A local-global conjugacy question arising from arithmetic dynamics

Vefa Goksel

Abstract. In his earlier work, the author introduced a group theory question that arises in the study of iterated Galois groups of post-critically finite quadratic polynomials. In this paper, we prove the first non-trivial results on this question.

1. Introduction

Let K be a field, and $f \in K[x]$ a quadratic polynomial. We define the n-th iterate of f inductively by setting $f^n(x) = f(f^{n-1}(x))$ for $n \geq 1$, where we make the convention that $f^0(x) = x$. Suppose that all iterates of f are separable over K. Then f^n-pre-images of 0 form a complete binary rooted tree as follows: For each root of α of f^{n-1}, we draw edges from α to two roots β_1, β_2 of f^n, where $f(\beta_1) = f(\beta_2) = \alpha$. We will denote this *pre-image tree* of f by T. We also let T_n be the subtree of the first n levels of T. The absolute Galois group naturally acts on T, which gives a continuous homomorphism

$$\rho \colon \mathrm{Gal}(K^{\mathrm{sep}}/K) \to \mathrm{Aut}(T).$$

This action on the binary rooted tree is the dynamical analog of the Galois action on the ℓ-power torsion points on an elliptic curve. For this reason, ρ is called an *arboreal Galois representation*, which is a terminology introduced by Boston and Jones in 2007 [4].

If we let $G_n(f)$ be the Galois group of f^n over K, these Galois groups give an inverse system via the natural surjections $G_{n+1}(f) \twoheadrightarrow G_n(f)$. Letting $G(f) := \varprojlim G_n(f)$, we have $\mathrm{im}(\rho) = G(f)$. The question of describing this image as a subgroup of $\mathrm{Aut}(T)$ is one major open question in arithmetic dynamics. There has been a lot of recent work on this topic, see, for instance, [1, 3–6, 8–19, 22–26] for a limited list. Based on the existent results, it is believed that $G(f)$ should have finite index in $\mathrm{Aut}(T)$ for most quadratic polynomials f. See [18, Conjecture 3.11] for a precise conjecture in this direction. However, similar to the fact that elliptic curves with complex multiplication are excluded in Serre's celebrated open image theorem, there are some well-known exceptional families

of f for which $G(f)$ has infinite index in $\mathrm{Aut}(T)$. One such exceptional case is when f is *post-critically finite* (see below for a definition).

A polynomial f is called *post-critically finite* (or PCF in short) if all its critical points have finite orbits under iteration by f. The exact description of the profinite group $G(f)$ as a subgroup of $\mathrm{Aut}(T)$ when f is PCF is still mysterious in general, and partial results are known only in some special cases. See, for instance, [1,2,4,5] on this topic. In [10], for certain PCF quadratic polynomials f, the author used a Markov model to construct special profinite subgroups $M(f)$ of $\mathrm{Aut}(T)$ which conjecturally contain $G(f)$. If this containment can be established, the author believes that the groups $M(f)$ can be a good candidate for a dynamical analog of Mumford–Tate groups in the classical theory of Galois representations for elliptic curves. The author gave some evidence indicating that a positive answer to certain special cases of a purely group theoretic question will imply this containment. In this paper, we will prove the first non-trivial results on this question.

Before we introduce the aforementioned group theory question, we first briefly give some notation and definitions: The groups $\mathrm{Aut}(T_n)$ form an inverse system via the natural surjections $\pi_n \colon \mathrm{Aut}(T_n) \twoheadrightarrow \mathrm{Aut}(T_{n-1})$. We set $K_n = \mathrm{Ker}(\pi_n)$. It is well known that K_n is an elementary abelian 2-group with rank 2^{n-1}, i.e., we have $K_n \cong (\mathbb{Z}/2\mathbb{Z})^{2^{n-1}}$.

Definition 1.1. Let $H, G \leq \mathrm{Aut}(T_n)$ be two subgroups of $\mathrm{Aut}(T_n)$. We say that H *is elementwise K_n-conjugate into G* if each element of H can be conjugated into G by an element of K_n. We say that H *is globally K_n-conjugate into G* if H can be conjugated into G by an element of K_n.

Definition 1.2. Let $H, G \leq \mathrm{Aut}(T_n)$ be two subgroups of $\mathrm{Aut}(T_n)$. We say that $\mathcal{P}(H, G)$ *holds* if we have

$$H \text{ is elementwise } K_n\text{-conjugate into } G \iff H \text{ is globally } K_n\text{-conjugate into } G.$$

Definition 1.2 naturally raises the question that we will study.

Question 1.3. Let $n \geq 1$. For which subgroups $H, G \leq \mathrm{Aut}(T_n)$ does $\mathcal{P}(H, G)$ hold?

Question 1.3 seems difficult in general. It would also be perhaps interesting to note that similar questions in the context of Lie groups already exist in the literature, which also have applications to number theory, particularly to Langland's global functoriality conjecture. See, for instance, [7, 20, 21, 27–29]. Specifically, compare the question in [7, p. 99] with Question 1.3.

Note that $\mathcal{P}(H, G)$ trivially holds when H is a cyclic subgroup of $\mathrm{Aut}(T_n)$. We now state the first non-trivial result regarding Question 1.3.

Theorem 1.4. *Let $n \geq 1$ and $H, G \leq \mathrm{Aut}(T_n)$. Suppose that $|H| = |G|$ and $H \cap K_n = \{\mathrm{id}\}$. Then $\mathcal{P}(H, G)$ holds.*

The proof of Theorem 1.4 requires one to use the iterated wreath product structure of $\mathrm{Aut}(T_n)$.

The structure of the paper will be as follows. In Section 2, we will give some background and motivation for Question 1.3. In Section 3, we will present some preliminaries from group theory. In Section 4, we will prove some auxiliary lemmas that will be crucial in the proof of Theorem 1.4. We will prove Theorem 1.4 in Section 5. We will finish the paper by stating a conjecture in Section 6.

2. Background and motivation

Let $f \in \mathbb{Z}[x]$ be a monic PCF quadratic polynomial. It is well known (and easy to prove) that all such polynomials are conjugates of x^2, $x^2 - 1$ or $x^2 - 2$ by the linear map $x \to x + a$ for $a \in \mathbb{Z}$. Let $G_n(f)$ denote the Galois group of the n-th iterate of $\mathbb{Q}(i)$, where we choose the base field as $\mathbb{Q}(i)$ for a technical reason, as explained in [10, Section 2]. In [10], the author used the factorization data of iterates of f over finite fields together with a Markov process to construct the *Markov groups* $M_n(f)$, and conjectured that $G_n(f)$ is contained in $M_n(f)$ for $n \geq 1$. Moreover, the author made a connection between Question 1.3 and this conjecture. Namely, the author gave an argument indicating that $G_n(f)$ is elementwise K_n-conjugate into $M_n(f)$ for all n. If this is true, then establishing that $\mathcal{P}(G_n(f), M_n(f))$ holds for all n will prove the conjecture above. Note that groups $M_n(f)$ are explicitly known, so this is a quite special case of Question 1.3.

To give an example of groups $M_n(f)$, let $f := (x + a)^2 - a - 1$ for some $a \in \mathbb{Z}$. This family is particularly interesting because it does not come from endomorphisms of algebraic groups. Recall that for $n \geq 1$, the permutations $a_1 = (1, 2)$, $a_2 = (1, 3)(2, 4)$, $\ldots, a_n = (1, 2^{n-1} + 1)(2, 2^{n-1} + 2) \cdots (2^{n-1}, 2^n)$ are the standard generators of $\mathrm{Aut}(T_n)$. Then, $x_n := a_1 a_2 \cdots a_n \in \mathrm{Aut}(T_n)$ acts transitively on the n-th level of the tree [10, Lemma 3.3]. One can also think of x_i for $i < n$ as an element of $\mathrm{Aut}(T_n)$, by using the natural inclusion $\mathrm{Aut}(T_i) \hookrightarrow \mathrm{Aut}(T_n)$. Finally, define $m_1 := \mathrm{id} \in \mathrm{Aut}(T_1)$, and $m_{n+1} := x_n^2 m_n x_n^{-1}$ for $n \geq 1$. Then, if $a \neq \pm b^2$ for any $b \in \mathbb{Z}$, we have $M_1(f) = \langle (1, 2) \rangle$, $M_2(f) = \langle (1, 3, 2, 4), (1, 2) \rangle$, and $M_n(f)$ is given by

$$M_n(f) = \langle x_n, m_n, x_{n-1}^2, x_{n-2}^2, \ldots, x_2^2 \rangle \tag{1}$$

for $n \geq 3$. If $a = \pm b^2$ for some $b \in \mathbb{Z}$, then $M_n(f)$ is an explicit index-2 subgroup of the group given in (1) (see [10, Corollary 6.28]). For $n \geq 1$, the author constructed the groups $M_n(f)$ inductively, by introducing the so-called *Markov map*, which can be applied to above generators of $M_n(f)$ to obtain generators of $M_{n+1}(f)$. See [10, Section 6] for more details.

It also follows from the work of the author in [10] that the parameters a used above can be taken in $\mathbb{Q}$, and the main results of [10] will still hold. The author conjectures that the groups $M_n(f)$, the so-called *Markov groups*, exist for *any* PCF quadratic polynomial over any number field, and that $G_n(f)$ is always contained in $M_n(f)$ for every n. This conjecture is based on extensive MAGMA computations combined with the theoretic evidence given in [10], and is an ongoing project of the author. The author believes that there

is potentially a rich theory behind these Markov groups, which may eventually lead to a dynamical analog of Mumford–Tate groups, as alluded to in the previous section.

3. Preliminaries

In this section, we will recall some standard facts from group theory that will be necessary in the proof of Theorem 1.4. We set $W_n = \text{Aut}(T_n)$ for simplicity, which is the notation that we will be using throughout the paper. It is well known that W_n is isomorphic to the n-fold wreath product of C_2 (the cyclic group of order 2), which can be inductively given by $W_1 \cong C_2$ and $W_n \cong W_{n-1} \wr C_2$ for $n \geq 2$. By definition, this allows us to identify W_n with the semi-direct product $\mathbb{F}_2^{2^{n-1}} \rtimes W_{n-1}$, where $\mathbb{F}_2^{2^{n-1}}$ stands for the 2^{n-1}-dimensional vector space defined over $\mathbb{F}_2$, the finite field with 2 elements. In this semi-direct product, W_{n-1} acts on $\mathbb{F}_2^{2^{n-1}}$ simply by permuting the coordinates. Concretely, for $v = (v_1, \ldots, v_{2^{n-1}}) \in \mathbb{F}_2^{2^{n-1}}$ and $\sigma \in W_{n-1}$, we have

$$\sigma(v) = (v_{\sigma^{-1}(1)}, \ldots, v_{\sigma^{-1}(2^{n-1})}).$$

Hence, throughout the article, we will think of the elements of W_n as pairs (v, s), $v \in \mathbb{F}_2^{2^{n-1}}$, $s \in W_{n-1}$. With this notation, if $\sigma_1 = (v, s), \sigma_2 = (w, t) \in W_n$ are two elements in W_n, their product is given by

$$\sigma_1 \sigma_2 = (v + s(w), st). \tag{2}$$

If $G := \{g_1, \ldots, g_k\} \leq W_n$, where $g_i = (v_i, s_i)$ for $i = 1, \ldots, k$, we will also often use the identification

$$\pi_n(G) = \{s_1, \ldots, s_k\} \leq W_{n-1}. \tag{3}$$

By the iterated wreath product definition of W_n, it immediately follows that each W_n is a 2-group for all $n \geq 1$, thus are all its subgroups. In fact, it is well known that W_n is isomorphic to the Sylow 2-subgroup of $\text{Sym}(2^n)$ for all $n \geq 1$, where $\text{Sym}(2^n)$ stands for the full symmetric group of degree 2^n.

Recall that for a group X, *the Frattini subgroup of X*, denoted by $\Phi(X)$, is defined as the intersection of all maximal subgroups of X. It is well known that for a 2-group X, $\Phi(X)$ is generated by squares and commutators, i.e., we have

$$\Phi(X) = X^2[X, X]. \tag{4}$$

Finally, we introduce the following notation, which will be very convenient in calculations throughout the paper.

Definition 3.1. Let $\sigma \in W_n$ for some $n \geq 1$. We define the set $\text{Fix}(\sigma)$ by

$$\text{Fix}(\sigma) = \{v \in \mathbb{F}_2^{2^n} \mid \sigma(v) = v\}.$$

Similarly, for $G \leq W_n$, we define the set $\text{Fix}(G)$ by

$$\text{Fix}(G) = \{v \in \mathbb{F}_2^{2^{n-1}} \mid \sigma(v) = v \text{ for all } \sigma \in G\}.$$

4. Auxiliary lemmas

In this section, we will prove several auxiliary lemmas that will be used in the proof of Theorem 1.4.

Lemma 4.1. *For $n \geq 1$, let $H, G \leq W_n$ be two subgroups of W_n. Suppose that H is elementwise K_n-conjugate into G, $|H| = |G|$ and $H \cap K_n = \{\mathrm{id}\}$. Then $G \cap K_n = \{\mathrm{id}\}$.*

Proof. Let $|H| = |G| = k$. If H is ℓ-generated, set $H = \langle x_1, x_2, \ldots, x_\ell \rangle$. Then we can write $H = \{h_1, h_2, \ldots, h_k\}$, where $h_i = w_i(x_1, x_2, \ldots, x_\ell)$ for some word w_i in $x_1, x_2, \ldots, x_\ell$ for $i = 1, \ldots, k$. Since H is elementwise K_n-conjugate into G, $x_1^{a_1}, x_2^{a_2}, \ldots, x_\ell^{a_\ell} \in G$ for some $a_1, a_2, \ldots, a_\ell \in K_n$. Note that

$$\pi_n(w_i(x_1, x_2, \ldots, x_\ell)) = \pi_n(w_i(x_1^{a_1}, x_2^{a_2}, \ldots, x_\ell^{a_\ell}))$$

since $a_1, \ldots, a_\ell \in K_n = \mathrm{Ker}(\pi_n)$, hence

$$\pi_n(w_i(x_1^{a_1}, x_2^{a_2}, \ldots, x_\ell^{a_\ell})) \neq \pi_n(w_j(x_1^{a_1}, x_2^{a_2}, \ldots, x_\ell^{a_\ell}))$$

for $i \neq j$ since $H \cap K_n = \{\mathrm{id}\}$. This gives $|G| \geq |\pi_n(G)| \geq k = |G|$, hence $|\pi_n(G)| = |G|$, which proves $G \cap K_n = \{\mathrm{id}\}$, as desired. ∎

Lemma 4.2. *For $n \geq 1$, let $H, G \leq W_n$ be two subgroups of W_n. Suppose that H is elementwise K_n-conjugate into G, $|H| = |G|$ and $H \cap K_n = \{\mathrm{id}\}$. Then for any $H_1 \leq H$, there exists $G_1 \leq G$ such that $|H_1| = |G_1|$ and H_1 is elementwise K_n-conjugate into G_1.*

Proof. Let $H_1 = \{h_1, \ldots, h_k\} \leq H$. Since H is elementwise K_n-conjugate into G, there exist $a_1, \ldots, a_k \in K_n$ such that $h_i^{a_i} \in G$ for $i = 1, \ldots, k$. We set $G_1 = \langle h_1^{a_1}, \ldots, h_k^{a_k} \rangle$. Clearly, H_1 is K_n-conjugate into G_1. We also claim that $|H_1| = |G_1|$. To see this, note that by Lemma 4.1, $G \cap K_n = \{\mathrm{id}\}$, hence $G_1 \cap K_n = \{\mathrm{id}\}$. Since $a_1, \ldots, a_k \in K_n$, we have $\pi_n(H_1) = \pi_n(G_1)$. Since we have $H_1 \cap K_n = G_1 \cap K_n = \{\mathrm{id}\}$, this immediately implies $|H_1| = |G_1|$, as desired. ∎

Lemma 4.3. *For $n \geq 1$, let $H, G \leq W_n$ be two non-cyclic subgroups of W_n such that $H \cap K_n = \{\mathrm{id}\}$, $|H| = |G|$, and H is elementwise K_n-conjugate into G. For two distinct maximal subgroups $H_1, H_2 \trianglelefteq H$, suppose that $H_1^a, H_2^b \leq G$ for some $a, b \in K_n$. Then $G = \langle H_1^a, H_2^b \rangle$.*

Proof. Since H_1 and H_2 are distinct maximal subgroups of H, we clearly have $H = \langle H_1, H_2 \rangle$. Note that since $a, b \in K_n$, we have $\pi_n(H) = \pi_n(\langle H_1, H_2 \rangle) = \pi_n(\langle H_1^a, H_2^b \rangle) \leq \pi_n(G)$. Since $H \cap K_n = \{\mathrm{id}\}$ and $G \cap K_n = \{\mathrm{id}\}$ (by Lemma 4.1), this gives

$$|H| = |\pi_n(H)| = |\pi_n(\langle H_1, H_2 \rangle)| = |\pi_n(\langle H_1^a, H_2^b \rangle)| \leq |\pi_n(G)| = |G|,$$

which, since $|H| = |G|$, implies that all quantities must be equal, and in particular

$$|\pi_n(\langle H_1^a, H_2^b \rangle)| = |\pi_n(G)|.$$

Recalling that $G \cap K_n = \{\mathrm{id}\}$ (thus $\langle H_1^a, H_2^b \rangle \cap K_n = \{\mathrm{id}\}$), this gives $\langle H_1^a, H_2^b \rangle = G$, as desired. ∎

In the following lemma and throughout the rest of the article, for any subgroup $H \leq W_n$ of W_n, $C_{K_n}(H)$ denotes the group of elements of K_n which commute with each element of H. Similarly, for any $x \in W_n$, $C_{K_n}(x)$ denotes the set of elements of K_n which commute with x.

Lemma 4.4. *For $n \geq 1$, let $H, G \leq W_n$ be two non-cyclic subgroups of W_n such that $H \cap K_n = \{\mathrm{id}\}$, $|H| = |G|$, and H is elementwise K_n-conjugate into G. For two distinct maximal subgroups $H_1, H_2 \trianglelefteq H$, suppose that $G = \langle H_1, H_2^a \rangle$ for some $a \in K_n$. Then H is globally K_n-conjugate into G if and only if $a \in C_{K_n}(H_1)C_{K_n}(x)$ for some $x \in H_2 \setminus H_1$.*

Proof. We first assume that $a \in C_{K_n}(H_1)C_{K_n}(x)$ for some $x \in H_2 \setminus H_1$. Write $a = bc$ for $b \in C_{K_n}(H_1)$, $c \in C_{K_n}(x)$. Since H_1 has index 2 in H, we have $H = \langle H_1, x \rangle$. Since $\pi_n(x^a) = \pi_n(x)$, this gives $\pi_n(H) = \pi_n(\langle H_1, x^a \rangle)$. Since $H \cap K_n = G \cap K_n = \{\mathrm{id}\}$ (by Lemma 4.1), this immediately implies that $G = \langle H_1, x^a \rangle$. We have

$$H^b = \langle H_1^b, x^b \rangle = \langle H_1, x^{ac} \rangle = \langle H_1, x^a \rangle = G,$$

where we used the fact that K_n is an elementary abelian 2-group in second and third equalities. This finishes the proof of one direction.

We now assume that H is globally K_n-conjugate into G, i.e., there exists $b \in K_n$ such that $H^b = G$ (since $|H| = |G|$). Consider an arbitrary element $x \in H_2 \setminus H_1$. Note that $H = \langle H_1, H_2 \rangle$. Since $G \cap K_n = \{\mathrm{id}\}$ by Lemma 4.1, we immediately get $H_1^b = H_1$ and $H_2^b = H_2^a$, which, since $H_1 \cap K_n = H_2 \cap K_n = \{\mathrm{id}\}$ and $a, b \in K_n$, implies that $b \in C_{K_n}(H_1)$ and $ab \in C_{K_n}(H_2)$. This gives

$$a = b(ab) \in C_{K_n}(H_1)C_{K_n}(H_2) \leq C_{K_n}(H_1)C_{K_n}(x),$$

as desired. ∎

Lemma 4.5. *For $n \geq 1$, let $H, G \leq W_n$ be two non-cyclic subgroups of W_n such that $H \cap K_n = \{\mathrm{id}\}$, $|H| = |G|$, and H is elementwise K_n-conjugate into G. For two distinct maximal subgroups $H_1, H_2 \trianglelefteq H$, suppose that $G = \langle H_1, H_2^a \rangle$ for some $a \in K_n$. Then $a \in C_{K_n}(\Phi(H))$.*

Proof. Take $\alpha \in \Phi(H)$. Since $\alpha \in H_1 \cap H_2$, we must have $\alpha, \alpha^a \in G$. Note that $\pi_n(\alpha) = \pi_n(\alpha^a)$. Since $G \cap K_n = \{\mathrm{id}\}$ by Lemma 4.1, this gives $\alpha = \alpha^a$, as desired. ∎

Lemma 4.6. *Let $n \geq 1$. For $a \in K_n$, $x \in W_n$, write $a = (u, 1)$, $x = (v, s)$ for some $u, v \in \mathbb{F}_2^{2^{n-1}}$, $s \in W_{n-1}$. Then $a \in C_{K_n}(x) \Leftrightarrow u \in \mathrm{Fix}(s)$.*

Proof. If we rewrite the equality $x^a = x$ using (2), we obtain

$$(u, 1)(v, s)(u, 1) = (v, s) \Leftrightarrow (u + v + s(u), s) = (v, s).$$

This immediately gives $s(u) = u$, as desired. ∎

Lemma 4.7. *For $n \geq 1$, let $H \leq W_n$ be a subgroup of W_n. Suppose that $H \cap K_n = \{\mathrm{id}\}$. Then $\pi_n(\Phi(H)) = \Phi(\pi_n(H))$.*

Proof. For any finite group G, let $m(G)$ denote the size of the minimal set of generators of G. Note that $m(H) = m(\pi_n(H))$ because H and $\pi_n(H)$ are isomorphic by the assumption $H \cap K_n = \{\mathrm{id}\}$.

For any finite 2-group G, by Burnside's basis theorem, we have

$$\left| \frac{G}{\Phi(G)} \right| = \frac{|G|}{|\Phi(G)|} = 2^{m(G)}.$$

Therefore, from above, we have

$$\frac{|H|}{|\Phi(H)|} = \frac{|\pi_n(H)|}{|\Phi(\pi_n(H))|}.$$

Since $|H| = |\pi_n(H)|$ by the assumption $H \cap K_n = \{\mathrm{id}\}$, this gives

$$|\Phi(\pi_n(H))| = |\Phi(H)| = |\pi_n(\Phi(H))|, \tag{5}$$

where we used the fact that $\Phi(H) \cap K_n = \{\mathrm{id}\}$ in the last equality. On the other hand, considering the surjection $\pi_n \colon H \twoheadrightarrow \pi_n(H)$, it is a well-known (and easy) exercise to show that

$$\pi_n(\Phi(H)) \leq \Phi(\pi_n(H)). \tag{6}$$

We can now combine (5) and (6) to conclude that $\pi_n(\Phi(H)) = \Phi(\pi_n(H))$, as desired. ∎

Lemma 4.8. *Let $x, y \in W_n$, $a, b \in K_n$. Suppose that x, y, a, b satisfy the equality*

$$xy^a = (xy)^b.$$

Setting $x = (v, s)$, $y = (w, t)$, $a = (u, 1)$ and $b = (z, 1)$, we have

$$s(u) + st(u) = z + st(z).$$

Proof. By direct computation using (2), we get

$$xy^a = (v, s)(u + w + t(u), t) = (v + s(u) + s(w) + st(u), st).$$

Similarly, we have

$$(xy)^b = (z + v + s(w) + st(z), st).$$

If we set the expressions for xy^a and $(xy)^b$ equal to each other, we immediately get

$$s(u) + st(u) = z + st(z),$$

as desired. ∎

5. Proof of Theorem 1.4

We will start with the following proposition, which will be the key ingredient in the inductive step in the proof of Theorem 1.4.

Proposition 5.1. *Let $X \leq W_n$ be a subgroup of W_n. Take $\alpha \in W_n \setminus X$ and also set $Y = \langle X, \alpha \rangle \leq W_n$. Suppose that a vector $v = (v_1, \ldots, v_{2^n}) \in \mathbb{F}_2^{2^n}$ satisfies the following three properties:*

(a) $v_i + v_{\alpha(i)} = v_{\beta(i)} + v_{\beta\alpha(i)}$ *for any $\beta \in X$ and $i \in \{1, \ldots, 2^n\}$.*

(b) $v_i = v_j$ *if* $\mathrm{Orb}_\alpha(i) = \mathrm{Orb}_\alpha(j)$ *and* $\mathrm{Orb}_\beta(i) = \mathrm{Orb}_\beta(j)$ *for some $\beta \in X$ and $i, j \in \{1, \ldots, 2^n\}$.*

(c) $v \in \mathrm{Fix}(\Phi(Y))$.

Then $v \in \mathrm{Fix}(\alpha) + \mathrm{Fix}(X)$.

Proof. We start by noting that, since $v \in \mathrm{Fix}(\Phi(Y))$, throughout the proof, we will feel free to use $v_{\sigma(i)}$ instead of $v_{\sigma^{-1}(i)}$ for any $\sigma \in Y$ because $\sigma(\sigma^{-1})^{-1} = \sigma^2 \in \Phi(Y)$ by (4).

If Y is cyclic, then we must have $Y = \langle \alpha \rangle$ since $\alpha \notin X$. In this case, since $X \leq \langle \alpha \rangle$, condition (b) becomes "$v_i = v_j$ if $\mathrm{Orb}_\alpha(i) = \mathrm{Orb}_\alpha(j)$" and we also get

$$\mathrm{Fix}(\alpha) + \mathrm{Fix}(X) = \mathrm{Fix}(X).$$

Since any v satisfying (b) clearly lies in $\mathrm{Fix}(\alpha) \subseteq \mathrm{Fix}(X)$, we are done.

We can now assume that Y is non-cyclic. Take a vector $v \in \mathbb{F}_2^{2^n}$ that satisfies all three conditions. Consider an arbitrary $i \in \{1, \ldots, 2^n\}$, and its orbit $O(i) := O_Y(i)$ under the action of Y. By definition, for any $j, j' \in O(i)$, there exist $\sigma, \sigma' \in Y$ such that

$$j = \sigma(i), \quad j' = \sigma'(i).$$

For any $y \in Y$, let $\bar{y}$ denote the image of y under the quotient map $Y \twoheadrightarrow Y/\Phi(Y)$. Since v satisfies condition (c), $v_j = v_{j'}$ if $\bar{\sigma} = \bar{\sigma}'$. Suppose that the group Y is $(\ell + 1)$-generated for some $\ell \geq 1$. Since $\alpha \notin X$, we can write $Y = \langle \beta_1, \ldots, \beta_\ell, \alpha \rangle$ for some $\beta_1, \ldots, \beta_\ell \in X$ with $X = \langle \beta_1, \ldots, \beta_\ell \rangle$. By Burnside's basis theorem, Y is a union of $2^{\ell+1}$ distinct cosets of $\Phi(Y)$. More concretely, we can write Y as a disjoint union

$$Y = \left(\bigcup_{i=1}^{2^\ell} A_i \right) \cup \left(\bigcup_{i=1}^{2^\ell} \alpha A_i \right),$$

where each A_i (hence αA_i) is a coset of $\Phi(Y)$, and $X = \bigcup_{i=1}^{2^\ell} A_i$. Fix the representatives $i_1, \ldots, i_k$ of distinct orbits of $\{1, \ldots, 2^n\}$ under the action of Y, i.e.,

$$\bigcup_{j=1}^{k} O(i_j) = \{1, \ldots, 2^n\}.$$

Definition 5.2. Let $v \in \mathbb{F}_2^{2^n}$. We say $\mathcal{P}_Y(v)$ *holds* if v satisfies the following condition:

- For any $\sigma, \sigma' \in Y$ and $j \in \{1, \ldots, k\}$, $v_{\sigma(i_j)} = v_{\sigma'(i_j)} = a_{i_j}^{(t)}$ for some $a_{i_j}^{(t)} \in \{0, 1\}$ if $\sigma \in A_t, \sigma' \in \alpha A_t$ for some $1 \le t \le 2^\ell$.

We define the subspace $V_Y \subseteq \mathbb{F}_2^{2^n}$ by

$$V_Y = \{u \in \mathbb{F}_2^{2^n} \mid \mathcal{P}_Y(u) \text{ holds}\}.$$

The proof of Proposition 5.1 will now follow from the next claim.

Claim 5.3. *There exists $v' \in V_Y$ such that $v' \in \mathrm{Fix}(\alpha)$ and $v - v' \in \mathrm{Fix}(X)$.*

Proof. Any vector in V_Y already lies in $\mathrm{Fix}(\alpha)$ by definition. Thus, to finish the proof, we need to find $v' \in V_Y$ such that $v - v' \in \mathrm{Fix}(X)$.

For any $\sigma_1, \sigma_2 \in Y$, we have

$$\sigma_1 \sigma_2^{-1} \in \Phi(Y) \iff \sigma_1, \sigma_2 \in A_t \text{ or } \sigma_1, \sigma_2 \in \alpha A_t \text{ for some } t \in \{1, \ldots, 2^\ell\}.$$

Therefore, by definition, any $v' \in V_Y$ lies in $\mathrm{Fix}(\Phi(Y))$. Since $v \in \mathrm{Fix}(\Phi(Y))$ by assumption, we conclude that $v - v' \in \mathrm{Fix}(\Phi(Y))$.

Also note that since $X = \bigcup_{i=1}^{2^\ell} A_i$, for any $\sigma_1, \sigma_2 \in Y$, we have

$$\sigma_1 \sigma_2^{-1} \in X \iff \sigma_1 \in A_t, \sigma_2 \in A_{t'} \text{ or } \sigma_1 \in \alpha A_t, \sigma_2 \in \alpha A_{t'} \text{ for some } t, t' \in \{1, \ldots, 2^\ell\}.$$

Thus, it follows that for any $v' \in V_Y$, we have $v - v' \in \mathrm{Fix}(X)$ if and only if the following two conditions are satisfied for $j = 1, \ldots, k$:

(1) $(v - v')_{\sigma_1(i_j)} = (v - v')_{\sigma_2(i_j)}$ if $\sigma_1 \in A_i, \sigma_2 \in A_{i'}$ for some $i, i' \in \{1, \ldots, 2^\ell\}$.

(2) $(v - v')_{\sigma_3(i_j)} = (v - v')_{\sigma_4(i_j)}$ if $\sigma_3 \in \alpha A_i, \sigma_4 \in \alpha A_{i'}$ for some $i, i' \in \{1, \ldots, 2^\ell\}$.

We will now show that a vector $v' \in V_Y$ that satisfies both conditions indeed exists.

Condition (1): With the notation in Definition 5.2, condition (1) is equivalent to the equality

$$v_{\sigma_1(i_j)} + v_{\sigma_2(i_j)} = a_{i_j}^{(i)} + a_{i_j}^{(i')} \tag{7}$$

for some $a_{i_j}^{(i)}, a_{i_j}^{(i')} \in \{0, 1\}$. Note that if the variables $a_{i_j}^{(i)}, a_{i_j}^{(i')} \in \{0, 1\}$ are independent, then we can choose them so that (7) holds. If they are not independent, this gives us four different cases.

Case 1. $\pi_1(i_j) = \pi_2(i_j)$ for some $\pi_1 \in A_i, \pi_2 \in A_{i'}$. In this case, $a_{i_j}^{(i)} + a_{i_j}^{(i')} = 0$ by Definition 5.2. Recalling that $v \in \mathrm{Fix}(\Phi(Y))$, the left-hand side of (7) also vanishes since $v_{\sigma_1(i_j)} = v_{\pi_1(i_j)} = v_{\pi_2(i_j)} = v_{\sigma_2(i_j)}$, where we used Definition 5.2 in the first and the third equalities. Hence, (7) holds.

Case 2. $\pi_1(i_j) = \alpha \pi_2(i_j)$ for some $\pi_1 \in A_i$ and $\pi_2 \in A_{i'}$. In this case, we have that $\mathrm{Orb}_\alpha(\pi_1(i_j)) = \mathrm{Orb}_\alpha(\pi_2(i_j))$ and $\mathrm{Orb}_{\pi_1(\pi_2)^{-1}}(\pi_1(i_j)) = \mathrm{Orb}_{\pi_1(\pi_2)^{-1}}(\pi_2(i_j))$. Thus, as $\pi_1 \pi_2^{-1} \in X$, condition (b) in Proposition 5.1 implies that $v_{\pi_1(i_j)} = v_{\pi_2(i_j)}$. Recalling that

$v \in \text{Fix}(\Phi(Y))$, and that $\pi_1 \sigma_1^{-1}, \pi_2 \sigma_2^{-1} \in \Phi(Y)$, this immediately gives $v_{\sigma_1(i_j)} = v_{\sigma_2(i_j)}$ since $v_{\sigma_1(i_j)} = v_{\pi_1(i_j)}$ and $v_{\sigma_2(i_j)} = v_{\pi_2(i_j)}$. Therefore, to show that (7) holds, it remains to see that $a_{i_j}^{(i)} + a_{i_j}^{(i')}$ vanishes. But, this is immediate by Definition 5.2 and the condition $\pi_1(i_j) = \alpha \pi_2(i_j)$, hence we are done.

Case 3. $\alpha \pi_1(i_j) = \alpha \pi_2(i_j)$ for some $\pi_1 \in A_i$, $\pi_2 \in A_{i'}$. Applying α^{-1} to both sides of $\alpha \pi_1(i_j) = \alpha \pi_2(i_j)$, we obtain case 1, hence the result follows from case 1.

Case 4. $\alpha \pi_1(i_j) = \pi_2(i_j)$ for some $\pi_1 \in A_i$, $\pi_2 \in A_{i'}$. Applying α^{-1} to both sides of $\alpha \pi_1(i_j) = \pi_2(i_j)$, we obtain $\pi_1(i_j) = \alpha^{-1} \pi_2(i_j)$. By definition of $A_{i'}$, since $\alpha(\alpha^{-1})^{-1} = \alpha^2 \in \Phi(Y)$ by (4), there exists $\pi_3 \in A_{i'}$ such that $\alpha^{-1} \pi_2(i_j) = \alpha \pi_3(i_j)$. This yields $\pi_1(i_j) = \alpha \pi_3(i_j)$, and the result now follows from case 2.

Condition (2): This condition is clearly equivalent to the condition

$$(v - v')_{\alpha \sigma_1(i_j)} = (v - v')_{\alpha \sigma_2(i_j)} \quad \text{if } \sigma_1 \in A_i, \ \sigma_2 \in A_{i'} \text{ for some } i, i' \in \{1, \dots, 2^\ell\}. \tag{8}$$

Applying α to both sides of the equality in (8), we obtain

$$(v - v')_{\sigma_1(i_j)} = (v - v')_{\sigma_2(i_j)},$$

which is the same as condition (1). Hence, the proof follows from the first part. We have covered all possible cases, hence we are done. ∎

The proof of Proposition 5.1 now follows from Claim 5.3. ∎

The following will be crucial in showing that certain vectors that will appear in the proof of Theorem 1.4 do indeed satisfy the conditions given in Proposition 5.1, hence the conclusion of Proposition 5.1.

Proposition 5.4. *Let $X \leq W_n$ be a subgroup of W_n. Take $\alpha \in W_n \setminus X$ and also set $Y = \langle X, \alpha \rangle \leq W_n$. Suppose that a vector $v \in \mathbb{F}_2^{2^n}$ satisfies the following conditions:*

(1) *For any $\beta \in X$, there exists $u^{(\beta)} \in \text{Fix}(\Phi(Y))$ such that*

$$\alpha(v) + \alpha\beta(v) = u^{(\beta)} + \alpha\beta(u^{(\beta)}).$$

(2) *$v \in \text{Fix}(\Phi(Y))$.*

Then we have $v \in \text{Fix}(\alpha) + \text{Fix}(X)$.

Proof. To prove the proposition, it suffices to show that the vector v satisfies the conditions (a) and (b) in Proposition 5.1. Note that we have the equality

$$\alpha(v) + \alpha\beta(v) = u^{(\beta)} + \alpha\beta(u^{(\beta)}). \tag{9}$$

If we apply $\alpha\beta$ to both sides of (9), since $v, u^{(\beta)} \in \text{Fix}(\Phi(Y))$ and $(\alpha\beta)^2, (\alpha\beta\alpha)(\beta)^{-1} \in \Phi(Y)$, we obtain

$$v + \beta(v) = u^{(\beta)} + \alpha\beta(u^{(\beta)}). \tag{10}$$

Adding (9) and (10) yields

$$v + \beta(v) = \alpha(v) + \alpha\beta(v). \tag{11}$$

Comparing the coordinates of both sides in (11), we obtain

$$v_i + v_{\beta^{-1}(i)} = v_{\alpha^{-1}(i)} + v_{(\alpha\beta)^{-1}(i)}$$

for any $i \in \{1, \ldots, 2^n\}$. Recalling that $v \in \text{Fix}(\Phi(Y))$, this can be rewritten as

$$v_i + v_{\beta(i)} = v_{\alpha(i)} + v_{\alpha\beta(i)}$$

for any $i \in \{1, \ldots, 2^n\}$. Since this can be done for any $\beta \in X$, it follows that v satisfies the condition (a) of Proposition 5.1.

It now remains to show that the vector v satisfies condition (b) of Proposition 5.1. To that end, suppose that for some $\beta \in X$, $\text{Orb}_\alpha(i) = \text{Orb}_\alpha(j)$ and $\text{Orb}_\beta(i) = \text{Orb}_\beta(j)$ for some $i, j \in \{1, \ldots, 2^n\}$. Write $\alpha^a(i) = \beta^b(i) = j$ for some $a, b \in \mathbb{N}$. If at least one of a or b is even, then at least one of α^a or β^b lies in $\Phi(Y)$ by (4), which immediately gives that $v_i = v_j$ since $v \in \text{Fix}(\Phi(Y))$. Thus, we can assume without loss of generality that a and b are both odd. By comparing coordinates of both sides in (10) and using the fact that $v, u^{(\beta)} \in \text{Fix}(\Phi(Y))$, we have

$$v_i + v_{\beta(i)} = u_i^{(\beta)} + u_{\alpha\beta(i)}^{(\beta)}. \tag{12}$$

Since $v \in \text{Fix}(\Phi(Y))$, and $\beta^{b-1} \in \Phi(Y)$ by (4) (recall that b was odd), we have $v_{\beta(i)} = v_{\beta^b(i)} = v_j$, which, using (12), yields

$$v_i + v_j = u_i^{(\beta)} + u_{\alpha\beta(i)}^{(\beta)}. \tag{13}$$

We also have $\alpha\beta(i) = \alpha\beta^{1-b}\beta^b(i) = \alpha\beta^{1-b}(j)$. Recalling that $u^{(\beta)} \in \text{Fix}(\Phi(Y))$ and that $1 - a$ and $1 - b$ are even, this gives

$$u_{\alpha\beta(i)}^{(\beta)} = u_{\alpha\beta^{1-b}(j)}^{(\beta)} = u_{\alpha(j)}^{(\beta)} = u_{\alpha^{-a}(j)}^{(\beta)} = u_i^{(\beta)}.$$

Finally, putting this in (13), we obtain $v_i + v_j = u_i^{(\beta)} + u_i^{(\beta)} = 0$, hence $v_i = v_j$, as desired.   ∎

We are finally ready to prove Theorem 1.4.

Proof of Theorem 1.4. We will use induction on $|H|$. Note that the statement trivially holds for $|H| = 1$ and $|H| = 2$ since in those cases H is cyclic. We now assume that the statement holds for $|H| = 2^k$ for some $k \geq 1$, and to finish the inductive step, we will prove the statement for $|H| = 2^{k+1}$. By the induction assumption and Lemma 4.2, if we take any maximal ideal $H_1 \trianglelefteq H$, there exist $G_1 \trianglelefteq G$ and $a \in K_n$ such that $H_1^a = G_1$. Thus, conjugating G by a if necessary, we can assume without loss of generality that

$H_1 \trianglelefteq G$. Note that this also implies $\Phi(H) \leq G$ since $\Phi(H)$ is contained in H_1. The statement already holds if H is cyclic, so we can assume without loss of generality that H is non-cyclic, which gives two distinct maximal subgroups H_1, H_2 of H with $H = \langle H_1, H_2 \rangle$. By the induction assumption and Lemma 4.2, there exists $b \in K_n$ such that $H_2^b \trianglelefteq G$. By Lemma 4.3, this yields $G = \langle H_1, H_2^b \rangle$. By Lemma 4.5, then, we obtain $b \in C_{K_n}(\Phi(H))$. To prove that H and G are conjugate under K_n, by Lemma 4.4, we need to show that $b \in C_{K_n}(H_1) C_{K_n}(x)$ for some $x \in H_2 \setminus H_1$. Setting $b = (u, 1)$, $x = (v, s)$ for $u, v \in \mathbb{F}_2^{2^{n-1}}$, $s \in W_{n-1}$, by Lemma 4.6, this is equivalent to showing that

$$u \in \text{Fix}(\pi_n(H_1)) + \text{Fix}(s), \tag{14}$$

where we used the identification given in (3) when writing $\text{Fix}(\pi_n(H))$.

Fix some $x \in H_2 \setminus H_1$. For each $h_i \in H_1$, if we consider a maximal subgroup $H^{(i)} \trianglelefteq H$ of H that contains $h_i x$, by the induction assumption and Lemma 4.2, there exists $c_i \in K_n$ such that $(H^{(i)})^{c_i}$ is a maximal subgroup of G. Since $G \cap K_n = \{\text{id}\}$ (by Lemma 4.1), $\Phi(H) \leq H_1 \leq G$ and $\Phi(H)^{c_i} \leq (H^{(i)})^{c_i} \leq G$, this immediately gives $\Phi(H) = \Phi(H)^{c_i}$, i.e., $c_i \in C_{K_n}(\Phi(H))$. Recall that $H_2^b \leq G$, thus $x^b \in G$. Since both $(h_i x)^{c_i}$ and $h_i x^b$ lie in G, $\pi_n(h_i x^b) = \pi_n((h_i x)^{c_i})$, and $G \cap K_n = \{\text{id}\}$, we obtain

$$h_i x^b = (h_i x)^{c_i} \tag{15}$$

for $i = 1, \ldots, |H_1| = 2^k$. Setting $h_i = (w_i, t_i)$, $c_i = (z_i, 1)$ (and recalling $x = (v, s)$, $b = (u, 1)$), using Lemma 4.8, (15) yields

$$t_i(u) + t_i s(u) = z_i + t_i s(z_i) \tag{16}$$

for $i = 1, \ldots, 2^k$. Recall from above that $c_i \in C_{K_n}(\Phi(H))$, i.e., by Lemma 4.6,

$$z_i \in \text{Fix}(\pi_n(\Phi(H))) = \text{Fix}(\Phi(\pi_n(H))),$$

where we used Lemma 4.7 in the last equality. Also recall from the first part of the proof that $b \in C_{K_n}(\Phi(H))$, i.e., by Lemma 4.6, $u \in \text{Fix}(\Phi(\pi_n(H)))$. If we now take $X = \langle t_1, \ldots, t_{2^k} \rangle$, $Y = \pi_n(H)$, $\alpha = s$, $v = u$ in Proposition 5.4, recalling (16), the vector u satisfies both conditions in Proposition 5.4. It immediately follows that

$$u \in \text{Fix}(\langle t_1, \ldots, t_{2^k} \rangle) + \text{Fix}(s) = \text{Fix}(\pi_n(H_1)) + \text{Fix}(s),$$

which completes the proof of Theorem 1.4 by (14). ∎

6. A conjecture

We close the paper by a conjecture based on extensive MAGMA computations.

Conjecture 6.1. *For $n \geq 1$, let $H \leq W_n$ be a subgroup of W_n. Suppose that H contains a permutation $\sigma \in W_n$ that acts transitively on $\{1, \ldots, 2^n\}$. Then $\mathcal{P}(H, G)$ holds for any subgroup $G \leq W_n$.*

The author's interest in Conjecture 6.1 comes from the following: It has the potential of being particularly useful for the number theory application mentioned in Section 2, because for most polynomials f, for $n \geq 1$, the group $G_n(f)$ *does* contain an element that acts transitively on $\{1, \ldots, 2^n\}$. Thus, in such cases, Conjecture 6.1 will imply that a conjugate of $G_n(f)$ is contained in $M_n(f)$ as long as $G_n(f)$ is elementwise K_n-conjugate into $M_n(f)$.

References

[1] F. Ahmad, R. L. Benedetto, J. Cain, G. Carroll, and L. Fang, The arithmetic basilica: A quadratic PCF arboreal Galois group. *J. Number Theory* **238** (2022), 842–868 Zbl 1503.37099 MR 4430121

[2] R. L. Benedetto, X. Faber, B. Hutz, J. Juul, and Y. Yasufuku, A large arboreal Galois representation for a cubic postcritically finite polynomial. *Res. Number Theory* **3** (2017), article no. 29 Zbl 1427.11118 MR 3736808

[3] R. L. Benedetto and J. Juul, Odoni's conjecture for number fields. *Bull. Lond. Math. Soc.* **51** (2019), no. 2, 237–250 Zbl 1470.11289 MR 3937585

[4] N. Boston and R. Jones, Arboreal Galois representations. *Geom. Dedicata* **124** (2007), 27–35 Zbl 1206.11069 MR 2318536

[5] N. Boston and R. Jones, The image of an arboreal Galois representation. *Pure Appl. Math. Q.* **5** (2009), no. 1, 213–225 Zbl 1167.11011 MR 2520459

[6] A. Bridy and T. J. Tucker, Finite index theorems for iterated Galois groups of cubic polynomials. *Math. Ann.* **373** (2019), no. 1–2, 37–72 Zbl 1476.37113 MR 3968866

[7] G. Chenevier, Subgroups of Spin(7) or SO(7) with each element conjugate to some element of G_2 and applications to automorphic forms. *Doc. Math.* **24** (2019), 95–161 Zbl 1475.20083 MR 3946712

[8] A. Ferraguti and G. Micheli, An equivariant isomorphism theorem for mod $\mathfrak{p}$ reductions of arboreal Galois representations. *Trans. Amer. Math. Soc.* **373** (2020), no. 12, 8525–8542 Zbl 1464.37091 MR 4177267

[9] A. Ferraguti, C. Pagano, and D. Casazza, The inverse problem for arboreal Galois representations of index two. 2023, arXiv:1907.08608

[10] V. Goksel, Markov processes and some PCF quadratic polynomials. *Res. Number Theory* **5** (2019), no. 3, article no. 29 Zbl 1470.11292 MR 3998214

[11] R. Gottesman and K. Tang, Quadratic recurrences with a positive density of prime divisors. *Int. J. Number Theory* **6** (2010), no. 5, 1027–1045 Zbl 1244.11014 MR 2679455

[12] C. Gratton, K. Nguyen, and T. J. Tucker, ABC implies primitive prime divisors in arithmetic dynamics. *Bull. Lond. Math. Soc.* **45** (2013), no. 6, 1194–1208 Zbl 1291.37121 MR 3138487

[13] S. Hamblen, R. Jones, and K. Madhu, The density of primes in orbits of $z^d + c$. *Int. Math. Res. Not. IMRN* **2015** (2015), no. 7, 1924–1958 Zbl 1395.11128 MR 3335237

[14] W. Hindes, Average Zsigmondy sets, dynamical Galois groups, and the Kodaira–Spencer map. *Trans. Amer. Math. Soc.* **370** (2018), no. 9, 6391–6410 Zbl 1394.37130 MR 3814334

[15] W. Hindes, Classifying Galois groups of small iterates via rational points. *Int. J. Number Theory* **14** (2018), no. 5, 1403–1426 Zbl 1441.11281 MR 3806313

[16] P. Ingram, Arboreal Galois representations and uniformization of polynomial dynamics. *Bull. Lond. Math. Soc.* **45** (2013), no. 2, 301–308 Zbl 1280.37058 MR 3064415

[17] R. Jones, The density of prime divisors in the arithmetic dynamics of quadratic polynomials. *J. Lond. Math. Soc. (2)* **78** (2008), no. 2, 523–544 Zbl 1193.37144 MR 2439638

[18] R. Jones, Galois representations from pre-image trees: an arboreal survey. In *Actes de la Conférence "Théorie des Nombres et Applications"*, pp. 107–136, Publ. Math. Besançon Algèbre Théorie Nr. 2013, Presses Universitaires Franche-Comté, Besançon, 2013 Zbl 1307.11069 MR 3220023

[19] J. Juul, H. Krieger, N. Looper, M. Manes, B. Thompson, and L. Walton, Arboreal representations for rational maps with few critical points. In *Research directions in number theory—Women in Numbers IV*, pp. 133–151, Assoc. Women Math. Ser. 19, Springer, Cham, 2019 Zbl 1436.11135 MR 4069382

[20] M. Larsen, On the conjugacy of element-conjugate homomorphisms. *Israel J. Math.* **88** (1994), no. 1–3, 253–277 Zbl 0898.20025 MR 1303498

[21] M. Larsen, On the conjugacy of element-conjugate homomorphisms. II. *Q. J. Math.* **47** (1996), no. 185, 73–85 Zbl 0898.20026 MR 1380951

[22] R. W. K. Odoni, The Galois theory of iterates and composites of polynomials. *Proc. Lond. Math. Soc. (3)* **51** (1985), no. 3, 385–414 Zbl 0622.12011 MR 805714

[23] R. W. K. Odoni, On the prime divisors of the sequence $w_{n+1} = 1 + w_1 \cdots w_n$. *J. Lond. Math. Soc. (2)* **32** (1985), no. 1, 1–11 Zbl 0574.10020 MR 813379

[24] R. W. K. Odoni, Realising wreath products of cyclic groups as Galois groups. *Mathematika* **35** (1988), no. 1, 101–113 Zbl 0662.12010 MR 962740

[25] R. Pink, Profinite iterated monodromy groups arising from quadratic polynomials. 2013, arXiv:1307.5678

[26] M. Stoll, Galois groups over $\mathbb{Q}$ of some iterated polynomials. *Arch. Math. (Basel)* **59** (1992), no. 3, 239–244 Zbl 0758.11045 MR 1174401

[27] S. Wang, Dimension data, local and global conjugacy in reductive groups. 2007, arXiv:0707.0144

[28] S. Wang, On dimension data and local vs. global conjugacy. In *Fifth International Congress of Chinese Mathematicians. Part 1, 2*, pp. 365–382, Stud. Adv. Math. 2, American Mathematical Society, Providence, RI, 2012 Zbl 1246.22028 MR 2908081

[29] S. Wang, On local and global conjugacy. *J. Algebra* **439** (2015), 334–359 Zbl 1332.22021 MR 3373375

Vefa Goksel

Department of Mathematics and Statistics, University of Massachusetts Amherst, 710 N. Pleasant Street, Amherst, MA 01003-9305; Department of Mathematics, Towson University, 7800 York Road, Towson, MD 21252-0001, USA; vgoksel@towson.edu