SYMMETRIC GALOIS GROUPS UNDER SPECIALIZATION

TALI MONDERER AND DANNY NEFTIN

ABSTRACT. Given an irreducible bivariate polynomial $f(t,x) \in \mathbb{Q}[t,x]$, what groups H appear as the Galois group of $f(t_0,x)$ for infinitely many $t_0 \in \mathbb{Q}$? How often does a group H as above appear as the Galois group of $f(t_0,x)$, $t_0 \in \mathbb{Q}$? We give an answer for f of large x-degree with alternating or symmetric Galois group over $\mathbb{Q}(t)$. This is done by determining the low genus subcovers of coverings $\tilde{X} \to \mathbb{P}^1_{\mathbb{C}}$ with alternating or symmetric monodromy groups.

1. INTRODUCTION

Let $f(t,x) \in \mathbb{Q}(t)[x]$ be a polynomial with coefficients depending on a parameter t and let G be its Galois group. For all but finitely many specializations $t \mapsto t_0 \in \mathbb{Q}$, the Galois group $\mathrm{Gal}(f(t_0,x),\mathbb{Q})$ is a subgroup of G; and Hilbert's irreducibility theorem guarantees that the Galois group remains G for infinitely many $t_0 \in \mathbb{Q}$. It may still hold that a proper subgroup of G occurs for infinitely many $t_0 \in \mathbb{Q}$. For example, the polynomial $f(t,x) := x^2 - t$ has a nontrivial Galois group over $\mathbb{Q}(t)$, and all specializations of the form $t \mapsto q^2$ for some $q \in \mathbb{Q}$ yield a rational polynomial that splits over $\mathbb{Q}$. Given a polynomial $f(t,x) \in \mathbb{Q}(t)[x]$, what subgroups of $\mathrm{Gal}(f(t,x),\mathbb{Q}(t))$ occur as $\mathrm{Gal}(f(t_0,x),\mathbb{Q})$ for infinitely many rational $t_0 \in \mathbb{Q}$?

We are interested in the "general" case where $G := \mathrm{Gal}(f(t,x),\mathbb{Q}(t))$ is a symmetric group S_n. Most notably it is known that: 1) every intransitive $H \leq S_n$ for $n > 5$, that occurs as $\mathrm{Gal}(f(t_0,x),\mathbb{Q})$ for infinitely many integral $t_0 \in \mathbb{Z}$, must be contained in S_{n-1} [18]; and 2) a maximal subgroup $H \leq S_n$, for sufficiently large n, that occurs as $\mathrm{Gal}(f(t_0,x),\mathbb{Q})$ for infinitely many rational $t_0 \in \mathbb{Q}$ must be either S_{n-1} or $S_{n-2} \times S_2$ [20]. The following theorem answers the above question when $G = S_n$, for large n, with no maximality assumption on H. For $g \geq 0$, let N_g be the constant defined in Theorem 2.6, cf. Remark 2.8 concerning the value N_1.

Theorem 1.1. *Let $f(t,x) \in \mathbb{Q}(t)[x]$ be a polynomial with Galois group A_n or S_n for $n > N_1$. Suppose $\mathrm{Gal}(f(t_0,x),\mathbb{Q}) \cong H$ for infinitely many $t_0 \in \mathbb{Q}$. Then either*

(1) *$H = A_n$ or S_n; or*
(2) *$H = A_{n-1}$ or S_{n-1}; or*
(3) *$A_{n-2} \lneq H \leq S_{n-2} \times S_2$.*

Case (3) occurs only with explicit ramification listed in Proposition 4.1.

Assume $\deg f = n$[1]. The most probable case in which $f(t_0, x)$ is reducible is case (2), where $f(t_0, x)$ factors as a product of a linear factor and an irreducible factor of degree $n-1$. This case appears with growth rate:

$$\#\{t_0 \in \mathbb{Q} \mid \mathrm{ht}(t_0) \leq N, \mathrm{Gal}(f(t_0, x)) \cong A_{n-1} \text{ or } S_{n-1}\} \asymp N^{2/n},$$

where ht is the natural height $\mathrm{ht}(\frac{m}{n}) = \max\{|m|, |n|\}$ for coprime $m, n \in \mathbb{Z} \setminus \{0\}$, and $g \asymp h$ for positive valued functions $g, h : \mathbb{N} \to \mathbb{R}$ means that $c_1 h(n) \leq g(n) \leq c_2 h(n)$ for all $n \in \mathbb{N}$, where $c_1, c_2 \in \mathbb{R}$ are positive constants. In case (3), $f(t_0, x)$ has an irreducible factor of degree $n-2$. This is the next probable reducible case, appearing with growth $\asymp N^{4/n(n-1)}$. Case (1) is the most probable one with growth $\asymp N^2$, as the complement of cases (2), (3) and a finite set. The growth of specializations with Galois group H is inferred from the index $[G : H]$ using [21, §9.7, Case 0].

Theorem 1.1 applies to polynomials over any finitely generated field of characteristic 0, and moreover, each of the options (1)-(3) occurs for infinitely many specializations over some number field. As case (3) happens only for specific polynomials, these are the only polynomials with Galois group A_n or S_n for which $f(t_0, x)$ has an irreducible factor $h \in \mathbb{Q}[x]$ of degree $2 \leq \deg h \leq n-2$ for infinitely many $t_0 \in \mathbb{Q}$.

Low genus subfields and their group-theoretic description. The main ingredient in proving Theorem 1.1 is classifying low genus covers with monodromy A_n or S_n. Here, for simplicity assume $f \in \mathbb{Q}(t)[x]$ is irreducible over $\mathbb{C}(t)$ and denote by X the curve defined by f, cf. §6 for the reducible scenario. Let $\pi : X \to \mathbb{P}^1_{\mathbb{C}}$ be the projection to the t-coordinate, and $\tilde{X}$ be its Galois closure. Thus the Galois group G acts on $\tilde{X}$ and $\tilde{X}/(G \cap S_{n-1}) \cong X$, cf. §2.4.

It is well known that a subgroup $H \leq G$ appears as the Galois group of $f(t_0, x)$ for infinitely many $t_0 \in \mathbb{Q}$ only when $\tilde{X}/H$ is of genus ≤ 1, cf. §6. The maximal subgroups H of $G \in \{A_n, S_n\}$ for which $\tilde{X}/H$ is of genus ≤ 1 were classified in [9] and [20]. We do this for arbitrary subgroups of A_n or S_n:

Theorem 1.2. *Let $g \geq 0$ and $\pi : X \to \mathbb{P}^1_{\mathbb{C}}$ be a covering of degree $n > N_g$, Galois closure $\tilde{X}$, and monodromy group $G = A_n$ or S_n. Suppose $H \leq G$ does not contain A_{n-1}, and $\tilde{X}/H$ is of genus at most g. Then $A_{n-2} \leq H \leq S_{n-2} \times S_2$, and the ramification of π is given in Proposition 4.1. In fact, $\tilde{X}/H$ is of genus at most 1.*

The proof of Theorem 1.1 is straightforward from Theorem 1.2 using Faltings' theorem, see §6. The main ingredient in proving Theorem 1.2 is an analysis of the transitivity of the action of H on unordered sets, using results such as the Livingstone–Wagner theorem and results on multiply transitive groups. The above action is connected to the genus of $\tilde{X}/H$ by two results from the classification of primitive

[1]Note that the theorem allows $\deg f \neq n$, that is, the Galois group may act in an arbitrary permutation representation.

monodromy groups: an inequality [9, Lemma 2.0.13] by Guralnick–Shareshian which connects the genus of $\tilde{X}/H$ to the genera g_i of the quotients of $\tilde{X}$ by stabilizers of sets of cardinality i; and the inequalities $g_{i+1} - g_i > 2$ from [20].

In the case of polynomial coverings, that is, when $\pi : \mathbb{P}^1_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$ is given by a polynomial $p \in \mathbb{C}[x]$, in combination with [9] we have the following further result:

Theorem 1.3. *Let $p : \mathbb{P}^1_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$ be a polynomial covering of degree $n > 20$, monodromy group $G = A_n$ or S_n, and Galois closure $\tilde{X}$. Suppose $A_{n-1} \neq H < G$ is nonmaximal, and $\tilde{X}/H$ is of genus 0. Then $H = S_{n-2}$ and p is the composition of the map $\mathbb{A}^1_{\mathbb{C}} \to \mathbb{A}^1_{\mathbb{C}}$, $x \mapsto x^a(x-1)^{n-a}$, for $\gcd(a, n) = 1$, with linear polynomials.*

The proof is similar to that of Theorem 1.2, however instead of relying on the inequalities $g_{i+1} - g_i > 2$ from [20], we rely on estimates from [9]. See the more general Theorem 5.3 for the genus 1 case.

Reducible specializations. In similarity to other results concerning the genus 0 problem, the classification of low genus subfields given in Theorems 1.2 and 1.3 is expected to have many further applications. We develop here one application which is closely related to Theorem 1.1. Given a polynomial $f \in \mathbb{Q}(t)[x]$, it is desirable to describe the set Red_f of values $t_0 \in \mathbb{Q}$ where $f(t_0, x)$ is (defined and) reducible over $\mathbb{Q}$. This was studied in particular by Fried [4, 5], König [11], Langmann [14], Müller [17, 18, 19] and others. It is well-known that for every f, there exists a finite set of coverings $h_i : X \to \mathbb{P}^1_{\mathbb{Q}}$ such that Red_f differs by a finite set from the union of value sets $\bigcup_{i=1}^m h_i(X_i(\mathbb{Q}))$. We show that when the Galois group of f is A_n or S_n for sufficiently large n (which is not necessarily $\deg f$), the number of value sets m is at most 3 and this upper bound is sharp. Let N_1 be the constant from Remark 2.8.

Theorem 1.4. *Let $f \in \mathbb{Q}(t)[x]$ be an irreducible polynomial with Galois group A_n or S_n for $n > N_1$. Then there exist three coverings $h_i : X_i \to \mathbb{P}^1_{\mathbb{Q}}, i = 1, 2, 3$ over $\mathbb{Q}$ such that Red_f and $\bigcup_{i=1}^3 h_i(X_i(\mathbb{Q}))$ differ by a finite set.*

If moreover we are not in case (3) of Theorem 1.2, then Red_f differs from $h_1(X_1(\mathbb{Q})) \cup h_2(X_2(\mathbb{Q}))$ by a finite set, for two coverings $h_i : X_i \to \mathbb{P}^1_{\mathbb{Q}}, i = 1, 2$. If furthermore $\deg f = n$, then Red_f and $h_1(X_1(\mathbb{Q}))$ differ by a finite set.

Other expected future applications of Theorem 1.2 stem from the relation of rational (i.e., genus 0) subfields to problems of functional decomposition. These include determining the arithmetically indecomposable rational functions which are geometrically decomposable [8, §6], and the Davenport-Lewis-Schinzel problem concerning the reducibility of a polynomials of the form $f(x) - g(y) \in \mathbb{C}[x, y]$ [12, 3].

Acknowledgements. We thank Michael Zieve for helpful discussions, which initiated this project, and Peter Müller for helpful comments, which in particular

simplified the proof of Proposition 3.3. The generous financial help of the Technion, ISF grants 577/15 and 662/15, and BSF grant 2014173 is gratefully acknowledged.

2. Notation and preliminaries

Let k be a field of characteristic 0. Denote by $\overline{k}$ its algebraic closure. Throughout the section, we assume $k = \overline{k}$.

2.1. **Multiply Transitive Groups.** All group actions are left actions. A set of cardinality m is called an m-set. If a permutation group G on n elements has a single orbit on (ordered) m-tuples of distinct elements from $\{1, \dots, n\}$, it is called *m-transitive*, and if it has a single orbit on unordered m-sets of $\{1, \dots, n\}$ it is called *m-homogeneous*. Denote the number of orbits of G on unordered m-sets by $O_m(G)$. A theorem of Livingstone–Wagner [15] asserts that an m-homogeneous group G is m-transitive for $m \geq 5$; and also that $O_m(G) \leq O_{m+1}(G)$ for $m \leq \lfloor \frac{n}{2} \rfloor - 1$. A consequence of the classification of finite simple groups is that the only 6-transitive groups are A_n and S_n. Without relying on this classification, the order of transitivity of a permutation group of degree n, other than A_n or S_n, is known to be bounded by a function of n; one such result is Babai and Seress' elementary proof that the transitivity degree of such a group is at most $32(\log(n))^2/\log\log n$ [2]. Take D to be an integer such that $D < \lfloor \frac{n}{2} \rfloor$ and a D-transitive group on n elements must be A_n or S_n. When assuming the classification of finite simple groups, $D = 6$ suffices; otherwise, such an integer D exists but we take D depending on n, e.g. $\lceil 32(\log(n))^2/\log\log n \rceil$.

2.2. **Function fields and ramification.** A general reference on this topic is [22]. A *function field* over k is a finite extension of $k(t)$, where t is transcendental over k.

Let F_1/F be an extension of function fields over k. For a place Q of F_1 lying over a place P of F write $e(Q|P)$ for the ramification index (cf. [22, Definition 3.1.5]) of Q over P. Let $Q_1, \dots Q_r$ be the places of F_1 lying above a place P of F. The multiset $E_{F_1/F}(P) := [e(Q_1|P), \dots, e(Q_r|P)]$ is called the *ramification type of P in F_1*. The place P is called a *branch point* of F_1/F if $e(Q_i/P) > 1$ for some i. Letting S be the set of branch points, we recall that S is finite. The multiset $\{E_{F_1/F}(P) : P \in S\}$ is called the *ramification type of F_1/F*.

Let Ω/F be the Galois closure of F_1/F, and put $G := \mathrm{Gal}(\Omega/F)$, $H := \mathrm{Gal}(\Omega/F_1)$, and $n := [G : H] = [F_1 : F]$. We let G act on places of Ω with a right action. Since k is algebraically closed, the stabilizer of a place $\tilde{Q}$ of Ω lying over P (also known as the decomposition group) identifies with the cyclic inertia group $I_P = I(\tilde{Q}|P)$ over P. There is a well known one to one correspondence (see [10, Section 3]) between places Q of F_1 over P, and orbits O of I_P on G/H, such that $e(Q|P) = \#O$. More precisely, the correspondence sends the orbit of xH, $x \in G$, to the restriction of

$\tilde{Q}^x$ to F_1. We refer to this correspondence as the ramification-orbit correspondence. Moreover, if $F_2 = \Omega^{H_2}$ for $H_2 \leq H$, so that $F_1 \subseteq F_2 \subseteq \Omega$, then the ramification-orbit correspondences for F_1 and F_2, over P, can be picked so that restriction of places from F_2 to F_1 is compatible with the natural projection $G/H_2 \to G/H_1$. In other words, if Q is a place of F_2 that corresponds to the orbit of xH_2, then $Q \cap F_1$ corresponds to the orbit of xH.

The correspondence also implies the equivalence of the following versions of the Riemann–Hurwitz formula:

$$\begin{aligned} 2(g_{F_1}-1) &= 2n(g_F-1) + \sum_{Q \text{ place of } F_1} (e(Q|Q\cap F)-1) \\ &= 2n(g_F-1) + \sum_{P \text{ place of } F} \big(n - \#E_{F_1/F}(P)\big) \\ &= 2n(g_F-1) + \sum_{P \text{ place of } F} \big([G:H] - \#\{\text{orbits of } I_P \text{ on } G/H\}\big). \end{aligned} \tag{2.1}$$

To compute the ramification in composita of extensions, we use:

Lemma 2.1 (Abhyankar's Lemma [22, Theorem 3.9.1], [20, Lemma 9.2])**.** *Let F_1/F and F_2/F be function field extensions and F_1F_2 their compositum. Let Q be a place of F_1F_2 that lies over places Q_1,Q_2 and P in F_1, F_2 and F, respectively. Then*

$$e(Q|P) = \operatorname{lcm}(e(Q_1|P), e(Q_2|P)).$$

Moreover, if F_1 and F_2 are linearly disjoint over F, then the number of places Q, over fixed Q_1, Q_2 as above, is $\gcd(e(Q_1|P), e(Q_2|P))$.

2.3. **The fields fixed by 2-set and 2-point stabilizers.** Suppose P is a place of a function field $F/k(t)$. Let F_1/F be a degree n extension with Galois closure Ω and doubly transitive Galois group $G \leq S_n$. Let G_2 be a 2-set stabilizer. The ramification-orbit correspondence then shows that the ramification type of P in $\Omega^{G_2}/k(t)$ is in one to one correspondence with the orbits of I_P on G/G_2, or equivalently on 2-sets. Letting x be a generator of I_P, the latter is given by the following basic count of orbits [20, Lemma 4.1]:

Lemma 2.2. *Let $R_1, R_2 \subseteq S$ be orbits of $x \in S_n$ 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 x on T consist of*

1. $\gcd(r_1, r_2)$ *orbits of cardinality* $\operatorname{lcm}(r_1, r_2)$ *if $R_1 \neq R_2$;*
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 2-set $\{c, d\} \in T$ 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 $R_1 \neq R_2$ (resp. $R_1 = R_2$), there are $r_1 r_2/\mathrm{lcm}(r_1, r_2) = \gcd(r_1, r_2)$ (resp. $(r_1-1)/2$) such orbits if $R_1 \neq R_2$ (resp. if $R_1 = R_2$ and r_1 is odd), proving (1) and (2). If $R_1 = R_2$ and r_1 is even, all pairs $\{a, x^{r_1/2}(a)\}$ 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 $\{a, x^{r_1/2}(a)\}$, these comprise $r_1/2 - 1$ orbits, proving (3). □

Keeping the above setup, the following lemma describes the Riemann–Hurwitz contribution of the extension induced by a 2-set stabilizer and a 2-point stabilizer, cf. [20, Proposition 5.1].

Lemma 2.3. *Assume $G = \mathrm{Gal}(\Omega/F) \leq S_n$ is 2-transitive and let G_2 and $\hat{G}_2$ be its 2-set stabilizer and 2-point stabilizer, respectively. Let $\mathcal{E}_P$ be the ramification type of P. Then the Riemann–Hurwitz contribution $\sum_{Q \mid P}(e(Q|Q \cap \Omega^{G_2}) - 1)$, of places over P, to $\Omega^{\hat{G}_2}/\Omega^{G_2}$ equals the number of even entries in $\mathcal{E}_P$.*

Proof. Since the action of G is doubly transitive, the ramification-orbit correspondence shows that the places of $\Omega^{\hat{G}_2}$ (resp. Ω^{G_2}) over P are in one to one correspondence with the orbits of the inertia group I_P on ordered pairs of distinct elements (resp. 2-sets) from $\{1, \dots, n\}$. Moreover, we choose the two correspondences compatibly, that is, if $\hat{Q}$ and Q are places of $\Omega^{\hat{G}_2}$ and Ω^{G_2} corresponding to the orbits of the ordered tuples $[a, b]$ and unordered sets $\{a, b\}$, respectively, then $\hat{Q}$ lies over Q. Such a place Q is ramified in $\Omega^{\hat{G}_2}/\Omega^{G_2}$ if and only if there is only one place of $\Omega^{\hat{G}_2}$ over it. The latter occurs if and only if the orbits of $[a, b]$ and $[b, a]$ under I_P coincide. We call such orbits symmetric.

It remains to count the number of symmetric orbits of $I_P = \langle x \rangle$. For this, we may assume a, b are in the same orbit R of x, and set $r = \#R$. The only way for the orbits of $[a, b]$ and $[b, a]$ to coincide is if r is even, and $x^{r/2}$ swaps a and b. The pairs $\{a, b\}$ from R which are swapped by $x^{r/2}$ then form a single orbit of x. Hence in total, the number of symmetric orbits of I_P equals the number of even length orbits of I_P, which in turn is the number of even entries in $\mathcal{E}_P$, as desired. □

Finally, we also use the following lemma to count branch points. We keep the setting of Lemma 2.3, so that F_1/F is a degree n extension, and the Galois group $G = \mathrm{Gal}(\Omega/F)$ of its Galois closure Ω is doubly transitive with 2-point stabilizer $\hat{G}_2$:

Lemma 2.4. *Let Q_1, Q_2 be distinct places of F_1 over P, and $e_i = e(Q_i|P)$, $i = 1, 2$. If e_2 does not divide e_1, then Q_1 is a branch point of $\Omega^{\hat{G}_2}/F_1$.*

Proof. Put $F_2 := \Omega^{\hat{G}_2}$. The ramification-orbit correspondence shows that the places of F_1 (resp. F_2) over P correspond to orbits of the inertia group I_P (resp. orbits of I_P on ordered pairs of distinct elements). Moreover, we choose the two correspondences compatibly. In other words, if $\hat{Q}$ and Q are places of F_2 and F_1 corresponding to the orbits of $[a_1, a_2]$ and $\{a_1\}$, then $\hat{Q}$ lies over Q.

Suppose Q_i corresponds to the orbit R_i of a_i, for $i = 1, 2$, and let $\hat{Q}$ denote a place of F_2 corresponding to the orbit of $[a_1, a_2]$. Since e_i is the length of R_i, $i = 1, 2$, the length of the orbit of $[a_1, a_2]$ is $\operatorname{lcm}(e_1, e_2)$. Hence $e(\hat{Q}|P) = \operatorname{lcm}(e_1, e_2)$, by the above correspondence. Thus, $e(\hat{Q}|P) > e_1$ by assumption, and $e(\hat{Q}|Q_1) > 1$ as desired. □

2.4. **Relation to coverings.** A general reference on this topic is [6, Chp. 4]. A covering $\pi : X \to \mathbb{P}^1_k$ is a morphism of (smooth projective irreducible) curves over k. It is well known ([6, Chapter 7] for example) that by associating to π the function field extension $k(X)/k(\mathbb{P}^1_k)$, one obtains a 1-to-1 correspondence between equivalence classes of coverings $\pi : X \to \mathbb{P}^1_k$ and isomorphism classes of function field extensions $F/k(t)$. In particular we define the Galois closure $\tilde{X}$ of π to denote the curve corresponding to the Galois closure Ω of $k(X)/k(\mathbb{P}^1_k)$, equipped with an action of $G := \operatorname{Gal}(\Omega/k(\mathbb{P}^1_k))$. Note that π is indecomposable if and only if $k(X)/k(\mathbb{P}^1_k)$ is *minimal*, that is, has no nontrivial intermediate extensions.

For a function field $F = k(X)$, we denote by g_F the genus of the curve X. Note that $g_F = 0$ if and only if F is rational, that is, $F = k(x)$ for some x transcendental over k. A polynomial map $\pi : \mathbb{P}^1_k \to \mathbb{P}^1_k$ is a covering for which $\pi^{-1}(\infty) = \{\infty\}$, that is, where ∞ is totally ramified in the function field extension $k(x)/k(t)$ corresponding to π. Such a covering is given by $y \mapsto p(y)$ for some polynomial $p \in \mathbb{C}[y]$, in which case x can be chosen to be a root of the irreducible polynomial $p(Y) - t \in k(t)[Y]$ and hence $[k(x) : k(t)] = \deg p$. We shall translate Theorems 1.2 and 1.3 to function fields and restrict to this language.

Finally note that π can be viewed as a topological covering. The topological theory then gives elements $x_1, \ldots, x_r \in G$, called *branch cycles*, with product $x_1 \cdots x_r = 1$ that generate G. Moreover, the branch cycles correspond to the branch points $P_1, \ldots, P_r$ of π, so that each x_j generates an inertia group I_j over P_j, for $j = 1, \ldots, r$.

2.5. **Monodromy classification.** We shall use the following two theorems from [20] to bound the difference between genera of fixed fields of set stabilizers. Let D be as in Section 2.1.

Theorem 2.5. *For $g \geq 0$, there exists a constant $N'_g \geq 20$ with the following property. Let $\Omega/k(t)$ be a Galois extension with group $G = A_n$ or S_n for $n > N'_g$, $G_1 := G \cap S_{n-1}$ its point stabilizer, and let g_i denote the genus of the fixed field of the stabilizer of an i-set for $1 \leq i \leq n/2$. Then $g_i - g_{i-1} > g$ holds for all $i = 3, \ldots, D$. If the ramification of $\Omega^{G_1}/k(t)$ is not in Table 2.1, then $g_2 - g_1 > g$ holds as well.*

Proof. By [20, Theorem 3.1], there exist $c, d > 0$ such that

$$g_i - g_{i-1} > (cn - di^{15}) \frac{\binom{n}{i}}{\binom{n}{2}} \tag{2.2}$$

holds for all $i = 2, \dots, \lfloor n/2 \rfloor$ if the ramification of $\Omega^{G_1}/k(t)$ is not in Table 2.1, and for all $i = 3, \dots, \lfloor n/2 \rfloor$ otherwise. Since we chose $D \ll (\log n)^2$, we may pick N_g' so that the right hand side of (2.2) is $\geq g$ for all $n > N_g'$ and $2 \leq i \leq D$. □

Theorem 2.6. *For $g \geq 0$, there exists $N_g \geq \max\{N_g', 4g\}$ with the following property. For every Galois extension $\Omega/k(t)$ with group $G \in \{A_n, S_n\}$ for $n > N_g$, and every maximal $H \leq G$, $H \neq A_n$, either Ω^H is of genus $> g$, or H is a point stabilizer, or the ramification of $\Omega^{G \cap S_{n-1}}/k(t)$ is in Table 2.1 and H is a 2-set stabilizer.*

Proof. Set $G_1 = G \cap S_{n-1}$. By [20, Theorem 1.2], there exist constants $a > 0$ and $N > 0$ such that for all $n > N$ and maximal $H \leq G$, $H \neq A_n$, either the genus of Ω^H is $> an$, or H is a point stabilizer, or the ramification is in Table 2.1 and H is a 2-set stabilizer. The assertion follows by setting $N_g := \max\{N, 4g, N_g', g/a\}$ since then the genus of Ω^H is greater than $an > aN_g \geq g$. □

For extensions of nonrational fields one has:

Remark 2.7. Fix $g \geq 1$. By [7, Corollaries 2.2 and 2.4], a minimal extension of degree $n > N_g \geq 4g$ and genus at most g of a function field of genus at least 1 cannot have an alternating or symmetric Galois group.

Remark 2.8. Throughout the paper, the constant N_1 denotes an integer ≥ 20 for which the conclusions of Theorems 2.5 and 2.6 hold for $g = 1$. The proof[2] of [20, Theorem 1.2] provides the large value $N_1 = 6 \times 10^{10}$, partially in order to keep the proof elementary and self contained, avoiding the classification of finite simple groups. Assuming the classification of finite simple groups, [20] allows $N_1 = 3.5 \times 10^6$. In view of further work in progress, more specific to coverings of genus ≤ 1, the value of N_1 is expected to be smaller than 400.

For extensions $\Omega/k(t)$ with at least 5 branch points, or in case $\Omega^{G \cap S_{n-1}}/k(t)$ has a totally ramified point, the constant N_g can be replaced by 20 by [9, Theorem 1.1.2] and [9, Theorem 1.2.1]. In the latter case (resp. former case), if H is a 2-point stabilizer then the ramification of $\Omega^{G \cap S_{n-1}}/k(t)$ is one of the types (I1)-(I2.8) (resp. (F1.1), (F1.2)) in Table 2.1.

[2]The proof in [20] is concerned with giving an optimal asymptotic growth for N_g with g, and does not discuss specific values of g. However, a closer inspection gives these explicit constants.

TABLE 2.1. Ramification types for coverings $h : \mathbb{P}^1 \to \mathbb{P}^1$ of degree $n \geq 13$ and monodromy group A_n or S_n. Here $a \in \{1, \ldots, n-1\}$ is odd, $\gcd(a, n) = 1$, and in each type n satisfies the necessary congruence conditions to make all exponents integral. The third column indicates when the genus g_A of $\tilde{X}/(A_{n-2} \times S_2)$ is 0, 1 or more, where $\tilde{X}$ is the Galois closure of h. In the rest of the cases, $g_A > 1$.

$I1.1$	$[n], [a, n-a], [1^{n-2}, 2]$	
$I2.1$	$[n], [1^3, 2^{(n-3)/2}], [1, 2^{(n-1)/2}], [1^{n-2}, 2]$	
$I2.2$	$[n], [1^2, 2^{(n-2)/2}]$ twice, $[1^{n-2}, 2]$	
$I2.3$	$[n], \left[1^3, 2^{(n-3)/2}\right], [2^{(n-3)/2}, 3]$	$g_A = 1$ for $n \equiv 1 \bmod 4$
$I2.4$	$[n], \left[1^2, 2^{(n-2)/2}\right], [1, 2^{(n-4)/2}, 3]$	
$I2.5$	$[n], \left[1, 2^{(n-1)/2}\right], [1^2, 2^{(n-5)/2}, 3]$	$g_A = 1$ for $n \equiv 3 \bmod 4$
$I2.6$	$[n], \left[1^3, 2^{(n-3)/2}\right], [1, 2^{(n-5)/2}, 4]$	$g_A = 1$ for $n \equiv 1 \bmod 4$
$I2.7$	$[n], \left[1^2, 2^{(n-2)/2}\right], [1^2, 2^{(n-6)/2}, 4]$	
$I2.8$	$[n], \left[1, 2^{(n-1)/2}\right], [1^3, 2^{(n-7)/2}, 4]$	$g_A = 1$ for $n \equiv 3 \bmod 4$
$I2.9$	$[a, n-a], [1^2, 2^{(n-2)/2}], [2^{n/2}], [1^{n-2}, 2]$	
$I2.10$	$[a, n-a], [1, 2^{(n-1)/2}]$ twice, $[1^{n-2}, 2]$	
$I2.11$	$[a, n-a], \left[2^{n/2}\right], [1^2, 2^{(n-6)/2}, 4]$	$g_A = 0$ for $n \equiv 2 \bmod 4$
$I2.12$	$[a, n-a], \left[1, 2^{(n-1)/2}\right], [1, 2^{(n-5)/2}, 4]$	
$I2.13$	$[a, n-a], \left[1^2, 2^{(n-2)/2}\right], [2^{(n-4)/2}, 4]$	$g_A = 0$ for $n \equiv 0 \bmod 4$
$I2.14$	$[a, n-a], \left[1, 2^{(n-1)/2}\right], [2^{(n-3)/2}, 3]$	
$I2.15$	$[a, n-a], \left[2^{n/2}\right], [1, 2^{(n-4)/2}, 3]$	$g_A = 0$ for $n \equiv 2 \bmod 4$
$F1.1$	$[1^{n-2}, 2], [2^{n/2}], [1^2, 2^{(n-2)/2}]$ thrice	
$F1.2$	$[1^{n-2}, 2], [1^3, 2^{(n-3)/2}], [1, 2^{(n-1)/2}]$ thrice	
$F1.3$	$\left[1^3, 2^{(n-3)/2}\right], [2^{(n-3)/2}, 3], [1, 2^{(n-1)/2}]$ twice	
$F1.4$	$\left[2^{n/2}\right], [1, 2^{(n-4)/2}, 3], [1^2, 2^{(n-2)/2}]$ twice	
$F1.5$	$\left[1^2, 2^{(n-5)/2}, 3\right], [1, 2^{(n-1)/2}]$ thrice	$g_A = 1$ for $n \equiv 3 \bmod 4$
$F1.6$	$\left[1^3, 2^{(n-3)/2}\right], [1, 2^{(n-5)/2}, 4], [1, 2^{(n-1)/2}]$ twice	
$F1.7$	$\left[2^{n/2}\right], [1^2, 2^{(n-6)/2}, 4], [1^2, 2^{(n-2)/2}]$ twice	
$F1.8$	$\left[1^3, 2^{(n-7)/2}, 4\right], [1, 2^{(n-1)/2}]$ thrice	$g_A = 1$ for $n \equiv 3 \bmod 4$
$F1.9$	$\left[2^{(n-4)/2}, 4\right], [1^2, 2^{(n-2)/2}]$ thrice	$g_A = 1$ for $n \equiv 0 \bmod 4$
$F3.1$	$\left[1^2, 2^{(n-2)/2}\right], [1, 3, 4^{(n-4)/4}], [4^{n/4}]$	
$F3.2$	$\left[1, 2^{(n-1)/2}\right], [1, 4^{(n-1)/4}], [2, 3, 4^{(n-5)/4}]$	
$F3.3$	$\left[1, 2^{(n-1)/2}\right], [1, 2, 4^{(n-3)/4}], [3, 4^{(n-3)/4}]$	
$F4.1$	$\left[1^2, 2^{(n-2)/2}\right], [1, 2, 3^{(n-3)/3}], [6^{n/6}]$	
$F4.2$	$\left[1^2, 2^{(n-2)/2}\right], [2, 3^{(n-2)/3}], [2, 6^{(n-2)/6}]$	
$F4.3$	$\left[1, 2^{(n-1)/2}\right], [1, 3^{(n-1)/3}], [3, 4, 6^{(n-7)/6}]$	$g_A = 0$ for $n \equiv 7 \bmod 12$
$F4.4$	$\left[1, 2^{(n-1)/2}\right], [1, 2, 3^{(n-3)/3}], [3, 6^{(n-3)/6}]$	
$F4.5$	$\left[1^2, 2^{(n-2)/2}\right], [1, 3^{(n-1)/3}], [4, 6^{(n-4)/6}]$	$g_A = 0$ for $n \equiv 4 \bmod 12$
$F4.6$	$\left[1, 2^{(n-1)/2}\right], [2, 3^{(n-2)/3}], [2, 3, 6^{(n-5)/6}]$	

3. From low genus covers to multiply transitive actions

Throughout the section, let k be an algebraically closed field of characteristic 0. The following theorem yields a group theoretic condition on orbits of subgroups with low genus fixed field. Let N'_g be the constant from Theorem 2.5.

Proposition 3.1. *Fix $g \geq 0$. For every Galois extension $\Omega/k(t)$ with group $G = A_n$ or S_n for $n > N'_g$, and subgroup $H \leq G$ fixing a subfield of genus at most g, one has $O_2(H) = O_D(H)$. Let F be the subfield of Ω fixed by a point stabilizer of G. If the ramification type of $F/k(t)$ is not in Table 2.1, then $O_1(H) = O_2(H)$ as well.*

Proof. Set $O_i := O_i(H)$ for all i. Guralnick and Shareshian [9, Lemma 2.0.13] relate the genus of Ω^H to the number of k-orbits of the action of H on $\{1, \dots, n\}$ as follows:

$$g_{\Omega^H} \geq \sum_{i=2}^{\lfloor \frac{n}{2} \rfloor} (O_i - O_{i-1})(g_i - g_{i-1}) \tag{3.1}$$

where g_i is the genus of a subfield of Ω fixed by a stabilizer of an i-set. Since $O_i - O_{i-1} \geq 0$ by the Livingstone-Wagner theorem, and since $g_i - g_{i-1} \geq 0$ by [9, Lemma 2.0.12], the summands of (3.1) are nonnegative, and hence

$$g_{\Omega^H} \geq (O_i - O_{i-1})(g_i - g_{i-1}) \tag{3.2}$$

for $2 \leq i \leq \lfloor \frac{n}{2} \rfloor$. Since $g_{\Omega^H} \leq g$ and $g_i - g_{i-1} > g$ as $n > N'_g$, the right hand side of (3.2) must equal 0 for $i = 3, \dots, D$, and hence $O_2 = O_3 = \cdots = O_D$ by Theorem 2.5. Similarly, if the ramification of $F/k(t)$ is not in Table 2.1, then $g_2 - g_1 > g$ and $O_1 = O_2$. □

For polynomial coverings, the equality $O_2 = O_3$ follows already for $n > 20$ in case $g \leq 1$, as a consequence of [9]:

Proposition 3.2. *Let Ω be the splitting field of $f(t, x) := p(x) - t \in k(t)[x]$. Suppose $G := \mathrm{Gal}(\Omega/k(t)) = A_n$ or S_n for $n > 20$. Let $H \neq A_n$ be a subgroup of G that fixes a subfield of genus 0 or 1. Then $O_2(H) = O_3(H)$.*

Proof. Let g_i be the genus of a subfield of Ω fixed by a stabilizer of an i-set. By [9, Lemma 12.0.68] we have $g_3 - g_2 > 2$ if $n > 48$, and furthermore for $n > 20$ if there are at least 4 branch points. The inequality is also shown for $20 < n \leq 48$ in [9, Theorem A.4.2] when there are at most 4 branch points. As in the proof of Proposition 3.1, since $g_3 - g_2 > 1 \geq g_{\Omega^H}$, (3.1) shows that $O_2(H) = O_3(H)$. □

In case H has a fixed point the following proposition shows that the derived condition $O_2(H) = O_d(H)$ implies that H acts multiply transitively on a subset:

Proposition 3.3. *Let $n \geq 8$. Suppose $O_2(H) = O_d(H)$ for $H \leq S_n$ and $d \geq 3$.*

(1) *If H fixes exactly one point n, then H acts d-homogeneously on $\{1, \dots, n-1\}$.*

(2) *If H stabilizes $\{n-1,n\}$, then H acts d-homogeneously on $\{1,\dots,n-2\}$.*

Proof. Note that $O_{n-m}(H) = O_m(H)$ for $m = 1, ..., \lfloor \frac{n}{2} \rfloor$ and so we may assume that $d \leq \frac{n}{2}$. First consider case (1). Put $A' := \{1, ..., n-1\}$, and let $O'_m(H)$ denote the number of orbits of H on m-sets of A'. Dividing subsets of $\{1,\dots,n\}$ into those containing n and those that do not, we have:

$$O_2(H) = O'_2(H) + O'_1(H)$$
$$O_d(H) = O'_d(H) + O'_{d-1}(H)$$

Since $O_2(H) = O_d(H)$ by assumption, and since $O'_1(H) \leq O'_d(H)$ and $O'_2(H) \leq O'_{d-1}(H)$ by the Livingstone–Wagner theorem (as $d \geq 3$), we deduce that $O'_1(H) = O'_d(H)$ and so $O'_1(H) = O'_2(H) = \cdots = O'_d(H)$ by the Livingstone–Wagner theorem.

It remains to show that $O'_1(H) = 1$. By assumption the orbits of H on A' are of length at least two. For each such orbit O, there is at least one orbit of H on 2-sets from O. Thus there are at least $O'_1(H)$ distinct orbits on 2-sets from A'. If however $O'_1(H) > 1$, there are additional orbits on 2-sets from A' consisting of 2-sets with elements from distinct orbits of H, contradicting $O'_2(H) = O'_1(H)$. Thus $O'_1(H) = 1$.

Next, consider case (2). Put $B := \{n-1, n\}$, $A'' = \{1,\dots,n-2\}$, and denote by $O''_m(H)$ the number of orbits of H on m-sets from A''. First suppose H fixes B pointwise. Dividing subsets of $\{1,\dots,n\}$ according to their intersection with B, we have

$$\begin{aligned} O_2(H) &= O''_2(H) + O''_1(H) + O''_1(H) + O''_0(H), \\ O_d(H) &= O''_d(H) + O''_{d-1}(H) + O''_{d-1}(H) + O''_{d-2}(H). \end{aligned} \tag{3.3}$$

Here, $O''_0(H) = 1$ corresponds to the single orbit of H on B. Since $d \geq 3$, the Livingstone-Wagner theorem implies the following inequalities:

$$O''_2(H) \leq O''_{d-1}(H), O''_1(H) \leq O''_{d-1}(H), O''_1(H) \leq O''_{d-2}(H), \text{ and } O''_0(H) \leq O''_d(H).$$

Thus, as $O_2(H) = O_d(H)$, (3.3) implies these are equalities. Hence, $O''_d(H) = O''_0(H) = 1$, and $O''_1(H) = \cdots = O''_d(H) = 1$ by the Livingstone–Wagner theorem.

Finally, consider the case where H is transitive on B. Then the action $H \to \mathrm{Sym}(B)$ has kernel H_0 of index 2 in H. Note that the number of points in the intersection of an m-set from $\{1,\dots,n\}$ with B remains invariant under the action of H. Moreover since H is transitive on B, every orbit of H on sets that intersect B at a single element is the union of two equal size orbits of H_0, one consisting of sets that contain $n-1$, and the other of those containing n. It follows that such orbits of H on m-sets from $\{1,\dots,n\}$ are in one to one correspondence with orbits of H_0 on $(m-1)$-sets from A''. Thus, by dividing subsets of $\{1,\dots,n\}$ according to the

cardinality of their intersection with B, we have:

$$\begin{aligned} O_2(H) &= O_2''(H) + O_1''(H_0) + O_0''(H) \\ O_d(H) &= O_d''(H) + O_{d-1}''(H_0) + O_{d-2}''(H). \end{aligned} \tag{3.4}$$

As $d \geq 3$, we have $O_2''(H) \leq O_d''(H)$, $O_1''(H_0) \leq O_{d-1}''(H_0)$, and $1 = O_0''(H) \leq O_{d-2}''(H)$ by the Livingstone–Wagner theorem. Since $O_2(H) = O_d(H)$, (3.4) implies that these are equalities. If $d \geq 4$, this gives $O_d''(H) = O_2''(H) \leq O_{d-2}''(H) = 1$ and hence $O_1''(H) = \cdots = O_d''(H)$ by the Livingstone–Wagner theorem.

For $d = 3$, the resulting equalities are $O_2''(H) = O_3''(H), O_1''(H_0) = O_2''(H_0)$, and $O_1''(H) = 1$. We claim that in fact $O_1''(H_0) = 1$, and hence $O_2''(H_0) = 1$, so that $O_3''(H) = O_2''(H) \leq O_2''(H_0) = 1$, yielding the assertion. To see the claim, note that since A'' is an orbit of H and $[H : H_0] = 2$, A'' is either an orbit of H_0 or breaks into two orbits A_1, A_2 of H_0. In the latter case $O_1''(H_0) = 2$, but H_0 has at least three orbits on 2-sets from A'': for, 2-sets with zero, one, and two elements from A_1 are never in the same orbit of H_0. This contradicts the equality $O_1''(H_0) = O_2''(H_0)$, thus yielding the claim. □

We have the following corollary to Proposition 3.3. Let $S_2 \times_{C_2} S_{n-2}$ denote the fiber product $\{(\sigma, \tau) \in S_2 \times S_{n-2} : \mathrm{sgn}(\sigma) = \mathrm{sgn}(\tau)\}$, where $sgn : S_m \to \{\pm\}$ is the sign map for $m \geq 2$.

Corollary 3.4. *Let $n \geq 8$, and suppose $H \leq S_n$ satisfies $O_2(H) = O_D(H)$.*

1. *If H has exactly one fixed point, then H is A_{n-1} or S_{n-1}.*
2. *If H stabilizes a 2-set, then H is A_{n-2}, S_{n-2}, $S_2 \times S_{n-2}$, $S_2 \times_{C_2} S_{n-2}$ or $S_2 \times A_{n-2}$.*

Proof. If H has a unique fixed point, Proposition 3.3 implies that H acts D-homogeneously on a set U_1 of cardinality $n - 1$. Hence by definition of D, the projection of H to $\mathrm{Sym}(U_1)$ contains A_{n-1} and thus $H = A_{n-1}$ or S_{n-1}.

Similarly, if H stabilizes a 2-set B, then Proposition 3.3 implies that H acts D-homogeneously on the complement U_2 of B. By definition of D, this implies that the projection H_2 of H to $\mathrm{Sym}(U_2)$ is either A_{n-2} or S_{n-2}.

If H fixes B pointwise, then $H = H_2$ is either A_{n-2} or S_{n-2}. Henceforth assume the projection H_B of H to $\mathrm{Sym}(B) = S_2$ is onto. By Goursat's lemma, the group H is then a fiber product of projections of H_B and H_2 onto a shared quotient. The only shared quotients of S_{n-2} and S_2 are $\{e\}$ or S_2, and the only shared quotient of A_{n-2} and S_2 is $\{e\}$. Therefore in this case H is $S_{n-2} \times S_2$, $S_{n-2} \times_{C_2} S_2$, or $A_{n-2} \times S_2$. □

4. The ramification types for $A_{n-2} \leq G \leq S_{n-2} \times S_2$

Let k be an algebraically closed field of characteristic 0, and $\Omega/k(t)$ a Galois extension with group $G = A_n$ or S_n. The combination of Proposition 3.1 and Corollary

3.4 gives the possibilities for groups $H \leq G$ with fixed field Ω^H of genus 0 or 1. The following proposition gives the possible ramification types from Table 2.1 for each such H.

Proposition 4.1. *Let $\Omega/k(t)$ be a Galois extension with Galois group $G = A_n$ or S_n with $n \geq 13$. Let F be the subfield of Ω fixed by $G \cap S_{n-1}$, and assume that the ramification type $\mathcal{E}$ of $F/k(t)$ is listed in Table 2.1. Then there exist constants $c > 0$ and $d \geq 0$ satisfying the following. If $G = A_n$:*

(1) *The fields fixed by stabilizers of points or of 2-sets, that is, by A_{n-1} or by $S_{n-2} \times_{C_2} S_2$, are of genus 0.*
(2) *The genus of the field fixed by A_{n-2} is at least $\max\{2, cn - d\}$.*

If $G = S_n$:

(1) *The fields fixed by stabilizers of points or of 2-sets, that is, by S_{n-1} or by $S_{n-2} \times S_2$, are of genus 0.*
(2) *The genus of the field fixed by S_{n-2} is either 0 or at least $\max\{2, cn - d\}$. It is of genus 0 if and only if*

$$\mathcal{E} = [n], [a, n-a], [2, 1^{n-2}] \quad \textit{(Type (I1.1) in Table 2.1)}.$$

(3) *The field fixed by $A_{n-2} \times S_2$ is of genus 0 if and only if $\mathcal{E}$ is one of the following ramification types from Table 2.1:*
(I2.11) $[a, n-a], \left[2^{n/2}\right], [1^2, 2^{(n-6)/2}, 4]$, *with* $n \equiv 2 \bmod 4$, *or*
(I2.13) $[a, n-a], \left[1^2, 2^{(n-2)/2}\right], [2^{(n-4)/2}, 4]$, *with* $n \equiv 0 \bmod 4$, *or*
(I2.15) $[a, n-a], \left[2^{n/2}\right], [1, 2^{(n-4)/2}, 3]$, *with* $n \equiv 2 \bmod 4$, *or*
(F4.3) $[1, 2^{(n-1)/2}], [1, 3^{(n-1)/3}], [3, 4, 6^{(n-7)/6}]$, *with* $n \equiv 7 \bmod 12$, *or*
(F4.5) $[1^2, 2^{(n-2)/2}], [1, 3^{(n-1)/3}], [4, 6^{(n-4)/6}]$, *with* $n \equiv 4 \bmod 12$.
It is of genus 1 if and only if $\mathcal{E}$ is one of the following:
(I2.3) $[n], [1^3, 2^{\frac{n-3}{2}}], [2^{\frac{n-3}{2}}, 3]$, *with* $n \equiv 1 \bmod 4$, *or*
(I2.5) $[n], \left[1, 2^{(n-1)/2}\right], [1^2, 2^{(n-5)/2}, 3]$, *with* $n \equiv 3 \bmod 4$, *or*
(I2.6) $[n], \left[1^3, 2^{(n-3)/2}\right], [1, 2^{(n-5)/2}, 4]$, *with* $n \equiv 1 \bmod 4$, *or*
(I2.8) $[n], \left[1, 2^{(n-1)/2}\right], [1^3, 2^{(n-7)/2}, 4]$, *with* $n \equiv 3 \bmod 4$, *or*
(F1.5) $\left[1^2, 2^{(n-5)/2}, 3\right], [1, 2^{(n-1)/2}]$ *thrice, with* $n \equiv 3 \bmod 4$, *or*
(F1.8) $\left[1^3, 2^{(n-7)/2}, 4\right], [1, 2^{(n-1)/2}]$ *thrice, with* $n \equiv 3 \bmod 4$, *or*
(F1.9) $\left[2^{(n-4)/2}, 4\right], [1^2, 2^{(n-2)/2}]$ *thrice, with* $n \equiv 0 \bmod 4$.
If the genus of $\Omega^{A_{n-2} \times S_2}$ is more than 1, then it is also at least $cn - d$.
(4) *The field fixed by $S_{n-2} \times_{C_2} S_2$ is of genus 0 if and only if*

$$\mathcal{E} = [1, 2^{\frac{n-1}{2}}], [1, 4^{\frac{n-1}{4}}], [2, 3, 4^{\frac{n-5}{4}}] \textit{ for } n \equiv 5 \bmod 8 \textit{ (Type (F3.2) in Table 2.1)}.$$

If it is not of genus 0, it is of genus at least $\max\{2, cn - d\}$.

Proof. We use Magma to carry out the following algorithm on each $\mathcal{E}$ in Table 2.1. A computer free proof appears in [16].

Notation and assumptions: View $\mathcal{E}$ as a set of conjugacy classes of S_n or A_n (i.e., partitions of n), each corresponding to (the conjugacy class of an inertia group of) a single place P of $k(t)$. Denote $\mathcal{E} = \{\mathcal{E}_P\}$ where P runs over the branch points of $k(t)$.

Algorithm:

Step 0: *Find the genus of a point stabilizer in G; Determine if G is alternating or symmetric; If symmetric, calculate the genus of Ω^{A_n}.* Plug $\mathcal{E}$ into the Riemann–Hurwitz formula for the degree n extension fixed by a point stabilizer. This gives the one-point part of Case (1) for both $G = A_n$ and $G = S_n$. Next, count the number s of ramification types $\mathcal{E}_P \in \mathcal{E}$ that correspond to an odd permutation. If $s = 0$, then $G = A_n$, otherwise $G = S_n$ (as $\mathcal{E}$ denotes the conjugacy classes of a generating set of G). In the latter case, due to the ramification-orbit correspondence described in §2.2, and since a permutation in S_n is transitive on S_n/A_n if and only if it is odd, the number s also gives the Riemann–Hurwitz contribution of the extension $\Omega^{A_n}/k(t)$. Thus, we calculate the genus of Ω^{A_n} using the Riemann–Hurwitz formula.

Step I: *In case $G = S_n$, find the ramification type $\mathcal{E}'$ of $\Omega^{A_{n-1}}/\Omega^{A_n}$.*

To form $\mathcal{E}'$, run the following procedure:

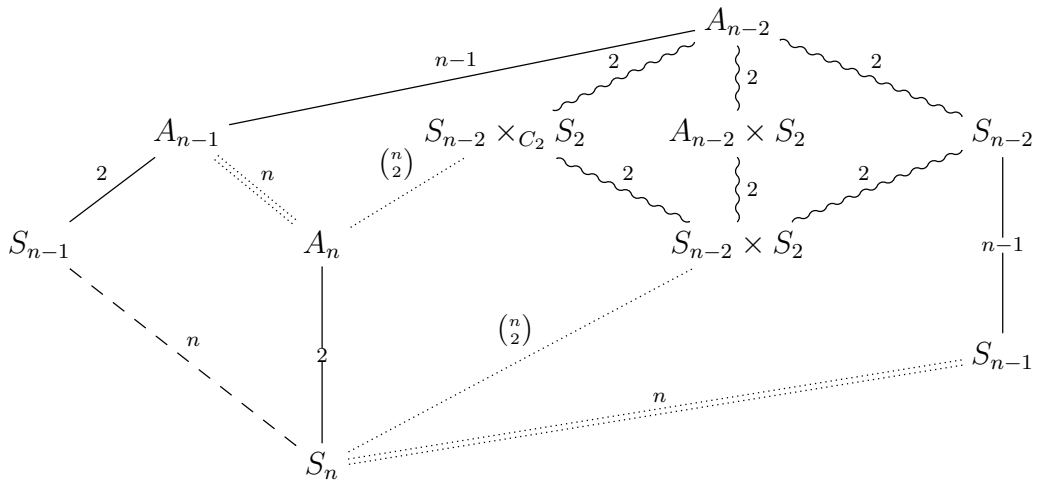
Procedure I: For each branch point P of $F/k(t)$ with corresponding ramification $\mathcal{E}_P \in \mathcal{E}$, do:

(1) If $\mathcal{E}_P$ corresponds to an even permutation, include it twice into $\mathcal{E}'$;
(2) If $\mathcal{E}_P$ corresponds to an odd permutation, construct and include the multiset $\mathcal{E}'_P$ in $\mathcal{E}'$. To construct $\mathcal{E}'_P$, for each $r \in \mathcal{E}_P$ do:
   - if r is even, include $r/2$ twice in $\mathcal{E}'_P$;
   - if r is odd, include r once in $\mathcal{E}'_P$.

(In Figure 1, Procedure I is applied to the dashed line in order to compute the ramification of the double dotted line above it.)

Validity of Procedure I: We claim that the ramification type $\mathcal{E}'$ is indeed the ramification type of $\Omega^{A_{n-1}}/\Omega^{A_n}$. Since Ω^{A_n} and $F = \Omega^{S_{n-1}}$ are linearly disjoint, this is deduced from Abhyankar's lemma as follows. For each branch point P of $F/k(t)$, if $\mathcal{E}_P$ corresponds to an even permutation, then the place P splits in the quadratic extension $\Omega^{A_n}/k(t)$. Hence Ω^{A_n} has two places Q_1 lying over it, and by Abhyankar's lemma $E_{\Omega^{A_{n-1}}/\Omega^{A_n}}(Q_1)$ is the same as $E_{\Omega^{S_{n-1}}/k(t)}(P)$ for both possibilities for Q_1. If $\mathcal{E}_P$ corresponds to an odd permutation, then there is single place Q_1 of Ω^{A_n} lying over P with $e(Q_1|P) = 2$. Abhyankar's lemma then implies that for every place Q_2 of $\Omega^{S_{n-1}}$, there is either a unique place Q of $\Omega^{A_{n-1}}$ lying over both Q_1 and Q_2

FIGURE 1. Candidate genus 0 and 1 subgroups of S_n



if $e := e(Q_2|P)$ is odd, or there are two such places Q if e is even. In the former case, $e(Q|Q_1) = e$ for the unique place Q lying over Q_1, and in the latter case $e(Q|Q_1) = e/2$ for both places Q lying above Q_1, proving the claim.

Step II: *If $G = A_n$, find the genus of a 2-set stabilizer. If $G = S_n$, find the genus and ramification of 2-set stabilizers $S_n \times_{C_2} S_2$ and $S_{n-2} \times S_2$ in A_n and S_n, respectively.* The following procedure takes the cycle structure $\mathcal{C}_P$ of an element $x_P \in S_n$ (i.e., a partition of n, or the multiset of cardinalities of the orbits of x_P on $\{1, \dots, n\}$) and gives a partition $\mathcal{C}_{2,P}$ of $\binom{n}{2}$ which represents the cardinalities of orbits of x_P on 2-sets of $\{1, \dots, n\}$ (i.e., the cycle structure of x_P as an element of $S_{\binom{n}{2}}$). See Lemma 2.3 for validity.

Procedure II: Given a partition $\mathcal{C}_P$ of n, construct a partition $\mathcal{C}_{2,P}$ of $\binom{n}{2}$:

(1) For every two entries $r_1, r_2 \in \mathcal{C}_P$, add $\gcd(r_1, r_2)$ copies of $\operatorname{lcm}(r_1, r_2)$ to $\mathcal{C}_{2,P}$;
(2) For each $r \in \mathcal{E}'_P$:
   - For every even entry $r \in \mathcal{C}_P$, add $r/2$ copies of r and a single copy of $r/2$ to $\mathcal{C}_{2,P}$;
   - For every odd entry $r \in \mathcal{C}_P$, add $(r-1)/2$ copies of r to $\mathcal{C}_{2,P}$.

By the ramification-orbit correspondence, Procedure II applied to all elements of $\mathcal{E}$ yields the ramification type $\mathcal{E}_2$ of $\Omega^{G_2}/k(t)$, where G_2 is the stabilizer of a 2-set. Plug $\mathcal{E}_2$ into the Riemann–Hurwitz formula for this extension to find the genus of Ω^{G_2}. This completes Case (1) for both $G = A_n$ and $G = S_n$. For $G = S_n$, apply

Procedure II to all elements of the multiset $\mathcal{E}'$ found in the previous step in order to find the ramification type $\mathcal{E}_2'$ of $\Omega^{S_{n-2}\times C_2 S_2}/\Omega^{A_n}$.

(In Figure 1, Procedure II is applied to the double dotted lines in order to compute the ramification of the dotted lines.) Afterwards, use the Riemann–Hurwitz formula for $\Omega^{S_{n-2}\times C_2 S_2}/\Omega^{A_n}$ to find the genus of $\Omega^{S_{n-2}\times C_2 S_2}$. (The ramification type $\mathcal{E}'$ gives the Riemann–Hurwitz contribution of this extension, and the genus of the field fixed by A_n is found in the previous step.)

Step III: *In case $G = S_n$, find the genus of the 2-point stabilizers A_{n-2} and S_{n-2} of A_n and S_n respectively.* Calculate the Riemann–Hurwitz contribution in the extensions $\Omega^{S_{n-2}}/\Omega^{S_{n-2}\times S_2}$ and $\Omega^{A_{n-2}}/\Omega^{S_{n-2}\times C_2 S_2}$ using the following procedure described in Lemma 2.3.

Procedure III:

(1) Count the total number of even entries in $\mathcal{E}$ (yielding the Riemann–Hurwitz contribution in $\Omega^{S_{n-2}}/\Omega^{S_{n-2}\times S_2}$).
(2) Count the total number of even entries in $\mathcal{E}'$ (yielding the Riemann–Hurwitz contribution in $\Omega^{A_{n-2}}/\Omega^{S_{n-2}\times C_2 S_2}$).

Afterwards, plug into the Riemann–Hurwitz formula to calculate the genera of $\Omega^{A_{n-2}}$ and $\Omega^{S_{n-2}}$.

Step IV: *In case $G = S_n$, Find the genus of $A_{n-2} \times S_2$.* Let g_1, g_2, g_3 denote the genera of $\Omega^{S_{n-2}}, \Omega^{S_{n-2}\times C_2 S_2}$, and $\Omega^{A_{n-2}\times S_2}$, respectively. Denote by g_0 and $\hat{g}$ the genera of $\Omega^{S_{n-2}\times S_2}$ and $\Omega^{A_{n-2}}$. A formula for the genera of intermediate extensions of a biquadratic extension is given in [1]:

$$g_3 = \hat{g} - g_1 - g_2 + 2g_0 \tag{4.1}$$

The formula is applicable as $\Omega^{S_{n-2}}$, $\Omega^{S_{n-2}\times C_2 S_2}$ and $\Omega^{A_{n-2}\times S_2}$ are the three quadratic intermediate extensions of the biquadratic extension $\Omega^{A_{n-2}}/\Omega^{S_{n-2}\times S_2}$. (In Figure 1, this biquadratic extension is denoted by the squiggly lines).

Step V: *If $G = A_n$, calculate the genus of $\Omega^{A_{n-2}}$.* In this case, A_{n-2} is a two-point stabilizer of G and so as in Step III, calculate its genus using the Riemann Hurwitz formula for $\Omega^{A_{n-2}}/\Omega^{S_{n-2}}$, where the Riemann–Hurwitz contribution is given by counting the total number of even entries in $\mathcal{E}$. □

5. Proofs of Theorems 1.2 and 1.3

Let k be an algebraically closed field of characteristic 0. The following theorem is the function field version of Theorem 1.2. Let N_g be as in Remark 2.8.

Theorem 5.1. *Fix $g \geq 0$. Let $F/k(t)$ be an extension of degree $n > N_g$ with Galois closure Ω, and assume $G := \mathrm{Gal}(\Omega/k(t))$ is A_n or S_n. Suppose Ω^H is of genus $\leq g$*

for some $H \leq G$, such that $H \not\geq A_{n-1}$. Then $A_{n-2} \lneq H \leq S_{n-2} \times S_2$, and the ramification of $F/k(x)$ is listed in Proposition 4.1. In fact, Ω^H is of genus ≤ 1.

Proof. If $H \subseteq A_n$, we may assume that the genus of the field fixed by A_n is 0 (otherwise the field Ω^{A_n} is of genus 1, which is impossible when $n > N_g$, see Remark 2.7), and thus replace G by A_n. Let M be the maximal subgroup of G containing H. (In particular, $M \neq A_n$). Thus $g_{\Omega^M} \leq g$. As $n > N_g$, M is guaranteed to be either a point stabilizer or a 2-set stabilizer of G, by Theorem 2.6. Thus H is contained in a point stabilizer or a 2-set stabilizer of G. Due to the genus assumption on Ω^H, Proposition 3.1 implies that $O_2(H) = O_D(H)$. If furthermore the ramification type of $F/k(t)$ is not one of the exceptions given in Table 2.1, then we also get $O_1(H) = O_2(H)$. Corollary 3.4 therefore gives the list of possibilities for H. Proposition 4.1 then gives the occurring ramification types for each possibility for H, and also implies that the genus of Ω^H is less than or equal to 1. □

To prove Theorem 1.3, we shall also need:

Lemma 5.2. *Let $f(t,x) = p(x) - t \in k(t)[x]$ be a polynomial with splitting field Ω, and Galois group $G = A_n$ or S_n for $n \geq 20$. Let $G_1 \leq G$ be the stabilizer of a root x_1, and G_2 the stabilizer of a 2-set which does not contain x_1. Then:*

1. *The extension $\Omega/k(x_1)$ has at least 5 branch points;*
2. *If the ramification of $k(x_1)/k(t)$ is of one of the types (I1.1)-(I2.8) in Table 2.1, then $\Omega^{G_2}(x_1)/\Omega^{G_2}$ has at least 5 branch points.*

See Appendix A for the proof. We next prove a strengthening of Theorem 1.3:

Theorem 5.3. *Let $f(t,x) = p(x) - t \in k(t)[x]$ be a degree $n > 20$ polynomial with splitting field Ω and Galois group $G = A_n$ or S_n. Suppose Ω^H is of genus at most 1 for nonmaximal $H \leq G$ which does not contain A_{n-1}. Then $H = S_{n-2}$ or $A_{n-2} \times S_2$.*

Furthermore, if $H = S_{n-2}$, then the genus of Ω^H is 0, and up to composition with linear polynomials p equals $x^a(x-1)^{n-a}$ for some $1 \leq a < n$ coprime to n. If $H = A_{n-2} \times S_2$, then the genus of Ω^H is 1, and the ramification of the polynomial covering p is one of types (I2.3), (I2.5), (I2.6), (I2.8) in Table 2.1.

Proof. Let G act on the set $\{1, \ldots, n\}$. As in the proof of Theorem 5.1, if $H \subseteq A_n$, we replace G by A_n. Let M be the maximal subgroup of G containing H. (In particular, $M \neq A_n$). By [9, Theorem 1.2.1], M is a point or 2-set stabilizer. Thus Proposition 3.2 implies that $O_2(H) = O_3(H)$. If H has only one fixed point, then H is 3-homogeneous on a subset U_1 of cardinality $n-1$ by Proposition 3.3.(1). If on the other hand H stabilizes a 2-set, then H is 3-homogeneous on a subset U_2 of cardinality $n-2$ by Proposition 3.3.(2). Henceforth fix $i \in \{1,2\}$ such that H is 3-homogeneous on U_i, and let $G_i \supseteq H$ be the stabilizer of an i-set. Let $\overline{H}$ and $\overline{G_i}$ be

the images of H and G_i under the projection $\pi_i : G_i \to \mathrm{Sym}(U_i) \cong S_{n-i}$, respectively. Let $\overline{\Omega} = \Omega^{\ker \pi_i}$, so that $\mathrm{Gal}(\overline{\Omega}/\Omega^{G_i}) \cong \overline{G}_i \cong A_{n-i}$ or S_{n-i}.

Letting $V \leq \overline{G}_i$ be a stabilizer of a point in U_i, Lemma 5.2 implies[3] that $\overline{\Omega}^V/\Omega^{G_i}$ has at least 5 branch points. If the core of $\overline{H}$ in $\overline{G}_i$ is trivial, then $\overline{\Omega}^H/\Omega^{G_i}$ also has at least 5 branch points. Since in addition $\overline{\Omega}^H/\Omega^{G_i}$ is of genus ≤ 1 with 3-homogeneous stabilizer $\overline{H}$ in the action on U_i, [9, Theorem 1.1.2] implies that $\overline{H} \cong A_{n-i}$ or S_{n-i}.

Since H does not contain A_{n-1}, it contains A_{n-2} and as in the proof of Corollary 3.4, H is one of the groups A_{n-2}, S_{n-2}, $S_2 \times S_{n-2}$, $S_2 \times_{C_2} S_{n-2}$ or $S_2 \times A_{n-2}$. The corresponding ramification types are then given by Proposition 4.1. The only resulting ramification types with an n-cycle are (I1.1) with $H = S_{n-2}$ and genus 0, or (I2.3), (I2.5), (I2.6) and (I2.8) with $H = A_{n-2} \times S_2$ and genus 1. In case the ramification is (I1.1), by composing with linears we may assume that the branch point of type $[a, n-a]$ is $t \mapsto 0$, and its preimages under p are the places $x \mapsto 0$ and $x \mapsto 1$. Thus, $p(x)$ is a constant multiple of $x^a(x-1)^{n-a}$. □

6. Hilbert irreducibility

Let k be a finitely generated field of characteristic 0. Let $f \in k(t)[x]$ be a polynomial with splitting field Ω and Galois group A. For a place $t \mapsto t_0 \in k$, let $D_P \leq A$ denote the decomposition group of a place P of the integral closure of $k[t]$ in Ω which lies over $t \mapsto t_0$. Note that by varying P over the places of Ω lying above $t \mapsto t_0$, we obtain the conjugates of D_P in A. We denote by D_{t_0} the conjugacy class of such subgroups. For $D \leq A$, we write $D = D_{t_0}$ to denote that D is some conjugate of D_P. For every $t_0 \in k$ which is not a root of the discriminant $\delta_f \in k(t)$ of f, it is well known that $\mathrm{Gal}(f(t_0, x), k)$ is permutation isomorphic to D_P [13, Lemma 2].

The following (well known) proposition describes the relevant properties of D_{t_0}, see [12, Prop. 2.4]. Let $\tilde{X}$ be the (irreducible smooth projective) curve corresponding to Ω, and $\tilde{f} : \tilde{X} \to \tilde{X}/A \cong \mathbb{P}^1_k$ the natural projection. If D is the decomposition group at an unramified place $t \mapsto t_0 \in k$, then there exists a covering $f_D : X_D \to \mathbb{P}^1_k$ from the quotient $X_D := \tilde{X}/D$, whose composition with the natural projection $\tilde{X} \to \tilde{X}/D$ is $\tilde{f}$.

Proposition 6.1. *Let $f \in k(t)[x]$ be irreducible with Galois groups G and A over $\overline{k}(t)$ and $k(t)$, respectively. Suppose $t_0 \in k$ is neither a root nor a pole of $\delta_f(t)$, and $D = D_{t_0}$ is its decomposition group. Then:*

1. *$t_0 \in f_D(X_D(k))$, and $DG = A$ (so that X_D is geometrically irreducible);*
2. *$f(t_0, x) \in k[x]$ is reducible if and only if D is intransitive.*

[3] Note that if $i = 2$, then the ramification of $\Omega^{G_1}/k(t)$ is one of types (I1.1)-(I2.8) in Table 2.1, and hence the lemma can be applied.

As a corollary to Theorem 1.2 we therefore have the following strengthening of Theorem 1.1. Let N_1 be the constant from Remark 2.8.

Theorem 6.2. *Let $f(t,x) \in k(t)[x]$ be a polynomial with Galois group $A = A_n$ or S_n over $k(t)$ (resp. Galois group G over $\overline{k}(t)$) for $n > N_1$. If $D \leq A$ appears as the Galois group of $f(t_0,x) \in k[X]$ for infinitely many $t_0 \in k$, then either $D \geq A_{n-1}$, or the ramification of the extension fixed by $G \cap S_{n-1}$ is listed in Proposition 4.1 and $A_{n-2} \lneq D \leq S_{n-2} \times S_2$.*

Proof. If $f(t,x)$ splits over $\overline{k}$, then the splitting field Ω of f over $k(t)$ is a constant extension $\Omega = L(t)$, in which case $\mathrm{Gal}(f(t_0,x),k) \cong \mathrm{Gal}(L/k) \cong A \in \{A_n, S_n\}$ for all $t_0 \in k$. Henceforth, assume f does not split over $\overline{k}$ and hence G is nontrivial. Since $G \lhd A$ [12, §2] and $n > N_1 > 4$, it follows that $G \supseteq A_n$.

By Proposition 6.1, $DG = A$ and if $D = \mathrm{Gal}(f(t_0,x),k)$ for infinitely many $t_0 \in k$, then $X_D(k)$ is infinite. Since in addition X_D is geometrically irreducible (as $DG = A$), X_D is of genus ≤ 1 by Faltings' theorem. Setting $C := D \cap G$, Theorem 1.2 therefore implies that either $A_{n-1} \leq C \leq S_n$ or $A_{n-2} \lneq C \leq S_{n-2} \times S_2$ and the ramification of the extension $(\Omega\overline{k})^{G_1}/\overline{k}(t)$ fixed by $G_1 = G \cap S_{n-1}$ is described by Proposition 4.1. It follows that $D \supseteq C$ is also of the required form. □

The following is a well known corollary to Proposition 6.1.

Corollary 6.3. [12, Corollary 2.5] *Let $f(t,x) \in k(t)[x]$ be an irreducible polynomial with Galois groups A and G over $k(t)$ and $\overline{k}(t)$, respectively. Then Red_f and $\bigcup_D f_D(X_D(k))$ differ by a finite set, where D runs over maximal intransitive subgroups of A for which X_D is of genus ≤ 1 and $DG = A$.*

We can now deduce Theorem 1.4:

Proof of Theorem 1.4. Let A and G be the Galois groups of f over $k(t)$ and $\overline{k}(t)$, respectively. By Corollary 6.3, the set Red_f and the union $\bigcup_D f_D(X_D(k))$ differ by a finite set, where D runs over the set $\mathcal{D}$ of conjugacy classes of maximal intransitive subgroups $D \leq A$ for which $DG = A$ and X_D is of genus ≤ 1. As in the proof of Theorem 6.2, $C := D \cap G$ and D are either intermediate subgroups between A_{n-1} and S_n, or intermediate subgroups between A_{n-2} and $S_{n-2} \times S_2$ which are different from A_{n-2}. In the latter case, the ramification of $f_{A \cap S_{n-1}}$ is in Table 2.1. Since by Proposition 4.1, at most one of the curves X_D is of genus ≤ 1 for $D \in \{S_{n-2}, S_{n-2} \times_{S_2} S_2, A_{n-2} \times S_2\}$, the largest subset of $\mathcal{D}$ consisting of conjugacy classes of subgroups D for which $C = D \cap G \in \{S_n, A_n, S_{n-1}, A_{n-1}, S_{n-2} \times S_2, S_{n-2} \times_{S_2} S_2, A_{n-2} \times S_2\}$, and in which no group contains the other, is of cardinality 3, cf. Figure 1[4]. □

[4]To obtain three such groups D, one can pick $\mathcal{D} = \{A_n, S_{n-1}, S_{n-2} \times S_2\}$.

The following example shows that three is a sharp bound on the number of value sets in Corollary 6.3.

Example 6.4. Fix $n > N_1$. Let Ω be the splitting field of $x^a(x-1)^{n-a}-t \in \mathbb{Q}(t)[x]$ so that $\mathrm{Gal}(\Omega/\mathbb{Q}) = S_n$. Let $f(t,x) \in \mathbb{Q}(t)[x]$ be the minimal polynomial of a primitive element for Ω. Letting $\mathcal{D} = \{S_{n-1}, S_{n-2} \times S_2, A_n\}$, the fixed fields Ω^D, $D \in \mathcal{D}$ are of genus 0, and moreover $\mathcal{D}$ is the set of maximal subgroups of S_n with fixed field of genus ≤ 1. Since the action of $\mathrm{Gal}(f(t,x),\mathbb{Q})$ is regular, every $D \in \mathcal{D}$ is intransitive. Thus, here Red_f is the union of three value sets and a finite set by Corollary 6.3.

Appendix A. Proof of Lemma 5.2

Let F be the fixed field of a two point stabilizer contained in G_1, so that $F \supset k(x_1)$. Consider the finite branch points $P_1, \dots, P_s$ of $k(x_1)/k(t)$. Since $G \in \{A_n, S_n\}$ is non-cyclic and generated by s branch cycles, we have $s > 1$. Letting $r_i := \#E_{k(x_1)/k(t)}(P_i)$, the Riemann–Hurwitz formula gives:

$$n-1 = \sum_{i=1}^{s}(n-r_i) \text{ or equivalently } \sum_{i=1}^{s} r_i = (s-1)n+1. \tag{A.1}$$

Let $u_i = \#\{e \in E_{k(x_1)/k(t)}(P_i) \,|\, e = 1\}$ and $v_i = \#\{e \in E_{k(x_1)/k(t)}(P_i) \,|\, e > 1\}$, so that $r_i = u_i + v_i$. Since $u_i + 2v_i \leq n$, we have $v_i \leq (n-u_i)/2$. Thus $r_i = u_i + v_i \leq (n+u_i)/2$. In combination with (A.1) this gives $\sum_{i=1}^{s}(n+u_i)/2 \geq (s-1)n+1$ or $\sum_{i=1}^{s} u_i \geq (s-2)n+2$. For $s \geq 3$, we have $\sum_{i=1}^{s} u_i \geq n+2 > 5$, and hence Lemma 2.4 implies that $F/k(x_1)$ has at least 5 branch points.

It remains to consider the case $s = 2$. If $u_1 + u_2 \geq 5$, the conclusion follows from Lemma 2.4. Henceforth assume $2 \leq u_1 + u_2 \leq 4$. By the Riemann–Hurwitz formula one has:

$$n-1 = \sum_{i=1}^{2}\sum_{e \in E_i}(e-1) = \sum_{i=1}^{2}\left(v_i + \sum_{e \in E_i, e \geq 3}(e-2)\right),$$

where $E_i := E_{k(x_1)/k(t)}(P_i)$, $i = 1, 2$. Since $v_i = r_i - u_i$ and $r_1 + r_2 = n+1$ by (A.1),

$$\sum_{e \in E_1, e \geq 3}(e-2) + \sum_{e \in E_2, e \geq 3}(e-2) = u_1 + u_2 - 2. \tag{A.2}$$

If $u_1 + u_2 = 2$, then by (A.2) the orbits of the branch cycles x_1, x_2 over P_1, P_2 are of length ≤ 2 and hence x_1 and x_2 are involutions. As in Section 2.4, G is generated by the two involutions, contradicting that G is not dihedral. It follows that $u_1 + u_2 = 3$ or 4, and hence the multiset of entries in $E_1 \cup E_2$ that are greater than 2 is one of the following $\{4\}$, $\{3,3\}$, or $\{3\}$. Without loss of generality, suppose one of these entries is in E_1. Since $u_1 + u_2 \leq 4$ and the sum of greater than 2 entries in E_1 is at most 6, the number of entries in E_1 that equal 2 is at least $(n-10)/2$. Since E_1

contains an entry that is greater than 2, Lemma 2.4 shows that each of the places Q of $k(x_1)$ over P_1 with $e(Q|P_1) = 2$ is a branch point of $F/k(x_1)$. Thus, there are at least $(n-10)/2 \geq 5$ such places, completing the proof of (1).

For part (2), recall that the natural action of G on $S = \{1, \dots, n\}$ is equivalent to its action on G/G_1, and that the action of G on 2-sets from S is equivalent to its action on G/G_2. Under this equivalence, for a place P of $k(t)$ with branch cycle $x_P \in G$, there is a one to one correspondence between the orbits U of x_P on 2-sets and the places Q_U of Ω^{G_2} lying over P.

Given orbits $R_1, R_2, R_3 \subseteq S$ of x_P with lengths r_1, r_2, r_3, respectively, such that r_1 does not divide $\operatorname{lcm}(r_2, r_3)$, we claim that every place Q_U of Ω^{G_2} lying over P, which corresponds to an orbit $U \subseteq R_2 \cup R_3$ on 2-sets, is a branch point of $\Omega^{G_2}(x_1)/\Omega^{G_2}$. Note that since $1 \notin G_2$, the ramification-orbit correspondence implies that the orbits $\hat{U}$ of x_P on pairs (s, C), where $C \subseteq S$ is a 2-set and $s \in S \setminus C$, are in one to one correspondence with the places $Q_{\hat{U}}$ of $\Omega^{G_1 \cap G_2} = \Omega^{G_2}(x_1)$. Moreover, we pick the correspondence so that $Q_{\hat{U}}$ lies over a place Q_U (resp. Q_R) of Ω^{G_2} (resp. $k(x_1)$) if and only if U (resp. R) is the image of $\hat{U}$ under the projection $(s, C) \mapsto C$ (resp. $(s, C) \mapsto s$). Let Q_{R_1} be a place of $k(x_1)$ and Q_U be a place of Ω^{G_2} for $U \subseteq R_2 \cup R_3$ with $R_1 \neq R_2, R_3$. Since r_1 does not divide $\operatorname{lcm}(r_2, r_3)$, we have $R_1 \neq R_2, R_3$ and hence for every orbit U of x_P acting on 2-sets from $R_2 \cup R_3$, there is a place $Q_{\hat{U}}$ of $\Omega^{G_2}(x_1)$ lying over Q_U and Q_{R_1}. Now by Abhyankar's lemma $e(Q_{\hat{U}}|P) = \operatorname{lcm}(r_1, e)$, where $e := e(Q_U|P)$, and e divides $\operatorname{lcm}(r_2, r_3)$. Thus $e(\hat{Q}_U|Q_U) = \operatorname{lcm}(r_1, e)/e = r_1/\gcd(r_1, e) > 1$, and Q_U is a branch point, proving the claim.

For types (I1.1)-(I2.2), let x_3 be the branch cycle whose cycle structure is listed last in the ramification type. Then x_3 has an orbit R_1 of length 2 which is larger than $\operatorname{lcm}(r_2, r_3)$ for any two fixed points R_2, R_3 of x_3. Since there are $n-2$ such fixed points, we have at least $(n-2)(n-3)/2 > 5$ branch points. Similarly, for types (I2.3)-(I2.8), let x_2 be the branch cycle that has an orbit R_1 of length 3 or 4. As $\operatorname{lcm}(r_2, r_3) = 2 < 3$ for any two length 2 orbits R_2, R_3 of x_2, and there are at least $(n-7)/2$ length 2 orbits of x_2, this implies that $\Omega^{G_2}(x_1)/\Omega^{G_2}$ has at least $\binom{(n-7)/2}{2} > 5$ branch points.

References

[1] R. Accola, Two Theorems on Riemann Surfaces with Noncyclic Automorphism Groups, Proc. AMS 25 (1970), 598–602. 16

[2] L. Babai, Á. Seress, On the degree of transitivity of permutation groups: A short proof, Journal of Combinatorial Theory, Series A 45 (1987), 310–315. 4

[3] O. David, Y. Karasik, D. Neftin, M. Zieve, Reducibility of fiber products. In preparation. 3

[4] M. D. Fried, On Hilbert's Irreducibility Theorem, J. Number Theory 6 (1974), 211–231. 3

[5] M. D. Fried, Applications of the classification of simple groups to monodromy, part ii: Davenport and Hilbert–Siegel problems, preprint (1986), 1–55. 3
[6] W. Fulton, Algebraic Curves: An Introduction to Algebraic Geometry. Advanced Book Classics. Addison-Wesley Publishing Company, Advanced Book Program, Redwood City, CA, 1989. 7
[7] R. M. Guralnick, Monodromy Groups of Coverings of Curves. Galois groups and fundamental groups, 1–46, Math. Sci. Res. Inst. Publ., 41, Cambridge Univ. Press, Cambridge (2003). 8
[8] R. M. Guralnick, P. Müller, J. Saxl, The rational function analogue of a question of Schurand exceptionality of permutation representations. Memoirs of the American Mathematical Society, Band 162, AMS (2003). 3
[9] R. M. 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). 2, 3, 8, 10, 17, 18
[10] R. M. Guralnick, T. J. Tucker, M. E. Zieve, Exceptional covers and bijections on rational points. Internat. Math. Res. Notices rnm004 (2007). 4
[11] J. König, On the reducibility behaviour of Thue polynomials. J. Number Theory 176 (2017), 37–45. 3
[12] J. König, D. Neftin, Reducible specializations of polynomials: the nonsolvable case. Preprint, arXiv:2001.03630. 3, 18, 19
[13] J. König, D. Neftin, The admissibility of M_{11} over number fields. J. Pure and Applied Algebra 222 (2018), 2456–2464. 18
[14] K. Langmann, Werteverhalten holomorpher Funktionen auf Überlagerungen und zahlentheoretische Analogien. Math. Ann. 299 (1994), 127–153. 3
[15] D. Livingstone, A. Wagner, Transitivity of finite permutation groups on unordered sets. Math. Z. 90 (1965), 393–403. 4
[16] T. Monderer Genus 0 Subfields of Symmetric and Alternating Extensions. M.Sc. Thesis. Technion 2017. 14
[17] P. Müller, Permutation groups with a cyclic two-orbits subgroup and monodromy groups of Laurent polynomials. Ann. Sc. Norm. Super. Pisa Cl. Sci. XII (2013), 369–438. 3
[18] P. Müller, Hilberts irreducibility theorem for prime degree and general polynomials, Isr. J. Math. 109 (1999) 319–337. 1, 3
[19] P. Müller, Finiteness results for Hilbert's irreducibility theorem. Annales de l'institut Fourier 52 (2002), 983–1015. 3
[20] D. Neftin, M. Zieve, Monodromy groups of indecomposable covers with bounded genus. Preprint, November 2020 version. Available on D.N.'s webpage. 1, 2, 3, 5, 6, 7, 8
[21] J.-P. Serre, Lectures on the Mordell-Weil Theorem. (1997). 2
[22] H. Stichtenoth, Algebraic function fields and codes. Universitext. Springer-Verlag, Berlin (1993). 4, 5

Department of Mathematics, Technion - IIT, Haifa 32000, Israel
E-mail address: talimon@campus.technion.ac.il

Department of Mathematics, Technion - IIT, Haifa 32000, Israel
E-mail address: dneftin@technion.ac.il