ITERATED MONODROMY GROUPS OF RATIONAL FUNCTIONS AND PERIODIC POINTS OVER FINITE FIELDS

ANDREW BRIDY, RAFE JONES, GREGORY KELSEY, AND RUSSELL LODGE

Abstract. Let q be a prime power and ϕ a rational function with coefficients in a finite field $\mathbb{F}_q$. For $n \geq 1$, each element of $\mathbb{P}^1(\mathbb{F}_{q^n})$ is either periodic or strictly preperiodic under iteration of ϕ. Denote by a_n the proportion of periodic elements. Little is known about how a_n changes as n grows, unless ϕ is a power map or Chebyshev polynomial. We give the first results on this question for a wider class of rational functions: a_n has lim inf 0 when q is odd and ϕ is quadratic and neither Lattès nor conjugate to a one-parameter family of exceptional maps. We also show that a_n has limit 0 when ϕ is a non-Chebyshev quadratic polynomial with strictly preperiodic finite critical point and q is an odd square. Our methods yield additional results on periodic points for reductions of post-critically finite (PCF) rational functions defined over number fields.

The difficulty of understanding a_n in general is that $\mathbb{P}^1(\mathbb{F}_{q^n})$ is a finite set with no ambient geometry. In fact, ϕ can be lifted to a PCF rational map on the Riemann sphere, where we show that a_n is given by counting elements of the iterated monodromy group (IMG) that act with fixed points at all levels of the tree of preimages. Using a martingale convergence theorem, we translate the problem to determining whether certain IMG elements exist. This in turn can be decisively addressed using the expansion of PCF rational maps in the orbifold metric.

1. Introduction

Let $\mathbb{F}_q$ denote a finite field of characteristic p, with algebraic closure $\overline{\mathbb{F}_q}$. Every $\phi(x) \in \mathbb{F}_q(x)$ acts on $\mathbb{P}^1(\overline{\mathbb{F}_q})$, and the orbit of every point under this action is defined over a finite extension of $\mathbb{F}_q$, and hence eventually enters a cycle. This allows us to make a fundamental distinction between two kinds of points in $\mathbb{P}^1(\overline{\mathbb{F}_q})$: those that lie in a cycle under ϕ, which we call *periodic*, and those that do not. For any set S on which ϕ is a self-map, denote by $\mathrm{Per}(\phi, S)$ the set of points of S that are periodic under ϕ.

Question 1.1. Fix a prime power q and rational function $\phi \in \mathbb{F}_q(x)$ of degree at least two. How does $\#\mathrm{Per}(\phi, \mathbb{P}^1(\mathbb{F}_{q^n}))/(q^n + 1)$ vary as $n \to \infty$?

There has been recent interest in questions about the periodic points of mappings in finite fields, partially motivated by an attempt to provide a rigorous analysis of

Date: March 7, 2022.

The authors thank Sarah Koch for suggesting the collaboration. Greg and Russell thank Kevin Pilgrim for fruitful research visits, and Russell acknowledges the generous support of NCTS in Taipei.

n	x^2	x^2-1	x^2-2	$\frac{x^2-2}{x^2}$	$\frac{x^2-2}{x^2-1}$	$\frac{x^2-1}{x^2}$
1	0.750	0.750	0.500	0.250	0.500	0.750
2	0.300	0.500	0.400	0.300	0.200	0.500
3	0.536	0.214	0.393	0.250	0.286	0.321
4	0.085	0.061	0.293	0.329	0.073	0.159
5	0.504	0.299	0.377	0.250	0.254	0.176
6	0.127	0.060	0.314	0.325	0.052	0.105
7	0.501	0.085	0.375	0.250	0.250	0.043
8	0.032	0.017	0.266	0.315	0.023	0.046
9	0.500	0.031	0.375	0.250	0.250	0.014
10	0.125	0.011	0.313	0.328	0.003	0.021

TABLE 1. $\#\mathrm{Per}(\phi, \mathbb{P}^1(\mathbb{F}_{3^n}))/(3^n+1)$ for various quadratic $\phi \in \mathbb{F}_3(x)$. Note that x^2-2 is a Chebyshev polynomial and $\frac{x^2-2}{x^2}$ is a Lattès map.

Pollard's famous "rho method" for integer factorization [19]. Despite this, almost nothing is known about a general answer to Question 1.1, even in a qualitative sense, except for highly constrained mappings such as power maps. Pollard's analysis of the rho method uses the heuristic that the dynamics of specific mappings mimic those of random mappings. A random mapping on a set of size k has $O(\sqrt{k})$ periodic points (see e.g. [3, Theorem 2]), so by this heuristic, $\#\mathrm{Per}(\phi, \mathbb{P}^1(\mathbb{F}_{q^n}))/(q^n+1)$ should approach zero as n grows. However, because ϕ is a rational function, it must exhibit certain non-random behavior. Crucially, the actions of ϕ on $\mathbb{P}^1(\mathbb{F}_{q^n})$ as n varies are not independent of one another. Table 1 presents some data on Question 1.1 for $q = 3$ and $\deg \phi = 2$, and suggests the complexities involved.

The answer to Question 1.1 is well understood in the case that ϕ is a power map or Chebyshev polynomial [11]. Recent work of Garton [5] sheds some light on the complementary problem of finding $\#\mathrm{Per}(\phi, \mathbb{P}^1(\mathbb{F}_{q^n}))/(q^n+1)$ when n is fixed and ϕ varies, while Juul [9] studies the size of the image set $\phi^m(\mathbb{P}^1(\mathbb{F}_{q^n}))$ for fixed m as n grows, under certain hypotheses on ϕ.

Question 1.1 is in some sense a "vertical" question, because one moves up a tower of finite fields. A "horizontal" question of similar flavor may be posed for a rational function defined over a number field K. Given $\phi \in K(x)$, for all but finitely many primes $\mathfrak{p}$ in the ring of integers $\mathcal{O}_K$ of K, one may reduce the coefficients of ϕ modulo $\mathfrak{p}$

to obtain a morphism $\phi_{\mathfrak{p}} : \mathbb{P}^1(\mathbb{F}_{\mathfrak{p}}) \to \mathbb{P}^1(\mathbb{F}_{\mathfrak{p}})$ with $\deg \phi = \deg \tilde{\phi}$, where $\mathbb{F}_{\mathfrak{p}}$ is the residue field $\mathcal{O}_K/\mathfrak{p}$. Denote by $N(\mathfrak{p})$ the norm of $\mathfrak{p}$, so that $1 + N(\mathfrak{p})$ is the size of $\mathbb{P}^1(\mathbb{F}_{\mathfrak{p}})$.

Question 1.2. Let K be a number field, and let $\phi \in K(x)$ have degree at least two. How does $\#\mathrm{Per}(\phi_{\mathfrak{p}}, \mathbb{P}^1(\mathbb{F}_{\mathfrak{p}}))/(1 + N(\mathfrak{p}))$ vary as $N(\mathfrak{p}) \to \infty$?

The known approaches to Questions 1.1 and 1.2 proceed via Galois theory. When all the critical points of ϕ have independent, infinite orbits, the Galois groups that arise (see Definition 1.6) are relatively well-understood, and in fact are iterated wreath products in general. This has led to significant progress on Question 1.2 in this case [10]. At the other extreme lie ϕ for which all critical points have finite orbits, called post-critically finite (PCF). Here the relevant Galois groups are quite different – they are finitely generated and so far little understood in arithmetic contexts. By definition every $\phi \in \mathbb{F}_q(x)$ is PCF, and this in large part accounts for our collective state of ignorance on Question 1.1.

However, Galois groups related to PCF rational functions have been studied in some depth in the setting of complex dynamics. In this article we harness ideas from complex dynamics to give results on Question 1.1 for quadratic maps, and to address Question 1.2 in the PCF case.

Theorem 1.3. *Let $\mathbb{F}_q$ be a finite field of odd characteristic, and let $\phi(x) \in \mathbb{F}_q(x)$ have degree 2. Assume that ϕ is not a Lattès map or Möbius-conjugate over $\overline{\mathbb{F}_q}$ to a map of the form $(x^2 + a)/(x^2 - (a + 2))$ for $a \in \overline{\mathbb{F}_q}$. Then*

$$\liminf_{n\to\infty} \frac{\#\mathrm{Per}(\phi, \mathbb{P}^1(\mathbb{F}_{q^n}))}{q^n + 1} = 0. \tag{1.1}$$

Indeed we show something slightly stronger (see Theorem 3.1): for every $\epsilon > 0$ there exists $m \geq 1$ such that

$$\frac{\#\mathrm{Per}(\phi, \mathbb{P}^1(\mathbb{F}_{q^{mk}}))}{q^{mk} + 1} < \epsilon \tag{1.2}$$

for sufficiently large integers k. See Section 2 for a definition of Lattès maps over $\mathbb{F}_q$ and a classification of the maps to which Theorem 1.3 does not apply. We remark that being $\overline{\mathbb{F}_q}$-conjugate to a map of the form $(x^2 + a)/(x^2 - (a + 2))$ is equivalent to having a critical point that maps to a fixed point after two iterations; in particular, this family includes the degree-2 Chebyshev polynomial. Among quadratic maps up to $\overline{\mathbb{F}_q}$-conjugacy, there are eight Lattès maps, unless $\mathbb{F}_q$ has characteristic 7 (see Section 2). None of the maps in Table 1 apart from $x^2 - 2$ and $\frac{x^2-1}{x^2}$ is $\overline{\mathbb{F}_3}$-conjugate to a map of the form $(x^2 + a)/(x^2 - (a + 2))$.

The equality (1.1) in Theorem 1.3 does not hold for all quadratic $\phi \in \mathbb{F}_q(x)$. For the degree-two monic Chebyshev polynomial $\phi(x) = x^2 - 2$, it is shown in [11] that the lim inf in (1.1) is $1/4$, and indeed a complete accounting of $\#\mathrm{Per}(\phi, \mathbb{P}^1(\mathbb{F}_{q^n}))/(q^n + 1)$ is given for this map [11, Theorem 5.6]. We prove in Theorem 2.5 that the lim inf

in (1.1) is at least 1/8 for a certain class of quadratic Lattès maps. We suspect that the lim inf is positive for other Lattès maps of degree 2, but that the lim inf is zero for non-Chebyshev, non-Lattès maps that are $\overline{\mathbb{F}_q}$-conjugate to $(x^2+a)/(x^2-(a+2))$. However, our methods do not allow us to prove this at present.

The integer m in (1.2) depends on the constant field extension contained within the splitting fields of $\phi^n(x)-t$ over $\mathbb{F}_q(t)$ (we use ϕ^n to denote the nth iterate of ϕ, and take $\phi^0(x)=x$). When ϕ is a quadratic polynomial with non-periodic critical point, results of Pink [17] imply that $m \leq 2$ for all ϵ, provided that ϕ is not conjugate to a Chebyshev polynomial. In fact, when q is a square, $m=1$ regardless of ϵ, and we obtain:

Theorem 1.4. *Let $\mathbb{F}_q$ be a finite field of odd characteristic, and let $\phi \in \mathbb{F}_q[x]$ have degree 2. Suppose that q is a square and the unique finite critical point of ϕ is strictly preperiodic. If ϕ is not $\overline{\mathbb{F}_q}$-conjugate to a Chebyshev polynomial, then*

$$\lim_{k\to\infty} \frac{\#\mathrm{Per}(\phi, \mathbb{P}^1(\mathbb{F}_{q^k}))}{q^k+1} = 0. \tag{1.3}$$

We turn now to Question 1.2. The principal known results are those in [10], and concern the case where ϕ is "post-critically generic" in the sense that for all $m, n \geq 0$ and all critical points γ and γ' of ϕ, we have $\phi^n(\gamma) \neq \phi^m(\gamma')$ unless $m=n$ and $\gamma=\gamma'$. In this case, Theorem 1.3 of [10] gives

$$\liminf_{N(\mathfrak{p})\to\infty} \frac{\#\mathrm{Per}(\phi_{\mathfrak{p}}, \mathbb{P}^1(\mathbb{F}_{\mathfrak{p}}))}{1+N(\mathfrak{p})} = 0. \tag{1.4}$$

We establish (1.4) for many PCF rational functions. To state our result we require two definitions. First, a rational function with coefficients in a field K is *dynamically exceptional*[1] if there is $\Gamma \subset \mathbb{P}^1(\overline{K})$ with $\phi^{-1}(\Gamma) \setminus C_\phi = \Gamma$, where $C_\phi \subset \mathbb{P}^1(\overline{K})$ is the set of critical points of ϕ. Observe that this condition implies that Γ contains no critical points of ϕ, and that $\phi^{-1}(\Gamma)$ consists of Γ and a subset of C_ϕ. Second, let $\phi \in \mathbb{C}(x)$, P_ϕ be the post-critical set of ϕ (see Definition 2.1), and $z_0 \in \mathbb{C} \setminus P_\phi$. We say ϕ has *doubly transitive monodromy* if the monodromy action of $\pi^1((\mathbb{P}^1(\mathbb{C}) \setminus P_\phi), z_0)$ on $\phi^{-1}(z_0)$ is doubly transitive. Equivalently, the Galois group of $\phi(x)-t$ over $\mathbb{C}(t)$ acts doubly transitively on the roots of $\phi(x)-t$ in $\overline{\mathbb{C}(t)}$.

Theorem 1.5. *Let K be a number field and let $\phi \in K(x)$ have degree $d \geq 2$. Assume that ϕ is PCF and not dynamically exceptional. Then* (1.4) *is true if any of the following holds:*

1. *d is prime;*
2. *ϕ has doubly transitive monodromy;*
3. *ϕ is $\overline{K}$-conjugate to polynomial.*

[1] In other work, such as [8], the terminology *exceptional* is used. However, in the arithmetic setting treated in this article, an *exceptional rational function* has a pre-existing, and quite distinct, meaning.

The lim inf in (1.4) is not zero for all ϕ. In [10, Example 7.2], it is shown that when $\phi = T_d$, the degree-d monic Chebyshev polynomial, the lim inf in (1.4) is $1/4$ when d is a power of 2, $1/2$ when d is a power of an odd prime, and 0 otherwise.

Questions 1.1 and 1.2 are linked in more than an intuitive sense. By studying a single Galois-theoretic object, we prove Theorems 1.3 and 1.5 simultaneously.

Definition 1.6. Let k be a field with algebraic closure $\overline{k}$ and let $\phi \in k(x)$ have degree $d \geq 2$. Assume that for all $n \geq 1$, $\phi^n(x) = t$ has d^n distinct solutions in an algebraic closure of $\overline{k}(t)$. The *profinite geometric iterated monodromy group* of ϕ over k, written $\mathrm{pgIMG}(\phi)/k$, is the inverse limit as $n \to \infty$ of the Galois groups of $\phi^n(x) - t$ over $\overline{k}(t)$.

The terminology *geometric* in the definition is because the Galois groups are considered over the ground field $\overline{k}(t)$. One can also consider the Galois groups over $k(t)$, and this object is known as the profinite arithmetic iterated monodromy group of ϕ. See Section 3 for precise definitions and [8, Section 2] or [17] for more discussion.

Crucially for the considerations in this article, $\mathrm{pgIMG}(\phi)/k$ comes equipped with a natural action on the tree of preimages

$$T_k(\phi) := \bigsqcup_{n \geq 0} \phi^{-n}(t) \subset \overline{k(t)},$$

where $\phi^{-n}(t) = \{\alpha \in \overline{k(t)} : \phi^n(\alpha) = t\}$ for $n \geq 0$ and edges are assigned according to the action of ϕ. Let $d = \deg \phi$, and assume that the characteristic of k is either 0 or does not divide d. Then $\phi^n(x) = t$ has d^n distinct solutions in an algebraic closure of $\overline{k}(t)$, and hence $T_k(\phi)$ is a complete d-ary rooted tree, with root t. The action of $\mathrm{pgIMG}(\phi)/k$ on $T_k(\phi)$ comes from the natural action of Galois groups on the roots of polynomials.

We describe an abstract complete d-ary rooted tree as the set X^* of all words in the alphabet $X = \{0, \ldots, d-1\}$, with an edge connecting vx to v for each $v \in X^*$ and $x \in X$. The root of X^* is the empty word. Denote by X^n the set of words in X of length n, which gives the nth level of X^*. Let $\mathrm{Aut}(X^*)$ be the set of tree automorphisms, and note that any $G \leq \mathrm{Aut}(X^*)$ has quotient groups $G_n \leq \mathrm{Aut}(X^n)$ for $n \geq 1$ that are the image of the natural restriction maps. Define the *fixed-point proportion* of G_n to be

$$\mathrm{FPP}(G_n) := \frac{\#\{g \in G_n : g \text{ fixes at least one element of } T_n\}}{\#G_n}, \tag{1.5}$$

and the fixed-point proportion of G to be $\lim_{n\to\infty} \mathrm{FPP}(G_n)$. Observe that the sequence is non-increasing, and hence the limit must exist. Through the action of $\mathrm{pgIMG}(f)/k$ on $T_k(\phi)$, we identify the former with a subgroup of $\mathrm{Aut}(X^*)$. This subgroup is unique up to conjugacy in $\mathrm{Aut}(X^*)$, and in particular $\mathrm{FPP}(\mathrm{pgIMG}(\phi)/k)$ is well-defined.

In Section 3 we use the Chebotarev density theorem for function fields to show that if $\mathbb{F}_q$ is a finite field of characteristic p, $\phi \in \mathbb{F}_q(x)$ has degree d, and $p > d$, then

$$\liminf_{n\to\infty} \frac{\#\mathrm{Per}(\phi, \mathbb{P}^1(\mathbb{F}_{q^n}))}{q^n+1} \leq \mathrm{FPP}(\mathrm{pgIMG}(\phi)/\mathbb{F}_q).$$

See Corollary 3.5. Building on results in [10], we show in Theorem 3.11 that if K is a number field and $\phi \in K(x)$, then

$$\liminf_{N(\mathfrak{p})\to\infty} \frac{\#\mathrm{Per}(\phi_{\mathfrak{p}}, \mathbb{F}_{\mathfrak{p}})}{1+N(\mathfrak{p})} \leq \mathrm{FPP}(\mathrm{pgIMG}(\phi)/\mathbb{C}). \tag{1.6}$$

We appeal to work of Pink [16] to show that when q is odd and $\phi \in \mathbb{F}_q(x)$ is quadratic, there is a map $\tilde{\phi} \in \mathbb{C}(x)$ with the same ramification portrait[2] as ϕ, such that $\mathrm{pgIMG}(\phi)/\mathbb{F}_q$ and $\mathrm{pgIMG}(\tilde{\phi})/\mathbb{C}$ have conjugate actions on their respective trees (Theorem 3.9), and in particular

$$\mathrm{FPP}(\mathrm{pgIMG}(\phi)/\mathbb{F}_q) = \mathrm{FPP}(\mathrm{pgIMG}(\tilde{\phi})/\mathbb{C}). \tag{1.7}$$

In light of (1.6) and (1.7), we study $\mathrm{pgIMG}(f)/\mathbb{C}$ for arbitrary PCF $f \in \mathbb{C}(x)$. Let P_f be the post-critical set of f, and $z_0 \in \mathbb{C} \setminus P_f$. The iterated monodromy group of f, denoted $\mathrm{IMG}(f)$, is the quotient of the fundamental group $\pi_1((\mathbb{P}^1(\mathbb{C}) \setminus P_f, z_0)$ by the subgroup acting trivially by monodromy on the tree of preimages $T_{f,z_0} \subset \mathbb{C}$ of z_0 under f (Definition 4.6). Through its action on T_{f,z_0}, one can identify $\mathrm{IMG}(f)$ with a subgroup of $\mathrm{Aut}(X^*)$ (even in an explicit way; see Definition 4.7 or [15, Section 5.2]), which is unique up to conjugacy in $\mathrm{Aut}(X^*)$. After conjugating if necessary, we may assume

$$\mathrm{IMG}(f) \subset \mathrm{pgIMG}(f)/\mathbb{C} \subseteq \mathrm{Aut}(X^*).$$

Moreover, $\mathrm{pgIMG}(f)/\mathbb{C}$ is the closure in $\mathrm{Aut}(X^*)$ of $\mathrm{IMG}(f)$ [15, Proposition 6.4.2], and thus both have the same quotients $G_n \leq \mathrm{Aut}(X^n)$. In particular,

$$\mathrm{FPP}(\mathrm{pgIMG}(f)/\mathbb{C}) = \mathrm{FPP}(\mathrm{IMG}(f)).$$

See Section 4.2 for details. In light of this, we study FPP of iterated monodromy groups. The following is our main result in this direction.

Theorem 1.7. *Let f be a PCF rational function of degree $d \geq 2$ with coefficients in $\mathbb{C}$, and assume that f is not dynamically exceptional. If either d is prime or f has doubly transitive monodromy, then $FPP(IMG(f)) = 0$.*

Crucially for our proof of Theorem 5.1, $\mathrm{IMG}(f)$ is a self-similar, level-transitive, recurrent subgroup of $\mathrm{Aut}(X^*)$ (see Section 4.1 for definitions). In the case where f is a PCF polynomial, Theorem 1.1 of [8] proves that $\mathrm{FPP}(\mathrm{IMG}(f)) = 0$. To prove Theorem 1.7, we must generalize the group-theoretic tools of [8], which presents considerable technical obstacles.

[2]This is the natural graph encoding the dynamics and local degrees of the critical orbits of ϕ. See Section 2 for a precise definition.

First, one loses the special element of $\mathrm{IMG}(f)$ that arises from monodromy at infinity. For polynomial f, this gives a spherically transitive element in $\mathrm{IMG}(f)$, which is used in [8] to prove the crucial assertion that the fixed-point process associated to $\mathrm{IMG}(f)$ is a martingale. See Section 5 for definitions. To draw the same conclusion for non-polynomial f, we show that if f has prime degree or doubly transitive monodromy, then the fixed-point process attached to $\mathrm{IMG}(f)$ is a martingale (Corollaries 5.11 and 5.13). Indeed, when d is prime Corollary 5.11 gives the same conclusion for the fixed point process attached to any self-similar, level-transitive subgroup of $\mathrm{Aut}(X^*)$.

Second, once one knows that the fixed-point process of $\mathrm{IMG}(f)$ is a martingale, one can prove $\mathrm{FPP}(\mathrm{IMG}(f)) = 0$ provided that every element of the set

$$\mathcal{N}_1 := \{g \in \mathrm{IMG}(f) : g(w) = w \text{ and } g|_w = g \text{ for some } w \in X^*\} \tag{1.8}$$

fixes infinitely many ends of X^*, i.e. infinite paths through X^* beginning in X^0. (See Section 4 for definitions and see Theorem 5.1 for the result.) When f is a polynomial, this last assertion is proved in [8] using a result of Nekrashevych [15, Corollary 6.10.7] showing that the actions on $\mathrm{Aut}(X^*)$ of a set of generators for $\mathrm{IMG}(f)$ may be given by the states of a finite automaton satisfying certain strong properties. No equivalent result exists for general rational functions, and indeed until recently very few IMGs have even been computed for non-polynomial rational functions.

Using tools from complex dynamics, we show:

Theorem 1.8. *Let f be a PCF rational function of degree $d \geq 2$ with coefficients in $\mathbb{C}$. Then every element of $\mathcal{N}_1$ fixes infinitely many ends of X^* if and only if f is not dynamically exceptional.*

See Section 6. The main ingredient in the proof of Theorem 1.8 is the fact that a PCF $f \in \mathbb{C}(x)$ is subhyperbolic, i.e., expanding (in some orbifold metric) away from post-critical periodic points. This expansion forces lifts of loops under iterates of f to contract, which imposes strong conditions on elements of $\mathcal{N}_1$. In particular, an element of $\mathcal{N}_1$ that fixes only finitely many ends of X^* must be a loop encircling (in $\widehat{\mathbb{C}} \setminus P_f$) a single repelling periodic point in P_f, and moreover every backward orbit of this point must either remain in P_f or contain a critical point. This forces f to be dynamically exceptional.

2. Dynamically exceptional rational functions over finite fields

In this section we study the exceptions to Theorem 1.3. In particular, we discuss Lattès maps over finite fields and give a characterization of dynamically exceptional quadratic rational functions over an arbitrary field of characteristic $\neq 2$.

Recall from Section 1 that a rational function with coefficients in a field K is dynamically exceptional if there is $\Gamma \subset \mathbb{P}^1(\overline{K})$ with $\phi^{-1}(\Gamma) \setminus C_\phi = \Gamma$, where $C_\phi \subset \mathbb{P}^1(\overline{K})$ is the set of critical points of ϕ. In this section we study dynamically exceptional rational functions of degree 2 over an arbitrary field of characteristic different from 2.

Let K be a field with fixed algebraic closure $\overline{K}$, and let $\phi \in K(x)$. For $\alpha \in \mathbb{P}^1(\overline{K})$ with $\alpha \neq \infty$ and $\phi(\alpha) \neq \infty$, the *ramification index* $e_\phi(\alpha)$ of ϕ at α is the multiplicity of α as a root of the numerator of $\phi(x) - \phi(\alpha)$. If $\alpha = \infty$ or $\phi(\alpha) = \infty$, then $e_\phi(\alpha) = e_{\mu\circ\phi\circ\mu^{-1}}(\mu(\alpha))$, where μ is a Mobius transformation mapping both α and $\phi(\alpha)$ away from infinity. We call α a critical point for ϕ if $e_\phi(\alpha) > 1$.

Define the *ramification portrait* of ϕ to be the edge-labeled directed graph whose vertex set is the union of the orbits of all critical points of $\phi \in \mathbb{P}^1(\overline{K})$, and where each vertex α has an arrow to $\phi(\alpha)$ with label $e_\phi(\alpha)$. Note that the graph is not vertex-labeled, so we do not record the specific points involved.

For instance, if K has characteristic not equal to 2, then $\phi(x) = (x^2-2)/x^2$ has critical points 0 and ∞, with $0 \to \infty \to 1 \to -1 \to -1$. This gives ramification portrait $\bullet \xrightarrow{2} \bullet \xrightarrow{2} \bullet \to \bullet \circlearrowleft$. Because we deal here with quadratic maps, and so every critical point α has $e_\phi(\alpha) = 2$, we rewrite this as

$$\bullet \to \bullet \to \circ \to \circledcirc, \tag{2.1}$$

where $\bullet$ denotes a critical point, $\circ$ a non-critical point, and $\circledcirc$ a non-critical fixed point. Denote a critical fixed point by $\odot$. As another example, if ϕ is the degree-2 Chebyshev polynomial $x^2 - 2$, then ϕ has ramification portrait

$$\odot \qquad \bullet \to \circ \to \circledcirc, \tag{2.2}$$

We note that the ramification portraits in (2.1) and (2.2) uniquely determine ϕ up to Mobius conjugation.

The next definition is used throughout the remainder of the paper.

Definition 2.1. Let K be a field and $\phi \in K(x)$. Let $\gamma_1, \ldots, \gamma_j$ be the critical points of ϕ, which lie in $\mathbb{P}^1(\overline{K})$. The *post-critical* set of ϕ is

$$P_\phi := \bigcup_{i=1}^{j} \bigcup_{k\geq 1} \phi^k(\gamma_i) \subset \mathbb{P}^1(\overline{K}).$$

For the purposes of this article, we define $\phi \in K[x]$ to be a *Lattès map* if there exists a function $r : \mathbb{P}^1(\overline{K}) \to \mathbb{Z}$ such that

$$r(\phi(\alpha)) = e_\phi(\alpha) r(\alpha) \text{ and } r(\alpha) = 1 \text{ outside of } P_\phi. \tag{2.3}$$

When K is a finite field, these are precisely the liftable maps that lift to Lattès maps defined over $\mathbb{C}$ (see Section 3 for a definition of lifting). This is because over $\mathbb{C}$, the existence of the function r is equivalent to the usual definition of Lattès maps as given by a finite quotient of a self-map of an elliptic curve; see [14, Theorem 4.1].

Proposition 2.2. *Let K be a field of characteristic not equal to 2, and let $\phi \in K(x)$ have degree 2. Then ϕ is a Lattès map if and only if the ramification portrait of ϕ is the one in* (2.1) *or one of the following:*

$$\bullet \to \circ \to \circledcirc \quad \bullet \to \circ \to \circledcirc, \qquad \bullet \to \circ \to \circ \rightleftarrows \circ \leftarrow \circ \leftarrow \bullet \tag{2.4}$$

$$\bullet \longrightarrow \circ \longrightarrow \circ \longleftarrow \circ \longleftarrow \bullet \qquad \downarrow \qquad \circledcirc \tag{2.5}$$

Proof. Let $\Delta = \{\alpha \in \mathbb{P}^1(\overline{K}) : r(\alpha) > 1\}$. By definition of r, we have $\Delta = P_\phi$ and $\phi^{-1}(\Delta) = \Delta \cup C_\phi$. Thus

$$2\#\Delta = \sum_{\alpha \in \phi^{-1}(\Delta)} e_\phi(\alpha) \leq \#\Delta + 2\#C_\phi, \tag{2.6}$$

with equality if and only if Δ and C_ϕ are disjoint. Because K has characteristic not equal to 2, $\#C_\phi = 2$, and we conclude from (2.6) that $\#\Delta \leq 4$, with equality if and only if $\Delta \cap C_\phi = \emptyset$.

Suppose that $\#\Delta < 4$, and let $\gamma \in \Delta \cap C_\phi$. Observe that $\phi^{-1}(\gamma) \subset C_\phi \cup P_\phi$ and thus if $\phi^{-1}(\gamma)$ contains no critical points, then $\phi^{-1}(\gamma)$ consists of two post-critical points. But there is only one critical point of ϕ besides γ, so it is impossible for both points in $\phi^{-1}(\gamma)$ to be post-critical. Hence $\phi^{-1}(\gamma)$ consists of a critical point. Now γ cannot be periodic, for otherwise $r(\gamma)$ is not well-defined. Hence if $\phi(\gamma)$ is periodic, then it is a fixed point. But then $\phi^{-1}(\phi(\gamma))$ contains both γ and $\phi(\gamma)$, which is impossible. Hence $\phi(\gamma)$ cannot be periodic. Because $\#\Delta \leq 3$, it must be the case that $\phi^2(\gamma)$ is a fixed point, and we have ramification portrait (2.1).

Suppose now that $\#\Delta = 4$, and thus $P_\phi \cap C_\phi = \emptyset$. Because ϕ cannot have a periodic critical point, P_ϕ must contain a cycle, and for each α in this cycle, $\phi^{-1}(\alpha)$ cannot contain a critical point, as otherwise $\phi^{-1}(\alpha)$ consists only of a critical point, which must then be periodic. It follows that the length of this cycle can be at most 2. If P_ϕ contains a 2-cycle, one easily checks that the only possible ramification portrait is the second one in (2.4).

Now a fixed point in P_ϕ cannot have a pre-image that is a critical point, and hence P_ϕ can contain at most two fixed points. If there are exactly two, then we must have the first ramification portrait in (2.4). If there is only one, then we must have the ramification portrait in (2.5). □

We now describe quadratic Lattès maps over a field of characteristic not equal to 2. We use the normal form $\phi(x) = (x^2 + a)/(x^2 + b), a \neq b$, which exists for every degree-2 rational function except those conjugate over $\overline{K}$ to $x^{\pm 2}$, and can be obtained by conjugating a map's two critical points to 0 and ∞, and then conjugating again so $\phi(\infty) = 1$. We observe that this conjugation is defined over K if and only if the map's critical points lie in K; otherwise the conjugation is over a quadratic extension of K. The normal form is unique except that if $ab \neq 0$, then conjugation by $x \mapsto a/(bx)$ takes $(x^2 + a)/(x^2 + b)$ to $(x^2 + (a^2/b^3))/(x^2 + (a/b^2))$. This is the normal form found in [16], and is related to the normal form for critically marked quadratic rational functions given in [12, Section 6].

Proposition 2.3. *If K is a field of characteristic not equal to 2, then every degree-2 Lattès map is conjugate (over $\overline{K}$) to one of the following:*

$$\frac{x^2-2}{x^2}, \qquad \frac{x^2+\alpha_1}{x^2-\alpha_1}, \qquad \frac{x^2+\alpha_2}{x^2-\alpha_2}, \qquad \frac{x^2+\alpha_3}{x^2-(\alpha_3+2)}, \qquad \frac{x^2+\frac{1}{\alpha_3}}{x^2-\frac{1}{\alpha_3+2}}, \tag{2.7}$$

where α_1 is a root of y^2+1 (in $\overline{K}$), α_2 is a root of y^2-2y-1, and α_3 is a root of y^2+5y+8.

Remark. The two maps $\frac{x^2+\alpha_2}{x^2-\alpha_2}$, where α_2 is either root of y^2-2y-1, are in fact conjugate to each other by $x \mapsto -1/x$. Otherwise, no two maps in (2.7) are conjugate. Hence there are 8 conjugacy classes of Lattès maps (over $\overline{K}$) if K has characteristic not equal to 7. If K has characteristic 7, then y^2+5y+8 has only one root in $\overline{K}$, and hence there are only 6 conjugacy classes of Lattès maps.

Proof. Let $\phi \in K(x)$ be a degree-2 Lattès map. It follows from Proposition 2.2 that ϕ is not conjugate to $x^{\pm 2}$, and hence we may write $\phi(x) = (x^2+a)/(x^2+b)$ for some $a, b \in \overline{K}$ with $a \neq b$. Each of the ramification portraits described in Proposition 2.2 then gives rise to two polynomial conditions on a and b. For instance, the portrait in (2.5) forces $\phi^2(0) = \phi^2(\infty)$, which implies $b = -a$. The same portrait implies $\phi^4(\infty) = \phi^3(\infty)$, which gives $(a^2+1)(a^2-2a-1) = 0$. The ramification portrait (2.1) leads to the first map in (2.7), and the portraits in (2.4) lead to the fourth and fifth maps in (2.7), respectively. □

We now give our characterization of dynamically exceptional quadratic rational functions.

Proposition 2.4. *Let K be a field of characteristic $\neq 2$, and let $\phi \in K(x)$ have degree 2. Then ϕ is dynamically exceptional if and only if ϕ is a Lattès map or conjugate over $\overline{K}$ to $(x^2+a)/(x^2-(a+2))$ for some $a \in \overline{K}$.*

Remark. Maps conjugate to the degree-2 Chebyshev polynomial, as well as Lattès maps with ramification portrait (2.4), are conjugate to $(x^2+a)/(x^2-(a+2))$ for appropriate $a \in \overline{K}$.

Proof. By definition, there is $\Gamma \subset \mathbb{P}^1(\overline{K})$ with $\phi^{-1}(\Gamma) \setminus C_\phi = \Gamma$. This implies that $\Gamma \subseteq \phi^{-1}(\Gamma)$ and $\Gamma \cap C_\phi = \emptyset$. Hence

$$2\#\Gamma = \sum_{\alpha \in \phi^{-1}(\Gamma)} e_\phi(\alpha) = \#\Gamma + 2\#(\phi^{-1}(\Gamma) \cap C_\phi), \tag{2.8}$$

and it follows that $\#\Gamma \in \{2, 4\}$, according to whether $\#(\phi^{-1}(\Gamma) \cap C_\phi)$ is 1 or 2.

First suppose that $\#\Gamma = 2$ and $\phi^{-1}(\Gamma)$ contains a single critical point c. Because $\phi(\Gamma) \subseteq \Gamma$, c cannot be periodic, for then $c \in \Gamma$. Similarly, $\phi(c)$ cannot be periodic, for then its unique preimage c must be periodic as well. Thus $\phi^2(c)$ is a fixed point for ϕ, and after conjugation we may assume $c = \infty$, $\phi(c) = 1$, and $\phi^2(c) = -1$,

giving the map $(x^2+a)/(x^2-(a+2))$ for some $a \in \overline{K}$. We remark that any map with ramification portrait (2.4) or (2.2), and hence any map conjugate to the degree-2 Chebyshev polynomial, is a special case.

Now suppose that $\#\Gamma = 4$, and $\phi^{-1}(\Gamma)$ contains both critical points of ϕ, i.e., $\phi^{-1}(\Gamma) = \Gamma \cup C_\phi$. Then we may define a function $r : \mathbb{P}^1(\overline{K}) \to \mathbb{Z}$ satisfying (2.3) by taking $r(\alpha) = 2$ for $\alpha \in \Gamma$ and $r(\alpha) = 1$ for $\alpha \notin \Gamma$. Hence ϕ is a Lattès map. □

In general we expect a Lattès map ϕ defined over a finite field $\mathbb{F}_q$ to satisfy

$$\liminf_{n\to\infty} \frac{\#\mathrm{Per}(\phi, \mathbb{P}^1(\mathbb{F}_{q^n}))}{q^n+1} > 0,$$

much as happens with Chebyshev polynomials [11]. Using work of Ugolini [21], we prove this happens in a certain case:

Theorem 2.5. *Let $K = \mathbb{F}_p$ with $p \equiv 1 \bmod 4$, and suppose that ϕ is conjugate over K to the Lattès map $\frac{x^2+a}{x^2-a}$, where $a \in K$ and $a^2+1=0$. Then*

$$\liminf_{n\to\infty} \frac{\#\mathrm{Per}(\phi, \mathbb{P}^1(\mathbb{F}_{p^n}))}{p^n+1} \geq \frac{1}{8} \tag{2.9}$$

Remark. There are ϕ that are $\overline{K}$-conjugate to $\frac{x^2+a}{x^2-a}$, where $a \in K$ with $a^2+1=0$, but not K-conjugate to any such map. Indeed, if ϕ is $\overline{K}$-conjugate to a map of this kind, then it is K-conjugate to such a map if and only if its critical points lie in K.

Proof. Because ϕ is conjugate over K to a map whose critical points are defined over K, the critical points of ϕ must be defined over K. Applying a conjugacy that moves these critical points to ± 1, we see that ϕ is conjugate over K to $\psi(x) = k(x+x^{-1})$, where $k^2 + \frac{1}{4} = 0$. As detailed in [21, Section 3], the map ψ descends from a degree-2 endomorphism on the elliptic curve $y^2 = x^3 + x$ defined over $\mathbb{F}_p$, which has endomorphism ring $R := \mathbb{Z}[i]$. Moreover, because $p \equiv 1 \bmod 4$, the two degree-2 maps in R, namely $[1 \pm i]$, are both defined over $\mathbb{F}_p$, and indeed have the form $(x,y) \mapsto (\psi(x), y\tau(x))$ with $\tau(x) = c(x^2-1)/x^2 \in \mathbb{F}_p(x)$.

Our analysis of the action of ψ on $\mathbb{P}^1(\mathbb{F}_{p^n})$ begins by partitioning $\mathbb{P}^1(\mathbb{F}_{p^n})$ into two ψ-invariant sets which, by the Hasse bound, have approximately equal size when p^n is large. Let S be the three roots of x^3+x, which lie in $\mathbb{F}_p$ since $p \equiv 1 \bmod 4$. Set

$$A_n = \begin{cases} \{x \in \mathbb{F}_{p^n} : \text{there is } y \in \mathbb{F}_{p^n} \text{ with } (x,y) \in E(\mathbb{F}_{p^n})\} \cup \{\infty\} & \text{if } \sqrt{2} \in \mathbb{F}_{p^n} \\ \{x \in \mathbb{F}_{p^n} : \text{there is } y \in \mathbb{F}_{p^n} \text{ with } (x,y) \in E(\mathbb{F}_{p^n})\} \setminus S & \text{if } \sqrt{2} \notin \mathbb{F}_{p^n} \end{cases}$$

and take $B_n = \mathbb{P}^1(\mathbb{F}_{p^n}) \setminus A_n$.

Because endomorphisms of E preserve $E(\mathbb{F}_{p^n})$, we immediately have $\psi(A_n) \subseteq A_n$ if $\sqrt{2} \in \mathbb{F}_{p^n}$. If $\sqrt{2} \notin \mathbb{F}_{p^n}$ and $\alpha \in A_n$, then $\psi(\alpha) \in A_n$ unless $\psi(\alpha) \in S$. But $\psi^{-1}(S) = S \cup \{\pm 1\}$, and $\pm 1 \notin A_n$ since $\sqrt{2} \notin \mathbb{F}_{p^n}$. Thus $\psi^{-1}(S) \cap A_n = \emptyset$. Suppose now that $\alpha \in B_n$, and let β satisfy $(\alpha, \beta) \in E(\overline{\mathbb{F}}_p)$. The y-coordinate of $[1 \pm i](\alpha, \beta)$ has

the form $\beta\tau(\alpha)$. But $\tau(\alpha) \in \mathbb{F}_{p^n}$, so $\beta\tau(\alpha) \in \mathbb{F}_{p^n}$ if and only if $\beta \in \mathbb{F}_{p^n}$ or $\tau(\alpha) = 0$ (i.e. $\alpha = \pm 1$). If $\sqrt{2} \in \mathbb{F}_{p^n}$, then $\{\pm 1\} \cap B_n = \emptyset$, whence $\psi(B_n) \subseteq B_n$. If $\sqrt{2} \notin \mathbb{F}_{p^n}$, then the entire orbits of ± 1 under ψ are contained in B_n, and so again we have $\psi(B_n) \subseteq B_n$.

If we put $f(n) = (\#A_n)/(p^n+1)$ and $g(n) = (\#B_n)/(p^n+1)$, then the Hasse bound implies that both $f(n)$ and $g(n)$ are $1/2 + O(p^{-n/2})$. In particular,

$$\lim_{n\to\infty} \frac{\#A_n}{p^n+1} = \lim_{n\to\infty} \frac{\#B_n}{p^n+1} = \frac{1}{2}. \tag{2.10}$$

Let $\pi_p \in R$ denote the Frobenius endomorphism of E (which is given explicitly by $(r + \sqrt{r^2 - 4p})/2$ where $r = p + 1 - \#E(\mathbb{F}_p)$), and let $\mathfrak{p}$ be the ideal $(1+i)$ of R. Theorem 3.5 of [21] implies that each periodic point in A_n (resp. B_n) is the root of a complete binary rooted tree whose depth is given by $v_\mathfrak{p}(\pi_p^n - 1)$ (resp. $v_\mathfrak{p}(\pi_p^n + 1)$), where $v_\mathfrak{p}$ denotes the $\mathfrak{p}$-adic valuation. The only exception is the fixed point at ∞, whose tree includes the critical points ± 1 but otherwise is a complete binary tree with depth given as in the previous sentence. We have

$$2 = v_\mathfrak{p}(2) = v_\mathfrak{p}((\pi_p + 1) - (\pi_p - 1)) \geq \min\{v_\mathfrak{p}(\pi_p + 1), v_\mathfrak{p}(\pi_p - 1)\},$$

and it follows that either A_n or B_n is composed of periodic points for ψ, each one mapped to by a binary tree of non-periodic points of depth at most 2. Without loss of generality, say that A_n satifies this condition. Then

$$\liminf_{n\to\infty} \frac{\#\mathrm{Per}(\psi, A_n)}{\#A_n} \geq 1/4. \tag{2.11}$$

Combining (2.10) and (2.11) gives

$$\begin{aligned}
\liminf_{n\to\infty} \frac{\#\mathrm{Per}(\psi, \mathbb{P}^1(\mathbb{F}_{p^n}))}{p^n+1} &\geq \liminf_{n\to\infty} \frac{\#\mathrm{Per}(\psi, A_n)}{p^n+1} \\
&= \liminf_{n\to\infty} \left(\frac{\#\mathrm{Per}(\psi, A_n)}{\#A_n} \cdot \frac{\#A_n}{p^n+1} \right) \\
&\geq \frac{1}{4} \cdot \frac{1}{2} = \frac{1}{8}.
\end{aligned}$$

□

To illustrate the results of this section, we give some further discussion of the maps in Table 1, which gives data for $K = \mathbb{F}_3$ and all quadratic maps $\phi(x) = (x^2 - a)/(x^2 - b)$ with $a, b \in K$. The cases $(a, b) = (1, 2)$ and $(a, b) = (2, 1)$ produce maps that are conjugate over $\mathbb{F}_3$ and thus have the same dynamics on $\mathbb{F}_3^n$, while all other choices of (a, b) with $a \neq b$ yield maps that are not conjugate over $\overline{\mathbb{F}_3}$. Taking $(a, b) = (0, 2)$ gives a map with ramification portrait (2.2), which is thus $\overline{\mathbb{F}_3}$-conjugate to the degree-2 Chebyshev polynomial $x^2 - 2$. Taking $(a, b) = (2, 0)$ gives a Lattès map with ramification portrait (2.4). Taking $(a, b) \in \{(0, 1), (1, 2), (1, 0)\}$ gives a map that is not dynamically exceptional. We note that $(a, b) = (0, 2)$ gives a map conjugate to $x^2 - 1$.

Table 1 shows $\#\mathrm{Per}(\phi, \mathbb{P}^1(\mathbb{F}_{3^n}))/3^n$ for $n \leq 10$, and also includes the map x^2, whose periodic points in $\mathbb{P}^1(\mathbb{F}_{3^n})$ are the same as $1/x^2$.

3. Reducing Theorems 1.3 and 1.5 to statements about IMGs

In this section we show that to prove Theorems 1.3 and 1.5, it is enough to prove Theorem 1.7.

For each $n \geq 1$, let K_n^{arith} be the extension of $\mathbb{F}_q(t)$ obtained by adjoining the roots of $\phi^n(x) - t$, and K_n^{geom} the extension of $\overline{\mathbb{F}_q}(t)$ obtained by adjoining the roots of $\phi^n(x) - t$ (recall our standing assumption that $\phi^n(x) - t$ has d^n distinct roots in $\overline{\mathbb{F}_q(t)}$). We note that K_n^{geom} is equal to the compositum $K_n^{\mathrm{arith}}\overline{\mathbb{Q}}$, which in turn is equal to the compositum $K_n^{\mathrm{arith}}\overline{\mathbb{Q}}(t)$.

Denote by G_n the Galois group of K_n^{geom} over $\overline{\mathbb{F}_q}(t)$, and note that G_n is the natural quotient of $\mathrm{pgIMG}(\phi)/\mathbb{F}_q$ $(= \varprojlim G_n)$ obtained by restricting its action on $T(\phi)$ to the set $T_n(\phi)$ of vertices having distance n from the root of $T(\phi)$. The first main result of this section relates $\mathrm{FPP}(G_n)$ to certain counts of periodic points.

Theorem 3.1. *Let $\mathbb{F}_q$ be a finite field of characteristic p and $\phi \in \mathbb{F}_q(x)$ have degree d with $2 \leq d < p$. Let $n \geq 1$ and let $K_n^{arith} \cap \overline{\mathbb{F}_q} = \mathbb{F}_{q^m}$, so that $\mathbb{F}_{q^m}$ is the maximal constant field subextension of K_n^{arith}. Then for every $\delta > 0$ there is a constant k_0 such that*

$$\frac{\#\mathrm{Per}(\phi, \mathbb{P}^1(\mathbb{F}_{q^{mk}}))}{q^{mk}+1} < FPP(G_n) + \delta \tag{3.1}$$

for all $k > k_0$.

To prove Theorem 3.1, we begin with two elementary lemmas, the first of which is Lemma 5.2 of [10].

Lemma 3.2 ([10])**.** *If f is a function acting on a finite set $\mathcal{U}$, then $Per(f,\mathcal{U}) = \bigcap_{n\geq 0} f^n(\mathcal{U})$. In particular $\#Per(f,\mathcal{U}) \leq \#f^n(\mathcal{U})$ for every $n \geq 0$.*

We say that the degree of $\beta \in \mathbb{F}_q$, written $\deg \beta$, is the degree of the minimal polynomial of β over $\mathbb{F}_q$.

Lemma 3.3. *Let $\mathbb{F}_q$ be a finite field with q elements, and let $k > 1$ be an integer. Then*

$$\#\{\beta \in \mathbb{F}_{q^k} : \deg \beta < k\} \leq 2q^{k/2}. \tag{3.2}$$

Proof. The subfields of $\mathbb{F}_{q^k}$ are precisely $\mathbb{F}_{q^r}$ for $r \mid k$, and $\mathbb{F}_q(\beta) = \mathbb{F}_{q^{\deg\beta}}$. Thus $\#\{\beta \in \mathbb{F}_{q^k} : \deg \beta < k\}$ is bounded above by $\sum_{r|k, r\neq k} q^r$, and

$$\sum_{r|k, r\neq k} q^r \leq q^{k/2} + q^{(k/2)-1} + q^{(k/2)-2} + \cdots = q^{k/2}\left(1 + \frac{1}{q} + \frac{1}{q^2} + \cdots\right) \leq 2q^{k/2}.$$

□

Proof of Theorem 3.1. Begin by observing that $\#\phi^n(\mathbb{P}^1(\mathbb{F}_{q^{mk}})) \leq \phi^n(\mathbb{F}_{q^{mk}}) + 1$, and so

$$\frac{\#\phi^n(\mathbb{P}^1(\mathbb{F}_{q^{mk}}))}{q^{mk}+1} \leq \frac{\#\phi^n(\mathbb{F}_{q^{mk}})}{q^{mk}} + \frac{1}{q^{mk}+1}. \tag{3.3}$$

We will bound $\frac{\#\phi^n(\mathbb{F}_{q^{mk}})}{q^{mk}}$ for sufficiently large k. To do so, we study the extension $K_n^{\mathrm{arith}}/\mathbb{F}_{q^m}(t)$. Because $\mathbb{F}_{q^m}$ is the maximal constant field subextension of K_n^{arith}, we have $\mathrm{Gal}\,(K_n^{\mathrm{arith}}/\mathbb{F}_{q^m}(t)) = G_n$.

Each place P of $\mathbb{F}_{q^m}(t)$ (resp. $\mathfrak{p}$ of K_n^{arith}), has a corresponding discrete valuation v_P (resp. $v_\mathfrak{p}$), and we denote by $\mathcal{O}_P$ (resp. $\mathcal{O}_\mathfrak{p}$) the ring of integers $\{z \in \mathbb{F}_{q^m}(t)^* : v_P(z) \geq 0\}$ (resp. $\{z \in K_n^{\mathrm{arith}*} : v_\mathfrak{p}(z) \geq 0\}$) and we denote by $\mathfrak{m}_P$ (resp. $\mathfrak{m}_\mathfrak{p}$) the maximal ideal $\{z \in \mathcal{O}_P : v_P(z) > 0\}$ (resp. $\{z \in \mathcal{O}_\mathfrak{p} : v_p(z) > 0\}$). We denote the residue fields $\mathcal{O}_P/\mathfrak{m}_P$ and $\mathcal{O}_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}$ by $\mathbb{F}_P$ and $\mathbb{F}_\mathfrak{p}$, respectively, and we denote the canonical maps $\mathcal{O}_P \to \mathbb{F}_P$ and $\mathcal{O}_\mathfrak{p}$ to $\mathbb{F}_\mathfrak{p}$ by π_P and $\pi_\mathfrak{p}$, respectively.

Let $\alpha_1, \ldots, \alpha_{d^n}$ be the roots of $\phi^n(x) - t$ in $\overline{\mathbb{F}_{q^m}(t)}$, and observe that these are all distinct. Let T be the set of places P of $\mathbb{F}_{q^m}(t)$ satisfying all of the following:

(1) P is not ramified in K_n^{arith};
(2) every extension $\mathfrak{p}$ of P to K_n^{arith} satisfies $v_\mathfrak{p}(\alpha_i - \alpha_j) = 0$ for all $i \neq j$;
(3) every extension $\mathfrak{p}$ of P to K_n^{arith} satisfies $v_\mathfrak{p}(\alpha_i) \geq 0$ for all i;
(4) P is not the place at infinity.

(We remark that condition (2) implies condition (1), though we do not need that for the proof.) Let $P \in T$, and let $\mathfrak{p}$ be an extension of P to K_n^{arith}. Condition (4) ensures there is an irreducible polynomial $p(t) \in \mathbb{F}_{q^m}[t]$ of some degree $k \geq 1$ such that v_P is given by $\mathrm{ord}_p(\cdot)$. In particular, $\mathbb{F}_P = \mathbb{F}_{q^m}[t]/(p(t))$, which is a finite field of q^{mk} elements. Moreover, condition (3) ensures $\alpha_i \in \mathcal{O}_\mathfrak{p}$ for all $i = 1, \ldots, d^n$, and condition (2) ensures

$$\pi_\mathfrak{p} : \{\alpha_1, \ldots, \alpha_{d^n}\} \to \{\pi_p(\alpha_1), \ldots, \pi_\mathfrak{p}(\alpha_{d^n})\} \text{ is a bijection.} \tag{3.4}$$

Let $D(\mathfrak{p}/P) \subset G_n$ be the decomposition group of $\mathfrak{p}$, i.e.

$$\{g \in G_n : v_\mathfrak{p}(g(z)) = v_\mathfrak{p}(z) \text{ for all } z \in K_n^{\mathrm{arith}} \setminus \{0\}\}.$$

Observe that any $g \in D(\mathfrak{p}/P)$ gives a map $\mathcal{O}_\mathfrak{p} \to \mathcal{O}_\mathfrak{p}$ that descends to $\overline{g} \in \mathrm{Gal}\,(\mathbb{F}_\mathfrak{p}/\mathbb{F}_P)$ given by $\overline{g}(z + \mathfrak{p}) = g(z) + \mathfrak{p}$. For any α_i, we have

$$\pi_\mathfrak{p}(g(\alpha_i)) = g(\alpha_i) + \mathfrak{p} = \overline{g}(\alpha_i + \mathfrak{p}) = \overline{g}(\pi_\mathfrak{p}(\alpha_i)),$$

and it follows from (3.4) that g permutes $\{\alpha_1, \ldots, \alpha_{d^n}\}$ in the same way that $\overline{g}$ permutes $\{\pi_\mathfrak{p}(\alpha_1), \ldots, \pi_\mathfrak{p}(\alpha_{d^n})\}$.

Because ϕ is defined over $\mathbb{F}_{q^m}$, it commutes with $\pi_\mathfrak{p}$, so we have

$$\pi_\mathfrak{p}(t) = \pi_\mathfrak{p}(\phi^n(\alpha_i)) = \phi^n(\pi_\mathfrak{p}(\alpha_i)), \tag{3.5}$$

whence $\{\pi_\mathfrak{p}(\alpha_1), \ldots, \pi_\mathfrak{p}(\alpha_{d^n})\}$ are the preimages of $\pi_\mathfrak{p}(t)$ under ϕ^n. Now $\pi_\mathfrak{p}(t)$ is a root of $p(t)$ in $\mathbb{F}_\mathfrak{p}$, and hence lies in $\mathbb{F}_P$, since the latter is $\mathcal{O}_P/(p(t))$. Let $\beta = \pi_\mathfrak{p}(t)$, and

let β' be any other root of $p(t)$ in $\mathbb{F}_P$. Then there is $\sigma \in \mathrm{Gal}\,(\mathbb{F}_\mathfrak{p}/\mathbb{F}_P)$ with $\sigma(\beta) = \beta'$. Now σ commutes with ϕ, and so applying σ to (3.5) shows that the preimages of β' under ϕ^n are $\{\sigma(\pi_\mathfrak{p}(\alpha_1)), \ldots, \sigma(\pi_\mathfrak{p}(\alpha_{d^n}))\}$. Moreover, $\mathrm{Gal}\,(\mathbb{F}_\mathfrak{p}/\mathbb{F}_P)$ is abelian, and so $\overline{g}$ and σ commute for any $g \in D(\mathfrak{p}/P)$. It follows that g has a fixed point in $\{\pi_\mathfrak{p}(\alpha_1), \ldots, \pi_\mathfrak{p}(\alpha_{d^n})\}$ if and only if it has a fixed point in $\{\sigma(\pi_\mathfrak{p}(\alpha_1)), \ldots, \sigma(\pi_\mathfrak{p}(\alpha_{d^n}))\}$.

Still assuming that $P \in T$, condition (1) implies that the map $g \to \overline{g}$ gives an isomorphism $D(\mathfrak{p}/P) \to \mathrm{Gal}\,(\mathbb{F}_\mathfrak{p}/\mathbb{F}_P)$ [20, Theorem 9.6]. The inverse image of the Frobenius map $x \mapsto x^{q^{mk}}$ is denoted $\mathrm{Frob}(\mathfrak{p}/P)$, and the set $\{\mathrm{Frob}(\mathfrak{p}/P) : \mathfrak{p} \text{ extends } P\}$ is a conjugacy class of G_n [20, Proposition 9.7], which we denote $\mathrm{Frob}(P)$. Observe that if $\mathrm{Frob}(\mathfrak{p}/P)$ fixes one of the α_i for some extension $\mathfrak{p}$ of P, then so does every element of $\mathrm{Frob}(P)$.

Now $\mathrm{Frob}(\mathfrak{p}/P)(\alpha_i) = \alpha_i$ is equivalent to $(\pi_p(\alpha_i))^{q^{mk}} = \pi_\mathfrak{p}(\alpha_i)$, which is equivalent to $\alpha_i \in \mathbb{F}_{q^{mk}}$. Thus if $\beta_1, \ldots, \beta_k$ are the roots in $\mathbb{F}_{q^{mk}}$ of $p(t)$, we have

$$\begin{aligned}(3.6)\quad &\mathrm{Frob}(P) \text{ acts on } \{\alpha_1, \ldots, \alpha_{d^n}\} \text{ with at least one fixed point}\\ &\qquad\qquad \Longleftrightarrow \text{for every } j \in \{1, \ldots, k\}, \text{ there is } y \in \mathbb{F}_{q^{mk}} \text{ with } \phi^n(y) = \beta_j\end{aligned}$$

Observe that the latter condition in (3.6) is equivalent to $\{\beta_1, \ldots, \beta_k\} \subset \phi^n(\mathbb{F}_{q^{mk}})$.

Let $U = \{\text{places } P \text{ of } \mathbb{F}_{q^m}(t) \text{ that are unramified in } K_n^{\mathrm{arith}}\}$. The Chebotarev Density Theorem for function fields (see e.g. [20, Theorem 9.13B]) states that for any conjugacy class $C \subset G_n$, there is a constant Δ such that

$$(3.7)\qquad \#\{P \in U : \deg P = k \text{ and } \mathrm{Frob}(P) = C\} \le \frac{\#C}{\#G_n} \cdot \frac{q^{mk}}{k} + \Delta \frac{q^{mk/2}}{k}.$$

Both U and T contain all but finitely many places of $\mathbb{F}_{q^m}(t)$, and so there exists k_1 such that for any $k \ge k_1$, all places of degree k lie in both U and T. The set of $g \in G_n$ acting on $\{\alpha_1, \ldots, \alpha_{d^n}\}$ with at least one fixed point is a union of conjugacy classes of G_n, and it follows from (3.6) and (3.7) that for $k \ge k_1$,

$$\#\{P : \deg P = k \text{ and } \{\beta_1, \ldots, \beta_k\} \subset \phi^n(\mathbb{F}_{q^{mk}})\} \le \mathrm{FPP}(G_n) \cdot \frac{q^{mk}}{k} + \Delta \frac{q^{mk/2}}{k}.$$

Thus for $k \ge k_1$ we have

$$(3.8)\qquad \frac{\#\{\beta \in \phi^n(\mathbb{F}_{q^{mk}}) : \deg \beta = k\}}{k} \le \mathrm{FPP}(G_n) \cdot \frac{q^{mk}}{k} + \Delta \frac{q^{mk/2}}{k}.$$

From Lemma 3.3, we have $\#\{\beta \in \phi^n(\mathbb{F}_{q^{mk}}) : \deg \beta < k\} \le 2q^{mk/2}$, and (3.8) then gives

$$(3.9)\qquad \#\phi^n(\mathbb{F}_{q^{mk}}) \le \mathrm{FPP}(G_n) \cdot q^{mk} + (\Delta + 2) q^{mk/2}$$

for $k \geq k_1$. Finally, combining (3.9) with Lemma 3.2 and equation (3.3), we obtain for $k \geq k_1$,

$$\begin{aligned}\frac{\#\mathrm{Per}(\phi, \mathbb{P}^1(\mathbb{F}_{q^{mk}}))}{q^{mk}+1} &\leq \frac{\#\phi^n(\mathbb{P}^1(\mathbb{F}_{q^{mk}}))}{q^{mk}+1} \leq \frac{\#\phi^n(\mathbb{F}_{q^{mk}})}{q^{mk}} + (q^{mk}+1)^{-1} \\ &\leq \mathrm{FPP}(G_n) + (q^{mk}+1)^{-1} + (\Delta+2)q^{-mk/2}\end{aligned}$$

Let $\delta > 0$. Taking k_0 large enough so that $k_0 \geq k_1$ and $(q^{mk_0}+1)^{-1}+(\Delta+2)q^{-mk_0/2} < \delta$ completes the proof. □

We obtain the following Corollary of Theorem 3.1:

Corollary 3.4. *Let $\mathbb{F}_q$ be a finite field of characteristic p and $\phi \in \mathbb{F}_q(x)$ have degree d with $2 \leq d < p$. Then for every $\epsilon > 0$ there are positive integers M and k_0 such that*

$$\frac{\#\mathrm{Per}(\phi, \mathbb{P}^1(\mathbb{F}_{q^{Mk}}))}{q^{Mk}+1} < FPP(pgIMG(\phi)/\mathbb{F}_q) + \epsilon$$

for all $k > k_0$. Moreover, $M \leq \limsup_{n\to\infty} m_n$, where $m_n = [(K_n^{arith} \cap \overline{\mathbb{F}_q}) : \mathbb{F}_q]$.

Proof. Let $\epsilon > 0$ be given. By definition $\mathrm{FPP}(\mathrm{pgIMG}(\phi)/\mathbb{F}_q) = \lim_{i\to\infty} \mathrm{FPP}(G_i)$, and so there is an infinite set I such that $\mathrm{FPP}(G_i) \leq \mathrm{FPP}(\mathrm{pgIMG}(\phi)/\mathbb{F}_q) + \epsilon/2$ for any $i \in I$. For each $i \in I$, we may take $\delta = \epsilon/2$ in Theorem 3.1 to obtain m_i and k_0 such that

$$\frac{\#\mathrm{Per}(\phi, \mathbb{P}^1(\mathbb{F}_{q^{m_i k}}))}{q^{m_i k}+1} \leq \mathrm{FPP}(\mathrm{pgIMG}(\phi)/\mathbb{F}_q) + \epsilon/2 + \epsilon/2$$

for all $k \geq k_0$. If $\limsup_{n\to\infty} m_n = \infty$, then any choice of $i \in I$ proves the Corollary. If $\limsup_{n\to\infty} m_n = L < \infty$, then we may take $i \in I$ large enough so that $m_i \leq L$. □

Recall that a finite extension E of $\mathbb{F}_q(t)$ is geometric (over $\mathbb{F}_q(t)$) if $E \cap \overline{\mathbb{F}_q} = \mathbb{F}_q$. Hence K_n^{arith} is geometric if and only if $m_n = 1$ for all $n \geq 1$.

Corollary 3.5. *Let $\mathbb{F}_q$ be a finite field of characteristic p and $\phi \in \mathbb{F}_q(x)$ have degree d with $2 \leq d < p$. Then*

$$\liminf_{k\to\infty} \frac{\#\mathrm{Per}(\phi, \mathbb{P}^1(\mathbb{F}_{q^k}))}{q^k+1} \leq FPP(pgIMG(\phi)/\mathbb{F}_q).$$

If in addition K_n^{arith} is geometric over $\mathbb{F}_q(t)$ for all $n \geq 1$, then

$$\limsup_{k\to\infty} \frac{\#\mathrm{Per}(\phi, \mathbb{P}^1(\mathbb{F}_{q^k}))}{q^k+1} \leq FPP(pgIMG(\phi)/\mathbb{F}_q).$$

Proof. The first statement follows from Corollary 3.4 and the second from Theorem 3.1. □

In particular, if K_n^{arith} is geometric over $\mathbb{F}_q(t)$ for all $n \geq 1$ and $\text{FPP}(\text{pgIMG}(\phi)/\mathbb{F}_q) = 0$, then the second statement of Corollary 3.5 gives

$$\lim_{k\to\infty} \frac{\#\text{Per}(\phi, \mathbb{P}^1(\mathbb{F}_{q^k}))}{q^k+1} = 0.$$

At present the constant field sub-extensions $\mathbb{F}_{q^{m_n}}$ (which we recall is $K_n^{\text{arith}} \cap \overline{\mathbb{F}_q}$) are in general poorly understood. The main result is in the case of quadratic polynomials, and due to Pink:

Theorem 3.6 (Pink [17])**.** *Let $\mathbb{F}_q$ be a finite field of odd characteristic, and let $\phi \in \mathbb{F}_q[x]$ have degree 2. Suppose that the unique finite critical point of ϕ is strictly preperiodic and that ϕ is not conjugate to a Chebyshev polynomial. Then*

$$K_n^{arith} \cap \overline{\mathbb{F}_q} \subseteq \mathbb{F}_q(\zeta_8),$$

where ζ_8 is a primitive 8th root of unity. In particular, if q is a square then K_n^{arith} is geometric over $\mathbb{F}_q(t)$ for all $n \geq 1$.

Together with Corollary 3.5, this gives:

Corollary 3.7. *Let $\mathbb{F}_q$ be a finite field of odd characteristic, and let $\phi \in \mathbb{F}_q[x]$ have degree 2. Suppose that q is a square, the unique finite critical point of ϕ is strictly preperiodic, and ϕ is not conjugate over $\overline{\mathbb{F}_q}$ to a Chebyshev polynomial. If $FPP(pgIMG(\phi)/\mathbb{F}_q) = 0$, then*

$$\lim_{k\to\infty} \frac{\#\text{Per}(\phi, \mathbb{P}^1(\mathbb{F}_{q^k}))}{q^k+1} = 0.$$

We now wish to show that $\text{FPP}(\text{pgIMG}(\phi)/\mathbb{F}_q) = \text{FPP}(\text{pgIMG}(\tilde{\phi})/\mathbb{C})$, thereby reducing the proofs of both Theorems 1.3 and 1.4 to the computation of $\text{FPP}(\text{pgIMG}(\tilde{\phi})/\mathbb{C})$. To do so, we take advantage of theorems about lifting Galois groups from characteristic p to characteristic 0. Let T and T' be two complete d-ary rooted trees. If $\iota : T \to T'$ is an isomorphism of rooted trees, then any $G \leq \text{Aut}(T)$ embeds as a subgroup $\iota \circ G \circ \iota^{-1}$ of $\text{Aut}(T')$. A different choice of ι alters the image of this embedding by a conjugacy in $\text{Aut}(T')$. In particular, $\text{FPP}(G) = \text{FPP}(\iota \circ G \circ \iota^{-1})$ independent of choice of ι, since FPP is invariant under conjugacy.

Definition 3.8. Let $\mathbb{F}_q$ be a finite field of characteristic p and let $\phi \in \mathbb{F}_q(x)$ have degree $d \geq 2$ with $\text{pgIMG}(\phi)/\mathbb{F}_q = G_\infty$ acting on the tree $T_{\mathbb{F}_q}(\phi)$ of preimages of t in $\overline{\overline{\mathbb{F}_q}(t)}$. We call ϕ **liftable** if there exists a map $\tilde{\phi} \in \mathbb{C}(x)$ with $\text{pgIMG}(\tilde{\phi})/\mathbb{C} = \tilde{G}_\infty$ acting on the tree $T_{\mathbb{C}}(\tilde{\phi})$ of preimages of t in $\overline{\mathbb{C}(t)}$ such that

(1) ϕ and $\tilde{\phi}$ have the same ramification portrait, and
(2) there is a tree isomorphism $\iota : T_{\mathbb{F}_q}(\phi) \to T_{\mathbb{C}}(\tilde{\phi})$ such that $\iota \circ G_\infty \circ \iota^{-1} = \tilde{G}_\infty$.

Not all $\phi \in \mathbb{F}_q(x)$ are liftable; for instance if $\phi(x) = x^p - x$ then ∞ is the only critical point in $\mathbb{P}^1(\overline{\mathbb{F}_q})$, and no lift $\tilde{\phi} \in \mathbb{C}(x)$ can have the same ramification portrait.

Note that condition (2) of Definition 3.8 ensures that if ϕ is liftable, then

$$\mathrm{FPP}(\mathrm{pgIMG}(\phi)/\mathbb{F}_q) = \mathrm{FPP}(\mathrm{pgIMG}(\tilde{\phi})/\mathbb{C}). \tag{3.10}$$

In Section 4 we show that the latter is equal to $\mathrm{FPP}(\mathrm{IMG}(\tilde{\phi}))$ (see p. 22).

We remark that the action of $\mathrm{pgIMG}(\tilde{\phi})/\mathbb{C}$ on $T_{\mathbb{C}}(\tilde{\phi})$ is given by the action of the topological fundamental group $\pi_1(\mathbb{P}^1_{\mathbb{C}} \setminus P_{\tilde{\phi}}, z_0)$, where z_0 is any point outside of $P_{\tilde{\phi}}$ The latter may be computed by pulling back loops in $\mathbb{P}^1_{\mathbb{C}} \setminus P_{\tilde{\phi}}$, which allows for the use of topological and geometric tools.

In order to harness these new tools, we need to know that the maps we study are liftable. For this we appeal to a result of R. Pink.

Theorem 3.9 (Pink [16], Corollary 4.4)**.** *Let $\mathbb{F}_q$ be a finite field of odd characteristic, and let $\phi \in \mathbb{F}_q(x)$ have degree 2. Then ϕ is liftable.*

To prove Theorem 3.9, Pink constructs a fine moduli scheme M_Γ for Γ-marked quadratic morphisms, i.e. quadratic morphisms with specified ramification portrait Γ. The construction is explicit, and M_Γ has several desirable properties, the most crucial being that it is quasi-finite over $\operatorname{Spec} \mathbb{Z}[\frac{1}{2}]$ [16, Theorem 3.3]. These properties lead to a proof that any Γ-marked quadratic morphism over a finite field of odd characteristic p lifts to characteristic zero: it is isomorphic to the special fiber of a Γ-marked quadratic morphism over $\operatorname{Spec} R$, where R is a discrete valuation ring that is finitely generated over $\mathbb{Z}_{(p)}$ [16, Corollary 3.6]. Liftability in the sense of Definition 3.8 then follows as a direct consequence of Grothendieck's Specialization Theorem for tame fundamental groups; see [18, Section 4].

The key step in Pink's argument is the quasi-finiteness of M_Γ, which is equivalent to the statement that that any quadratic morphism over a function field of characteristic $\neq 2$ is isotrivial, i.e. defined over a finite extension of the constant field after a change of variables. Using p-adic methods that are completely different from those of [16], this statement was proven in [2, Corollary 6.3].

Finally, note that because of condition (1) in Definition 3.8, a liftable map $\phi \in \mathbb{F}_q(x)$ is dynamically exceptional if and only if its lift is. From Theorem 3.9, Corollary 3.5, and Corollary 3.7, we then obtain:

Corollary 3.10. *Theorem 1.7 implies Theorem 1.3 and Theorem 1.4.*

We now turn to Question 1.2, the "horizontal" question involving finite fields of different characteristics. Recall that if K is a number field and $\phi \in K(x)$, then for all but finitely many primes $\mathfrak{p}$ in the ring of integers $\mathcal{O}_K$ of K, one may reduce the coefficients of ϕ modulo $\mathfrak{p}$ to obtain a morphism $\phi_\mathfrak{p} : \mathbb{P}^1(\mathbb{F}_\mathfrak{p}) \to \mathbb{P}^1(\mathbb{F}_\mathfrak{p})$ with $\deg \phi = \deg \tilde{\phi}$, where $\mathbb{F}_\mathfrak{p}$ is the residue field $\mathcal{O}_K/\mathfrak{p}$. Denote by $N(\mathfrak{p})$ the degree of $\mathbb{F}_\mathfrak{p}$ over its prime field, so that $1 + N(\mathfrak{p})$ is the size of $\mathbb{P}^1(\mathbb{F}_\mathfrak{p})$.

Theorem 3.11. *Let K be a number field and $\phi \in K(x)$. Then*

$$\liminf_{N(\mathfrak{p})\to\infty} \frac{\#\mathrm{Per}(\phi_{\mathfrak{p}}, \mathbb{F}_{\mathfrak{p}})}{1+N(\mathfrak{p})} \leq FPP(pgIMG(\phi)/\mathbb{C}), \tag{3.11}$$

where the lim inf is over primes $\mathfrak{p}$ of K.

Proof. Let K_n^{geom} be the splitting field of $\phi^n(x)-t$ over $\overline{\mathbb{Q}}(t)$, and $G_n = \mathrm{Gal}\,(K_n^{\mathrm{geom}}/\overline{\mathbb{Q}}(t))$, so that $\lim_{n\to\infty} \mathrm{FPP}(G_n) = \mathrm{FPP}(\mathrm{pgIMG}(\phi)/\overline{\mathbb{Q}})$. Because K_n^{geom} is an algebraic extension of $\overline{\mathbb{Q}}(t)$, for any extension field F of $\overline{\mathbb{Q}}$ we have that the field of constants of $K_n^{\mathrm{geom}} \cap F(t)$ is an algebraic extension of $\overline{\mathbb{Q}}$. Hence $K_n^{\mathrm{geom}} \cap F(t) = \overline{\mathbb{Q}}(t)$. By the theorem on natural irrationalities, it follows that the Galois group of the compositum FK_n^{geom} over $F(t)$ is isomorphic to G_n. Choosing an embedding $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$, we may take $F = \mathbb{C}$. This embedding can be extended to an embedding $\overline{\overline{\mathbb{Q}}(t)} \hookrightarrow \overline{\mathbb{C}(t)}$, which carries $T_{\overline{\mathbb{Q}}}(\phi)$ onto $T_{\mathbb{C}}(\phi)$. It follows that $\mathrm{pgIMG}(\phi)/\overline{\mathbb{Q}} \cong \mathrm{pgIMG}(\phi)/\mathbb{C}$, and the action of the former on $T_{\overline{\mathbb{Q}}}(\phi)$ is conjugate to the action of the latter on $T_{\mathbb{C}}(\phi)$ (where the conjugacy depends on the choice of embeddings).

Let $L_n = K_n^{\mathrm{arith}} \cap \overline{\mathbb{Q}}$, and recall that $K_n^{\mathrm{arith}}\overline{\mathbb{Q}}(t) = K_n^{\mathrm{arith}}\overline{\mathbb{Q}} = K_n^{\mathrm{geom}}$. Then $K_n^{\mathrm{arith}}\overline{\mathbb{Q}}(t)$ is a geometric extension of $L_n(t)$ with Galois group G_n, by the theorem on natural irrationalities. From [10, Proposition 5.3] we have that for primes $\mathfrak{P}$ of L_n and for any $\delta > 0$,

$$\frac{\#\mathrm{Per}(\phi_{\mathfrak{P}}, \mathbb{F}_{\mathfrak{P}})}{1+N(\mathfrak{P})} \leq \mathrm{FPP}(G_n) + \delta \tag{3.12}$$

for $N(\mathfrak{P})$ sufficiently large, where $N(\mathfrak{P})$ is the norm of $\mathfrak{P}$. From [10, Lemma 6.3] and (3.12) we obtain

$$\liminf_{N(\mathfrak{p})\to\infty} \frac{\#\mathrm{Per}(\phi_{\mathfrak{p}}, \mathbb{F}_{\mathfrak{p}})}{1+N(\mathfrak{p})} \leq \mathrm{FPP}(G_n) + \delta, \tag{3.13}$$

where $\mathfrak{p}$ varies over primes of K. To prove (1.6), let $\epsilon > 0$. Let n be such that $\mathrm{FPP}(G_n) \leq \mathrm{FPP}(\mathrm{pgIMG}(\phi)/\overline{\mathbb{Q}}) + \epsilon/2$. Applying (3.13) with $\delta = \epsilon/2$ gives

$$\liminf_{N(\mathfrak{p})\to\infty} \frac{\#\mathrm{Per}(\phi_{\mathfrak{p}}, \mathbb{F}_{\mathfrak{p}})}{1+N(\mathfrak{p})} \leq \mathrm{FPP}(\mathrm{pgIMG}(\phi)/\overline{\mathbb{Q}}) + \epsilon,$$

from which (3.11) follows, because $\mathrm{FPP}(\mathrm{pgIMG}(\phi)/\overline{\mathbb{Q}}) = \mathrm{FPP}(\mathrm{pgIMG}(\phi)/\mathbb{C})$ by the first paragraph of the proof. □

Theorem 3.11 shows that the only obstacle to proving Theorem 1.5 is establishing that $\mathrm{FPP}(\mathrm{pgIMG}(\phi)/\mathbb{C}) = 0$. When ϕ is conjugate over $\overline{K}$ to a polynomial, this is Theorem 1.1 of [8]. If ϕ has prime degree or doubly transitive monodromy, this is Theorem 1.7. We thus have:

Corollary 3.12. *Theorem 1.7 implies Theorem 1.5.*

4. Background and definitions on IMGs and wreath recursion

The proof of Theorem 1.7, which requires a proof of Theorem 1.8, occupies the remainder of the article. From this section on, we work in a more topological context, and so use the notation $\widehat{\mathbb{C}}$ in place of $\mathbb{P}^1_{\mathbb{C}}$. We now use f to denote a rational function with complex coefficients, and we use z as the variable. Given $f \in \mathbb{C}(z)$, we wish to understand the action of $\mathrm{pgIMG}(f)/\mathbb{C}$ on $T_{\mathbb{C}}(f)$. In Section 4.1 we discuss tools for studying the action of an arbitrary group on a complete d-ary infinite rooted tree X^*. In Section 4.2 we define the iterated monodromy group and describe its standard action on X^*. In Section 4.3 we give some basic properties of the monodromy action on roots of a polynomial that will be used in Section 6.

4.1. **Wreath recursion and definitions.** Let $d \geq 2$, put $X = \{0, \ldots, d-1\}$, and let S_d denote the symmetric group on d letters. Denote by X^* the set of all words in X, arranged as a tree in the natural way: there is an edge connecting vx to v for each $v \in X^*$ and $x \in X$. Denote by X^n the set of words in X of length n, which gives the nth level of X^*. By X^0 we mean the set consisting only of the empty word. An *end* of X^* is an infinite, non-retracing path beginning at the empty word. Thus the set of all ends of X^* is the inverse limit of the X^n under the natural maps $X^n \to X^{n-1}$.

Define $\mathrm{Aut}(X^*)$ to be the set of tree automorphisms. A salient feature of X^* is its self-similarity, and we use this to describe elements of $\mathrm{Aut}(X^*)$ recursively.

Let $g \in \mathrm{Aut}(X^*)$, and for a vertex $v \in X^*$ consider the subtrees vX^* and $g(v)X^*$ with root v and $g(v)$, respectively. Both are naturally isomorphic to X^*, and identifying them gives an automorphism $g|_v \in \mathrm{Aut}(X^*)$, called the *restriction* of g at v.

There is a natural isomorphism

$$\psi : \mathrm{Aut}(X^*) \to S_d \wr \mathrm{Aut}(X^*),$$

where $\wr$ denotes the wreath product, that takes g to $(\sigma, (g|_0, \ldots, g|_{d-1}))$, where $\sigma \in S_d$ is the action of g on X (i.e., on the first level of X^*). In other words, we may describe g by specifying its action on X and its restriction at each element of X. We call this the *wreath recursion* describing g. We generally drop the outer parentheses and equate g with its image under ψ, writing

$$g = \sigma(g|_0, \ldots, g|_{d-1}).$$

We write the identity element as 1, and when the permutation σ is the identity, we omit it. Hence the identity element of $\mathrm{Aut}(X^*)$ is given in wreath recursion by $(1, 1, \ldots, 1)$. Note that the element $a = (a, 1, 1, \ldots, 1)$ is also the identity, since by induction it acts trivially on X^n for all n, and thus acts trivially on X^*. Given $g = \sigma(g|_0, \ldots, g|_{d-1})$, we can make explicit its action on any X^n thanks to the following formulas, which are straightforward to prove:

$$g|_{vw} = g|_v|_w \qquad g(vw) = g(v)g|_v(w), \tag{4.1}$$

for any $v, w \in X^*$.

One can multiply elements in wreath recursion form using the usual multiplication in a semi-direct product:

$$\sigma(g_0 \dots, g_{d-1}) \cdot \tau(h_0 \dots, h_{d-1}) = \sigma\tau(g_{\tau(0)}h_0 \dots, g_{\tau(d-1)}h_{d-1}). \tag{4.2}$$

If we take $v \in X^*$ of length n, we may consider (4.2) as giving the wreath recursion of $g, h \in \mathrm{Aut}(X^*)$ acting on X^n. This gives

$$(gh)(v) = g(h(v)) \qquad \text{and} \qquad (gh)|_v = g|_{h(v)} \cdot h|_v \tag{4.3}$$

Definition 4.1. A subgroup G of $\mathrm{Aut}(X^*)$ is *level-transitive* if for all $n \geq 1$, G acts transitively on X^n.

Definition 4.2. A subgroup G of $\mathrm{Aut}(X^*)$ is *self-similar* if for all $g \in G$ we have $g|_v \in G$ for every $v \in X^*$.

Definition 4.3. A subgroup G of $\mathrm{Aut}(X^*)$ is *recurrent* if G is self-similar, G acts transitively on X, and for each $x \in X$, the map

$$\{g \in G : g(x) = x\} \to G \quad \text{given by} \quad g \mapsto g|_x \tag{4.4}$$

is surjective.

We note that the map in (4.4) is known as the virtual endomorphism associated to g and x.

Definition 4.4. A subgroup G of $\mathrm{Aut}(X^*)$ is *contracting* if G is self-similar and there is a finite set $\mathcal{N} \subset G$ with the following property: for each $g \in G$, there is $M > 0$ such that $g|_v \in \mathcal{N}$ for every word $v \in X^*$ of length at least M.

We record here a consequence of [15, Corollary 2.8.5]:

Proposition 4.5. *A recurrent subgroup $G \leq \mathrm{Aut}(X^*)$ is level-transitive, and hence is infinite.*

Proof. The first assertion follows immediately from [15, Corollary 2.8.5]. A level-transitive subgroup of $\mathrm{Aut}(X^*)$ must be infinite, because it acts transitively on arbitrarily large sets. □

4.2. **Basic properties of IMGs.** Throughout this section, let $f : \widehat{\mathbb{C}} \to \widehat{\mathbb{C}}$ be a PCF rational function of degree $d \geq 2$ with post-critical set P_f (the same construction works any expanding PCF branched cover $f : \mathbb{S}^2 \to \mathbb{S}^2$ as in [1], but we will not use the extra generality here). Fix a choice of $z_0 \in \widehat{\mathbb{C}} \setminus P_f$. Given $\gamma \in \pi_1(\widehat{\mathbb{C}} \setminus P_f, z_0)$ and $z \in f^{-n}(z_0)$, there is a unique lift of γ beginning at z, whose endpoint we denote $z_\gamma \in f^{-n}(z_0)$. The map $z \mapsto z_\gamma$ defines a permutation of $f^{-n}(z_0)$, and the resulting homomorphism

$$\pi_1(\widehat{\mathbb{C}} \setminus P_f, z_0) \to \mathrm{Perm}(f^{-n}(z_0))$$

is called the monodromy action of $\pi_1(\widehat{\mathbb{C}} \setminus P_f, z_0)$ on $f^{-n}(z_0)$. Denote its kernel by K_n. The monodromy action extends to an action on the tree $T_{f,z_0} \subset \widehat{\mathbb{C}}$ of preimages of f,

rooted at z_0. (We use this notation rather than the previous $T_k(\phi)$ because this tree is a subset of $\widehat{\mathbb{C}}$ rather than of $\overline{k(t)}$.) Its kernel is $K = \bigcap_{n=1}^{\infty} K_n$, which we call the *faithful kernel* of the monodromy action.

Definition 4.6. With notation as above, the *iterated monodromy group* of f, written $\mathrm{IMG}(f)$, is the quotient of $\pi_1(\widehat{\mathbb{C}} \setminus P_f, z_0)$ by the faithful kernel K of the monodromy action on the tree T_{f,z_0}.

Select a labeling bijection $\Lambda : X \to f^{-1}(z_0)$, and for $i \in \{0, \dots, d-1\}$ select a path ℓ_i from z_0 to $\Lambda(i)$ in $\widehat{\mathbb{C}} \setminus P_f$. Then Λ extends inductively to an isomorphism $\Lambda^* : X^* \to T_{f,z_0}$ of rooted trees via the rule

$$\Lambda^*(xv) = \text{end of the path } f^{-n}(\ell_x) \text{ starting at } \Lambda^*(v) \tag{4.5}$$

for $v \in X^n$ [15, Proposition 5.2.1].

Definition 4.7. Fix choices of basepoint z_0, labeling map $\Lambda : X \to f^{-1}(z_0)$, and paths $\{\ell_i\}$. The corresponding standard action of $\pi_1(\widehat{\mathbb{C}} \setminus P_f, z_0)$ (resp. $\mathrm{IMG}(f)$) on X^* is the conjugation by Λ^* of the monodromy action of $\pi_1(\widehat{\mathbb{C}} \setminus P_f, z_0)$ (resp. $\mathrm{IMG}(f)$) on T_{f,z_0}.

A standard action gives a homomorphism $\pi_1(\widehat{\mathbb{C}} \setminus P_f, z_0) \to \mathrm{Aut}(X^*)$, which descends to an injective homomorphism $\mathrm{IMG}(f) \hookrightarrow \mathrm{Aut}(X^*)$ with identical image. Thus we may identify $\mathrm{IMG}(f)$ with a subgroup of $\mathrm{Aut}(X^*)$. A different choice of z_0, Λ, or $\{\ell_i\}$ only changes this group by a conjugacy in $\mathrm{Aut}(X^*)$. From now on we fix a standard action of $\pi_1(\widehat{\mathbb{C}} \setminus P_f, z_0)$, and hence of $\mathrm{IMG}(f)$, on $\mathrm{Aut}(X^*)$.

For given $n \geq 1$, it is a well-known result in the theory of Riemann surfaces that the permutation group of $f^{-n}(z_0)$ induced by the monodromy action of $\pi_1(\widehat{\mathbb{C}} \setminus P_f, z_0)$ is identical (after possibly a conjugation in the symmetric group) to that given by the action of the Galois group $\mathrm{Gal}\,(\mathbb{C}(f^{-n}(t))/\mathbb{C}(t))$ on the set $f^{-n}(t) \subset \overline{\mathbb{C}(t)}$. Thus after possibly conjugating in $\mathrm{Aut}(X^*)$, we have that the action of $\mathrm{pgIMG}(f)/\mathbb{C}$ on $f^{-n}(t)$ is the same as that of $\mathrm{IMG}(f)$ on X^n (see e.g. [4, Theorem 8.12]. Since $\mathrm{pgIMG}(f)/\mathbb{C}$ is a closed subgroup of $\mathrm{Aut}(X^*)$ and it has the same image as $\mathrm{IMG}(f)$ under the restriction maps $\mathrm{Aut}(X^*) \to \mathrm{Aut}(X^n)$, it follows that $\mathrm{pgIMG}(f)/\mathbb{C}$ is the closure of $\mathrm{IMG}(f)$ in $\mathrm{Aut}(X^*)$. This is [15, Proposition 6.4.2]. In particular, we have

$$\mathrm{IMG}(f) \subset \mathrm{pgIMG}(f)/\mathbb{C} \subseteq \mathrm{Aut}(X^*)$$

and $\mathrm{FPP}(\mathrm{pgIMG}(f)/\mathbb{C}) = \mathrm{FPP}(\mathrm{IMG}(f))$.

We now describe a standard action in terms of wreath recursion. Equation (4.6) in the following proposition is found in Proposition 5.2.2 of [15], and equation (4.7) is an immediate consequence of Definition 4.7 and equation (4.1)

Proposition 4.8. *Given a standard action of $\pi_1(\widehat{\mathbb{C}} \setminus P_f, z_0)$ (resp. IMG(f)) on X^*, $\gamma \in \pi_1(\widehat{\mathbb{C}} \setminus P_f, z_0)$ (resp. $\in$ IMG(f)), and $x \in X$, let $\tilde{\gamma}_x$ be the lift of γ starting at $\Lambda(x)$.*

Then the action of γ on X^* is given by

$$\gamma(xv) = \gamma(x)(\ell_{\gamma(x)}^{-1}\tilde{\gamma}_x\ell_x)(v) \tag{4.6}$$

where $\gamma(x)$ is the element of X such that $\tilde{\gamma}_x$ ends in $\Lambda(\gamma(x))$. Moreover, for $v \in X^*$,

$$\gamma|_{xv} = [(\ell_{\gamma(x)})^{-1}\tilde{\gamma}_x\ell_x]|_v. \tag{4.7}$$

A remark is in order about the statements in Proposition 4.8 regarding $\mathrm{IMG}(f)$. Because $\mathrm{IMG}(f)$ is a quotient of $\pi_1(\widehat{\mathbb{C}} \setminus P_f, z_0)$, the quantities γ, $\tilde{\gamma}_x$, and $\gamma|_x$ are only defined up to elements of the faithful kernel. However, the elements of the faithful kernel act trivially on T_{f,z_0}, and hence do not affect the corresponding elements of $\mathrm{Aut}(X^*)$.

Proposition 4.9. *A standard action of $\pi_1(\widehat{\mathbb{C}} \setminus P_f, z_0)$ or IMG(f) on $\mathrm{Aut}(X^*)$ is recurrent.*

Proof. Let G stand for either $\pi_1(\widehat{\mathbb{C}} \setminus P_f, z_0)$ or $\mathrm{IMG}(f)$. Observe that Proposition 4.8 (with v the empty word) implies that G is self-similar. We now show that G acts transitively on X. Let $i, j \in X$ and let p be a path from $\Lambda(i)$ to $\Lambda(j)$ in $\widehat{\mathbb{C}} \setminus f^{-1}(P_f)$. The path $f(p)$ has endpoints $f(\Lambda(i)) = f(\Lambda(j)) = z_0$, and thus $f(p)$ gives an element of G. Observe that the lift $\widetilde{f(p)}$ of $f(p)$ beginning at $\Lambda(i)$ is precisely p. By Proposition 4.8 we then have $(f(p))(i) = j$, showing that the action of G on X is transitive.

Finally, we show that given $i \in X$ the virtual endomorphism $g \mapsto g|_i$ is a surjective map from $\{g \in G : g(i) = i\}$ to G. Let $h \in G$ and take a representative curve for h (which we will also refer to as h in an abuse of notation) that avoids $f^{-1}(P_f)$. Let the path $\bar{h}$ be the composition $\ell_i h \ell_i^{-1}$. Notice that $\bar{h}$ is a loop in $\widehat{\mathbb{C}} \setminus f^{-1}(P_f)$ based at $\Lambda(i)$. So (the homotopy class of) $f(\bar{h})$ is a loop based at z_0, and thus gives an element of G. The lift of $f(\bar{h})$ beginning at $\Lambda(i)$ is $\bar{h}$, and thus $(f(\bar{h}))(i) = i$ by Proposition 4.8. The same proposition then yields

$$f(\bar{h})|_i = \ell_i^{-1}\bar{h}\ell_i = \ell_i^{-1}\ell_i h \ell_i^{-1}\ell_i,$$

which is homotopic to h, and thus equals h in G. Therefore, the map $g \mapsto g|_i$ is onto. □

Proposition 4.5 immediately gives:

Corollary 4.10. *A standard action of IMG(f) on $\mathrm{Aut}(X^*)$ is level-transitive, and hence IMG(f) is infinite.*

To this point, the results of this section hold more generally for PCF branched self-covers of the sphere. However, if f is specifically a post-critically-finite rational map, the expansion properties of f have further implications for the iterated monodromy group. Let $P_f^{per} \subset P_f$ denote the union of all periodic orbits containing a critical point. By [13, Theorem 19.6], f is subhyperbolic because every critical orbit is finite.

That theorem is proved by constructing an orbifold metric on $\widehat{\mathbb{C}} \setminus P_f^{per}$ so that for all $p \in \widehat{\mathbb{C}} \setminus f^{-1}(P_f)$, the derivative satisfies

$$||Df(p)|| > 1. \tag{4.8}$$

For $p \in P_f^{per}$ denote by $\mathcal{U}(p)$ an open Böttcher disk containing p (as in [13, Theorem 9.1]). There is a choice of the neighborhood $\mathcal{U}(p)$ for each $p \in P_f^{per}$ so that the collection

$$\mathcal{U}^{per} := \bigcup_{p \in P_f^{per}} \mathcal{U}_p$$

has complement $K = \widehat{\mathbb{C}} \setminus \mathcal{U}^{per}$ with the property that $K' := f^{-1}(K)$ is compactly contained in K. By compactness there is a constant $0 < \rho < 1$ so that

$$||Df(p)|| \geq \frac{1}{\rho} > 1 \tag{4.9}$$

for all $p \in K'$.

In the presence of this metric expansion, certain finiteness properties hold. For example, it was used by Nekrashevych to prove the following statement on contraction (recall Definition 4.4) of self-similar groups [15, Theorem 5.5.3].

Theorem 4.11. *If $f : \widehat{\mathbb{C}} \to \widehat{\mathbb{C}}$ is PCF, then $IMG(f)$ is contracting.*

4.3. **Peripheral loops.** Let $f : \widehat{\mathbb{C}} \to \widehat{\mathbb{C}}$ be a PCF rational function, and recall that we have fixed a standard action of $\pi_1(\widehat{\mathbb{C}} \setminus P_f, z_0)$ (and hence of $\mathrm{IMG}(f)$) on X^*. In Section 6 we study this action by analyzing loops, and here we record some elementary properties of loops that will prove useful.

We say that a homotopy class of paths based at a point z is a loop if it can be represented by a loop, or equivalently if every representative is a loop. The following lemma is an immediate consequence of Proposition 4.8:

Lemma 4.12. *The lift of $g \in \pi_1(\widehat{\mathbb{C}} \setminus P_f, z_0)$ to $z \in T_{f,z_0}$ is a loop if and only if $g(\Lambda^*(z)) = \Lambda^*(z)$.*

Definition 4.13. A nontrivial element $g \in \pi_1(\widehat{\mathbb{C}} \setminus P_f, z_0)$ is *peripheral about $p \in P_f$* if for any disk neighborhood $N(p)$ of p there exists a representative of g that is freely homotopic (i.e. homotopic with continuously moving basepoint) in $\widehat{\mathbb{C}} \setminus P_f$ to a loop that is contained in $N(p)$. We call g *peripheral* if there exists a $p \in P_f$ so that g is peripheral about p.

Definition 4.14. A nontrivial element $g \in \pi_1(\widehat{\mathbb{C}} \setminus P_f, z_0)$ is called *primitive* if $g = h^m$ for $h \in \pi_1(\widehat{\mathbb{C}} \setminus P_f, z_0)$ implies that $m = 1$ or $m = -1$.

Fix a disk neighborhood $N(p)$ of p so that each component of $f^{-1}(N(p))$ contains at most one element of $f^{-1}(p)$. Let $g \in \pi_1(\widehat{\mathbb{C}} \setminus P_f, z_0)$ be peripheral about p, which by

definition means that there is a loop g_p that is freely homotopic to g and contained in $N(p)$. A lift $\widetilde{g}$ of g is said to be *associated to a point* $q \in f^{-1}(p)$ if the free homotopy $g \simeq g_p$ lifts to a free homotopy $\tilde{g} \simeq \tilde{g}_q$ (in $\widehat{\mathbb{C}} \setminus f^{-1}(P_f)$) where $\tilde{g}_q$ is contained in the component of $f^{-1}(N_p)$ that contains q. We note that given $z \in f^{-1}(z_0)$ and g peripheral about $p \in P_f$, the lift of g beginning at z is associated to precisely one $q \in f^{-1}(p)$.

Lemma 4.15. *Let $g \in \pi_1(\widehat{\mathbb{C}} \setminus P_f, z_0)$ be primitive and peripheral about $p \in P_f$, and let $\tilde{g}$ be a lift of g beginning at $z \in f^{-1}(z_0)$. Suppose that $\tilde{g}$ is associated to $q \in f^{-1}(p)$. Then q is non-critical if and only if $g(\Lambda(z)) = \Lambda(z)$.*

Proof. Let $\tilde{g}$ be a lift of g associated to q, and let $U(q)$ be the component of $f^{-1}(N(p))$ that contains q. By Lemma 4.12 we have $g(\Lambda(z)) = \Lambda(z)$ if and only if $\tilde{g}$ is a loop. By definition $\tilde{g}$ is freely homotopic to $\widetilde{g_q} \subset U(q)$ that is a lift of a loop $g_p \subset N(p)$ freely homotopic to g. It follows from the homotopy lifting property that $\tilde{g}$ is a loop if and only if $\widetilde{g_q}$ is a loop.

Because f is a branched cover, the restriction $f : U(q) \to N(p)$ is modeled on the unit disk map $z \mapsto z^d$ where $d \geq 1$ is the local degree of f at q. A primitive nontrivial loop in $\mathbb{D} \setminus \{0\}$ lifts to a loop under $z \mapsto z^d$ if and only if $d = 1$, i.e. if and only if q is non-critical. □

Lemma 4.16. *Let $g \in \pi_1(\widehat{\mathbb{C}} \setminus P_f, z_0)$ be primitive and peripheral about $p \in P_f$, and let $\tilde{g}$ be a lift of g beginning at $z \in f^{-1}(z_0)$. If $\tilde{g}$ is a loop, then it is either trivial in $\pi_1(\widehat{\mathbb{C}} \setminus P_f, z_0)$ or it is peripheral about a non-critical point in P_f.*

Proof. Let $q \in f^{-1}(p)$ be such that $\tilde{g}$ is associated to q, let $N(q)$ be a disk neighborhood of q, and assume that $\tilde{g}$ is a loop. Because g is peripheral about p, we can select a loop g_p that is freely homotopic to g and contained in a neighborhood $N(p)$ of p such that $f^{-1}(N(p))$ has a component contained in $N(q)$. Then $\tilde{g}_q$ is freely homotopic to a loop contained in $N(q)$, and hence is peripheral about q. Note that if $q \notin P_f$, then $\tilde{g}$ is trivial in $\pi_1(\widehat{\mathbb{C}} \setminus P_f, z_0)$. Because $\tilde{g}$ is a loop we have from Lemma 4.12 that $g(\Lambda(z)) = \Lambda(z)$. Hence by Lemma 4.15 we have that q is non-critical. □

The following lemma connects the dynamical properties of the post-critical set to to the action of a loop on the tree of preimages.

Lemma 4.17. *Let $g \in \pi_1(\widehat{\mathbb{C}} \setminus P_f, z_0)$ be primitive and peripheral about $p \in P_f$. Then*

1. *g fixes an end of X^* if and only if there is a backward orbit of p that does not contain a critical point, and*
2. *g fixes infinitely-many ends of X^* if there is a backward orbit of p that contains no critical point and is not a subset of P_f.*

Proof. The first statement follows from Lemma 4.15. The second statement follows from the fact that the trivial action on a subtree fixes all ends of that subtree. □

5. The fixed-point process for self-similar groups

Throughout this section, we assume $X = \{0, \dots, d-1\}$ for $d \geq 2$, and let X^n be the collection of words in X of length n. In particular, $X = X^1$. Recall that we have fixed a standard action of $\pi_1(\widehat{\mathbb{C}} \setminus P_f, z_0)$ (and hence of $\mathrm{IMG}(f)$) on X^*. As in (1.8) in the introduction, we put

$$\mathcal{N}_1 = \{g \in \mathrm{IMG}(f) : g|_v = g \text{ and } g(v) = v \text{ for some non-empty } v \in X^*\}.$$

We denote by $\mathcal{N}_1(G)$ the analogous set for an arbitrary $G \leq \mathrm{Aut}(X^*)$

In this section, we prove the following result, which is a key step in the proof of Theorem 1.7:

Theorem 5.1. *Let $f \in \mathbb{C}(z)$ be a PCF rational function of degree $d \geq 2$. Assume that d is prime or that f has doubly transitive monodromy. If every $g \in \mathcal{N}_1$ fixes infinitely many ends of X^*, then $FPP(IMG(f)) = 0$.*

For each $n \geq 1$, let G_n denote the quotient of G by the kernel of the restriction map $G \to \mathrm{Aut}(X^n)$. Recall that the profinite completion G_∞ of G with respect to the G_n (equivalently, the inverse limit of G_n under the restriction maps $G_n \to G_{n-1}$) is a compact group, and its normalized Haar measure is a probability measure μ that projects to the discrete uniform measure on each G_n. Moreover, G_∞ carries a natural action on the set of ends X^ω. The key step in the proof of Theorem 5.1 is the following result.

Theorem 5.2. *Suppose that $G \leq \mathrm{Aut}(X^*)$ is self-similar and level-transitive. If either*

1. *d is prime, or*
2. *G is recurrent and acts doubly transitively on X,*

then

$$\mu(\{g \in G_\infty : g \text{ fixes infinitely many elements of } X^\omega\}) = 0.$$

Recall that G acts doubly transitively on X if for all $i, j, k, \ell \in X$ with $i \neq j$ and $k \neq \ell$, there exists $g \in G$ with $g(i) = k$ and $g(j) = \ell/$

Theorem 5.2 is proven in Corollaries 5.6, 5.11, and 5.13. The same conclusion as in Theorem 5.2 is reached in Theorem 1.4 of [8] under the assumption that G contains a spherically transitive element, which implies that G is level-transitive, though not necessarily self-similar. We remark too that in the special case $d = 2$, Theorem 1.2 of [7] implies the conclusion of Theorem 5.2 under the assumptions that G is level-transitive and for each n the sign homomorphism $\mathrm{sgn}_n : G_n \to \{\pm 1\}$ is surjective. In this paper we must handle groups with $d = 2$ that do not have a spherically transitive element, and for which sgn_n has trivial image for all n sufficiently large.

Here is a sketch of the proof of Theorem 5.1. We define a stochastic process – that is, an infinite collection of random variables defined on a common probability space – that encodes information about the number of fixed points in X^n of elements of G_n. We then generalize the techniques of [7] and [8] and to show that this process is a

martingale provided only that G is self-similar and level-transitive. An application of a martingale convergence theorem and a result of Nekrashevych on contracting actions of iterated monodromy groups yield the final steps in the proof of Theorem 5.1.

We now give the precise construction and proofs.

Let a group G act on a set S, and for $g \in G$ put $\mathrm{Fix}(g) = \{s \in S : g(s) = s\}$. Define a stochastic process $Y_1, Y_2, \ldots$ on G_∞ by taking

$$Y_i(g) = \#\mathrm{Fix}(\pi_i(g)),$$

where π_i is the restriction map $G_\infty \to G_i$, and G_i acts on X^i. We call this the *fixed point process* of G. Because $\mu(\pi_i^{-1}(T)) = \#T/\#G_i$ for any $T \subseteq G_i$, we have that $\mu(Y_1 = t_1, \ldots, Y_n = t_n)$ is given by

$$\frac{1}{\#G_n} \#\left\{g \in G_n : g \text{ fixes } t_i \text{ elements of } X^i \text{ for } i = 1, 2, \ldots, n\right\}. \tag{5.1}$$

We denote by $E(Y)$ the expected value of the random variable Y.

Definition 5.3. A stochastic process with probability measure μ and random variables $Y_1, Y_2, \ldots$ taking values in $\mathbb{R}$ is a *martingale* if for all $n \geq 2$ and any $t_i \in \mathbb{R}$,

$$E(Y_n \mid Y_1 = t_1, Y_2 = t_2, \ldots, Y_{n-1} = t_{n-1}) = t_{n-1},$$

provided $\mu(Y_1 = t_1, Y_2 = t_2, \ldots, Y_{n-1} = t_{n-1}) > 0$.

Martingales are useful tools because they often converge in the following sense:

Definition 5.4. Let $Y_1, Y_2, \ldots$ be a stochastic process defined on the probability space Ω with probability measure μ. The process *converges* if

$$\mu\left(\omega \in \Omega : \lim_{n\to\infty} Y_n(\omega) \text{ exists}\right) = 1.$$

We give one standard martingale convergence theorem (see e.g. [6, Section 12.3] for a proof).

Theorem 5.5. *Let $M = (Y_1, Y_2, \ldots)$ be a martingale whose random variables take nonnegative real values. Then M converges.*

Since the random variables in the fixed-point process take nonnegative integer values, we immediately have the following:

Corollary 5.6. *Let $G \leq \mathrm{Aut}(X^*)$ and suppose that the fixed-point process for G is a martingale. Then*

$$\mu(\{g \in G_\infty : Y_1(g), Y_2(g), \ldots \textit{ is eventually constant}\}) = 1.$$

In particular,

$$\mu(\{g \in G_\infty : g \textit{ fixes infinitely many elements of } X^\omega\}) = 0.$$

Thus to prove Theorem 5.2, it suffices to show that the fixed-point process for G is a martingale. We therefore characterize when this happens. Let H_n be the kernel of the restriction map $G_n \to G_{n-1}$.

Theorem 5.7. *Let $G \leq \mathrm{Aut}(X^*)$. Then the fixed-point process for G is a martingale if and only if for all $n \geq 1$ and $v \in X^{n-1}$, H_n acts transitively on the set $v* = \{vx : x \in X\}$.*

Proof. Assume that H_n acts transitively on $v*$. We must show

$$E(Y_n \mid Y_1 = t_1, \ldots, Y_{n-1} = t_{n-1}) = t_{n-1}, \tag{5.2}$$

where $t_1, \ldots, t_{n-1}$ satisfy $\mu(Y_1 = t_1, \ldots, Y_{n-1} = t_{n-1}) > 0$. Because the Y_i take integer values, each t_i must be an integer. By definition, the left-hand side of (5.2) is

$$\sum_k k \cdot \frac{\mu(Y_1 = t_1, \ldots, Y_{n-1} = t_{n-1}, Y_n = k)}{\mu(Y_1 = t_1, \ldots, Y_{n-1} = t_{n-1})}. \tag{5.3}$$

Put

$$\begin{aligned} S &= \{g \in G_n : g \text{ fixes } t_i \text{ elements of } X^i \text{ for } 1 \leq i \leq n-1\} \\ S_k &= \{g \in S : g \text{ fixes } k \text{ elements of } X^n\} \end{aligned}$$

By (5.1), the expression in (5.3) is equal to $\sum_k k \cdot (\#S_k/\#S)$. This in turn may be rewritten

$$\frac{1}{\#S} \sum_{g \in S} \#\mathrm{Fix}(g). \tag{5.4}$$

Each H_n acts trivially on X^{n-1}, so S is invariant under multiplication by elements of H_n, whence S is a union of cosets of H_n. Take $gH_n \subseteq S$, and let

$$R = \{vx : v \in X^{n-1}, g(v) = v, x \in X\}.$$

Note that because $g \in S$, we have $\#R = dt_{n-1}$. If $vx \in R$, then $g(vy) = vx$ for some unique $y \in X$. Because H_n acts transitively on $v*$, the set

$$Q := \{h \in H_n : h(vx) = vy\}$$

is non-empty, and is thus a coset of $\mathrm{Stab}_{H_n}(vx)$. By standard group theory, we then have $\#Q = \#H_n/\#O_{H_n}(vx) = \#H_n/d$, where the last equality follows from the transitivity of the action of H_n on $v*$.

Now let $I(g, s)$ be the function that takes the value 1 when $g(s) = s$ and 0 otherwise. Then we have $\sum_{h \in H_n} I(gh, vx) = \#Q$ and hence

$$\sum_{vx \in R} \sum_{h \in H_n} I(gh, vx) = \#Q \cdot dt_{n-1} = \#H_n t_{n-1}.$$

Inverting the order of summation and using that $g(w) \neq w$ for $w \notin R$, we have

$$\sum_{h \in H_n} \#\mathrm{Fix}(gh) = \#H_n t_{n-1}.$$

But S is a disjoint union of cosets of H_n, and hence the expression in (5.4) equals t_{n-1}.

Assume now that H_n does not act transitively on $v*$ for some $v \in X^{n-1}$. Then the action of H_n on X^n has k orbits for some $k > d^{n-1}$, and so by Burnside's lemma we have

$$\frac{1}{\#H_n} \sum_{h \in H_n} \#\mathrm{Fix}(h) = k > d^{n-1}.$$

Because H_n is the full set of elements of G_n that fix all d^i elements of X^i for each $i = 1, \ldots, d-1$, we have

$$E(Y_n \mid Y_1 = d, \ldots, Y_{n-1} = d^{n-1}) = k > d^{n-1},$$

and hence the fixed-point process for G is not a martingale. □

Remark. When G has a spherically transitive element, it is straightforward to see that H_n acts transitively on each set $v*$; indeed, a suitable power of the spherically transitive element will give such a transitive action. This together with Theorem 5.7 gives a proof of [8, Theorem 4.2].

In light of Theorem 5.7, we examine the action of H_n on X^n.

Lemma 5.8. *Let $G \leq \mathrm{Aut}(X^*)$ act transitively on X^n. Let H_n be the kernel of the restriction $G_n \to G_{n-1}$. Then the action of H_n on X^n consists of orbits of equal length r for some $r \mid d$.*

Proof. Let $u, w \in X^n$. By the transitivity of the action of G on X^n, there is $g \in G_n$ with $g(u) = w$. If $h(u) = u'$ for $h \in H_n$, then $h^g(w) = g(u')$, where $h^g := ghg^{-1} \in H_n$. Thus g furnishes a map $O_{H_n}(u) \to O_{H_n}(w)$, which is invertible since g is a permutation of X^n. Hence $\#O_{H_n}(u) = \#O_{H_n}(w)$. Now for any $v \in X^{n-1}$, H_n preserves $v* = \{vx : x \in X\}$. Thus $v*$ is a set of d elements that is a disjoint union of H_n-orbits. It follows that each orbit of H_n has r elements for $r \mid d$. □

Corollary 5.9. *Let d be prime and $G \leq \mathrm{Aut}(X^*)$. Suppose that G is level-transitive and H_n is non-trivial for all $n \geq 1$. Then for all $n \geq 1$ and all $v \in X^{n-1}$, H_n acts transitively on the set $v*$.*

Proof. We may apply Lemma 5.8 thanks to the level-transitivity of G, and the non-triviality of H_n gives $r > 1$. But d is prime, and so $r = d$. Now each orbit of H_n is contained in $v*$ for some $v \in X^{n-1}$, and thus each orbit equals $v*$ for some $v \in X^{n-1}$. □

Remark. When $d = 2$, there is in fact a *single element* of H_n that acts transitively on $v*$ for all $v \in X^{n-1}$. Indeed, in this case G_n is a 2-group, and so by the class equation

every non-trivial normal subgroup of G_n has non-trivial intersection with the center $Z(G_n)$ of G_n. Hence there is non-trivial $h \in H_n \cap Z(G_n)$. If $h(w) = w$ for some $w \in X^n$ then $h^g(g(w)) = g(w)$ for any $g \in X^n$, and thus $h(g(w)) = g(w)$. The transitivity of G_n then gives $h = e$, a contradiction. Thus h acts without fixed points on X^n, and since $d = 2$ this is equivalent to h acting transitively on each $v*$.

In light of Corollary 5.9, in some sense the crucial question is to determine when H_n is nontrivial for all $n \geq 1$. When $d = 2$, it is shown in [7, Corollary 4.9] that when sgn_n is surjective for all $n \geq 1$, then H_n is non-trivial for all $n \geq 1$, but the proof is quite involved. Here, in contrast to [7, Corollary 4.9], we assume that G is self-similar, and this allows for a much simpler proof of a much more general result.

To streamline our argument, we define a function $v : G \to \mathbb{Z}_{\geq 0} \cup \{\infty\}$ by $v(e) = \infty$ for the identity $e \in \mathrm{Aut}(X^*)$ and

$$v(g) = \max\{n \geq 0 : g \text{ acts trivially on } X^n\}$$

for $e \neq g \in \mathrm{Aut}(X^*)$. Note that each $g \in \mathrm{Aut}(X^*)$ fixes the lone element of X^0, and hence $v(g) \geq 0$. Moreover, for $n \geq 1$, H_n is non-trivial if and only if $n \in v(G)$. Finally, we remark that $v(g) = n \geq 1$ if and only if g acts trivially on X^1 and

$$\min\{v(g|_x) : x \in X\} = n - 1 \tag{5.5}$$

Proposition 5.10. *Let $G \leq \mathrm{Aut}(X^*)$ be infinite and self-similar. Then v is surjective.*

Proof. Suppose first that there is $N \geq 0$ with $v(g) \leq N$ for all $g \in G \setminus \{e\}$. We claim that the natural quotient map $\pi_N : G \twoheadrightarrow G_N$ is an isomorphism, and thus G is finite. Indeed, if $\pi_N(g) = \pi_N(h)$, then gh^{-1} acts trivially on X^N, and hence $v(gh^{-1}) > N$. Thus $gh^{-1} = e$, proving the claim.

Therefore the infinitude of G implies that $v(G)$ is infinite. Suppose now that $n \in v(G)$ for some $n \geq 1$, and let $g \in G$ with $v(g) = n$. From (5.5) there is $x \in X$ with $v(g|_x) = n - 1$. By the self-similarity of G, we have $g|_x \in G$, and thus $n - 1 \in v(G)$. By induction $\{0, 1, \ldots n\} \subseteq v(G)$. The infinitude of $v(G)$ then implies that v is surjective. □

We remark that Proposition 5.10 is not true in general if G fails to be self-similar. For example, let $d = 2$ and consider the group $J = \{e, (00\ 11)(01\ 10)\} \leq \mathrm{Aut}(X^2)$. Then the iterated wreath product of J gives a closed subgroup $G \leq \mathrm{Aut}(X^*)$ with the property that $2n \notin v(G)$ for all $n \geq 1$. Note that in this case G is a self-similar subgroup of $\mathrm{Aut}(Y^*)$, where $Y = X^2$.

Corollary 5.11. *Let d be prime and $G \leq \mathrm{Aut}(X^*)$. Suppose that G is self-similar and level-transitive. Then the fixed-point process associated to G is a martingale.*

Proof. The level-transitivity of G implies that G is infinite, and the Corollary then follows from Theorem 5.7, Corollary 5.9, and Proposition 5.10. □

Theorem 5.12. *Let $G \leq \mathrm{Aut}(X^*)$ be a recurrent group whose action on X is doubly transitive. Then for all $w \in X^n$ and $i, j \in X$ with $i \neq j$, there exists $g \in H_n$ such that $g|_w$ takes i to j.*

Proof. First note that by Proposition 4.5, G is infinite. By Proposition 5.10, the function $v : G \to \mathbb{Z} \cup \{\infty\}$ defined by

$$v(g) = \max\{n \geq 0 \mid g \text{ acts trivially on } X^n\}$$

is surjective, so there exists $g \in G$ with $v(g) = n$, i.e. $g \in H_n$ and g is non-trivial.

By Proposition 4.5, G is level-transitive. Thus by passing to a conjugate we may assume that g acts non-trivially on $w* = \{wx \mid x \in X\}$. Let $h = g|_w$. Since h acts non-trivially on X, there exist $k, \ell \in X$ with $k \neq \ell$ such that $h(k) = \ell$.

By double-transitivity, we can choose $t \in G$ such that $t(i) = k$ and $t(j) = \ell$. Since the action of G is recurrent, we can choose $s \in G$ such that $s(w) = w$ and $s|_w = t$. Now $s^{-1}gs$ fixes w and is also in H_n, because H_n is a normal subgroup of $\mathrm{Aut}(X^*)$. From (4.3) we then have

$$(s^{-1}gs)|_w = s^{-1}|_w g|_w s|_w = t^{-1}ht.$$

But $(t^{-1}ht)(i) = j$, as desired. □

Theorems 5.7 and 5.12 immediately give:

Corollary 5.13. *Let $G \leq \mathrm{Aut}(X^*)$ be a recurrent group whose action on X is doubly transitive. Then the fixed-point process for G is a martingale.*

Proof. By Theorem 5.12, for all $n \geq 1$, and all $v \in X^{n-1}$, the action of the elements of G that act trivially on X^{n-1} is transitive on the set $v* = \{vx \mid x \in X\}$. Notice that the images under the quotient map to G_n of elements of G that act trivially on X^{n-1} lie in H_n. Thus, by Theorem 5.7, the fixed-point process for G is a martingale. □

Suppose now that G is contracting, and let $\mathcal{N} \subset G$ be a finite set as in Definition 4.4. If $g \in \mathcal{N}_1(G)$, then by definition there is $v \in X^*$ with $g(v) = v$ and $g|_v = g$, and hence taking w_n to be the concatenation of v with itself n times, we have $g|_{w_n} = g$. It follows that $g \in \mathcal{N}$, and hence $\mathcal{N}_1(G)$ is finite.

We now provide the final step in the proof of Theorem 5.1.

Theorem 5.14. *Suppose that $G \leq \mathrm{Aut}(X^*)$ is contracting and its fixed point process is a martingale. If every $g \in \mathcal{N}_1(G)$ fixes infinitely many ends of X^*, then $FPP(G) = 0$.*

Proof. This is proven in [8, p. 2033], but we give the argument here for completeness. Let $\mathcal{N} \subset G$ be a finite set as in Definition 4.4. Suppose that $g \in G$ fixes some end $w = x_1x_2\cdots$ of X^*. Let $v_n = x_1x_2\cdots x_n$ for each $n \geq 1$, and consider the sequence of restrictions $g|_{v_1}, g|_{v_2}, \ldots$. For n large enough, we have $g|_{v_n} \in \mathcal{N}$, and $g|_{v_n}$ fixes the end $x_{n+1}x_{n+2}\cdots$ since g fixes w. Because $\mathcal{N}$ is finite, there must be $i < j$ with $g|_{v_i} = g|_{v_j}$. Let $h = g|_{v_i}$, and note that for $w = x_{i+1}x_{i+2}\cdots x_j$ we have $h(w) = w$ and $h|_w = h$. Hence $h \in \mathcal{N}_1(G)$, and by hypothesis fixes infinitely many ends of X^*. Inserting v_i on

the beginning of each of these ends, we obtain infinitely many ends of X^* fixed by g. Hence by Corollary 5.6, g lies in a set of measure zero, proving the theorem. □

Proof of Theorem 5.1. This is an immediate consequence of Corollary 5.11, Corollary 5.13, Theorem 5.14, and the fact that any standard action of $\mathrm{IMG}(\psi)$ on X^* is recurrent and contracting by Proposition 4.9 and Corollary 4.11 □

6. Iterated monodromy action of PCF rational functions

In light of Theorem 5.1, the proof of Theorem 1.7 will be complete once we establish Theorem 1.8, which we restate here for the convenience of the reader. First recall that we have fixed a standard action of $\pi_1(\widehat{\mathbb{C}} \setminus P_f, z_0)$ (and hence of $\mathrm{IMG}(f)$) on X^*, and recall the definition of $\mathcal{N}_1$ from (1.8) (or the beginning of Section 5).

Theorem 6.1 (Theorem 1.8)**.** *Let $f \in \mathbb{C}(z)$ be a PCF rational function that is not dynamically exceptional. Then every element of $\mathcal{N}_1$ fixes infinitely many ends of X^*.*

The key dynamical property underlying the proof of Theorem 6.1 is subhyperbolicity, i.e. that PCF rational functions are expanding away from periodic post-critical points in the orbifold metric as described on p. 23. We observe that this expansion fails to hold in general for PCF branched covers $f : \mathbb{S}^2 \to \mathbb{S}^2$, and there exist such covers (necessarily not rational functions) that are not dynamically exceptional yet have elements of $\mathcal{N}_1$ fixing only finitely many ends of X^*.

The converse of Theorem 6.1 holds as well, thus giving a characterization of exceptional rational functions. Though it is not necessary for this paper, we give a proof in Theorem 6.9.

6.1. **End behavior of non-exceptional maps: fundamental group.** The proof of Theorem 6.1 relies on lifts of loops representing elements of $\mathrm{IMG}(f)$. We thus work first on the level of the fundamental group and later argue that nothing is lost when passing to the faithful quotient (Proposition 6.6). We define the fundamental group version of $\mathcal{N}_1$, noting that it depends on the choice of standard action made on p. 22.

$$\mathcal{N}_1^\pi := \{g \in \pi_1(\widehat{\mathbb{C}} \setminus P_f) : \ \exists \text{ non-empty } w \in X^* \text{ so that } g(w) = w \text{ and } g|_w = g\}. \tag{6.1}$$

The basepoint of the fundamental group in (6.1) is not specified because the definition is independent of basepoint in the following narrow sense. Let α be a path in $\widehat{\mathbb{C}} \setminus P_f$ that connects a new basepoint z_1 to the original basepoint z_0. The map $\alpha_* : \pi_1(\widehat{\mathbb{C}} \setminus P_f, z_0) \to \pi_1(\widehat{\mathbb{C}} \setminus P_f, z_1)$ defined by $\alpha_*(g) = \alpha^{-1} g \alpha := g^\alpha$ is an isomorphism. We define a standard action of $\pi_1(\widehat{\mathbb{C}} \setminus P_f, z_1)$ on X^* by taking the paths connecting z_1 to $f^{-1}(z_1)$ to be $\tilde{\alpha}_x^{-1} \ell_x \alpha$ where $\tilde{\alpha}_x$ is the unique lift of α terminating at $\Lambda(x)$. The labeling map $\Lambda_\alpha : X \to f^{-1}(z_1)$ is defined by taking $\Lambda_\alpha(x)$ to be the beginning point of $\tilde{\alpha}_x$. Having specified the standard action at the basepoint z_1, we see that elements identified by the isomorphism α_* have equal actions on X^*.

Suppose that $g(x) = x$ for $g \in \pi_1(\widehat{\mathbb{C}} \setminus P_f, z_0)$. Then the lift of g^α based at x, denoted $\tilde{g^\alpha}$, satisfies

$$\tilde{g^\alpha} = \tilde{\alpha_x}^{-1} \tilde{g}_x \tilde{\alpha_x},$$

where $\tilde{g}_x$ is the unique lift of g based at $\Lambda(x)$. A consequence of this definition is that if $g|_x = g$ and $g(x) = x$, then from Proposition 4.8 we have

$$\begin{aligned} g^\alpha|_x &= (\tilde{\alpha}_x^{-1} \ell_x \alpha)^{-1} \tilde{g^\alpha} (\tilde{\alpha}_x^{-1} \ell_x \alpha) \\ &\simeq \alpha^{-1} \ell_x^{-1} \tilde{g}_x \ell_x \alpha \\ &= \alpha^{-1} g|_x \alpha \\ &\simeq \alpha^{-1} g \alpha \\ &= g^\alpha. \end{aligned}$$

Extending to words of higher length using Equations (4.1), we see that membership in $\mathcal{N}_1^\pi$ is unaffected by a change of basepoint.

Due to subhyperbolicity, the elements of $\mathcal{N}_1^\pi$ are very special. Recall the discussion of peripheral loops in Section 4.3.

Proposition 6.2. *Each nontrivial element of $\mathcal{N}_1^\pi$ is peripheral about a repelling periodic post-critical point.*

Proof. Suppose that $g \in \mathcal{N}_1^\pi$ is nontrivial. By the remarks immediately preceding this proposition, we may assume that the basepoint of the fundamental group is in the compact subset K' where the expansion of Equation (4.9) holds. Choose a representative γ of g so that γ lies in K'. By hypothesis there exists a non-empty $w \in X^*$ where $g(w) = w$ and $g|_w = g$. For $i \geq 1$, let γ_i be the lift of γ based at $\Lambda^*(w^i)$ where w^i is the concatenation of i copies of w. Since $g(w^i) = w^i$, Lemma 4.12 implies that each γ_i is a loop. Equation (4.7) implies that $g|_{w^i} = [\ell_{w^i}^{-1} \gamma_i \ell_{w^i}]$, where there is an evident free homotopy $\ell_{w^i}^{-1} \gamma_i \ell_{w^i} \simeq \gamma_i$ in $\widehat{\mathbb{C}} \setminus P_f$. Since $g|_{w^i} = g$ by hypothesis, it follows that there is a free homotopy $\gamma_i \simeq \gamma$ in $\widehat{\mathbb{C}} \setminus P_f$. Each γ_i is in the compact set K' since $f^{-1}(K') \subset K'$, so Equation (4.9) implies that the length of γ_i converges to 0 as $i \to \infty$, and hence the curves γ_i converge to a point $p \in \widehat{\mathbb{C}}$. Because g is nontrivial, g has non-trivial restrictions at arbitrarily long words, and hence p must be a periodic post-critical point. Each post-critical cycle of a PCF rational function either contains a critical point or is repelling. The compact set K' was produced by deleting neighborhoods of the periodic critical cycles, and therefore p is repelling. For large enough i, γ_i is peripheral about p, and because each γ_i is freely homotopic to $\gamma \in g$, we conclude that g is peripheral about the same point. □

An immediate application of Proposition 6.2 is that $\mathcal{N}_1^\pi$ is closed under passing to primitives:

Corollary 6.3. *If $g^m \in \mathcal{N}_1^\pi$ for some $g \in \pi_1(\widehat{\mathbb{C}} \setminus P_f)$, then $g \in \mathcal{N}_1^\pi$.*

Proof. Let $w \in X^*$ be such that $g^m(w) = w$ and $g^m|_w = g^m$. Denote the length of w by $|w|$. If g^m is trivial in $\pi_1(\widehat{\mathbb{C}} \setminus P_f)$, then so is g, whence $g \in \mathcal{N}_1^\pi$. Otherwise, by Proposition 6.2, g^m is peripheral about a repelling periodic point p. In the nontrivial case of $|P_f| > 2$ the universal cover of $\widehat{\mathbb{C}} \setminus P_f$ is the hyperbolic disk. The deck transformation corresponding to each peripheral loop is a parabolic element (a Möbius transformation with exactly one fixed point), and the deck transformation corresponding to each non-peripheral loop is hyperbolic (a Möbius transformation with exactly two fixed points). The power of a hyperbolic element is hyperbolic, so if g^m is peripheral g is also peripheral. Moreover the fixed set of the deck transformation corresponding to g coincides with that of g^m, so g must also be peripheral about p. Since a repelling periodic point contains no critical point in its forward orbit, each iterate of f is univalent on some neighborhood of p. Thus the lift of g based at $\Lambda^*(w)$ is a loop so by Lemma 4.12, $g(w) = w$. Thus $g|_w = g^k$ for some $k \in \mathbb{Z} \setminus \{0\}$. The fact that $f^{|w|}$ is univalent and orientation preserving near p implies that $k = 1$.

□

Remark. Each end of X^* that is fixed by g is also fixed by g^m. Thus if g^m fixes only finitely many ends, so must g.

Recall that a complex rational map is *dynamically exceptional* if there exists a finite, nonempty set Σ with

$$f^{-1}(\Sigma) \setminus C_f = \Sigma,$$

where $C_f \subset \widehat{\mathbb{C}}$ is the set of critical points of f. Let $p \in \Sigma$ and observe that every choice of a backward orbit of p must intersect the critical set with only one possible exception: p is contained in a periodic cycle (which necessarily contains no critical points, so will be a repelling cycle under forward iteration).

Proposition 6.4. *Suppose f is a PCF rational map with an element $g \in \mathcal{N}_1^\pi$ that fixes only finitely-many ends of X^*. Then f is dynamically exceptional.*

Proof. Since g is clearly not trivial, Proposition 6.2 implies g is peripheral about some post-critical point p that is contained in a non-critical cycle. We may assume that g is primitive and fixes only finitely many ends of X^* by Corollary 6.3 and the ensuing remark. Let $\Sigma \subset \widehat{\mathbb{C}}$ be the set of points whose forward orbit contains p but does not intersect C_f. Since p lies in a non-critical cycle, $p \in \Sigma$ and so $\Sigma \neq \emptyset$. Because g is primitive and peripheral, we may invoke the second part of Lemma 4.17 to conclude that every backward orbit of p either intersects C_f or is a subset of P_f. Thus $\Sigma \subset P_f$ and is hence finite.

We now argue that $\Sigma = f^{-1}(\Sigma) \setminus C_f$. Because p is periodic, it follows that $f(\Sigma) \subset \Sigma$. Thus $\Sigma \subset f^{-1}(\Sigma)$ and since $\Sigma \cap C_f = \emptyset$, it follows that $\Sigma \subset f^{-1}(\Sigma) \setminus C_f$. To see that $f^{-1}(\Sigma) \setminus C_f \subset \Sigma$, observe that if $x \in f^{-1}(\Sigma) \setminus C_f$ then $f(x) \in \Sigma$, and hence the forward orbit of $f(x)$ contains p. Thus the forward orbit of x contains p, and since x is not critical, $x \in \Sigma$. This proves that f is dynamically exceptional. □

6.2. **End behavior of non-exceptional maps: IMG.** A sequence of elements $(g_n)_{n=0}^{\infty}$ in a group is said to be *eventually periodic* (resp. *eventually peripheral*) if there is some integer N so that $(g_n)_{n=N}^{\infty}$ is periodic. (resp. peripheral) Note that periodic sequences are eventually periodic under this definition.

For any string $w \in X^n$ and a positive integer m, recall that we denote by w^m the string in X^{mn} formed by concatenating m copies of w.

Lemma 6.5. *Suppose that there is $g \in \pi_1(\widehat{\mathbb{C}} \setminus P_f)$ and a nonempty word w so that $g(w^m) = w^m$ for all $m > 0$. Then the sequence of restrictions $g_m := g|_{w^m}$ is eventually periodic.*

Remark. For a PCF rational map f it is known that $IMG(f)$ is contracting (Theorem 4.11). Since the finite set $\mathcal{N} \subset IMG(f)$ of Definition 4.4 is closed under restriction, the lemma clearly holds if "$\pi_1(\widehat{\mathbb{C}} \setminus P_f)$" is replaced with "$IMG(f)$". However, the same argument cannot be used to prove Lemma 6.5 because there is in general no finite set $\mathcal{N}$ as in Definition 4.4 for $G = \pi_1(\widehat{\mathbb{C}} \setminus P_f)$. Consider for example the Chebyshev map $f(z) = z^2 - 2$, which has a repelling fixed point at 2. Let α be a loop that is peripheral about 2. Observe that $f^{-1}(2) = \{\pm 2\}$, and so there is $x \in X$ such that $\alpha(x) = x$ and $\alpha|_x = \alpha$. Concatenating x with itself n times gives a word $w \in X^n$ with $\alpha(w) = w$ and $\alpha|_w = \alpha$. These same statements hold with α replaced by α^m, and because the α^m are pairwise non-homotopic this gives rise to an infinite subset of $\pi_1(\widehat{\mathbb{C}} \setminus P_f)$ that can occur as restrictions of arbitrarily long words. In conclusion, Lemma 6.5 is not an immediate consequence of the existing theory.

Remark. The following proof in fact shows that the sequence g_m is eventually constant, rather than merely eventually periodic. However, eventual periodicity is sufficient for our purposes.

Proof. Recall the construction of the backward-invariant compact set K' where expansion holds. As with the proof of Proposition 6.2, we may assume the basepoint y_0 for the fundamental group $\pi_1(\widehat{\mathbb{C}} \setminus P_f)$ is in K'. Let $F = f^{|w|}$, and fix a representative $\gamma \subset K'$ of the class g. Let $\gamma_m := \gamma|_{w^m}$. If there exists m_0 so that the homotopy class $[\gamma_{m_0}]$ is trivial, then $[\gamma_m]$ is trivial for all $m > m_0$, and hence $[\gamma_m]$ is eventually periodic (indeed, eventually constant). For the rest of the proof we assume that $[\gamma_m]$ is non-trivial for all m.

We recall the explicit construction of γ_m via a standard action, as described in Definition 4.7. We assume the paths $\{\ell_i\}$ in Definition 4.7 are selected to lie in K'. Because $g(w) = w$ it follows from Proposition 4.8 that $\gamma|_w = l_1^{-1}\tilde{\gamma}_w l_1$, where $\tilde{\gamma}_w$ is the lift of γ starting at $\Lambda^*(w)$ and l_1 is a concatenation of lifts of the paths ℓ_x, corresponding to the letters in the word w. Because K' is backward invariant and each $\ell_x \subset K'$, we have $l_1 \subset K'$. Denote by y_1 the endpoint of l_1, which by Equation (4.5) is the same as $\Lambda^*(w)$.

Now define the sequence $y_m := \Lambda^*(w^m) \in \widehat{\mathbb{C}}$. Let l_i be the unique lift of l_1 under F^{i-1} based at y_{i-1}, and observe that l_i connects y_{i-1} to y_i and is contained in K'. Finally, let λ_m be the concatenation of the paths $l_1, \ldots, l_m$, where evidently λ_m connects y_0 to y_m. Due to the geometric expansion of F on K' in the orbifold metric from equation (4.9), the lengths of the paths l_m decrease geometrically. Hence the sequence (y_i) is Cauchy and converges to a point $p \in \widehat{\mathbb{C}}$. Moreover, the length of λ_m is uniformly bounded and so λ_m converges to a path λ_∞ of finite length that connects y_0 to p.

The continuity of F and the equation $F(y_i) = y_{i-1}$ imply that $F(p) = p$. Let α_m be the unique lift of γ under F^m based at y_m. The hypothesis that $g(w^m) = w^m$ together with Lemma 4.12 imply that α_m is a loop and so $\gamma_m = \lambda_m^{-1}\alpha_m\lambda_m$ for each m. By (4.9), the length of α_m converges to 0, so α_m is arbitrarily small for large m. We have already dispensed with the case that α_m is homotopically trivial, thus it follows that α_m is eventually peripheral about $p \in P_f$.

Since both α_m and $\lambda_\infty \setminus \lambda_m$ have length converging to zero, for each disk of radius ϵ about p (denoted $D_\epsilon(p)$) there exists an integer N so that for $m > N$, the paths γ_m and γ_{m+1} coincide on the complement of $D_\epsilon(p)$ up to reparametrization. Fix ϵ so that $D_\epsilon(p) \cap P_f \setminus \{p\} = \emptyset$ and $\alpha_m \subset D_\epsilon(p)$ for all $m > N$. Since F maps α_{m+1} to α_m with degree 1, we have that the loops α_m and α_{m+1} are freely homotopic in $D_\epsilon(p) \setminus \{p\}$. We thus have two peripheral loops γ_m and γ_{m+1} that agree outside of $D_\epsilon(p)$ and are both freely homotopic to the same curve in $D_\epsilon(p)$. Therefore there is a based homotopy between γ_m and γ_{m+1}, showing that $g_m = g_{m+1}$. □

Proposition 6.6. *Let f be a PCF rational function. Then some element of $\mathcal{N}_1^\pi$ fixes only finitely many ends of X^* if and only if some element of $\mathcal{N}_1$ fixes only finitely many ends of X^*.*

Proof. Recall from Definition 4.6 that $\mathrm{IMG}(f)$ is the quotient of $\pi_1(\widehat{\mathbb{C}} \setminus P_f)$ by the faithful kernel K of the monodromy action on X^*. So if $g \in \mathcal{N}_1^\pi$ fixes only finitely-many ends of X^*, then its image under the quotient is an element of $\mathcal{N}_1$ that fixes only finitely-many ends of X^*.

Now assume there is an element $\bar{g} \in \mathcal{N}_1$ that fixes only finitely-many ends of X^*. It follows from the definition of $\mathcal{N}_1$ that there is a finite string $w \in X^n$ for some $n \geq 1$ so that $\bar{g}(w) = w$ and $\bar{g}|_w = \bar{g}$. Let $g \in \pi_1(\widehat{\mathbb{C}} \setminus P_f)$ be in the coset of K represented by $\bar{g}$. Then for each $m \geq 1$ we have $g(w^m) = w^m$, but we only know that $g|_{w^m}$ and g lie in the same coset of K.

Define the sequence $g_m := g|_{w^m}$, observing that each g_m fixes only finitely many ends of X^*. It follows from Lemma 6.5 that $g_{m_1} = g_{m_2}$ for some $m_1 \neq m_2$. Then the restriction of g_{m_1} to $w^{|m_2 - m_1|}$ is g_{m_2} (indeed, by the second remark before the proof of Lemma 6.5, we may take $m_2 - m_1 = 1$). This proves that $g_{m_1} \in \mathcal{N}_1^\pi$. □

Proof of Theorem 6.1 (a.k.a. Theorem 1.8). Let f be a PCF rational map that is not exceptional. The contrapositive of Proposition 6.4 guarantees that each element of $\mathcal{N}_1^\pi$

fixes infinitely many ends. Then Proposition 6.6 implies that each element of $\mathcal{N}_1$ fixes infinitely many ends. □

6.3. **Characterization of exceptional maps.** A characterization of dynamically exception maps is given in Theorem 6.9, though this result is not used elsewhere in this paper. The result is easily proved if the set Σ contains a fixed point, but the presence of higher period cycles requires some minor technicality about passing to iterates.

Recall the construction of the standard tree X^* from Section 4.2 in terms of the labeling map

$$\Lambda : X = \{0, \dots d-1\} \to f^{-1}(z_0). \tag{6.2}$$

In principle, one could use the construction of that section to associate a standard action to f^n using a labeling map $\{0, \dots, d^n - 1\} \to f^{-n}(z_0)$. However, we choose to use a labeling that is compatible with the standard action induced by Λ in (6.2). Specifically, our new labeling map

$$\Lambda_n : X^n \to f^{-n}(z_0)$$

is defined for a given point $w \in X^n$ by $\Lambda_n(w) = \Lambda^*(w)$, where Λ^* is the extension of Λ to elements of X^* described in (4.5). In this way, the point $\Lambda_n(w) \in f^{-n}(z_0)$ is labeled by a string of n characters in the alphabet X, even though it is a "first-level" preimage of z_0 under f^n. Define the connecting path for $z \in f^{-n}(z_0)$ to be $\ell_{\Lambda_n(z)}$. This data defines a tree isomorphism from the preimage tree T_{f^n,z_0} to a standard d^n-ary tree which we denote $(X, f^n)^*$, as well as a standard action by $\pi_1(\widehat{\mathbb{C}} \setminus P_{f^n})$. Since $P_{f^n} = P_f$, we have that

$$\pi_1(\widehat{\mathbb{C}} \setminus P_{f^n}) = \pi_1(\widehat{\mathbb{C}} \setminus P_f).$$

Using this newly defined standard action, we may now define the iterated analogue of Equation 6.1:

$$\mathcal{N}_1^\pi(f^m) := \{g \in \pi_1(\widehat{\mathbb{C}} \setminus P_f) \,:\, \exists \text{ nontrivial } w \in (X, f^m)^* \text{ so that } g(w) = w \text{ and } g|_w = g\}$$

Lemma 6.7. *Let f be a PCF rational map, and let $m \geq 1$. Then $\mathcal{N}_1^\pi(f^m) \subset \mathcal{N}_1^\pi$.*

Proof. Let $g \in \mathcal{N}_1^\pi(f^m)$. Then there exists nontrivial $w \in (X, f^m)^*$ so that $g(w) = w$ and $g|_w = g$. By construction $\Lambda^*(w) = \Lambda_m(w)$. Since $f^{m|w|} = (f^m)^{|w|}$, Proposition 4.8 implies that the action of g on w is independent of whether w is a vertex in X^* or $(X, f^m)^*$. Likewise, Equation 4.7 of Proposition 4.8 implies that $g|_w$ is independent of whether w is a vertex in X^* or $(X, f^m)^*$. Thus considering w now as an element of X^*, we have that the standard action on X^* satisfies $g(w) = w$ and $g|_w = g$.

□

Proposition 6.8. *Let f be a dynamically exceptional map that is PCF. Then for some n, there exists $g \in \mathcal{N}_1^\pi(f^{\circ n})$ that fixes only finitely-many ends of $(X, f^{\circ n})^*$.*

Proof. Recall that for a dynamically exceptional map, the set Σ satisfies $f(\Sigma) \subset \Sigma$, so there must be some point $p \in \Sigma$ that is periodic. By the defining property of Σ, the point p cannot lie in a critical cycle. Since f is PCF, p must then be repelling. Passing to an iterate, we assume that p is fixed. Let $\lambda := f'(p)$.

Recall that fixed repelling periodic points are linearizable [13, Thm 8.2], namely there is a univalent holomorphic change of coordinates $\phi(z) = w$ on some neighborhood U of p so that $\phi(p) = 0$ and $\phi \circ f \circ \phi^{-1} = \lambda w$. Choose U so that $f(U)$ intersects the post-critical set only at p (this is possible since f is PCF). Let A be the preimage under ϕ of a fundamental annulus in coordinates. Then ∂A consists of two topological circles C and C' with $f(C') = C$.

Fix a basepoint $z \in C$ and an orientation on C. Let g be a loop based at z that winds once around p (i.e. is primitive) and respects the orientation. Let g' be the unique lift of g contained in C', where evidently the map $g' \to g$ is univalent. Let $z' \in C'$ be the unique preimage of z under this map. Let $\ell_{z'}$ be some choice of connecting path in A that joins z to z'. The path $\ell_{z'}^{-1} g' \ell_{z'}$ is a loop in A based at z. Using the annular coordinates defined by $A \subset \widehat{\mathbb{C}} \setminus P_f$, it can be shown that $\ell_{z'}^{-1} g' \ell_{z'}$ is homotopic to g relative to the basepoint. Since f is orientation preserving, g and g' have the same orientation. Let w be the label of the point z', i.e. $\Lambda(w) = z'$. Then from what was just argued, $g|_w = g$. By the univalence of $g' \to g$, it follows that $g(w) = w$.

Since f is dynamically exceptional and p is fixed, any backward orbit other than the constant one at the fixed point p will meet a critical point. By Lemma 4.15, the only end of X^* that the action of g will fix is w^∞. □

Theorem 6.9. *A PCF complex rational map f is dynamically exceptional if and only if there is an element $g \in \mathcal{N}_1$ that fixes only finitely many ends of X^*.*

Proof. Suppose that f is dynamically exceptional and PCF. Then by Proposition 6.8, there is an element of $\mathcal{N}_1^\pi(f^m)$ that fixes only finitely-many elements of $(X, f^m)^*$. By Lemma 6.7, this element is also an element of $\mathcal{N}_1^\pi$. Proposition 6.6 guarantees existence of an element in $\mathcal{N}_1$ that fixes only finitely-many ends of $(X, f^m)^*$, and by the identification of the ends of $(X, f^m)^*$ with the ends of X^*, it only fixes finitely-many ends of X^* as well.

Suppose now instead that f is a PCF rational map such that there is an element of $\mathcal{N}_1$ that fixes only finitely-many ends. Then by Proposition 6.6 there is an element of $\mathcal{N}_1^\pi$ that fixes only finitely-many ends. By Proposition 6.4, the map is dynamically exceptional. □

References

[1] Laurent Bartholdi and Dzmitry Dudko. Algorithmic aspects of branched coverings IV/V. Expanding maps. *Trans. Amer. Math. Soc.*, 370:7679–7714, 2018.

[2] Robert Benedetto, Patrick Ingram, Rafe Jones, and Alon Levy. Attracting cycles in p-adic dynamics and height bounds for postcritically finite maps. *Duke Math. J.*, 163(13):2325–2356, 2014.

[3] Philippe Flajolet and Andrew M. Odlyzko. Random mapping statistics. In *Advances in cryptology—EUROCRYPT '89 (Houthalen, 1989)*, volume 434 of *Lecture Notes in Comput. Sci.*, pages 329–354. Springer, Berlin, 1990.
[4] Otto Forster. *Lectures on Riemann surfaces*, volume 81 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1991. Translated from the 1977 German original by Bruce Gilligan, Reprint of the 1981 English translation.
[5] Derek Garton. Periodic points of polynomials over finite fields, 2021.
[6] Geoffrey Grimmett and David Stirzaker. *Probability and random processes*. Oxford University Press, New York, third edition, 2001.
[7] Rafe Jones. Iterated Galois towers, their associated martingales, and the p-adic Mandelbrot set. *Compos. Math.*, 143(5):1108–1126, 2007.
[8] Rafe Jones. Fixed-point-free elements of iterated monodromy groups. *Trans. Amer. Math. Soc.*, 367(3):2023–2049, 2015.
[9] Jamie Juul. The image size of iterated rational maps over finite fields. *Int. Math. Res. Not. IMRN*, (5):3362–3388, 2021.
[10] 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.
[11] Michelle Manes and Bianca Thompson. Periodic points in towers of finite fields for polynomials associated to algebraic groups. *Rocky Mountain J. Math.*, 49(1):171–197, 2019.
[12] John Milnor. Geometry and dynamics of quadratic rational maps. *Experiment. Math.*, 2(1):37–83, 1993. With an appendix by the author and Lei Tan.
[13] John Milnor. *Dynamics in One Complex Variable*, volume 160 of *Annals of Mathematics studies*. Princeton University Press, 2006.
[14] John Milnor. On Lattès maps. In *Dynamics on the Riemann sphere*, pages 9–43. Eur. Math. Soc., Zürich, 2006.
[15] Volodymyr Nekrashevych. *Self-similar groups*, volume 117 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2005.
[16] Richard Pink. Finiteness and liftability of postcritically finite quadratic morphisms in arbitrary characteristic. Available at http://arxiv.org/abs/1305.2841.
[17] Richard Pink. Profinite iterated monodromy groups arising from quadratic polynomials. Available at http://arxiv.org/abs/1307.5678.
[18] Richard Pink. On the order of the reduction of a point on an abelian variety. *Math. Ann.*, 330(2):275–291, 2004.
[19] J. M. Pollard. A Monte Carlo method for factorization. *Nordisk Tidskr. Informationsbehandling (BIT)*, 15(3):331–334, 1975.
[20] Michael Rosen. *Number theory in function fields*, volume 210 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002.
[21] Simone Ugolini. On the iterations of certain maps $X \mapsto K \cdot (X + X^{-1})$ over finite fields of odd characteristic. *J. Number Theory*, 142:274–297, 2014.

Email address: andrewbridy@gmail.com

Departments of Political Science and Computer Science, Yale University, 125 Prospect St, New Haven, CT 06511, USA

Email address: rfjones@carleton.edu

Department of Mathematics and Statistics, Carleton College, 1 North College St, Northfield, MN 55057, USA

Email address: gkelsey@bellarmine.edu

Department of Mathematics, Bellarmine University, 2001 Newburg Rd., Louisville, KY 40205, USA

Email address: russell.lodge@indstate.edu

Department of Mathematics and Computer Science, Indiana State University, 200 North Seventh Street, Terre Haute, IN 47809, USA