Andrea Ferraguti

The set of stable primes for polynomial sequences with large Galois group

Proceedings of the American Mathematical Society
DOI: 10.1090/proc/13958

Accepted Manuscript

THE SET OF STABLE PRIMES FOR POLYNOMIAL SEQUENCES WITH LARGE GALOIS GROUP

ANDREA FERRAGUTI

Abstract. Let K be a number field with ring of integers $\mathcal{O}_K$, and let $\{f_k\}_{k\in\mathbb{N}} \subseteq \mathcal{O}_K[x]$ be a sequence of monic polynomials such that for every $n \in \mathbb{N}$, the composition $f^{(n)} = f_1 \circ f_2 \circ \ldots \circ f_n$ is irreducible. In this paper we show that if the size of the Galois group of $f^{(n)}$ is large enough (in a precise sense) as a function of n, then the set of primes $\mathfrak{p} \subseteq \mathcal{O}_K$ such that every $f^{(n)}$ is irreducible modulo $\mathfrak{p}$ has density zero. Moreover, we prove that the subset of polynomial sequences such that the Galois group of $f^{(n)}$ is large enough has density 1, in an appropriate sense, within the set of all polynomial sequences.

1. Introduction

In the recent years, there has been a growing interest in the field of arithmetic dynamics (see for example [2],[3],[8],[9],[10],[11],[12],[14],[15]). One of its main objects of study is the arithmetic of dynamical systems given by a pair $(\mathbb{P}^1(K), f)$, where K is a global field and f is a rational function on $\mathbb{P}^1$. Standard questions include the determination of the set of periodic and pre-periodic points, the determination of integral points in orbits, the structure of field extensions attached to the iterations of f, and many others (see for example [20] for a comprehensive introduction on the topic).

When looking at the iterates of a rational function, one can construct very naturally an infinite tree, carring a natural profinite topology, on which the absolute Galois group of K acts continuously, giving rise to what is called an *arboreal Galois representation* (cf. section 2 for details). These extremely interesting objects resemble in many aspects p-adic representations coming from geometry (see for example [13] for a survey), such as the Tate modules attached to elliptic curves. In the general case, not much is known about the behaviour of arboreal Galois representations, but a certain number of results are available when the rational function has degree two (see [3],[4],[13] and [14]). In particular, it seems that generically the image of these representations is "large", i.e. it has finite index in the group of automorphisms of the appropriate tree. This phenomenon recalls closely Serre's open image theorem for elliptic curves without complex multiplication [18].

Focusing on rational functions f which are actually polynomials with coefficients in the ring of integers of K yields a greater number of arithmetic questions, such as the determination of the set of prime divisors in orbits (see [11] and [17]) or, in the case where all iterates are irreducible, the determination of the set of primes $\mathfrak{p}$ such that all iterates of f are irreducible modulo $\mathfrak{p}$. Following the terminology of the existing literature, we will

2010 *Mathematics Subject Classification.* Primary 11R32, 11R45, 20E08.

Key words and phrases. Arboreal Galois representations, number fields, stable primes, natural density.

call such primes *stable.* In [12], the author focuses on the case of quadratic polynomials and conjectures that, under some hypotheses on the post-critical orbit of f, the set of stable primes is finite (see [12, Conjecture 6.2]).

In this paper, we address the problem of finding the density of the set of stable primes under a precise condition of largeness of the attached arboreal Galois representation (cf. Theorem 2.3), but for a more general class of objects that we will now introduce. In particular, our setting can be specialized to that of a dynamical system given by a single polynomial of any degree.

Let K be a number field with number ring $\mathcal{O}_K$, and let $\{f_k\}_{k\in\mathbb{N}}\subseteq\mathcal{O}_K[x]$ be a sequence of polynomials. For every $n\in\mathbb{N}$, let $f^{(n)}:=f_1\circ\ldots\circ f_n$, and suppose that $f^{(n)}$ is separable for all n. The study of arithmetic dynamical systems corresponds to the case where the sequence $\{f_k\}$ is constant. Generalizing the existing construction in arithmetic dynamics, one can attach an arboreal Galois representation to the sequence $\{f_k\}$, where the Galois group of $f^{(n)}$ acts on the set of vertices at level n of an infinite tree. In general, this is a spherically homogeneous tree but not a complete d-ary tree, unless all the f_k's have equal degree d. Now suppose that $f^{(n)}$ is irreducible for every n. We call a prime $\mathfrak{p}\subseteq\mathcal{O}_K$ *stable* for $\{f_k\}$ if $f^{(n)}$ is irreducible modulo $\mathfrak{p}$ for every n. Our main theorem is then the following.

Theorem 1.1. *Suppose that the image of the arboreal Galois representation attached to $\{f_k\}$ is large enough. Then the set of stable primes for $\{f_k\}$ has density 0.*

In section 2 we introduce the arboreal Galois representation attached to $\{f_k\}$, we explain the condition of "largeness" mentioned in Theorem 1.1 and we show some of the consequences of the theorem. In section 3 we describe the structure of the automorphism group of the infinite tree attached to $\{f_k\}$ and we compute the order of the automorphism group of the tree truncated at level n. In section 4 we prove Theorem 1.1, explaining how it follows from an application of Chebotarev density theorem together with the computations of section 3. Finally, in section 5 we address the following question: suppose we fix a sequence of degrees $\{d_k\}_{k\in\mathbb{N}}\subseteq\mathbb{N}$, and then we choose "at random" a sequence of polynomials $\{f_k\}$ such that f_k has degree d_k for every k. What are the odds that such sequence fulfils the hypotheses of Theorem 1.1? After introducing an adequate concept of density on the set of all polynomial sequences $\{g_k\}_{k\in\mathbb{N}}\subseteq\mathcal{O}_K[x]$ such that g_k has degree d_k for every k, we prove that the density of the set of polynomial sequences that fulfil such hypotheses is 1. The proof uses results of Cohen [6] and Odoni [16].

Acknowledgements

We would like to thank Giacomo Micheli, Rafe Jones and the anonymous referee for their helpful comments. The author was supported by Swiss National Science Foundation grant number 168459.

2. Arboreal Galois representations

Let K be a field and let $\{f_k\} := \{f_k\}_{k\in\mathbb{N}} \subseteq K[x]$ be a sequence of polynomials. For every $n \geq 1$, we set $d_n := \deg f_n$ and we let $f^{(n)}$ be the composition $f_1 \circ f_2 \circ \ldots \circ f_n$. We assume that $f^{(n)}$ is separable for every n.

It is possible to attach to $\{f_k\}$ an infinite tree $\mathcal{T}$ in the following way: the root of the tree is labeled by 0, and for every $n \geq 1$, the vertices at level n are labeled by the roots of $f^{(n)}$ in $\overline{K}$. A vertex α at level n descends from a vertex β at level $n-1$ if and only if $f_n(\alpha) = \beta$. Note that thanks to the separability assumption, every vertex at level n has exactly d_{n+1} descendants at level $n+1$. Such a tree is called a *spherically homogeneous rooted tree* (see for example [1] and [5]), and it depends only on the sequence of the degrees $\{d_k\}_{k\in\mathbb{N}}$, which is called the *spherical index* of $\mathcal{T}$. When the spherical index is constant and equal to some $d \in \mathbb{N}$, $\mathcal{T}$ is called a *complete rooted d-ary tree.*

For every $n \geq 1$, we let $\mathcal{T}_n$ be the tree truncated at level n. This consists of the finite tree formed by all vertices which have distance at most n from the root.

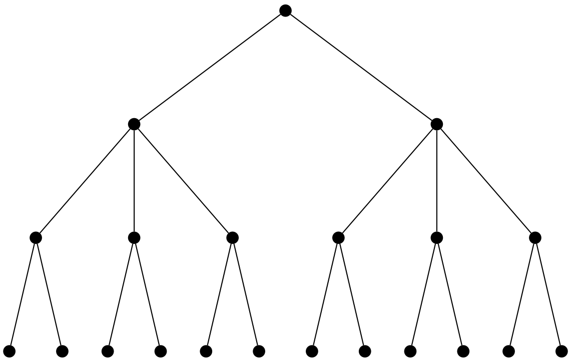

Figure 1. A spherically homogeneous tree of spherical index $\{2, 3, 2, \ldots\}$ truncated at level 3.

From now on, we let G_n be the Galois group of $f^{(n)}$. The action of G_n on the roots of $f^{(n)}$ extends naturally to an action on $\mathcal{T}_n$, and this yields an embedding of G_n into the group of automorphisms of $\mathcal{T}_n$. Recall that an automorphism of a tree is a bijection σ of the set of vertices such that a vertex v is connected with a vertex v' if and only if $\sigma(v)$ is connected with $\sigma(v')$. It follows immediately that a tree automorphism induces a permutation of the set of vertices at level n, for every n. Thus there are obvious projection maps $\pi_n\colon \operatorname{Aut}(\mathcal{T}_n) \to \operatorname{Aut}(\mathcal{T}_{n-1})$ and the automorphism group of $\mathcal{T}$ can be realized as

$$\operatorname{Aut}(\mathcal{T}) \simeq \varprojlim_n \operatorname{Aut}(\mathcal{T}_n).$$

On the other hand, it is immediate to check that for every n, the splitting field of $f^{(n)}$ is contained in the splitting field of $f^{(n+1)}$. Thus, there are surjections $G_{n+1} \to G_n$ and the profinite group $G_{\{f_k\}} := \varprojlim_n G_n$ acts on $\mathcal{T}$ as a subgroup of $\operatorname{Aut}(\mathcal{T})$, giving rise to a continuous embedding $G_{\{f_k\}} \to \operatorname{Aut}(\mathcal{T})$. This motivates the following definition, generalizing the one given in [3].

Definition 2.1. An *arboreal Galois representation* of a profinite group G is a continuous homomorphism $G \to \mathrm{Aut}(\mathcal{T})$, where $\mathcal{T}$ is a spherically homogeneous rooted tree.

In the particular case where $\{f_k\}$ is a constant sequence, one recovers [3, Definition 1.1].

From now on, K will be a number field with ring of integers $\mathcal{O}_K$, and $f_k \in \mathcal{O}_K[x]$ will be monic for every $k \in \mathbb{N}$. We assume throughout the paper that $f^{(n)}$ is irreducible for every n. We also set $d^{(0)} = 1$ and for every $n \geq 1$ we let $d^{(n)} := \deg f^{(n)}$.

Definition 2.2. We say that a prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$ is *stable* for $\{f_k\}$ if $f^{(n)}$ is irreducible modulo $\mathfrak{p}$ for every $n \geq 1$.

The set of stable primes for $\{f_k\}$ will be denoted by $\mathrm{St}(\{f_k\})$.

The main goal of this paper is to prove the following theorem.

Theorem 2.3. *Suppose that the index of G_n in $\mathrm{Aut}(\mathcal{T}_n)$ is $o(d^{(n)})$. Then $\mathrm{St}(\{f_k\})$ has density 0.*

Recall that if S is a set of prime ideals of $\mathcal{O}_K$, the *natural density* of S and the *Dirichlet density* of S are defined respectively as:

$$\lim_{x\to\infty} \frac{|\mathfrak{p} \in S \colon N_{K/\mathbb{Q}}(\mathfrak{p}) \leq x|}{|\mathfrak{p} \subseteq \mathcal{O}_K \colon N_{K/\mathbb{Q}}(\mathfrak{p}) \leq x|} \text{ and } \lim_{s\to 1^+} \frac{\sum_{\mathfrak{p}\in S} N_{K/\mathbb{Q}}(\mathfrak{p})^{-s}}{\sum_{\mathfrak{p}\subseteq \mathcal{O}_K} N_{K/\mathbb{Q}}(\mathfrak{p})^{-s}},$$

(provided that the limits exist). The word "density" in Theorem 2.3 refers to either concept of density, since the result is true for both. The density of a set of primes S will be denoted by $\delta(S)$. The *upper density* of S, which is defined using lim sup in place of lim in the above formulas, will be denoted by $\overline{\delta}(S)$.

Theorem 2.3 has the following immediate consequence.

Corollary 2.4. *Suppose that the sequence $\{d_k\}_{k\in\mathbb{N}}$ is not eventually 1 (i.e. that $d^{(n)} \to +\infty$) and that the arboreal Galois representation of $G_{\{f_k\}}$ has finite index image in $\mathrm{Aut}(\mathcal{T})$. Then the set of stable primes for $\{f_k\}$ has density 0.*

Proof. Just note that since $G_n \leq \mathrm{Aut}(\mathcal{T}_n)$ for every n, the group $G_{\{f_k\}}$ has finite index in $\mathrm{Aut}(\mathcal{T})$ if and only if the index of G_n in $\mathrm{Aut}(\mathcal{T}_n)$ is eventually constant, and therefore in particular it is $o(d^{(n)})$ as $d^{(n)} \to +\infty$. □

Remark 2.5. It is very easy to see that the conclusion of Theorem 2.3 fails if we drop the assumption on the size of G_n. For example, if $\{f_k\}$ is the constant sequence with $f_k = x^2 - 2 \in \mathbb{Z}[x]$, then the Galois group of $f^{(n)}$ is the cyclic group of order 2^n (see [3]). Now [12, Theorem 2.2] shows that, for every fixed n, $f^{(n)}$ is irreducible modulo p if and only if $p \equiv 3, 5 \bmod 8$. Thus in this case, the set of stable primes for $\{f_k\}$ has density $1/2$.

Clearly, one can use Theorem 2.3 in its contrapositive form to prove that the index of $G_{\{f_k\}}$ in $\mathrm{Aut}(\mathcal{T})$ is infinite. An explicit example can be constructed as follows. Let p be a fixed prime, and let $f_k := (x - p^{2k+1})^2 + p^{2k-1}$ for every $k \geq 1$. Then [8, Proposition 3.3] shows that if q is a prime with $\left(\dfrac{p}{q}\right) = \left(\dfrac{-p}{q}\right) = -1$, where $\left(\dfrac{\cdot}{q}\right)$ denotes the Legendre symbol modulo q, then the composition $f^{(n)}$ is irreducible modulo q for every $n \in \mathbb{N}$. Quadratic reciprocity easily implies the existence of a set of positive density of such q's, showing that the index of $G_{\{f_k\}}$ in $\mathrm{Aut}(\mathcal{T})$ is infinite.

The same argument furnishes a different proof of some cases of [13, Theorem 3.1]: if $f \in \mathcal{O}_K[x]$ is a monic polynomial of degree 2 such that all its iterates are irreducible and the affine span of its post-critical orbit in the $\mathbb{F}_2$-vector space K^*/K^{*2} is finite and does not contain the coset of 1, then the set of stable primes for f has positive density (see [12, Theorem 6.1]). Thus, by Theorem 2.3 the attached Galois representation has infinite index in $\mathrm{Aut}(\mathcal{T})$. This applies for example to the polynomial $(x-t)^2+t-1 \in \mathbb{Z}[x]$, where $t \in \mathbb{Z}$ is such that t and $\pm(t-1)$ are all non-squares.

When $\{f_k\}$ is a constant sequence of spherical index 2, we fall back in the setting studied for example in [3],[12],[13] or [14]. Let us briefly recall such setting. Let $\phi \in K(x)$ be a rational function of degree 2. A *critical point* γ of ϕ is a point $\gamma \in \mathbb{P}^1$ such that $\phi'(\gamma) = 0$. The map ϕ is said to be *post-critically finite* if the orbit of every critical point under ϕ is finite. Generalizing in the obvious way the construction we discussed above, one attaches a complete rooted 2-ary tree $\mathcal{T}$ to ϕ, and there is a continuous action of the absolute Galois group of K on it, giving rise to an arboreal Galois representation. Let G_ϕ be the image of such representation.

Conjecture 2.6 ([13, Conjecture 3.11]). *The index of G_ϕ in $\mathrm{Aut}(\mathcal{T})$ is finite if and only if one of the following holds:*

1. *The map ϕ is post-critically finite.*
2. *The two critical points γ_1 and γ_2 of ϕ have a relation of the form $\phi^{(r+1)}(\gamma_1) = \phi^{(r+1)}(\gamma_2)$ for some $r \geq 1$.*
3. *0 is periodic under ϕ.*
4. *There is a non-trivial Möbius transformation m that fixes 0 and such that $\phi \circ m = m \circ \phi$.*

Let now $f \in \mathcal{O}_K[x]$ be a monic polynomial of degree 2, let $f_k = f$ for every k and assume $f^{(n)}$ is irreducible for every n.

Corollary 2.7. *Let f be as above and assume Conjecture 2.6. If f is not post-critically finite, then the set of stable primes for f has density 0.*

Proof. By Corollary 2.4, it is enough to check that conditions (2),(3) and (4) are never satisfied by such a polynomial. Condition (2) clearly does not hold because f has two distinct critical points, one of which is ∞, and so it is fixed by f, and the other one is never mapped to ∞ by any iterate of f. Condition (3) cannot hold because $f^{(n)}$ is irreducible for every n by assumption. A direct computation shows that if (4) holds for an irreducible polynomial, then this polynomial must be $(x-1)^2+1$, which is post-critically finite (and conversely, such polynomial commutes with $x/(x-1)$). □

3. The automorphism group of $\mathcal{T}_n$

Let us fix a spherical index $\{d_k\}_{k\in\mathbb{N}}$ and let $\mathcal{T}$ the associated spherically homogeneous tree. In order to describe the group of automorphisms of the truncated tree $\mathcal{T}_n$, we first recall the construction of the wreath product of groups. Let G, H be two groups and R be a set on which G acts by permutations from the left. If $g \in G$ and $r \in R$, we denote by $g \cdot r$ the action of g on r. Let $H^R := \prod_{r\in R} H_r$, where each H_r is an isomorphic copy of H. The action of G extends naturally to H^R via $g \cdot (h_r)_{r\in R} = (h_{g^{-1}\cdot r})_{r\in R}$. This defines a homomorphism

$$\Phi\colon G \to \operatorname{Aut}(H^R)$$
$$g \mapsto (\varphi_g\colon (h_r)_r \mapsto g \cdot (h_r)_r).$$

The *wreath product* of G by H is defined by:

$$G \wr_R H := G \ltimes_\Phi H^R.$$

Now suppose that G is a subgroup of the symmetric group on d symbols S_d and H is a subgroup of S_e. Let $R := \{1, \ldots, d\}$ and $T = \{1, \ldots, e\}$. Then $G \wr_R H$ acts from the left on $R \times T$ via the following rule:

$$(g, (h_r)_r) \cdot (r_0, t_0) = (g \cdot r_0, h_{g\cdot r_0} \cdot t_0).$$

Theorem 3.1 ([5, Theorem 2.1.15])**.** *The automorphism group of $\mathcal{T}_n$ is isomorphic to the wreath product*

$$S_{d_1} \wr S_{d_2} \wr \ldots \wr S_{d_n}.$$

The wreath product of groups is associative and therefore Theorem 3.1 implies that we can think of $\operatorname{Aut}(\mathcal{T}_n)$ as $\operatorname{Aut}(\mathcal{T}_{n-1}) \wr S_{d_n}$; we will make use of this fact in what follows. From now on, we denote by W_n the automorphism group of $\mathcal{T}_n$.

Corollary 3.2. *The cardinality of W_n is $\displaystyle\prod_{i=1}^{n} (d_i!)^{d^{(i-1)}}$.*

Proof. If G, H are finite groups with G acting on a finite set R, it is clear from the definition that $|G \wr_R H| = |G| \cdot |H|^{|R|}$. The claim follows by an easy induction using Theorem 3.1 and the fact that $S_{d_1} \wr S_{d_2} \wr \ldots \wr S_{d_n}$ acts on $d^{(n)}$ symbols. □

Remark 3.3. It is useful to understand how elements of W_n act on the vertices of $\mathcal{T}_n$. Notice that W_n is a subgroup of $S_{d^{(n)}}$ by construction, and the set V_n of the vertices at level n has cardinality $d^{(n)}$. In fact, since automorphisms of $\mathcal{T}_n$ preserve connected vertices, in order to describe the action of W_n on the vertices of $\mathcal{T}_n$ it is enough to specify the action of W_n on V_n. For every $i \in \{1, \ldots, n\}$, let R_i be the set $\{1, \ldots, d_i\}$. Each element $v \in V_n$ can be uniquely identified by a sequence $(t_1, \ldots, t_n)$ where $t_i \in R_i$ for every i. This identification comes from labeling the descendants of a vertex at level i with the elements of R_{i+1}, so that the sequence $(t_1, \ldots, t_n)$ describes the unique path from the root of the tree to the corresponding vertex in V_n. Now, elements of W_n are of the form $(g, (h_r)_{r\in R^{(n-1)}})$, where $g \in W_{n-1}$, $h_r \in S_{d_n}$ for every r and $R^{(n-1)} = R_1 \times \ldots \times R_{n-1}$. Thus, g acts inductively on the sequence $(t_1,\dots,t_{n-1})$, yielding a new sequence $(t'_1,\dots,t'_{n-1})$, and we have that

$$(g,(h_r)_{r\in R^{(n-1)}})\cdot(t_1,\dots,t_n)=(t'_1,\dots,t'_{n-1},h_{(t'_1,\dots,t'_{n-1})}\cdot t_n).$$

4. Proof of the main theorem

Let us recall the hypotheses: let $\{f_k\}\subseteq\mathcal{O}_K[x]$ be a sequence of polynomials of spherical index $\{d_k\}$, let $G_n=\mathrm{Gal}(f^{(n)})$ and suppose that $[\mathrm{Aut}(\mathcal{T}_n):G_n]=o(d^{(n)})$. Our goal is to show that $\delta(\mathrm{St}(\{f_k\}))=0$.

Let $\mathrm{St}(f^{(n)})$ be the set of primes $\mathfrak{p}$ such that $f^{(n)}$ is irreducible modulo $\mathfrak{p}$. Notice that $\mathrm{St}(f^{(i)})\subseteq\mathrm{St}(f^{(j)})$ whenever $i\geq j$. It is immediate to see that

$$\mathrm{St}(\{f_k\})=\bigcap_{n\in\mathbb{N}}\mathrm{St}(f^{(n)}).$$

Since $\mathrm{St}(\{f_k\})\subseteq\mathrm{St}(f^{(n)})$ for every n, then $\overline{\delta}(\mathrm{St}(\{f_k\}))\leq\overline{\delta}(\mathrm{St}(f^{(n)}))$ for every n. Therefore, in order to prove Theorem 2.3 it is enough to show that $\delta(\mathrm{St}(f^{(n)}))$ exists for every n and converges to 0 as $n\to\infty$. In fact, if this happens then $\overline{\delta}(\mathrm{St}(f^{(n)}))$ converges to 0 as well, forcing $\overline{\delta}(\mathrm{St}(\{f_k\}))=0$ and finally $\delta(\mathrm{St}(\{f_k\}))=0$.

Thus, we reduced the proof of Theorem 2.3 to proving the following claim:

(♠) The density of $\mathrm{St}(f^{(n)})$ exists and converges to 0 as $n\to\infty$.

Let us now recall the following fundamental theorem, which is a weaker version of Chebotarev's density theorem.

Theorem 4.1 (Frobenius density theorem). *Let $g(x)\in\mathcal{O}_K[x]$ be monic and irreducible of degree d. Let $G\subseteq S_d$ be the Galois group of g. Let $a_1\leq a_2\leq\ldots\leq a_t$ be natural numbers such that $a_1+\ldots+a_t=d$. Let $\Gamma\subseteq G$ be the set of elements whose decomposition in disjoint cycles has the form $c_1\cdot c_2\cdot\ldots\cdot c_t$, where c_i is a cycle of length a_i. Then the set*

$$\{\textit{primes } \mathfrak{p}\subseteq\mathcal{O}_K \textit{ s.t. } g(x) \textit{ has decomposition type } (a_1,\dots,a_t) \textit{ modulo } \mathfrak{p}\}$$

has density $\dfrac{|\Gamma|}{|G|}$.

Recall that in our setting G_n is the Galois group of $f^{(n)}$, and is therefore a subgroup of $S_{d^{(n)}}$. The key lemma which allows us to prove claim (♠) is the following. Recall that $W_n=\mathrm{Aut}(\mathcal{T}_n)$.

Lemma 4.2. *Let $C_n\subseteq W_n$ be the set of cycles of length $d^{(n)}$. Then $\dfrac{|C_n|}{|W_n|}=\dfrac{1}{d^{(n)}}$.*

Let us first show that Lemma 4.2 implies claim (♠). Since $G_n\leq W_n$, the set $\Gamma_n\subseteq G_n$ of cycles of length $d^{(n)}$ is a subset of C_n. Thus, by Frobenius density theorem we get that

$$\delta(\mathrm{St}(f^{(n)}))=\frac{|\Gamma_n|}{|G_n|}\leq\frac{|C_n|}{|G_n|}=\frac{|C_n|}{|W_n|}\cdot[W_n:G_n].$$

Now Lemma 4.2, together with the fact that, by hypothesis, $[W_n:G_n]=o(d^{(n)})$, implies that $\delta(\mathrm{St}(f^{(n)}))\to 0$.

Proof of Lemma 4.2. By Corollary 3.2, the statement of the lemma is equivalent to proving that:

$$|C_n| = \prod_{i=1}^{n} (d_i - 1)!(d_i!)^{d^{(i-1)}-1}.$$

We will prove this by induction on n. For $n = 1$, the claim is true because W_1 is the symmetric group on d_1 symbols, and thus it contains exactly $(d_1 - 1)!$ cycles of length d_1. In order to prove the claim for C_n, we need a characterization of cycles of length $d^{(n+1)}$ inside W_{n+1}. For every $i \in \{1, \dots, n\}$, let $R_i := \{1, \dots, d_i\}$ and let $R^{(n)} = R_1 \times \dots \times R_n$. Recall that, by Theorem 3.1, $W_{n+1} = W_n \wr_{R^{(n)}} S_{d_{n+1}}$ for $n \geq 1$, and that for every n, W_n is naturally a subgroup of $S_{d^{(n)}}$ acting on the set of vertices of $\mathcal{T}$ at level n as explained in Remark 3.3. Let $\overline{g} = (g, (h_r)_{r \in R^{(n)}}) \in W_{n+1}$. We claim that $\overline{g} \in C_{n+1}$ if and only if the following two conditions hold:

(1) $g \in C_n$;

(2) for every $r \in R^{(n)}$, the element $\displaystyle\prod_{i=1}^{d^{(n)}} h_{g^{-i} \cdot r} \in S_{d_{n+1}}$ is a cycle of length d_{n+1}.

To prove this, let us first assume that $\overline{g} \in C_{n+1}$ and suppose that there is a cycle of length a in the decomposition of g into disjoint cycles. Then there is a vertex v of $\mathcal{T}$ at level n such that $g^a \cdot v = v$, and therefore $\overline{g}^a$ permutes the d_{n+1} vertices at level $n+1$ that descend from v. If such a permutation contains a cycle of length b, it follows that there exists a vertex w, descending from v, such that $\overline{g}^{ab} \cdot w = w$. Since $a \leq d^{(n)}$ and $b \leq d_{n+1}$, equalities must hold because $\overline{g}$ is a cycle of length $d^{(n+1)}$ and therefore no vertex at level $n+1$ can be mapped to itself with less than $d^{(n+1)}$ iterations of $\overline{g}$. This argument shows that $g \in C_n$ and that since $\overline{g}^{d^{(n)}} = \left(\text{id}, \left(\displaystyle\prod_{i=1}^{d^{(n)}} h_{g^{-i} \cdot r}\right)_{r \in R^{(n)}}\right)$, then $\displaystyle\prod_{i=1}^{d^{(n)}} h_{g^{-i} \cdot r}$ is a cycle of length d_{n+1} for every $r \in R^{(n)}$.

Conversely, let $\overline{g} = (g, (h_r)_{r \in R^{(n)}}) \in W_{n+1}$ have properties (1) and (2). Suppose that $\overline{g}$ contains a cycle of length a. Then there is a vertex v of $\mathcal{T}$ at level $n+1$ such that $\overline{g}^a \cdot v = v$, which implies in particular that $\overline{g}^a \cdot v$ has the same parent of v. Since g acts on the set of vertices at level n and is a cycle of length $d^{(n)}$, this proves that $a = d^{(n)}b$, for some $b \leq d_{n+1}$. Since $\overline{g}^{d^{(n)}} = \left(\text{id}, \left(\displaystyle\prod_{i=1}^{d^{(n)}} h_{g^{-i} \cdot r}\right)_{r \in R^{(n)}}\right)$, it follows that there exists some $r_0 \in R^{(n)}$ such that $\displaystyle\prod_{i=1}^{d^{(n)}} h_{g^{-i} \cdot r_0}$ permutes the vertices with the same parent of v. This permutation is a cycle of length d_{n+1} by (2) and this proves, together with the fact that $\overline{g}^a \cdot v = v$, that $b = d_{n+1}$, and finally that $\overline{g} \in C_{n+1}$.

We are now ready to enumerate the elements in C_{n+1}. Let g be an elment of C_n and fix $r_0 \in R^{(n)}$. For every $i \in \{1, \dots, d^{(n)}\}$ choose $h_{g^{-i} \cdot r_0} \in S_{d_{n+1}}$ such that the element

$$h := h_{g^{-1} \cdot r_0} \cdot h_{g^{-2} \cdot r_0} \cdot \dots \cdot h_{g^{-d^{(n)}} \cdot r_0}$$

is a cycle of length d_{n+1} (notice that since g is a cycle of maximal length, the set $\{g^{-1}\cdot r_0,\dots,g^{-d^{(n)}}\cdot r_0\}$ coincides with $R^{(n)}$). We claim that $\overline{g}:=(g,(h_r)_{r\in R^{(n)}})$ is a cycle of length $d^{(n+1)}$. By the characterization that we proved above, this is equivalent to proving that $h_r:=\displaystyle\prod_{i=1}^{d^{(n)}}h_{g^{-i}\cdot r}$ is a cycle of length d_{n+1} for every $r\in R^{(n)}$. Let $j\in\{1,\dots,d^{(n)}\}$ be the unique element such that $g^{-j}\cdot r=r_0$. Then $h=h_{g^{-j-1}\cdot r}\cdot h_{g^{-j-2}\cdot r}\cdot\dots\cdot h_{g^{-j-d^{(n)}}\cdot r}$, and setting

$$k:=h_{g^{-1}\cdot r}\cdot h_{g^{-2}\cdot r}\cdot\dots\cdot h_{g^{-j}\cdot r},$$

we have the equality

$$h_r=khk^{-1}.$$

This proves that h and h_r are conjugate in $S_{d_{n+1}}$, and therefore also h_r is a cycle of length d_{n+1}.

In other words, we have proved that for every $g\in C_n$, in order to construct an element $(g,(h_r)_{r\in R^{(n)}})\in W_{n+1}$ lying in C_{n+1} it is necessary and sufficient to fix $r_0\in R^{(n)}$ and to find, for every $i\in\{1,\dots,d^{(n)}\}$, an element $h_{g^{-i}\cdot r_0}\in S_{d_{n+1}}$ such that $\displaystyle\prod_{i=1}^{d^{(n)}}h_{g^{-i}\cdot r_0}$ is a cycle of length d_{n+1}. For every $g\in C_n$, we have complete freedom in choosing $h_{g^{-1}\cdot r_0},h_{g^{-2}\cdot r_0},\dots,h_{g^{-d^{(n)}+1}\cdot r_0}$, which means that we have $(d_{n+1}!)^{d^{(n)}-1}$ choices; we must then have

$$h_{g^{-d^{(n)}}\cdot r_0}=\left(\prod_{i=1}^{d^{(n)}-1}h_{g^{-i}\cdot r_0}\right)^{-1}\cdot c,$$

where c is a cycle of length d_{n+1}. This means that we are left with $(d_{n+1}-1)!$ choices for c, because this is the number of cycles of length d_{n+1}. All in all, we have $(d_{n+1}-1)!(d_{n+1}!)^{d^{(n)}-1}$ choices for every element $g\in C_n$. Since by the induction hypothesis we have that $|C_n|=\prod_{i=1}^n(d_i-1)!(d_i!)^{d^{(i-1)}-1}$, we easily get that

$$|C_{n+1}|=(d_{n+1}-1)!(d_{n+1}!)^{d^{(n)}-1}\cdot\prod_{i=1}^{n}(d_i-1)!(d_i!)^{d^{(i-1)}-1}=\prod_{i=1}^{n+1}(d_i-1)!\cdot(d_i!)^{d^{(i-1)}-1},$$

as desired. □

5. The generic case

It is a very hard problem, in general, to compute explicitly the Galois groups $G_n=\mathrm{Gal}(f^{(n)})$ for a given sequence $\{f_k\}\subseteq\mathcal{O}_K[x]$, even when such sequence is constant (see [2], [4] or [21] for examples in degree 2 and 3). It is natural to ask what is the generic behaviour of a sequence of fixed spherical index. In this section we will prove that for any fixed spherical degree $\{d_k\}$, the set of sequences $\{f_k\}$ of spherical degree $\{d_k\}$ whose associated arboreal Galois representation is surjective has density 1, in an adequate sense. This shows in particular that the set of sequences that fulful the hypotheses of Theorem 2.3 has density 1.

Let us first recall the notion of natural density for subsets of $\mathcal{O}_K^n$ (cf. [7]). Let $m := [K : \mathbb{Q}]$, fix a $\mathbb{Z}$-basis $\mathcal{B} := \{\omega_1, \ldots, \omega_m\}$ for $\mathcal{O}_K$ and define

$$\mathcal{O}_K[N, \mathcal{B}] := \left\{ \sum_{i=1}^{m} a_i \omega_i \in \mathcal{O}_K \colon |a_i| \leq N \ \forall i \in \{1, \ldots, m\} \right\}.$$

The density of a subset $A \subseteq \mathcal{O}_K^n$ (with respect to $\mathcal{B}$) is defined as

$$\mathbb{D}(A) := \lim_{N \to \infty} \frac{|A \cap \mathcal{O}_K[N, \mathcal{B}]^n|}{|\mathcal{O}_K[N, \mathcal{B}]^n|},$$

provided that the limit exists. As $\mathcal{O}_K^n$ is a countably infinite set, there is no uniform probability distribution on it. The above notion of density is to be thought as the limit, as $N \to \infty$, of the probability that a point chosen uniformly at random inside the mn-dimensional hypercube of side N and centered in the origin belongs to A, after chosing an identification of $\mathcal{O}_K^n$ with $\mathbb{Z}^{mn}$.

From now on, we will fix a spherical index $\{d_k\}_{k \in \mathbb{N}}$. For every $n \in \mathbb{N}$, let $\mathcal{X}_n := \prod_{i=1}^{n} \mathcal{O}_K^{d_i}$ and let $\mathcal{X} := \prod_{i=1}^{\infty} \mathcal{O}_K^{d_i}$. The set $\mathcal{X}_n$ can be naturally identified with the set of n-tuples of monic polynomials $\{f_1, \ldots, f_n\}$ such that each f_i has degree d_i, simply by mapping each f_i to the d_i-tuple of its coefficients in $\mathcal{O}_K^{d_i} \subseteq \mathcal{X}_n$. Analogously, the set $\mathcal{X}$ can be identified with the set of monic polynomial sequences $\{f_k\} \subseteq \mathcal{O}_K[x]$ of spherical index $\{d_k\}$. We will assume these identifications implicitly in what follows. Identifying $\mathcal{X}_n$ with $\mathcal{O}_K^{\sum_{i=1}^{n} d_i}$ in the obvious way, we get a well-defined notion of density on $\mathcal{X}_n$. Let $\pi_n \colon \mathcal{X} \to \mathcal{X}_n$ be the natural projection map.

Definition 5.1. The density of a subset $A \subseteq \mathcal{X}$ (with respect to $\mathcal{B}$) is defined as

$$\lim_{n \to \infty} \mathbb{D}(\pi_n(A)),$$

provided that the limit exists.

Again, this does not define a probability distribution on $\mathcal{X}$. However, one can think of choosing a sequence $\{f_k\}$ as an analogue of a discrete stochastic process; our definition of density on $\mathcal{X}$ serves then as an analogous of the concept of joint distribution of the process.

Recall that we denote by W_n the full automorphism group of the spherically homogeneous tree of spherical index $\{d_k\}$ truncated at level n, and that for a polynomial sequence $\{f_k\}$, we denote by G_n the Galois group of $f^{(n)} = f_1 \circ \ldots \circ f_n$. The goal of this section is to prove the following theorem.

Theorem 5.2. *Let $A \subseteq \mathcal{X}$ be the set of all polynomial sequences $\{f_k\}$ such that $G_n \simeq W_n$ for every $n \in \mathbb{N}$. Then $\mathbb{D}(\pi_n(A)) = 1$ for every n, and therefore $\mathbb{D}(A) = 1$.*

To prove the theorem, we need to recall the following results.

Theorem 5.3 ([16, Corollary 8.4])**.** *Let F be a field of characteristic 0, and let $f \in F[x]$ be monic and squarefree with Galois group G over F. For every $\ell \geq 2$, let $t_1, \ldots, t_\ell$ be indeterminates over F and let $g(x, t_1, \ldots, t_\ell) := x^\ell + t_1 x^{\ell-1} + \ldots + t_\ell \in F[x, t_1, \ldots, t_\ell]$. Then the Galois group of $f \circ g$ over $F(t_1, \ldots, t_\ell)$ is isomorphic to the wreath product $G \wr S_\ell$.*

The following theorem is stated in greater generality in [6]. We report it here in a simpler version which suffices for our purposes.

Theorem 5.4. *Let K be a number field, let $x, t_1, \dots, t_\ell$ be indeterminates over K and let $f(x, t_1, \dots, t_\ell) \in \mathcal{O}_K[x, t_1, \dots, t_\ell]$ have Galois group G over $K(t_1, \dots, t_\ell)$. Then there exist constants c_1, c_2, depending on f, K and $\mathcal{B}$, such that for all $N > c_1$, the number of ℓ-tuples $(\alpha_1, \dots, \alpha_\ell) \in \mathcal{O}_K[N, \mathcal{B}]^\ell$ such that the Galois group of $f(x, \alpha_1, \dots, \alpha_\ell)$ over K is not isomorphic to G does not exceed $c_2 N^{m(\ell-1/2)} \log N$.*

Proof. See [6, Theorem 2.1]. We remark that the set denoted by $\mathcal{O}_K[N, \mathcal{B}]$ by us, coincides with the set denoted by $\mathbb{Z}_K(N^m)$ in [6]. □

Proof of Theorem 5.2. We first notice that for every $n \in \mathbb{N}$, we have that

$$\pi_n(A) = \{(f_1, \dots, f_n) \in \mathcal{X}_n \colon \operatorname{Gal}(f^{(i)}) \simeq W_i \text{ for every } i \in \{1, \dots, n\}\}.$$

In fact, by definition the set $\pi_n(A)$ coincides with the set of n-tuples of polynomials $(f_1, \dots, f_n)$ that satisfy the following two conditions:

i) $G_i \simeq W_i$ for every $i \in \{1, \dots, n\}$;

ii) there exists a sequence of polynomials $\{f_{n+k}\}_{k\in\mathbb{N}}$ of spherical index $\{d_{n+k}\}_{k\in\mathbb{N}}$ such that $G_i \simeq W_i$ for every $i > n$.

Theorems 5.3 and 5.4 show that for every n-tuple of polynomials satisfying i) it is possible to construct a sequence (and in fact infinitely many) $\{f_{n+k}\}_{k\in\mathbb{N}}$ satisfying ii): let $(f_1, \dots, f_s) \in \mathcal{X}_s$ for some $s \geq n$ be such that $G_i \simeq W_i$ for every $i \in \{1, \dots, s\}$ and let $g \coloneqq x^{d_{s+1}} + t_1 x^{d_{s+1}-1} + \dots + t_{d_{s+1}} \in K[x, t_1, \dots, t_{d_{s+1}}]$. Then by Theorem 5.3, the polynomial $f^{(s)} \circ g$ has Galois group W_{s+1} over $K(t_1, \dots, t_{d_{s+1}})$ and by Theorem 5.4 there exist infinitely many specializations $(\alpha_1, \dots, \alpha_{d_{s+1}}) \in \mathcal{O}_K^{d_{s+1}}$ such that $(f^{(s)} \circ g)(x, \alpha_1, \dots, \alpha_{d_{s+1}})$ has Galois group W_{s+1}. Thus, it is enough to set $f_{s+1} \coloneqq g(x, \alpha_1, \dots, \alpha_{d_{s+1}})$ and to apply the same argument inductively to obtain a sequence $\{f_{n+k}\}_{k\in\mathbb{N}}$ satisfying ii).

To compute the density of $\pi_n(A)$, for every $i \in \{1, \dots, n\}$ set

$$g_i(x, t_1^{(i)}, \dots, t_{d_i}^{(i)}) \coloneqq x^{d_i} + t_1^{(i)} x^{d_i-1} + \dots + t_{d_i}^{(i)} \in K(t_1^{(i)}, \dots, t_{d_i}^{(i)})[x].$$

Here x and the $t_j^{(i)}$'s are algebraically independent indeterminates over K. It is a well-known fact (see for example [16, Corollary 7.3]) that the Galois group of g_1 over $K(t_1^{(1)}, \dots, t_{d_1}^{(1)})$ is isomorphic to S_{d_1}. Now applying Theorem 5.3 with $F = K(t_1^{(1)}, \dots, t_{d_1}^{(1)})$ it follows that the Galois group of $g_1 \circ g_2$ over $K(t_1^{(1)}, \dots, t_{d_1}^{(1)}, t_1^{(2)}, \dots, t_{d_2}^{(2)})$ is $S_{d_1} \wr S_{d_2}$. Repeating inductively the same argument shows that for every $i \in \{1, \dots, n\}$ the Galois group of $g^{(i)} \coloneqq g_1 \circ g_2 \circ \dots \circ g_i$ over $K(t_1^{(1)}, \dots, t_{d_i}^{(i)})$ is W_i. Letting $D_i \coloneqq \sum_{j=1}^{i} d_j$ for every $i \in \{1, \dots, n\}$, we therefore have that the set $\pi_n(A) \cap \mathcal{O}_K[N, \mathcal{B}]^{D_n}$ coincides with the set

$$\{(\alpha_j)_{j=1}^{D_n} \in \mathcal{O}_K[N, \mathcal{B}]^{D_n} \colon \operatorname{Gal}(g^{(i)}(x, \alpha_1, \dots, \alpha_{D_i})) \simeq W_i \ \forall\, i \in \{1, \dots, n\}\}.$$

By Theorem 5.4, we can find constants c_1, c_2, depending on all the g_i's, on $\mathcal{B}$ and on K, such that for all $N > c_1$ and for all $i \in \{1, \dots, n\}$, the number of $(\alpha_1, \dots, \alpha_{D_i}) \in$

$\mathcal{O}_K[N,\mathcal{B}]^{D_i}$ such that the Galois group of $g^{(i)}(\alpha_1,\dots,\alpha_{D_i})$ is not W_i does not exceed $c_2N^{m(D_i-1/2)}\log N$. Letting

$$B_i := \{(\alpha_1,\dots,\alpha_{D_n})\in\mathcal{O}_K[N,\mathcal{B}]^{D_n}\colon\ \mathrm{Gal}(g^{(i)}(x,\alpha_1,\dots,\alpha_{D_i}))\not\simeq W_i\}$$

for every $i\in\{1,\dots,n\}$, it follows that the cardinality of B_i is bounded by $c_2N^{m(D_n-1/2)}\log N$. Since $\mathcal{O}_K[N,\mathcal{B}]^{D_n}\setminus\pi_n(A)\subseteq\bigcup_{i=1}^n B_i$, we have that

$$|\pi_n(A)\cap\mathcal{O}_K[N,\mathcal{B}]^{D_n}|\geq|\mathcal{O}_K[N,\mathcal{B}]^{D_n}|-\sum_{i=1}^n|B_i|\geq|\mathcal{O}_K[N,\mathcal{B}]^{D_n}|-nc_2N^{m(D_n-1/2)}\log N,$$

and the claim follows simply by the fact that $|\mathcal{O}_K[N,\mathcal{B}]^{D_n}|=(2N+1)^{mD_n}$. □

Remark 5.5. It is possible prove a slightly sharper statement than the one of Theorem 5.2. One can show, using the arguments described in [19, Chapter 9], that there exists a thin set (in the sense of Serre) $S\subseteq K^{D_n}$ such that set for all $(\alpha_j)_{j=1}^{D_n}\in K^{D_n}\setminus S$, one has $\mathrm{Gal}(g^{(i)}(x,\alpha_1,\dots,\alpha_{D_i}))\simeq W_i$ for every $i\in\{1,\dots,n\}$ (we are using the notation of the proof of Theorem 5.2). It follows that $\pi_n(A)$ is "co-thin" in $\mathcal{X}_n$ for every n and therefore, in particular, it has density 1 by [19, p. 134]. On the other hand, the use of Theorem 5.4 yields a better asymptotic on $|\pi_n(A)\cap\mathcal{O}_K[N,\mathcal{B}]^{D_n}|$.

References

[1] Laurent Bartholdi, Rostislav Grigorchuk, and Volodymyr Nekrashevych. From fractal groups to fractal sets. In *Fractals in Graz 2001*, Trends Math., pages 25–118. Birkhäuser, Basel, 2003.

[2] Robert L. Benedetto, Xander Faber, Benjamin Hutz, Jamie Juul, and Yu Yasufuku. A large arboreal galois representation for a cubic postcritically finite polynomial. https://arxiv.org/abs/1612.03358, 2016.

[3] Nigel Boston and Rafe Jones. Arboreal Galois representations. *Geom. Dedicata*, 124:27–35, 2007.

[4] Nigel Boston and Rafe Jones. The image of an arboreal Galois representation. *Pure Appl. Math. Q.*, 5(1):213–225, 2009.

[5] Tullio Ceccherini-Silberstein, Fabio Scarabotti, and Filippo Tolli. *Representation theory and harmonic analysis of wreath products of finite groups*, volume 410 of *London Mathematical Society Lecture Note Series.* Cambridge University Press, Cambridge, 2014.

[6] S. D. Cohen. The distribution of Galois groups and Hilbert's irreducibility theorem. *Proc. London Math. Soc. (3)*, 43(2):227–250, 1981.

[7] Andrea Ferraguti and Giacomo Micheli. On the Mertens-Cesàro theorem for number fields. *Bull. Aust. Math. Soc.*, 93(2):199–210, 2016.

[8] Andrea Ferraguti, Giacomo Micheli, and Reto Schnyder. Irreducible compositions of degree two polynomials over finite fields have regular structure. https://arxiv.org/abs/1701.06040, 2017.

[9] Andrea Ferraguti, Giacomo Micheli, and Reto Schnyder. On sets of irreducible polynomials closed by composition. In *Arithmetic of finite fields*, volume 10064 of *Lecture Notes in Comput. Sci.*, pages 77–83. Springer, Cham, 2017.

[10] D. R. Heath-Brown and Giacomo Micheli. Irreducible polynomials over finite fields produced by composition of quadratics. `https://arxiv.org/abs/1701.05031`, 2017.

[11] Rafe Jones. The density of prime divisors in the arithmetic dynamics of quadratic polynomials. *J. Lond. Math. Soc. (2)*, 78(2):523–544, 2008.

[12] Rafe Jones. An iterative construction of irreducible polynomials reducible modulo every prime. *J. Algebra*, 369:114–128, 2012.

[13] Rafe Jones. Galois representations from pre-image trees: an arboreal survey. In *Actes de la Conférence "Théorie des Nombres et Applications"*, Publ. Math. Besançon Algèbre Théorie Nr., pages 107–136. Presses Univ. Franche-Comté, Besançon, 2013.

[14] Rafe Jones and Michelle Manes. Galois theory of quadratic rational functions. *Comment. Math. Helv.*, 89(1):173–213, 2014.

[15] Jamie Juul, Pär Kurlberg, Kalyani Madhu, and Tom J. Tucker. Wreath products and proportions of periodic points. *Int. Math. Res. Not. IMRN*, (13):3944–3969, 2016.

[16] R. W. K. Odoni. The Galois theory of iterates and composites of polynomials. *Proc. London Math. Soc. (3)*, 51(3):385–414, 1985.

[17] R. W. K. Odoni. On the prime divisors of the sequence $w_{n+1} = 1 + w_1 \cdots w_n$. *J. London Math. Soc. (2)*, 32(1):1–11, 1985.

[18] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.

[19] Jean-Pierre Serre. *Lectures on the Mordell-Weil theorem.* Aspects of Mathematics. Friedr. Vieweg & Sohn, Braunschweig, third edition, 1997. Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt, With a foreword by Brown and Serre.

[20] Joseph H. Silverman. *The arithmetic of dynamical systems*, volume 241 of *Graduate Texts in Mathematics.* Springer, New York, 2007.

[21] Michael Stoll. Galois groups over **Q** of some iterated polynomials. *Arch. Math. (Basel)*, 59(3):239–244, 1992.

University of Cambridge, DPMMS, Centre for Mathematical Sciences, Wilberforce Road, Cambridge, CB3 0WB, UK,

E-mail address: `af612@cam.ac.uk`