POLYNOMIALS WITH SURJECTIVE ARBOREAL GALOIS REPRESENTATIONS EXIST IN EVERY DEGREE

JOEL SPECTER

Abstract. Let $E$ be a Hilbertian field of characteristic 0. R.W.K. Odoni conjectured that for every positive integer $n$ there exists a polynomial $f \in E[X]$ of degree $n$ such that each iterate $f^{\circ k}$ of $f$ is irreducible and the Galois group of the splitting field of $f^{\circ k}$ is isomorphic to the automorphism group of a regular, $n$-branching tree of height $k$. We prove this conjecture when $E$ is a number field.

1. Introduction

Given a polynomial $f \in \mathbb{Q}[X]$, the roots of $f$ are the most evident set on which the absolute Galois group acts. This note concerns the Galois action on the second most evident set: the set of roots of all compositional iterates of $f$.

We begin by establishing some notation. All fields considered in this note have characteristic 0. If $F$ is a field and $f \in F[X]$ is a polynomial, for each positive integer $k$, we denote the $k$-th iterate of $f$ under composition by $f^{\circ k}$. The set of all pre-images of 0 under the iterates of $f$ is denoted $T_f := \prod_{k=0}^{\infty} \{ r \in F : f^{\circ k}(r) = 0 \}$.

To organize $T_f$, we give it the structure of a rooted tree: a zero $r_k$ of $f^{\circ k}$ is connected to a zero $r_{k-1}$ of $f^{\circ (k-1)}$ by an edge if $f(r_k) = r_{k-1}$. We call $T_f$ the pre-image tree of 0. The absolute Galois group $G_F$ of $F$ acts on $T_f$ by tree automorphisms. The resulting map $\rho_f : G_F \to \text{Aut}(T_f)$
is called the arboreal Galois representation associated to $f$. We will say $\rho_f$ is regular if $T_f$ is a regular, rooted tree of degree equal to the degree of $f$.

Interest in arboreal Galois representations originates from the study of prime divisors appearing in the numerators of certain polynomially-defined recursive sequences. Explicitly, given a polynomial $f \in \mathbb{Q}[X]$ and an element $c_0 \in \mathbb{Q}$, one wishes to understand the density of the set of primes

$$ S_{f,c_0} := \{ p : v_p(f^{\circ n}(c_0)) > 0 \text{ for some value of } n \} $$

inside the set of all prime integers. An observation, first made by Odoni in [Odo85b], is that one may bound this density from above using Galois theory. Specifically, if one excludes the primes $p$ for which $c_0$ and $f$ are not $p$-integral, a prime $p$ is contained in $S_{f,c_0}$ if and only if $c_0$ is a root of some iterate of $f \mod p$. By the Chebotarev Density Theorem, the proportion of primes $p$ for which $f^{\circ k} \mod p$ has a root is determined by the image of $\rho_f$. As a general
principle, if a polynomial has an arboreal Galois representation with large image, then few primes appear in $S_{f,c}$. For specific results, we refer the reader to [Odo85b] or [Jon08].

In [Odo85a], Odoni showed that for any field $F$ of characteristic 0, the arboreal Galois representation associated to the generic monic, degree $n$ polynomial

$$f_{gen}(X) := X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0 \in F(a_{n-1}, \ldots, a_0)[X]$$

is regular and surjective. When $F$ is Hilbertian, for example when $F = \mathbb{Q}$, one expects that most monic, degree $n$ polynomials behave like $f_{gen}$. Indeed, this expectation holds true for any finite number of iterates: for each $k > 0$, the set of monic, degree $n$ polynomials $f$ such that the Galois group of $f^k$ over $F$ is smaller than the Galois group of $f_{gen}$ over $F(a_{n-1}, \ldots, a_0)$ is thin. Alas, in general, the intersection of the complement of countably many thin sets may be empty; therefore, Odoni’s theorem does not imply the existence of any specialization with surjective arboreal Galois representation. He conjectures that such specializations exist.

**Conjecture 1.1** ([Odo85a], Conjecture 7.5). Let $E$ be a Hilbertian field of characteristic 0. For each positive integer $n$, there exists a monic, degree $n$ polynomial $f \in E[X]$ such that every iterate of $f$ is irreducible and the associated arboreal Galois representation

$$\rho_f : G_E \to \text{Aut}(T_f)$$

is surjective.

In this note, we prove Odoni’s conjecture when $E$ is a number field. More generally, we prove Conjecture 1.1 for extensions of $\mathbb{Q}$ that are unramified outside of finitely many primes of $\mathbb{Z}$.

**Theorem 1.2.** If $E/\mathbb{Q}$ is an algebraic extension that is unramified outside finitely many primes, then for each positive integer $n$ there exists a positive integer $a < n$ and infinitely many $A \in \mathbb{Q}$ such that the polynomial

$$f_{a,A}(X) := X^n(X - A)^{n-a} + A$$

and all of its iterates are irreducible over $E$ and the arboreal $G_E$-representation associated to $f_{a,A}$ is surjective.

Our choice to consider the polynomial families in Theorem 1.2 was inspired by examples of surjective arboreal Galois representations over $\mathbb{Q}$ constructed by Robert Odoni and Nicole Looper. In [Odo85b], Odoni shows that the arboreal $G_\mathbb{Q}$-representation associated to $X(X - 1) + 1$ is regular and surjective. In [Loo16], Looper proves Conjecture 1.1 for polynomials over $\mathbb{Q}$ of prime degree by analyzing the arboreal Galois representations associated to certain integer specializations of the trinomial family $X^n - ntX^{n-1} + nt = X^{n-1}(X - nt) + nt$.

In addition to our note, there have been a series of recent, independent works concerning Odoni’s conjecture. Borys Kadets [Kad18] has proved Conjecture 1.1 when $n$ is even and greater than 19, and $E = \mathbb{Q}$. Robert Benedetto and Jamie Juul [BJ18] have proved Conjecture 1.1 when $E$ a number field, and $n$ is even or $\mathbb{Q}(\sqrt{n}, \sqrt{n - 2}) \not\subseteq E$.

The organization of this paper is as follows. Section 2 provides a criterion with which to check if an arboreal Galois representation contains a congruence subgroup $\Gamma(N)$. This

---

1 Jamie Juul has shown that the arboreal Galois representation associated to the generic monic, degree $n$ polynomial over a field $F$ of any characteristic is regular and surjective under the assumption that the characteristic of $F$ and the degree $n$ do not both equal 2 [Juu14].
criterion is that the image of the arboreal Galois representation contains, up to conjugation, some set of preferred elements
\[ \{\sigma_0\} \cup \{\sigma_k : k > N\} \cup \{\sigma_{\infty, N}\} \]
which topologically generate a subgroup containing \( \Gamma(N) \). In Section 2, we show that for various explicit choices of \( A \) and \( a \) there are prime integers
\[ \{p_0\} \cup \{p_k : k > 0\} \cup \{p_{\infty}\} \]
such that the image of the inertia group \( I_{p_k} \leq G_{\mathbb{Q}_{p_k}} \) under \( \rho_{f_{a,A}} \) contains an element conjugate to \( \sigma_k \) if \( k < \infty \), and conjugate to either \( \sigma_{\infty,1} \) or \( \sigma_{\infty,0} \) if \( k = \infty \). By choosing \( A \) well, one can force \( p_k \) to lie outside any fixed, finite set of primes; hence if \( E/\mathbb{Q} \) is unramified outside finitely many primes, then there is a choice of \( a \) and \( A \) such that the image of \( G_E \) under \( \rho_{f_{a,A}} \) contains \( \Gamma(1) \). Given such a polynomial, its arboreal Galois representation is surjective if and only if its splitting field is an \( S_n \)-extension. In Section 4 we prove there are infinitely many values of \( A \) and \( a \) for which the representation \( \rho_{f_{a,A}} : G_E \to \text{Aut}(T_{f_{a,A}}) \) is surjective by means of a Hilbert Irreducibility argument.

### 2. Recognizing Surjective Representations

Fix a field \( F \) of characteristic 0 and let \( f \in F[X] \) be a polynomial. For every non-negative integer \( N \), let
\[ T_{f,N} := \prod_{k=0}^{N} \{ r \in \overline{F} : f^{\circ k}(r) = 0\} \subseteq T_f \]
denote the full subtree of \( T_f \) whose vertices have at most height \( N \). The subtree \( T_{f,N} \) is stable under the action of \( \text{Aut}(T_f) \). Let \( \Gamma(N) \leq \text{Aut}(T_f) \) be the vertex-wise stabilizer of \( T_{f,N} \) in \( \text{Aut}(T_f) \). In this section, we describe a condition under which the image of \( \rho_f \) contains \( \Gamma(\bar{N}) \). Since \( \Gamma(0) \) equals \( \text{Aut}(T_f) \), the case when \( N = 0 \) is of primary interest.

To state our criterion, we introduce some terminology. For each non-negative integer \( k \), we denote the splitting field of \( f^{\circ k} \) over \( F \) by \( F_k \). If \( k \) is negative, we define \( F_k := F \). By a branch of the tree \( T_f \), we mean a sequence of vertices \( (r_i)_{i=0}^{\infty} \) such that \( r_0 = 0 \) and \( f(r_i) = r_{i-1} \) for \( i > 0 \). The group \( G_F \) acts on the branches of \( T_f \). If \( X \) is some set of branches and \( \sigma \in G_F \), we say that \( \sigma \) acts transitively on \( X \) if the closed, pro-cyclic subgroup \( \langle \sigma \rangle \subseteq G_F \) stabilizes \( X \) and acts transitively in the usual sense.

The following is a sufficient condition for the image of a regular aboreal Galois representation to contain \( \Gamma(N) \).

**Lemma 2.1.** Let \( N \) be a non-negative integer, \( f \in F[X] \) be a monic polynomial of degree \( n \), and \( a < n \) be a positive integer such that either \( a = 1 \), or \( a < n/2 \) and \( n - a \) is prime. Assume that all iterates of \( f \) are separable. Furthermore, assume that:

1. there is an element \( \sigma_0 \in G_F \) which acts transitively on the branches of \( T_f \),
2. there is an element \( \sigma_{\infty,N} \in G_F \) and a regular, \((n - a)\)-branching subtree \( T \subseteq T_f \) such that \( \sigma_{\infty,N} \) acts transitively on the branches of \( T \), and
3. for every positive integer \( k > N \), there is an element \( \sigma_k \in \text{Gal}(F_k/F_{k-1}) \) which acts on the roots of \( f^{\circ k} \) in \( F_k \) as a transposition,

then all iterates of \( f \) are irreducible, and the image of the arboreal Galois representation associated to \( f \) contains \( \Gamma(N) \).
Proof. Since all iterates of \( f \) are separable, Hypothesis \( \square \) implies that all iterates of \( f \) are irreducible. We show that \( \Gamma(N) \) is contained in the image of \( \rho_f \).

For all integers \( k > N \), the subgroup \( \Gamma(k) \leq \Gamma(N) \) is finite index, and \( \Gamma(N) \) is isomorphic to the inverse limit \( \varprojlim_{k>N} \Gamma(N)/\Gamma(k) \). We regard \( \Gamma(N) \) as a topological group with respect to the topology induced by the system of neighborhoods \( \{ \Gamma(k) \}_{k>N} \). The map \( \rho_f : G_F \rightarrow \text{Aut}(T_f) \) is continuous in this topology. Since \( G_F \) is compact, the image, \( \rho_f(G_F) \), is closed.

To show that the closed subgroup \( \rho_f(G_F) \) contains \( \Gamma(N) \), it suffices to show that for all \( k > N \)
\begin{equation}
(\rho_f(G_F) \cap \Gamma(k-1))/(\rho_f(G_F) \cap \Gamma(k)) = \Gamma(k-1)/\Gamma(k) \tag{2.1}
\end{equation}

Fix an integer \( k > N \). Concretely, \( \Gamma(k-1)/\Gamma(k) \) is the group of permutations \( \sigma \) of the roots of \( f^{\circ k} \) which satisfy the relation \( \rho(\sigma(r)) = \rho(r) \). For each root \( \pi \) of \( f^{\circ (k-1)} \), let \( X_{\pi} \) denote the set of roots of \( f(X) - \pi \) in \( F \). The group \( \Gamma(k-1)/\Gamma(k) \) stabilizes \( X_{\pi} \), and there is an isomorphism
\begin{equation}
\Gamma(k-1)/\Gamma(k) \cong \bigoplus_{\pi \in X \text{ \Gamma(k-1)-conjugate to a transposition} \;
X_{\pi} \quad \text{given by the direct sum of the restriction maps. Note that } \text{Gal}(F_k/F_{k-1}) \text{ is the subquotient of } G_F \text{ which is mapped isomorphically to } (\rho_f(G_F) \cap \Gamma(k-1))/(\rho_f(G_F) \cap \Gamma(k)) \text{ via the map induced by } \rho_f.
\end{equation}

To show Equation (2.1) holds (and therefore prove the lemma), it suffices by Equation (2.2) to show that:

(\star) If \( (r r') \) is a transposition in the symmetric group on the roots \( f^{\circ k} \) and \( f(r) = f(r') \), then \( (r r') \) is realized by an element of the Galois group \( \text{Gal}(F_k/F_{k-1}) \).

We will say a transposition \( (r r') \) on the set of roots of \( f^{\circ k} \) lies above a root \( \pi \) of \( f^{\circ (k-1)} \) if
\[ f(r) = f(r') = \pi. \]

We conclude the proof by demonstrating that (\star) holds.

First, we show that \( \text{Gal}(F_k/F_{k-1}) \) contains at least one transposition above each root of \( f^{\circ (k-1)} \). Fix a root \( \pi \) of \( f^{\circ (k-1)} \). By Assumption \( \square \) the automorphism \( \sigma_k \in \text{Gal}(F_k/F_{k-1}) \) acts on roots of \( f^{\circ k} \) as a transposition. Since \( \sigma_k \) is an element of \( \text{Gal}(F_k/F_{k-1}) \), it necessarily lies above a root \( \pi' \) of \( f^{\circ (k-1)} \). By Assumption \( \square \) there is some \( \tau \in \langle \sigma_0 \rangle \) such that \( \tau(\pi') = \pi \). The conjugate \( \sigma_k^\tau \) acts on the roots of \( f^{\circ k} \) as a transposition above \( \pi \).

To conclude the proof, we show that \( \text{Gal}(F_k/F_{k-1}) \) contains every transposition above \( \pi \). Observe that elements of \( \text{Gal}(F_k/F_{k-1}) \) which are \( \text{Gal}(F_k/F_{k-1}) \)-conjugate to a transposition above \( \pi \) are also transpositions and lie above \( \pi \). We know \( \text{Gal}(F_k/F_{k-1}) \) contains some transposition above \( \pi \). To show \( \text{Gal}(F_k/F_{k-1}) \) contains all transpositions above \( \pi \), it suffices to show \( G_{F(\pi)} \) acts doubly transitively on \( X_{\pi} \).

Let \( F_{\pi} \) be the splitting field of \( f(X) - \pi \) over \( F(\pi) \). We want to show that \( G_{F(\pi)} \) acts doubly transitively on \( X_{\pi} \), we will show \( \text{Gal}(F_{\pi}/F(\pi)) \) is isomorphic to the symmetric group \( S_{X_{\pi}} \).

We use the following criterion for recognizing the symmetric group:

**Lemma 2.2** (pg. 98 [Gal73], Lemma 4.4.3 [Ser92]). Let \( G \) be a transitive subgroup of \( S_n \). Assume \( G \) contains a transposition. If \( G \) either contains

(i) an \( (n-1) \)-cycle, or
(ii) a \( p \)-cycle for some prime \( p > n/2 \),

then \( G \) is the symmetric group \( S_n \) or the alternating group \( A_n \).
then $G = S_n$.

We show these conditions hold for $\mathrm{Gal}(F_\pi/F(\pi)) \leq S_{X_\pi}$. First, by Assumption 1 the automorphism $\sigma_0$ acts on the roots of $f^{\circ k}$ as an $n^k$-cycle. It follows $\sigma_0^{k-1}$ is an element of $G_{F(\pi)}$ which acts on $X_\pi$ as an $n$-cycle. Consequently, $\mathrm{Gal}(F_\pi/F(\pi))$ acts transitively on $X_\pi$.

Next, consider the element $\sigma := \sigma_{\infty, N}^{(n-a)^{k-1}-1}$. If $\pi_2$ is a root of $f^{\circ k-1}$ contained in $T$, then $\sigma$ fixes $\pi_1$ and cyclically permutes the $(n-a)$-vertices of $T$ which lie above $\pi_1$. It follows that the image of $\sigma$ in $\mathrm{Gal}(F_{\pi_1}/F(\pi_1))$ is either a $(n-1)$-cycle, or has an order divisible by a prime $p := n - a > n/2$. Taking a further power of $\sigma$ if necessary, we deduce that there is a root $\pi_1$ of $f^{\circ k}$ such that the image of the permutation representation of $\mathrm{Gal}(F_{\pi_1}/F(\pi_1))$ on $X_{\pi_1}$ contains either an $(n-1)$-cycle or a $p$-cycle for some prime $p > n/2$. By Hypothesis 1 there is some element $\tau \in \langle \sigma_0 \rangle$ which maps $\pi_1$ to $\pi$. Under such an element $\tau$, the set $X_{\pi_1}$ is mapped to $X_\pi$, and the actions of $\mathrm{Gal}(F_{\pi_1}/F(\pi'))$ and $\mathrm{Gal}(F_\pi/F(\pi))$ are intertwined. In particular, the cycle types occurring in $\mathrm{Gal}(F_{\pi_1}/F(\pi_1))$ are the same as $\mathrm{Gal}(F_\pi/F(\pi))$. By Lemma 2.2, we conclude $\mathrm{Gal}(F_\pi/F(\pi)) \cong S_{X_\pi}$. \hfill \Box

**Remark 2.3.** Hypothesis 2 of Lemma 2.1 can be replaced by the weaker assumption that $T_f$ is a regular, $n$-branching tree and $G_F$ acts transitively on the branches of $T_f$, i.e. that $f^{\circ k}$ is irreducible for all $k$. We have chosen to state Lemma 2.1 in this form, as it better indicates our strategy for the proof of the main theorem of Section 3.

### 3. Almost Surjective Representations

Fix an integer $n \geq 2$ and a field $E \subset \overline{Q}$ that is ramified outside of finitely many primes in $\mathbb{Z}$. In this section, we give explicit examples of polynomials of degree $n$ whose arboreal $G_E$-representation contains $\Gamma(1)$. In fact, many of our examples have surjective arboreal Galois representation.

Given a non-zero rational number $\alpha$, define $\alpha^+ \in \mathbb{Z}^+$ and $\alpha^- \in \mathbb{Z}$ to be the unique positive integer and integer, respectively, such that $(\alpha^+, \alpha^-) = 1$ and $\alpha = \frac{\alpha^+}{\alpha^-}$. Our main theorem in this section is:

**Theorem 3.1.** Let $E/\mathbb{Q}$ be an extension which is unramified outside finitely many primes of $\mathbb{Z}$. Choose $a < n$ to satisfy:

- (a.1) if $n \leq 6$, then $a = 1$,
- (a.2) if $n \equiv 7 \mod 8$, then $a = 1$,
- (a.3) otherwise, $n - a$ is a prime and $a < n/2$.

Assume $A \in \mathbb{Q}$ satisfies:

- (A.1) if $p$ is a prime which ramifies in $E$, then $p$-adic valuation $v_p(A) > 0$,
- (A.2) there is a prime $p_0$ which is unramified in $E$ and prime to $n$ such that $v_{p_0}(A) = 1$,
- (A.3) $A > 2^{\frac{n}{n-1}} \left(\frac{a}{n}\right)^{\frac{n}{n-1}} |\frac{a}{n} - 1|^{-\frac{n}{n-1}} > 1$,
- (A.4) $v_2(A) \geq \frac{3}{n-1} + \frac{n}{n-1} v_2(n)$,
- (A.5) $(A^+, n) = 2^v_2(n)$,
- (A.6) $(A^-, a(a - n)) = 1$,
- (A.7) there is a prime $p_{\infty} > n$ which is unramified in $E$ such that $v_{p_{\infty}}(A) = -1$, and
- (A.8) if $n$ is even, then $A^- \not\equiv \pm 1 \mod 8$,

then the polynomial

$$f(X) := X^a(X - A)^{n-a} + A$$
and all of its iterates are irreducible over $E$ and the image of the arboreal $G_E$-representation associated to $f$:

(1) contains $\Gamma(1)$ if $a = 1$ and $n > 2$, (i.e. $n$ satisfies $2 < n \leq 6$ or $n \equiv -7 \mod 8$), and (2) equals $\text{Aut}(T_f)$, otherwise.

It is clear that there infinitely many values of $A$ satisfying Hypotheses $\text{(A.1)}$ - $\text{(A.8)}$. The fact that there is a value of $a$ satisfying Hypotheses $\text{(a.1)}$ - $\text{(a.3)}$ is a consequence of Bertrand’s postulate.

The remainder of this section constitutes the proof of Theorem 3.1. Fix elements $a < n$ and $A \in \mathbb{Q}$ which satisfy the hypotheses of this theorem, and let $f(X) = X^n(X - A)^{n-a} + A$. Let $N = 1$ if $a = 1$ and $n > 2$; otherwise, let $N = 0$. As in Section 2 for each non-negative integer $k$, we denote the extension of $E$ generated by all roots of $f^{\circ k}$ by $E_k \subseteq \overline{\mathbb{Q}}$. Finally, for each prime $p \in \mathbb{Z}$, fix for once and for all an embedding $\iota_p : \overline{\mathbb{Q}} \hookrightarrow \mathbb{Q}_p$. The map $\iota_p$ induces an inclusion on Galois groups $G_{\mathbb{Q}_p} \hookrightarrow G_{\mathbb{Q}}$. Throughout the remainder of this note, we will regard $\overline{\mathbb{Q}}$ as a subfield of $\mathbb{Q}_p$, and $G_{\mathbb{Q}_p}$ as a subgroup of $G_{\mathbb{Q}}$ via these maps. We denote the maximal unramified extension of $\mathbb{Q}_p$ by $\mathbb{Q}_p^{un}$.

We will use Lemma 2.1 to show that the image of $G_E$ under $\rho_f : G_{\mathbb{Q}} \rightarrow \text{Aut}(T_f)$ contains $\Gamma(N)$. To do so, we will show that $G_E$ contains a set of elements $\{\sigma_k : k \in \mathbb{N} \cup \{\infty\}\}$ that satisfy the hypotheses of Lemma 2.1 where $\sigma_\infty$ denotes $\sigma_{\infty,N}$, an element satisfying Hypothesis 2. As described in the introduction, our strategy will be to find a set of prime integers $\{p_k : k \in \mathbb{N} \cup \{\infty\}\}$ that are unramified in $E$ and have the property that the inertia subgroup $I_{p_k} \leq G_{\mathbb{Q}_p} \leq G_E$ contains an element $\sigma_k$ satisfying the relevant hypothesis of Lemma 2.1. The primes $p_0$ and $p_\infty$ are those primes described in Theorem 3.1 that satisfy hypotheses $\text{(A.2)}$ and $\text{(A.7)}$, respectively. The local behavior of $\rho_f$ at these primes mimic the local behavior at 0 and \(\infty\) in the arboreal Galois representation attached to $f(X,t) = X^a(X - t)^{n-a} + t$ over $\mathbb{C}(t)$. In Lemmas 3.2 and 3.3, we show that when $k$ is 0 or $\infty$, the $I_{p_k}$-action on $T_f$ factors through its tame quotient, and a lift $\sigma_k$ of any generator of tame inertia satisfies the relevant hypothesis of Lemma 2.1. From Lemma 3.2, we will also deduce all iterates of $f$ are separable. The primes $p_k$ for $k$ a positive integer are found in Lemma 3.3. Every iterate of the polynomial $f$ has a critical point at $\frac{a}{n}A$. Therefore, $f^{\circ k}(\frac{a}{n}A)$ divides the discriminant of $f^{\circ k}$. Furthermore, $\frac{a}{n}A$ is a simple critical point of $f$. In Lemma 3.3 we find a prime $p_k$ that is prime to the numerator of $A$ (and hence by Assumption $\text{(A.1)}$ is unramified in $E$) and divides the numerator of $f^{\circ k}(\frac{a}{n}A)$ to odd order. Assumptions $\text{(A.3)}$ - $\text{(A.6)}$ and $\text{(A.8)}$ are made to guarantee that such a prime divisor occurs. In Lemma 3.6 we show the ring of integers of $E_k$ is simply branched over $\text{Spec}(\mathbb{Z})$ at $p_k$. At such primes $p_k$, the elements of the inertia group $I_{p_k}$ that act non-trivially on the roots $f^{\circ k}$ act as a transposition $\sigma_k$.

We begin by verifying that all iterates of $f$ are separable and that Hypothesis 1 of Lemma 2.1 holds for $f$. Let $p_0$ be a prime that satisfies Assumption $\text{(A.2)}$. We wish to show that all iterates of $f$ are separable, and that there is an element $\sigma_0 \in G_E$, which acts transitively on the branches of $T_f$. We will show that all iterates of $f$ are separable over $\mathbb{Q}_{p_0}$, and that there is an element $\sigma_0 \in I_{p_0}$ which acts transitively on the branches. This is immediate consequence of the following lemma:

**Lemma 3.2.** Let $a \in \mathbb{Z}_+$ and $A \in \mathbb{Q}$ satisfy the assumptions of Theorem 3.1. Let $p_0$ be a prime that witnesses Assumption $\text{(A.2)}$. For all positive integers $i$, the polynomial $f^{\circ i}$ is irreducible over $\mathbb{Q}_{p_0}^{un}$ and splits over a cyclic extension.
**Proof.** We show that $f^{o_i}$ is an Eisenstein polynomial over $\mathbb{Z}_{p_0}$. By Assumption (A.2), the polynomial $f$ has $p_0$-integral coefficients, and satisfies the congruence $f \equiv X^n \mod p_0$. Therefore, $f^{o_k} \in \mathbb{Z}_{p_0}[X]$ and satisfies the congruence $f^{o_k}(X) \equiv X^{kn} \mod p_0$. Noting that $f(0) = A$ and that $A$ is a fixed point of $f$, we conclude that $f^{o_i}(0) = A$, which is a uniformizer in $\mathbb{Z}_{p_0}$. Therefore, $f^{o_i} \in \mathbb{Z}_{p_0}[X]$ is an Eisenstein polynomial.

Since the degree $\deg(f^{o_i}) = n^i$ is prime to $p_0$, an Eisenstein polynomial of this degree is irreducible over $\mathbb{Q}^{un}_{p_0}$ and splits over the cyclic, tame extension of $\mathbb{Q}^{un}_{p_0}$ of ramification degree $n^i$. \hfill $\Box$

Our next task is to verify that Hypothesis 2 of Lemma 3.1 holds for $f$. Note that the conditions (a.1)-(a.3) of Theorem 3.1 are those on $a$ that appear in the statement of Lemma 3.1. Therefore, we must show that there is a regular $(n-a)$-branching subtree $T \subseteq T_f$ whose lowest vertex has height $N$, and an element $\sigma_\infty \in G_E$ which preserves $T$ and acts transitively on the branches of $T$. This claim is vacuously true if $n = 2$; in this case one can take $T$ to be any branch of $T_f$ and $\sigma_\infty$ to be the identity. We may therefore restrict our attention to the case that $n > 2$.

Let $p_\infty$ be a prime that witnesses Assumption (A.7) of Theorem 3.1. Since $p_\infty > n$, the pro-$p_\infty$-Sylow of $\text{Aut}(T_f)$ is trivial and the action of $I_{p_\infty}$ on $T_f$ factors through its pro-cyclic, tame quotient. By the unramifiedness condition in (A.7), we have $I_{p_\infty} \leq G_E$. To verify the Hypothesis 2 it thus suffices to show there is an $I_{p_\infty}$-stable, regular, $(n-a)$-branching tree $T$ whose lowest vertex has height $N$ such that $I_{p_\infty}$-acts transitively on the branches of $T$. In Lemma 3.3 we will find such a tree.

Before proving Lemma 3.3 we prove the following lemma, which explains the failure of our methods to produce surjective arboreal Galois representations in Theorem 3.1 under the assumption that $a = 1$. In Section 4 we will utilize this lemma to produce examples of surjective arboreal Galois representations when $n \equiv 7 \mod 8$ or $n$ is in the range $3 \leq n \leq 6$, i.e. in the cases that $a = 1$.

**Lemma 3.3.** Let $l$ be a prime integer which does not divide $n-1$. Assume that $B \in \mathbb{Q}_l$ satisfies $v_l(B) = -1$. Then the polynomial

$$g(X) := X(X-B)^{n-1} + B$$

splits completely over an unramified extension of $\mathbb{Q}_l$.

**Proof.** Consider the polynomial

$$S(X) := B^{-1}f(B + X) = B^{-1}X^n + X^{n-1} + 1 \in \mathbb{Z}_l[X]$$

The polynomial $S$ splits over a given field if and only if $g$ does. We show $S$ splits over an unramified extension of $\mathbb{Q}_l$. Consider the Newton polygon of $S$; it has one segment of slope 0 and length $n-1$, and one segment of length 1 and slope 1. It follows that $S$ has $n-1$ roots of valuation 0 and one root of valuation $-1$. The root of valuation $-1$ is necessarily $\mathbb{Q}_l$-rational. As for the roots of valuation 0, since

$$S(X) \equiv X^{n-1} + 1 \mod l$$

is separable, these roots have distinct images in the residue field. By Hensel’s lemma, we conclude $S$ splits over an unramified extension of $\mathbb{Q}_l$. \hfill $\Box$

**Lemma 3.4.** Assume $n > 2$. Let $a \in \mathbb{Z}_+$ and $A \in \mathbb{Q}$ satisfy the assumptions of Theorem 3.1. Let $p_\infty$ be a prime that witnesses Assumption (A.7). Then there is a subtree $T \subseteq T_f$ whose

...
lowest vertex has height $N$ which is $I_{p_{\infty}}$-stable, regular, and $(n - a)$-branching such that $I_{p_{\infty}}$ acts transitively on the branches of $T$.

Proof. Consider the subtree of $T_{f_{\infty}} \subseteq T_f$ consisting of 0 and the roots $r \in \overline{Q}_{p_{\infty}}$ of $f^{\circ i}$ such that the valuation $v_{p_{\infty}}(f^{\circ i}(r)) = -1$ for all non-negative integers $j < i$. Since the action of $G_{Q_{p_{\infty}}}$ on $\overline{Q}_{p_{\infty}}$ preserves the valuation, the tree $T_{f_{\infty}}$ is $G_{Q_{p_{\infty}}}$-stable.

We claim that $T_{f_{\infty}}$ is a regular, $(n - a)$-branching tree. To see this, observe that if $\epsilon$ is any element of $\overline{Q}_{p_{\infty}}$ of valuation less than or equal to $-1$. Then the Newton polygon of

$$f(X) - \epsilon = X^a(X - A)^{n-a} + (A - \epsilon) = (A - \epsilon) + \sum_{j=a}^{n-a} \binom{n-a}{n-j} A^{n-j} X^j$$

has two segments: one has length $n - a$ and slope $-v_{p_{\infty}}(A) = 1$, and the other has length $a$ and slope

$$\frac{v_{p_{\infty}}(A^{n-a}) - v_{p_{\infty}}(A - \epsilon)}{a} = \frac{a - n - v_{p_{\infty}}(A - \epsilon)}{a} \leq \frac{a - n + 1}{a} \leq \frac{n}{a},$$

which is less than 1. It follows that the pre-image of $\epsilon$ under $f$ contains exactly $n - a$ elements of valuation $-1$. Specializing to the pre-image tree of 0, we deduce that the tree $T_{f_{\infty}}$ is regular and $(n - a)$-branching.

When $a = 1$, by Lemma 3.3 the polynomial $f$ splits completely over an unramified extension of $Q_{p_{\infty}}$. In this case, choose $T$ to be any of the $(n - a)$ full subtrees of $T_{f_{\infty}}$ whose lowest vertex has height 1. The inertia group $I_{p_{\infty}}$ acts on $T$. If $a > 1$, let $T$ equal $T_{f_{\infty}}$. We claim that the inertia group $I_{p_{\infty}}$ acts transitively on the branches of $T$.

Let $r_k$ be a root of $f^{\circ k}$ contained in $T_{f_{\infty}}$. The ramification index of $Q_{p_{\infty}}(r_k)/Q_{p_{\infty}}$ is the size of the orbit of $r_k$ in $\overline{Q}_{p_{\infty}}$ under $I_{p_{\infty}}$. We wish to show that $I_{p_{\infty}}$ acts transitively on $T$. By induction on $k$, it suffices to show that $r_k$ orbit has size:

$$e_k := \begin{cases} (n - a)^k, & \text{if } a > 1, \\ (n - a)^{k-1}, & \text{if } a = 1. \end{cases}$$

(3.1)

We show $e(Q_{p_{\infty}}(r_k)/Q_{p_{\infty}}) = e_k$. Note that $e(Q_{p_{\infty}}(r_k)/Q_{p_{\infty}})$ is at most $e_k$ as the size of the orbit of $r_k$ under $I_{p_{\infty}}$ is at most the number of vertices in $T$ that have height $k$ in $T_{f_{\infty}}$. To conclude the of proof, it suffices to show that $e_k$ greater than or equal to $e(Q_{p_{\infty}}(r_k)/Q_{p_{\infty}})$.

We will show a root $r_k$ of $f^{\circ k}$ contained in $T_{f_{\infty}}$ satisfies:

$$v_{p_{\infty}}((r_k - A)) = 1 + \sum_{i=1}^{k} \frac{n-1}{(n-a)^i}.$$  

(3.2)  

For each integer $i$ in the range $0 \leq i \leq k$ define

$$r_i := f^{\circ k-i}(r_k) \text{ and } \epsilon_i := (r_i - A)/A.$$

Equation (3.2) is equivalent to the assertion that

$$v_{p_{\infty}}(\epsilon_0) = 0 \text{ and } v_{p_{\infty}}(\epsilon_i) = \frac{v_{p_{\infty}}(\epsilon_{i-1})}{n-a} + \frac{n-1}{n-a} \quad \text{if } i > 1.$$  

(3.3)
We verify (3.3). The case when \( i = 0 \) is clear, as \( \epsilon_0 = -1 \). Consider the case where \( i > 0 \). Then since \( A(1 + \epsilon_i) = r_i \), we see that \( \epsilon_i \) is a root of
\[
g_i(X) := f(A(1 + X)) - r_{i-1}
= A^n(1 + X)^a X^{a - n} + (A - r_{i-1})
= A^n(1 + X)^a X^{a - n} + \epsilon_{i-1} A.
\]

Examining the Newton polygon of \( g_i \), one sees that \( g_i \) has exactly \( a \) roots of valuation 0 and \( n - a \) roots of valuation
\[
-\frac{v_{p_{\infty}}(\epsilon_{i-1} A) - v_{p_{\infty}}(A^n)}{n - a} = \frac{v_{p_{\infty}}(\epsilon_{i-1})}{n - a} + \frac{n - 1}{n - a}.
\]

Since \( f - r_{i-1} \) has exactly \( n - a \) roots of valuation \(-1\), it must be the case that \( \epsilon_i \) is a root of \( g_i \) of valuation
\[
\frac{v_{p_{\infty}}(\epsilon_{i-1})}{n - a} + \frac{n - 1}{n - a} > 0.
\]

Hence, Equation (3.2) holds and \( e_k \geq e(\mathbb{Q}_{p_{\infty}}(r_k)/\mathbb{Q}_{p_{\infty}}) \). \( \square \)

We thus conclude that Hypothesis 2 of Lemma 2.1 holds for \( f \).

The final hypothesis of Lemma 2.1 is that for every positive integer \( k > N \) the permutation representation of \( \text{Gal}(E_k/E_{k-1}) \) acting on the roots of \( f^ok \) in \( E_k \) contains a transposition. It is shown to hold for \( f \) for all values of \( k \geq 0 \) by the following two lemmas. Recall our convention for writing a rational number as a fraction: for \( \alpha \in \mathbb{Q} \), we denote by \( \alpha^+ \in \mathbb{Z}_+ \) and \( \alpha^- \in \mathbb{Z} \) the unique positive integer and integer, respectively, such that \((\alpha^+, \alpha^-) = 1\) and \( \alpha = \frac{\alpha^+}{\alpha^-} \).

Note that \( \frac{a}{n} A \) is a critical point of \( f \), and therefore by the chain rule, a critical point of all iterates of \( f \). The next lemma, Lemma 3.5, shows that for every \( k > 0 \), there is a prime \( p_k \) (satisfying certain conditions), which does not divide \( A^+ \), so that \( \frac{a}{n} A \) is a root of \( f^{ok} \mod p_k \).

By assumption A.2 all primes which ramify in \( E \) divide \( A^+ \). Hence, \( p_k \) is unramified in \( E \). In Lemma 3.6 we will show that under the Hypotheses of Lemma 3.5 the inertia group \( I_{p_k} \) acts on the roots of \( f^{ok} \) as a transposition.

**Lemma 3.5.** Let \( a \in \mathbb{Z}_+ \) and \( A \in \mathbb{Q} \) satisfy the assumptions of theorem 3.1. For each positive integer \( k \), there exists a prime integer \( p_k \nmid nA^- A^+ \) so that the \( p_k \)-adic valuation of \( f^{ok}(\frac{a}{n} A) \) is positive and odd.

**Proof.** For each positive integer \( k \), let \( c_k \) denote \( \frac{f^{ok}(\frac{a}{n} A)}{A} \). To prove this lemma it suffices to show for all positive integers \( k \) that \( c_k^+ \) is relatively prime to \( nA^- A^+ \) and is not a perfect square. We will show the following. First, we show that \( c_k^+ \) and \( A^+ \) are relatively prime. Then, we show that \( c_k = c_k^+ c_k^- \) is a square in \( \mathbb{Z}_2^\times \). To finish the proof, we analyze the denominator \( c_k^- \). We show that if \( n_2 = n/2^{n(a(n))} \), then \( n_2 A^- | c_k^- \) and that \( c_k^- \) is not a square in \( \mathbb{Z}_2^\times \). Noting that \( 2 | A^+ \) by Hypothesis (A.4), these claims imply that \( nA^- A^+ \) and \( c_k^+ \) are relatively prime, and that \( c_k^+ \) is not a square.

Define \( c_0 = \frac{a}{n} \). Then for all \( k > 0 \),
\[
(3.4) \quad c_k = A^{n-1} c_{k-1}^a (c_{k-1} - 1)^{n-a} + 1.
\]
Let \( p \neq 2 \) be a prime integer factor of \( A^+ \). By Assumption (A.5), the prime \( p \) is not a factor of \( n \). Hence, \( c_0 \) is \( p \)-integral. Using Equation (3.4), one concludes by induction that \( c_k \) is \( p \)-integral and \( c_k \equiv 1 \mod p \).

Now consider the case where \( p = 2 \). By Hypothesis (A.4), the valuation \( v_2(A) \) satisfies
\[
v_2(A) \geq \frac{3}{n-1} + \frac{n}{n-1} v_2(n) > 0.
\]

Combining this with Equation (3.4), we observe \( c \equiv 1 \mod 8 \) and therefore is not a square in \( \mathbb{Z}^\times_2 \). Furthermore, recalling that the squares in \( \mathbb{Z}^\times_2 \) are relatively prime. Furthermore, recalling that the squares in \( \mathbb{Z}^\times_2 \) are exactly the elements congruent to 1 mod 8. We conclude that \( c_k \) and \( A^+ \) are relatively prime. Furthermore, recalling that the squares in \( \mathbb{Z}^\times_2 \) are exactly the elements congruent to 1 mod 8. We conclude that \( c_k \) is a square in \( \mathbb{Z}^\times_2 \).

Now, we examine \( c_k^- \). We’ve seen that \( c_k^- \) is prime to 2. Let \( n_2 := n/2^{v_2(n)} \). We will show by induction that
\[
(3.5)\quad c_k^- = (A^-)^{k-1}n_2^{n^k}(-1)^{(n-a)n^{k-1}}.
\]

This equation shows that \( c_k^- \) is prime to \( n_2A^- \). More subtly, Equation (3.5) shows \( c_k^- \equiv 1 \mod 8 \), and therefore is not a square in \( \mathbb{Z}^\times_2 \). To see this, observe that
\[
(A^-)^{n^k-1}n_2^{n^k}(-1)^{(n-a)n^{k-1}} \equiv \begin{cases} 
\pm A^- \mod 8 & \text{if } n \equiv 0 \mod 2 \\
(-1)^{n-a} \mod 8 & \text{if } n \equiv 1 \mod 8 \\
\pm n \mod 8 & \text{if } n \equiv 3, 5 \mod 8 \\
(n(-1)^{(n-a)} \mod 8 & \text{if } n \equiv 7 \mod 8.
\end{cases}
\]

Hence, to conclude the proof, it suffices to confirm Equation (3.5).

We will prove Equation (3.5) by induction on \( k \). We begin by showing the equation holds when \( k = 1 \). The element
\[
c_1 = A^{n-1} \left(\frac{a}{n}\right)^a \left(\frac{a}{n} - 1\right)^{n-a} + 1 = (-1)^{n-a} \frac{(A^+)^{n-1}a^a(n-a)^{n-a}}{(A^-)^{n-1}n^n} + 1.
\]

So a prime \( p \) divides \( c_1^- \) only if \( p | A^- \) or \( p | n_2 \). To deduce Equation (3.5) in this case, we must show that for all \( p | A^-n_2 \) the valuation:
\[
(3.6)\quad v_p(c_1^-) = v_p((A^-)^{n-1}n_2^n),
\]

and the sign
\[
(3.7)\quad \frac{c_1^-}{|c_1^-|} = (-1)^{n-a}.
\]
These equalities hold if and only if

\[(A^{-}n_2, A^{+}a(n - a)) = 1,\]

and

\[(A^{+})^{n-1}a^n(n - a)^{n-a} > 1,\]

respectively. We prove (3.8) and (3.9). By Assumption (A.6), if \(p\) divides \(n_2\), then \(p\) is prime to \(A^{+}\). Since \(a\) and \(n\) are relatively prime, a prime \(p\) dividing \(n_2\) does not divide \(a(n - a)\). Similarly, if \(p\) divides \(A^{-}\), then by definition \(p\) is prime to \(A^{+}\), and by Assumption (A.6), the prime \(p\) does not divide \(a(n - a)\). We conclude Equation (3.8) holds. To see (3.9), observe that

\[(A^{+})^{n-1}a^n(n - a)^{n-a} > 1,\]

by Assumption (A.3). We conclude Equation (3.8) holds when \(k = 1\).

Now assume that Equation (3.5) holds \(k \geq 1\), we show Equation (3.5) holds for \(k + 1\). Observe that

\[c_{k+1} = A^{n-1}c_k^a(c_k - 1)^{n-a} + 1 = \frac{(A^{+})^{n-1}(c_k^+)^a((c_k - 1)^+)^{n-a}}{(A^-)^{n-1}(c_k^-)^n} + 1.\]

Hence, a prime \(p\) divides \(c_{k+1}^{-}\) only if \(p|A^{-}c_k^-\). By induction, it follows that all prime divisors of \(c_{k+1}^{-}\) must divide \(A^{-}n_2\). Note that,

\[(A^-)^{n-1}(c_k^-)^n = (A^-)^{n-1}((A^-)^{n}n_2^{-1}n_2^{-1})^n = (A^-)^{n}n_2^{-1}n_2^{-1}.
\]

Hence, to show Equation (3.5), it is sufficient to show for all \(p|A^{-}n_2\) the valuation

\[v_p(c_{k+1}^-) = v_p((A^{-})^{n-1}(c_k^-)^n),\]

and that the sign

\[\frac{c_{k+1}^-}{|c_{k+1}^-|} = \left(\frac{c_k^-}{|c_k^-|}\right)^n.\]

These equations are implied by

\[(A^{-}n_2, A^{+}c_k^+(c_k - 1)^+ = 1,\]

and

\[\left|\frac{(A^{+})^{n-1}(c_k^+)^a((c_k - 1)^+)^{n-a}}{(A^-)^{n-1}(c_k^-)^n}\right| = |A^{n-1}c_k^a(c_k - 1)^{n-a}| = |c_k+1 - 1| > 2 > 1,\]

respectively.

We conclude the proof by demonstrating equations (3.13) and (3.14). Because \(n_2\) and \(A^{+}\) are relatively prime (by Assumption (A.5)), and \(A^{-}n_2\) divides \(c_k^-\) and \(A^{-}n_2\) divides \((c_k - 1)^-\) by induction, we conclude equality (3.13) holds. By Equation (3.10), we see that \(|c_k + 1| > 2\) when \(k = 1\). It follows by induction that

\[|c_{k+1} - 1| = |A^{n-1}c_k^a(c_k - 1)^{n-a}| > |A|^{n-1}||c_k|^a|(c_k - 1)^{n-a} > 2^{n-a}.
\]

Hence, Equation (3.14) holds. \(\square\)
By Lemma 3.3, the prime \( p_k \) does not divide \( A^+ \). Therefore by Assumption (A.2), this prime is unramified in \( E \). To finish the proof of Theorem 3.1 we show that some element of the inertia group \( I_{p_k} \subset G_E \) acts on the roots of \( f^{ok} \), as a transposition.

**Lemma 3.6.** Let \( a \in \mathbb{Z}_+ \) and \( A \in \mathbb{Q} \) satisfy the assumptions of theorem 3.1. Let \( p_k \) be a prime integer such that \( p_k \not| nA^+A^+ \) and the \( p_k \)-adic valuation of \( f^{ok}(\frac{a}{n}A) \) is positive and odd, then

1. there is a factorization of \( f^{ok}(X) \equiv g(X)b(X) \mod p_k \) as where \( g(X) \) and \( b(X) \) are coprime, \( g(X) \) is a separable, and \( b(X) = (X - \frac{aA}{n})^2 \), and
2. the inertia group \( I_{p_k} \subset G_{\mathbb{Q}_{p_k}} \subset G_E \) acts on the set of roots \( f^{ok} \) in \( \mathbb{Q}_{p_k} \) as a transposition.

**Proof of Claim 4.** We show that \( \frac{a}{n}A \) is the unique multiple root of \( f^{ok} \) and its multiplicity is 2.

We begin by showing \( \frac{a}{n}A \) is a multiple root of \( f^{ok} \). A polynomial over a field \( F \) has a multiple root at \( \alpha \in \overline{F} \) if and only if \( \alpha \) is both a root and a critical point. By assumption, the value \( \frac{a}{n}A \) is a root of \( f^{ok} \mod p_k \). To see \( \frac{a}{n}A \) is a multiple root, observe that

\[
(f^{ok})'(X) = f'(X) \prod_{0 < i < k} f'(f^{oi}(X))
\]

and

\[
f'(X) = aX^{a-1}(X - A) + (n - a)X^a(X - A)^{n-a-1} = X^{a-1}X^{n-a-1}(nX - aA),
\]

and therefore \( \frac{a}{n}A \) is a critical point of \( f^{ok} \).

Now assume \( c \) is a root of \( f^{ok} \mod p_k \) with multiplicity \( m > 1 \). Let \( \mathbb{Z}_{p_k}^{ok} \) be the ring of integers of \( \mathbb{Q}_{p_k} \) and \( \mathfrak{m} \) be its maximal ideal. Because \( f^{ok} \) is separable, there exists exactly \( m \) roots \( r_1, \ldots, r_m \in \mathbb{Z}_{p_k} \) of \( f^{ok} \) such that \( r_i \equiv c \mod \mathfrak{m} \). Let \( L(c) := \{r_1, \ldots, r_m\} \). To prove Claim 4 it suffices to show \( c \) equals \( \frac{a}{n}A \) and \( m = |L(c)| \) equals 2.

For each pair of pairs of distinct roots \( r \) and \( r' \) lifting \( c \), let \( l(r, r') \) be the smallest positive integer such that \( f^{oi}(r, r')(r') = f^{oi}(r, r') \). Considering \( r \) and \( r' \) as vertices of the tree \( T_f \), the value \( l(r, r') \) is the distance to the most common recent ancestor between \( r \) and \( r' \). Let

\[
N(c) := \max\{l(r, r') : r, r' \in L(c)\}.
\]

We claim that if \( N(c) \) equals 1, then \( c \) equals \( \frac{a}{n}A \) and \( m \) equals 2. To see why, assume \( N(c) \) equals 1. Then \( r_1, \ldots, r_m \) are all roots of the polynomial \( f(X) - f(r_1) \). Therefore, \( c \) is a critical point of \( f(X) \mod \mathfrak{m} \). From Equation (3.16), one observes that the critical points of \( f(X) \) are \( 0, A \) and \( \frac{a}{n}A \). By assumption \( f^{ok}(c) \equiv 0 \mod \mathfrak{m} \). On the other hand, since \( A \) is a fixed point of \( f \) and \( f(0) = A \),

\[
f^{ok}(0) = f^{ok}(A) = A \not\equiv 0 \mod \mathfrak{m}.
\]

Thus, \( c \) must equal \( \frac{a}{n}A \). The critical point \( \frac{a}{n}A \) has multiplicity 1. Therefore, \( m = L(c) = 2 \).

To finish the proof we must show \( N(c) = 1 \). Assume this is not the case, and let \( r \) and \( r' \) be a pair of lifts such that \( l := l(r, r') \geq 2 \). Then \( f^{oi-l}(r) \) and \( f^{oi-l}(r') \) are distinct root of the polynomial

\[
g_{r, r'}(X) := f(X) - f^{oi-l}(r) = f(X) - f^{oi-l}(r')
\]
which reduce to \( f^{ol-1}(c) \) modulo \( m \). It follows \( f^{ol-1}(c) \) is a root of \( g'_{r,r'}(X) = f'(X) \), and hence equals \( A \) or 0 or \( \frac{a}{n} A \). Since \( f^{ok}(c) \equiv 0 \mod p_k \) and
\[
f^{ok-l-1}(0) = f^{ok-l-1}(A) = A \not\equiv 0 \mod p_k,
\]
it must be the case that \( f^{ol-1}(c) \) equals \( \frac{a}{n} A \). But this implies, as 0 \( \equiv f^{ok}(\frac{a}{n} A) \mod p_k \) by assumption, that
\[
0 \equiv f^{ok}(\frac{a}{n} A) \mod p_k
\]
\[
\equiv f^{ok}(f^{ol-1}(c)) \mod p_k
\]
\[
\equiv f^{l-1}(f^{ok}(c)) \mod p_k
\]
\[
\equiv f^{l-1}(0) \mod p_k
\]
\[
\equiv A \mod p_k,
\]
a contradiction. □

**Proof of Claim 2.** The factorization \( b(x)g(x) = f(x) \), appearing in Claim 1, lifts by Hensel’s Lemma to a factorization
\[
B(X)G(X) = f(X)
\]
in \( \mathbb{Z}_{p_k}[X] \), where \( B(X) \) and \( G(X) \) are monic polynomials such that
\[
B \equiv b \mod p_k \text{ and } G \equiv g \mod p_k.
\]
As \( g \) is separable, \( G \) splits over an unramified extension of \( \mathbb{Q}_{p_k} \). To show \( I_p \) acts a transposition, we show the splitting field of \( B \) is a ramified quadratic extension of \( \mathbb{Q}_{p_k} \).

Consider the quadratic polynomial \( B(X + \frac{a}{n} A) = X^2 + B'(\frac{a}{n} A)X + B(\frac{a}{n} A) \). As
\[
B'(\frac{a}{n} A)G(\frac{a}{n} A) + B(\frac{a}{n} A)G'(\frac{a}{n} A) = f'(\frac{a}{n} A) = 0,
\]
and
\[
G(\frac{a}{n} A) \equiv g(\frac{a}{n} A) \not\equiv 0 \mod p_k,
\]
we observe \( v_{p_k}(B'(\frac{a}{n} A)) \geq v_{p_k}(B(\frac{a}{n} A)) \). It follows that the Newton polygon \( B(X + \frac{a}{n} A) \) has a single segment of slope \( \frac{v_{p_k}(B(\frac{a}{n} A))}{2} \) and width 2. As
\[
v_{p_k}(B(\frac{a}{n} A)) = v_{p_k}(f(\frac{a}{n} A)) - v_{p_k}(G(\frac{a}{n} A)) = v_{p_k}(f(\frac{a}{n} A))
\]
the slope is non-integral. We conclude \( B(X + \frac{a}{n} A) \) is irreducible and splits over a ramified (quadratic) extension. □

Having verified that the conditions of Lemma 2.1 hold for \( f \), we conclude that Theorem 3.1 is true.
4. Bridging the Gap

Having proven Theorem 3.1 we observe that our main theorem, Theorem 1.2, holds in polynomial degrees $n$ satisfying $n \not\equiv 7 \mod 8$ and $n \geq 6$, or $n = 2$. In this section, we prove that Theorem 1.2 holds in all remaining cases.

Assume that either $n \equiv 7 \mod 8$, or $n$ is in the range $3 \leq n \leq 6$. Define

$$f(X, t) := X(X - t)^{n-1} + t \in \mathbb{Q}[t, X].$$

By Theorem 3.1 there are infinitely many values of $A \in \mathbb{Q}$ such that the image of the arboreal Galois representation $\rho_{f(X, A)} : G_E \to \text{Aut}(T_{f(X, A)})$ associated to the specialization $f(X, A) = X(X - A)^{n-1} + A \in \mathbb{Q}[X]$ contains $\Gamma(1)$. To prove Theorem 1.2, we will use the Hilbert Irreducibility Theorem to show that for some infinite subset of these values the splitting field of the specialization $f(X, A)$ over $E$ is an $S_n$-extension. For our first step, we calculate the geometric Galois group of the 1-parameter family $f(X, t)$.

Lemma 4.1. Let $F$ be a field of characteristic 0. The splitting field of the polynomial $f(X, t)$ over $F(t)$ is an $S_n$-extension.

Proof. Without loss of generality, we may assume $F$ is the complex numbers $\mathbb{C}$. Let

$$g(X, t) = f(X - t, -t) = X^n - tX^{n-1} - t.$$

It suffices to show that the splitting field of $g(X, t)$ over $\mathbb{C}(t)$ is an $S_n$-extension. Let $\pi : C_0 \to \mathbb{P}^1$ be the étale morphism whose fiber above a point $t_0 \in \mathbb{C}$ is the set of isomorphisms

$$\phi_t : \{0, \ldots, n-1\} \sim \{r \in \mathbb{C} : g(r, t_0) = 0\}.$$

Let $C$ be a smooth, proper curve containing $C_0$, and let $\pi : C \to \mathbb{P}^1$ be the map extending $\pi : C_0 \to \mathbb{P}^1$. The splitting field of $g$ is an $S_n$-extension if and only if $C$ is connected. We show the latter.

We will analyze the monodromy around the branch points of $\pi : C \to \mathbb{P}^1$. The cover $C$ is ramified above the roots of

$$\Delta g(X, t) = n^n \prod_{c \in \mathbb{C}(t), \frac{\partial g}{\partial t}(c, t) = 0} g(c, t)^{m_c}$$

$$= n^n g(0, t)^{n-2} g\left(\frac{n-1}{n}, t\right)$$

$$= n^n (-t)^{n-2} \left(\left(-\frac{1}{n}t\right)\left(\frac{n-1}{n}t\right)^{n-1} - t\right)$$

$$= n^n (-t)^{n-1} \left(\frac{1}{n}\left(\frac{n-1}{n}t\right)^{n-1} + 1\right)$$

where $m_c$ is the multiplicity of the critical point $c$. Hence, $\pi : C \to \mathbb{P}^1$ is branched at 0 and

$$\alpha_k := Me\left(\frac{2k+1}{n-1}\right),$$

where $k \in \{0, \ldots, n-2\}$ and $M$ is a positive real number which is independent of $k$. Each of the branch points $\alpha_k$ is simple. One may check (though it is not relevant to our proof)
that $\pi : C \to \mathbb{P}^1$ is unramified at $\infty$; for a proof, see Lemma 3.3. We let $D := \{0, \alpha_0, \ldots, \alpha_{n-2}\}$ denote the branch locus.

Since $g(X, t) = X^n - tX^{n-1} - t$ is $t$-Eisenstein, it splits over $\mathbb{C}[[t^{1/n}]]$. Observing that

$$t^{-1}g(Xt^{1/n}, t) \equiv X^n - 1 \mod t^{1/n},$$

it follows that each of the roots $r$ of $g$ in $\mathbb{C}[[t^{1/n}]]$ satisfy

$$r = e^{2\pi ik/n}t^{1/n} \mod t^{2/n}$$

for some unique value of $k \in \{0, \ldots, n-1\}$. Let $pt_{\alpha_0 \to 0}$ be the set $(0, |\alpha_0|)\alpha_0 \in \mathbb{C}$, i.e. the image of the straight line path from 0 to $\alpha_0$. Let $s : pt_{\alpha_0 \to 0} \to C$ be the unique holomorphic section of $\pi : C \to \mathbb{P}^1$ such that

$$\lim_{t \to 0^+} \frac{s(t)(k)}{|s(t)(k)|} = e^{\frac{2\pi ik}{n}} e^{\frac{\pi}{n(n-1)}}.$$

We consider the monodromy representation $\varphi : \pi_1(\mathbb{P}^1 \setminus D, pt_{\alpha_0 \to 0}) \to S_n$ which maps a path $p$ in $\mathbb{P}^1 \setminus D$ with endpoints in $pt_{\alpha_0 \to 0}$ to $\hat{p}(1)^{-1} \circ \hat{p}(0)$ where $\hat{p}$ is the unique lift of $p$ satisfying $\hat{p}(0) = s(p(0))$. To show $C$ is connected, it suffices to show $\varphi$ is surjective. Our strategy will be to show that the generators of the symmetric group $(0 \ 1 \ 2 \ldots n-1)$ and $(0 \ 1)$ are contained in the image of $\varphi$.

Consider a counterclockwise circular path $p_0$ around 0 with endpoints in $pt_{\alpha_0 \to 0}$. Since 0 is the only branch point contained in the circle bounded by $p_0$, the image of $p_0$ under $\varphi$ is the cycle $(0 \ 1 \ 2 \ldots n-1)$. Let $p_1$ be a path with endpoint in $pt_{\alpha_0 \to 0}$ which bounds a punctured disk in $\mathbb{P}^1 \setminus D$ around $\alpha_0$. Since the branch point $\alpha_0$ is simple, the image of $p_1$ under $\varphi$ is a transposition. We claim $\varphi(p_1) = (0 \ 1)$.

Let $S$ be the set of complex numbers $z$ which satisfies

$$\frac{\pi}{n(n-1)} \leq \text{Arg}(z) \leq \frac{2\pi}{n} + \frac{\pi}{n(n-1)}.$$ 

Note that $\alpha_0 \in S$. Furthermore, observe the boundary rays of $S$ are the two tangent directions by which the 0-th and 1-st root of $g(X, t_0)$ (in the labeling given by the section $s$) converge to 0. To show $\varphi(p_1) = (0 \ 1)$, we will demonstrate that

$$(\ast) \text{ for all } t_0 \in pt_{\alpha_0 \to 0} \text{ there exists a unique pair of roots of } g(X, t_0) \text{ contained in } S.$$

From $(\ast)$, one concludes by uniqueness $\varphi(p_1) = (0 \ 1)$.

Since $\alpha_0$ is a simple branch point contained in $S$, when $t_0$ is sufficiently close to $\alpha_0$ there are at least two roots in $S$. On the other hand, as $t_0$ approaches 0, there is a unique pair of roots whose tangent directions are contained in $S$. Hence for $t_0$ sufficiently close to 0, there are at most two roots contained in $S$. To prove $(\ast)$ for all $t_0 \in pt_{\alpha_0 \to 0}$, we will show that there is no value $t_0 \in pt_{\alpha_0 \to 0}$ such that $g(X, t_0)$ has a root $r$ whose argument equals $\frac{\pi}{n(n-1)}$ or $\frac{2\pi}{n} + \frac{\pi}{n(n-1)}$, i.e. roots cannot leave or enter the sector $S$ as one varies $t_0$ along $pt_{\alpha_0 \to 0}$.

Assume for the sake of contradiction that there is a value $t_0 \in pt_{\alpha_0 \to 0}$ and a root $r$ of $g(X, t_0)$ such that $\text{Arg}(r) = \frac{\pi}{n(n-1)}$ or $\text{Arg}(r) = \frac{\pi}{n(n-1)} + \frac{2\pi}{n}$. Then since $g(r, t_0) = 0$, one observes that $r^n = t_0(r^{n-1} + 1)$. 
And so,
\[
\frac{\pi}{n-1} \equiv \text{Arg}(r^n) \mod 2\pi \\
\equiv \text{Arg}(t_0) + \text{Arg}(r^{n-1} + 1) \mod 2\pi \\
\equiv \frac{\pi}{n-1} + \text{Arg}(r^{n-1} + 1) \mod 2\pi.
\]

From which it follows \(\text{Arg}(r^{n-1} + 1) \equiv 0 \mod 2\pi\). Note however,
\[
\text{Arg}(r^{n-1}) \equiv \begin{cases} 
\frac{\pi}{n} \mod 2\pi & \text{if } \text{Arg}(r) = \frac{\pi}{n(n-1)}, \\
2\pi - \frac{\pi}{n} \mod 2\pi, & \text{if } \text{Arg}(r) = \frac{\pi}{n(n-1)}.
\end{cases}
\]

Therefore, \(r^{n-1}\) is not a real number. It follows \(r^{n-1} + 1\) is not real, and therefore has non-zero argument, a contradiction. We conclude that there is no value \(t_0 \in \mathbb{P}_\alpha \to 0\) such that \(g(X, t_0)\) has a root with argument \(\frac{\pi}{n(n-1)}\) or \(\frac{\pi}{n(n-1)} + \frac{2\pi}{n}\). Therefore, \(\varphi(p_1) = (0 1)\) and \(C\) is connected.

We deduce our main theorem, Theorem 1.2, via a Hilbert irreducibility argument.

Proof of Theorem 1.2. If \(n \not\equiv 7 \mod 8\) or in the range \(3 \leq n \leq 6\), then the theorem is a consequence of Theorem 3.1.

Assume that \(n \equiv 7 \mod 8\) or \(3 \leq n \leq 6\). Without loss of generality, we may assume \(E\) is a Galois extension of \(\mathbb{Q}\). Let \(D\) be the unique positive, square-free integer which is divisible by the primes which ramify in \(E\) and those that divide \(n(n-1)\). In particular, note that \(2\) divides \(D\). Let \(B = D/(D,n-1)\). Consider the polynomial
\[
h(X, t) = f(X, B^{-1}(1 + Dt)) \in \mathbb{Q}[t, X].
\]

By Lemma 4.1, the polynomial \(h(X, t)\) has Galois group \(S_n\) over \(\mathbb{Q}(B^{-1}(1 + Dt)) = \mathbb{Q}(t)\). Therefore by the Hilbert Irreducibility Theorem, there exists infinitely many values \(t_0 \in \mathbb{Z}\) such that the splitting field \(K_{t_0}\) of \(h(X, t_0) = f(X, B^{-1}(1 + Dt_0))\) is an \(S_n\)-extension of \(\mathbb{Q}\). Fix such a value \(t_0\). We claim that there is a finite set \(L\) of prime integers which satisfy the following two conditions.

1. If \(l \in L\), then \(l \nmid D\).
2. The closed, normal subgroup \(S_L \leq G_{\mathbb{Q}}\) generated by the inertia groups \(I_l\) for \(l \in L\) acts on the roots \(f(X, B^{-1}(1 + Dt_0))\) as the full symmetric group \(S_n\).

Since there are no everywhere unramified extensions of \(\mathbb{Q}\), the set of primes which ramify in \(K_{t_0}\) satisfy Condition 2. We show this set satisfies Condition 1, i.e. that \(K_{t_0}\) is unramified at all primes dividing \(D\).

Recall that \(D = B(D,n-1)\). If \(l\) divides \(B\), then \(l\) is prime to \(n-1\) and the valuation \(v_l(B^{-1}(1 + Dt_0)) = -1\). It follows by Lemma 3.3 that the extension \(L_{t_0}\) is unramified at \(l\). On the other hand, if \(l\) divides \(n-1\), then \(f(X, B^{-1}(1 + Dt_0))\) has \(l\)-integral coefficients.

\footnote{the subgroup \(S_L\) is simply the absolute Galois group of the maximal extension of \(\mathbb{Q}\) in which all primes in \(L\) are unramified.}
then
\[ \Delta(f(X, B^{-1}(1 + Dt_0))) = n^n \prod_{c \in \mathbb{Q} : h'(c, t_0) = 0} f(c, B^{-1}(1 + Dt_0))^{m_c} \]
\[= n^n(B^{-1}(1 + Dt_0))^{n-1} \left((B^{-1}(1 + Dt_0))^{n-1} \left(\frac{1}{n} - 1\right) + 1 \right) \equiv B^{1-n} \mod l, \]
is prime to \( l \). Hence, \( K_{t_0} \) is unramified at \( l \). We conclude that \( K_{t_0} \) is unramified at all primes dividing \( D \).

To conclude the proof of the Theorem, we perturb \( B^{-1}(1 + Dt_0) \) in \( \prod_{l \in L} \mathbb{Q}_l \) to produce values of \( A \) for which \( f(X, A) \) has a surjective arboreal \( G_E \)-representation. Let \( X_0 \) denote the set of roots of \( f(X, B^{-1}(1+Dt_0)) \) over \( \mathbb{Q} \). Note that since the splitting field of \( f(X, B^{-1}(1+Dt_0)) \) over \( \mathbb{Q} \) is \( S_n \)-extension, the polynomial \( f(X, B^{-1}(1+Dt_0)) \) is separable over \( \mathbb{Q}_l \). Let
\[ \delta_l := \min\{|r_1 - r_2| : f(r_1, B^{-1}(1 + Dt_0)) = f(r_2, B^{-1}(1 + Dt_0)) = 0 \text{ and } r_1 \neq r_2 \} \]
be the minimum distance between a distinct pair of roots. By Krasner’s Lemma, there exists an open ball \( U_l \subseteq \mathbb{Q}_l \) centered at \( B^{-1}(1 + Dt_0) \) such that if \( A_l \in U_l \) and \( r \) is a root of \( f(X, B^{-1}(1 + Dt_0)) \), then there is a unique root \( r(A_l) \) of \( f(X, A_l) \) such that \(|r - r(A_l)|_l < \delta_l \).

Since the action of \( I_l \) on \( \mathbb{Q}_l \) preserves distances, the map \( r \mapsto r(A_l) \) is \( G_{\mathbb{Q}_l} \)-equivariant. Identifying the set of roots of \( f(X, A_l) \) and \( f(X, B^{-1}(1 + Dt_0)) \) via this map, we see that for all \( A_l \in U_l \) the image of \( I_l \) in the symmetric group \( S_{X_0} \) is locally constant.

The group \( S_L \) is the normal closure of the group generated by the subgroups \( I_l \) for \( l \in L \). Let \( U_L := \prod_{l \in L} U_l \). Since the action of \( S_L \) on \( X_0 \) surjects onto \( S_{X_0} \), for all \( A \in U_L \cap \mathbb{Q} \) the permutation representation of \( S_L \) on the roots of \( f(X, A) \) is surjective. Since \( E \) is Galois and unramified at the primes in \( L \), the group \( G_E \leq G_{\mathbb{Q}} \) is normal and contains \( S_L \). It follows that for any \( A \in U_L \cap \mathbb{Q} \) the splitting field of \( f(X, A) \) over \( E \) is an \( S_n \)-extension.

We conclude the proof by showing that there are infinitely many values \( A \in U_L \cap \mathbb{Q} \) such that the arboreal Galois representation attached to \( f_{1,A}(X) := f(X, A) \) contains \( \Gamma(1) \). By Theorem 4.1, it suffices show that there are infinitely many \( A \in U_L \cap \mathbb{Q} \) satisfying Hypotheses (A.1) - (A.8). Let \( p_0 \) and \( p_\infty \) be any choice of distinct primes which are greater than \( n \), unramified in \( E \), and not contained in \( L \). Then Hypotheses (A.1) - (A.7) are open local conditions on \( A \) at the finite set of places dividing \( Dp_0p_\infty \) and \( \infty \). In particular, they are conditions at places distinct from those in \( L \). Let \( U_{\Gamma(1)} \) denote the open subset of \( \mathbb{R} \times \prod_{p|Dp_0p_\infty} \mathbb{Q}_p \) consisting of values which satisfy Hypotheses (A.1) - (A.7) locally. Let \( S \) denote the set of places
\[ S := \{ | \cdot |_p : p \subseteq L, \text{ or } p = \infty, \text{ or } p|Dp_0p_\infty \}. \]
By weak approximation there are infinitely many values \( A_0 \in (U_{\Gamma(1)} \times U_L) \cap \mathbb{Q} \). Fix any such value. Since \( U_{\Gamma(1)} \times U_L \) is open, there exists a real number \( \epsilon > 0 \) such that if \( |1 - w|_p < \epsilon \) at all places in \( S \), then \( wa_0 \in U_{\Gamma(1)} \times U_L \). Fix such an \( \epsilon > 0 \). Let \( M \) be a positive integer such that \( |M|_p < \epsilon \) at all \( \text{finite} \) places \( | \cdot |_p \in S \). If \( x \) is any positive integer which is
(1) not divisible by the primes contained in \( S \), and
(2) sufficiently large: specifically \( M/x < \epsilon \),
then \( A_x := \frac{x-1}{M} A_0 \in U_{\Gamma(1)} \times U_L \), and therefore satisfies hypotheses (A.1) - (A.7). For such a value \( x \in \mathbb{Z}_+ \), if one additionally asks that
(3) \( (x, A_0^+) = 1 \) and \( x \equiv \pm(A_0^-)^{-1} \mod 8 \),
then $A_x \equiv A_0 x \not\equiv \pm 1 \mod 8$, and hence $A_x$ satisfies hypothesis (A.8). There are infinitely many $x \in \mathbb{Z}_+$ satisfying conditions 1, 2, and 3. For every such value, the arboreal $G_E$-representation associated to $f(X, A_x)$ is surjective.

Acknowledgements

The author would like to thank Nicole Looper for explaining her arguments in [Loo16], the University of Chicago for its hospitality, and Mathilde Gerbelli-Gauthier for reading a preliminary draft of this work.

References

[BJ18] Robert Benedetto and Jamie Juul, Odoni’s conjecture for number fields, arXiv e-prints arXiv:1803.01987 (2018).

[Gal73] Patrick X Gallagher, The large sieve and probabilistic galois theory, Proc. Sympos. Pure Math, vol. 24, 1973, pp. 91–101.

[Jon08] Rafe Jones, The density of prime divisors in the arithmetic dynamics of quadratic polynomials, Journal of the London Mathematical Society 78 (2008), no. 2, 523–544.

[Juu14] Jamie Juul, Iterates of generic polynomials and generic rational functions, arXiv preprint arXiv:1410.3814 (2014).

[Kad18] Borys Kadets, Large arboreal Galois representations, ArXiv e-prints arXiv:1802.09074 (2018).

[Loo16] Nicole R Looper, Dynamical galois groups of trinomials and Odoni’s conjecture, arXiv preprint arXiv:1609.03398 (2016).

[Odo85a] RWK Odoni, The galois theory of iterates and composites of polynomials, Proceedings of the London Mathematical Society 3 (1985), no. 3, 385–414.

[Odo85b] , On the prime divisors of the sequence $w_{n+1} = 1 + w_1 \ldots w_n$, Journal of the London Mathematical Society 2 (1985), no. 1, 1–11.

[Ser92] Jean-Pierre Serre, Topics in Galois theory, Jones and Bartlett Publishers, Boston, MA, 1992.