets and that for each $i\in I$ the multisets A_i and B_i are partitions of n, while for each $i\in J$ the multiset C_i is a partition of n. Combining (6.7) with Proposition 6.8 yields

$$\ell(6-2\mathfrak{g}_2)\geq\sum_{i\in I}\sum_{\substack{a\in A_i\\ b\in B_i}}\bigl(a+b-2(a,b)\bigr)+\sum_{i\in J}\sum_{a,b\in C_i}\bigl(a-(a,b)\bigr).\tag{6.11}$$

Likewise, by (6.3), (6.4), and Lemma 6.9,

$$\begin{aligned}2\mathfrak{g}-2=-4+\sum_{i\in J}(\#\text{ of odds in }C_i)=\ell(2\mathfrak{g}_2-2)+\sum_{i\in I}\sum_{\substack{a\in A_i\\ b\in B_i}}\bigl(a+b-2(a,b)\bigr)\\ +\sum_{i\in J}\sum_{a,b\in C_i}\bigl(a-(a,b)\bigr).\end{aligned}\tag{6.12}$$

We will use this in combination with (6.5) and (6.6) in order to deduce strong restrictions on the possibilities for the A_i's, B_i's, and C_i's.

6.4. **A bound on the Riemann-Hurwitz contribution.** To proceed, we must bound the Riemann-Hurwitz contribution from each multiset and pairs of multisets.

Lemma 6.13.

$$4\ell \geq \sum_{i\in I}\sum_{\substack{a\in A_i\\ b\in B_i}}\big(a+b-2(a,b)\big)+\sum_{i\in J}\sum_{a,b\in C_i}\big(a-(a,b)\big).$$

Proof. First, note that if $\mathfrak{g}_2>0$ the result is immediate from (6.11). If $\mathfrak{g}_2=0$ then $\mathfrak{g}_0=0$, since otherwise the two sides of (6.6) would have different signs. Now (6.5) implies that exactly two of the g_i's are not in K, so $|J|=2$. Then we have

$$4\ell-4\geq 2\ell-4+\sum_{i\in J}(\#\text{ of odds in }C_i)=\sum_{i\in I}\sum_{\substack{a\in A_i\\ b\in B_i}}\big(a+b-2(a,b)\big)+\sum_{i\in J}\sum_{a,b\in C_i}\big(a-(a,b)\big).\ \square$$

Analogously to Lemma 4.2, we can use this lemma to massively restrict the pairs of multisets (A_i,B_i) and C_i in the ramification type. Restricting the multisets C_i can be done analogously as in Lemma 4.3, so we fix our attention on the pairs of multisets (A_i,B_i). From Lemma 6.13, we can see that

$$4\ell\geq\sum_{\substack{a\in A_i\\ b\in B_i}}\big(a+b-2(a,b)\big).$$

We will generate A_i's and B_i's by first counting the number of 1's in A_i and in B_i, the number of twos, and so on. Searching this entire state space will take far too long, so we use a modified version of Lemma 4.3. Observe that

$$\begin{aligned}
4\ell &\geq \sum_{\substack{a\in A_i\\ b\in B_i}}\big(a+b-2(a,b)\big)\\
&\geq \sum_{\substack{a\in A_i,a\leq k\\ b\in B_i,b\leq k}}\big(a+b-2(a,b)\big)+\sum_{\substack{a\in A_i,a\leq k\\ b\in B_i,b>k}}\big(a+b-2(a,b)\big)+\sum_{\substack{a\in A_i,a>k\\ b\in B_i,b\leq k}}\big(a+b-2(a,b)\big)\\
&\geq \sum_{\substack{a\in A_i,a\leq k\\ b\in B_i,b\leq k}}\big(a+b-2(a,b)\big)+\sum_{\substack{a\in A_i,a\leq k\\ b\in B_i,b>k}}\frac{b}{2}+\sum_{\substack{a\in A_i,a>k\\ b\in B_i,b\leq k}}\frac{a}{2}\\
&= \sum_{\substack{a\in A_i,a\leq k\\ b\in B_i,b\leq k}}\big(a+b-2(a,b)\big)+\frac{1}{2}\left(\sum_{a\in A_i,a\leq k}\left(\ell-\sum_{b\in B_i,b\leq k}b\right)+\sum_{b\in B_i,b\leq k}\left(\ell-\sum_{a\in A_i,a\leq k}a\right)\right).
\end{aligned}$$

We implemented this in a C++ program: [26]. One can show that the ramification types produced will either have $\ell<350$ or be present in [18]. In the case where $\ell<350$, the largest case not present in [18] has $\ell=19$, so $\deg f=361$.

6.5. **Commentary on the cases $t \geq 3$.** The cases in which $t \geq 3$ are algebraically more involved but the bounding used is much simpler as t increases. For example, it had already been shown in [11] that there are no solutions when $t > 8$. Using similar methods to the above, we found that there were no rational functions which monodromy groups in Case (C3.3) when $4 \leq t \leq 8$, but exactly one in which $t = 3$. The degree of this rational function is $5^3 = 125$.

7. Notable Examples of Rational Functions

We provide examples of ways to lift the local monodromy elements $x_1, x_2, \ldots, x_s$ to $x'_1, x'_2, \ldots, x'_s$ as described in (5.1). First we give an explicit rational function.

Consider the rational function

$$f_1(X) = \frac{(X^2 + 8X - 2)^3}{X^2}.$$

The ramification data is $E_{f_1}(0) = [3^2]$, $E_{f_1}(-729) = [1^3, 3]$, and $E_{f_1}(\infty) = [2, 4]$. The monodromy group is A_6. Performing the lifting action just mentioned, we find that if H is a two-set stabilizer, then $G/H = [6]_2$ and the ramification types will be $E_{f_2}(0) = [3^5]$, $E_{f_2}(-729) = [1^3, 3^4]$, $E_{f_2}(\infty) = [1, 2, 4^3]$. One rational function with these ramification types and with monodromy group A_6 is

$$f_2(X) = \frac{(4X^5 - 9X^4 - 108X^3 - 234X^2 - 216X - 81)^3}{(X^3 + 3X^2 + 5X + 3)^4(2X + 3)^2}.$$

Note that this expression for $f_2(X)$ is fairly complicated, even though the degree is small. Higher-degree examples will generally be much more complicated. However, in practice, when proving results about rational functions one does not make use of the coefficients of the rational function, but instead only uses the values of crucial invariants such as the monodromy group and ramification type. In the examples that follow, we will be content to describe these invariants.

Now, we give more implicit representations of these rational functions, by stating the group G, a maximal subgroup H, the elements of the group $x_1, x_2, \ldots, x_s$, verifying the numerical condition (3), and either giving $x'_1, x'_2, \ldots, x'_s$ or describing their cycle structures.

We present an example in which $G = A_{15}$, and H is a three-set stabilizer, so $\deg f = \binom{15}{3} = 455$ and $G/H = [15]_3$. Let $x_1, x_2, x_3 \in G$ be the elements $x_1 = (4, 5)(6, 7)(8, 9)(10, 11)(12, 13)(14, 15)$, $x_2 = (1, 14, 6)(2, 12, 5)(3, 7, 13)(4, 8, 15)(9, 10, 11)$, and $x_3 = (x_1x_2)^{-1}$, so that $x_1x_2x_3 = 1$ and $G = \langle x_1, x_2, x_3 \rangle$. In the action on G/H, the cycle structures of x_1, x_2, x_3 are $[1^{19}, 2^{218}]$, $[1^5, 3^{150}]$, and $[7^{65}]$. We may check condition (3) of Theorem 5.1, since

$$2(455) - 2 = (455 - 237) + (455 - 155) + (455 - 65).$$

We present an example in which $G = A_8$, with size 20160, and H is the group $\mathrm{ASL}_3(\mathbb{F}_2)$, which has size $8(7)(6)(4) = 1344$, so $\deg f = 20160/1344 = 15$. Let $x_1, x_2, x_3, x_4 \in G$ be the elements $x_1 = (5,6)(7,8)$, $x_2 = (3,6)(4,8)$, $x_3 = (1,4,7,2)(3,6,5,8)$, $x_4 = (1,2,7)(4,5,8)$, so that $x_1x_2x_3x_4 = 1$ and $G = \langle x_1, x_2, x_3, x_4\rangle$. Since G/H cannot be easily represented in this case, we explicitly determine the actions of the liftings of x_1, x_2, x_3, x_4 on G/H. We get that they are

$$x_1' = (1,10)(2,3)(4,6)(5,12)(7,13)(8,9), \quad x_2' = (1,4)(3,15)(5,12)(6,7)(8,11)(10,13),$$

$$x_3' = (2,10,4,14)(3,7)(5,6,11,8)(9,13), \quad x_4' = (1,9,6)(2,15,7)(3,14,4)(5,8,13).$$

We may check condition (3) of Theorem 5.1, since

$$2(15) - 2 = (15-9) + (15-9) + (15-7) + (15-7).$$

8. Conclusions and Future Work

We have determined all possibilities for the monodromy group and ramification type of an indecomposable degree-n rational function, under the assumption that the monodromy group is not in $\{A_n, S_n\}$ and satisfies case (C3.2) or (C3.3) of the Aschbacher–Scott classification of primitive groups. These two cases seemed intractable before our work. The only remaining case is (C3.1), which has been resolved for sufficiently large n via methods that are expected to extend to all n; a team of group theorists is currently completing case (C3.1). In future work we will look into various places where rational functions arise in math, science, and engineering, and identify settings where this new classification of unusually-behaved rational functions can have an impact.

9. Acknowledgements

I want to acknowledge Professor Michael E. Zieve from the University of Michigan for suggesting this project and mentoring me. Professor Zieve has been a great influence on my mathematical maturity and development. Professor Danny Neftin from the Israel Institute of Technology - Technion helped proofread the paper. I would like to thank the PRIMES-USA program for providing me the wonderful opportunity to work with Dr. Zieve. I would like to thank my Research Science Institute mentors Professor Scott Duke Kominers and Ravi Jagadeesan, both from Harvard University, for giving me general paper-writing advice. I thank the immense contributions of my parents who encouraged me to follow my dreams. Finally, I want to thank Regeneron for sponsoring this research competition.

References

[1] M. Artin. *Algebra*. Pearson Education, 2014. 12

[2] Michael Aschbacher. On conjectures of Guralnick and Thompson. *J. Algebra*, 135(2):277 – 343, 1990. 3

[3] Michael Aschbacher and Leonard Scott. Maximal subgroups of finite groups. *J. Algebra*, 92(1):44–80, 1985. 3

[4] Yuri F. Bilu and Robert F. Tichy. The Diophantine equation $f(x) = g(y)$. *Acta Arith.*, 95(3):261–288, 2000. 1

[5] Miriam Briskin, Nina Roytvarf, and Yosef Yomdin. Center conditions at infinity for Abel differential equations. *Ann. of Math. (2)*, 172(1):437–483, 2010. 1

[6] Peter J. Cameron, Peter M. Neumann, and Jan Saxl. An interchange property in finite permutation groups. *Bull. London Math. Soc.*, 11(2):161–169, 1979. 7

[7] O. Chisini. Sulla risolubilità per radicali delle equazioni contenenti linearmente un parametro. *Rend. Reale Ist. lombardo sci. lett.*, 48:382–402, 1915. 3

[8] Daniel Frohardt and Kay Magaard. Composition factors of monodromy groups. *Ann. of Math. (2)*, 154(2):327–345, 2001. 3

[9] Dragos Ghioca, Thomas J. Tucker, and Michael E. Zieve. Intersections of polynomial orbits, and a dynamical Mordell–Lang conjecture. *Invent. Math.*, 171:463–483, 2008. 1

[10] Dragos Ghioca, Thomas J. Tucker, and Michael E. Zieve. Linear relations between polynomial orbits. *Duke Math. J.*, 161(7):1379–1410, 2012. 1

[11] Robert M. Guralnick and Michael G. Neubauer. Monodromy groups of branched coverings: the generic case. In *Recent developments in the inverse Galois problem (Seattle, WA, 1993)*, volume 186 of *Contemp. Math.*, pages 325–352. Amer. Math. Soc., Providence, RI, 1995. 19

[12] Robert M. Guralnick and John Shareshian. Symmetric and alternating groups as monodromy groups of Riemann surfaces. I. Generic covers and covers with many branch points. *Mem. Amer. Math. Soc.*, 189(886):vi+128, 2007. With an appendix by Guralnick and R. Stafford. 4, 6, 8

[13] Robert M. Guralnick and John G. Thompson. Finite groups of genus zero. *J. Algebra*, 131(1):303–341, 1990. 3

[14] Sergei K. Lando and Alexander K. Zvonkin. Graphs on surfaces and their applications, volume 141 of encyclopaedia of mathematical sciences, 2004. 13

[15] Martin W. Liebeck and Aner Shalev. Simple groups, permutation groups, and probability. *J. Amer. Math. Soc.*, 12(2):497–520, 1999. 3

[16] R.C. Lyndon. *Groups and Geometry*. Cambridge English Prose Texts. Cambridge University Press, 1985. 8

[17] B. Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, (47):33–186 (1978), 1977. 3

[18] Danny Neftin and Michael E. Zieve. Monodromy groups of indecomposable coverings with bounded genus. 52 pp. 3, 12, 18

[19] Rolf Nevanlinna. Einige Eindeutigkeitssätze in der Theorie der Meromorphen Funktionen. *Acta Math.*, 48(3-4):367–391, 1926. 3

[20] Fedor Pakovich. On polynomials sharing preimages of compact sets, and related questions. *Geom. Funct. Anal.*, 18(1):163–183, 2008. 1

[21] J. F. Ritt. On algebraic functions which can be expressed in terms of radicals. *Trans. Amer. Math. Soc.*, 24:21–30, 1922. 3

[22] J. F. Ritt. Prime and composite polynomials. *Trans. Amer. Math. Soc.*, 23(1):51–66, 1922. 1

[23] I. Schur. Über den Zusammenhang zwischen einem Problem der Zahlentheorie und einem Satz über algebraische Funktionen. *S.-B. Preuss. Akad. Wiss. Phys.-Math. Klasse*, pages 123–134, 1923. 1

[24] Tanchu Shih. A note on groups of genus zero. *Comm. Alg.*, 19(10):2813–2826, 1991. 3

[25] H. Volklein. *Groups as Galois Groups: An Introduction*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 1996. 14

[26] Franklyn Wang. AB-multisets: `https://pastebin.com/RKK2ni0r`. 18

[27] Franklyn Wang. Code for multiset partitions: `https://pastebin.com/eJRWqaEL`. 12

[28] Franklyn Wang. Frobenius counts: `https://pastebin.com/M1zTTfdX`. 14

[29] Oscar Zariski. Sopra una classe di equazioni algebriche contenenti linearmente un parametro e risolubili per radicali. *Rend. Circolo Mat. Palermo*, 50:196–218, 1926. 3