J. Juul et al. (2016) “Wreath Products and Proportions of Periodic Points,”
International Mathematics Research Notices, Vol. 2016, No. 13, pp. 3944–3969
Advance Access Publication September 25, 2015
doi:10.1093/imrn/rnv273

# Wreath Products and Proportions of Periodic Points

**Jamie Juul[1], Pär Kurlberg[2], Kalyani Madhu[1], and Tom J. Tucker[1]**

[1]Department of Mathematics, University of Rochester, Rochester,
NY 14627, USA and [2]Department of Mathematics, KTH, SE-100 44
Stockholm, Sweden

*Correspondence to be sent to: e-mail: thomas.tucker@rochester.edu*

Let $\varphi : \mathbb{P}^1 \longrightarrow \mathbb{P}^1$ be a rational map of degree greater than 1 defined over a number field $k$ with ring of integers $\mathfrak{o}_k$. For each prime $\mathfrak{p}$ of good reduction for $\varphi$, we let $\varphi_{\mathfrak{p}}$ denote the reduction of $\varphi$ modulo $\mathfrak{p}$. A random map heuristic suggests that for large $\mathfrak{p}$, the proportion of periodic points of $\varphi_{\mathfrak{p}}$ in $\mathbb{P}^1(\mathfrak{o}_k/\mathfrak{p})$ should be small. We show that this is indeed the case for many rational functions $\varphi$.

## 1 Introduction

Let $f$ be a polynomial in $\mathbb{Z}[x]$ of degree greater than 1. Then $f$ induces a map $f_p : \mathbb{F}_p \longrightarrow \mathbb{F}_p$ for each prime $p$ via reduction modulo $p$. Any point $\alpha \in \mathbb{F}_p$ will be *preperiodic* under $f_p$; the fact that $\mathbb{F}_p$ is finite means that there must be some $i \neq j$ such that $f_p^i(\alpha) = f_p^j(\alpha)$. On the other hand, $\alpha$ may not be *periodic*, since it is quite possible that there is no $n > 0$ such that $f_p^n(\alpha) = \alpha$.

The model of random maps, along with the heuristic of the birthday problem, suggests that for a typical $\alpha$ and a typical self-map $\varphi$ of $\mathbb{F}_p$, the size of the orbit $\mathrm{Orb}_\varphi(\alpha) = \{\alpha, \varphi(\alpha), \ldots, \varphi^m(\alpha), \ldots\}$ will be about $\sqrt{p}$ (see [1, 2, 4, 21]). Hence, one might guess that, for a typical polynomial reduction, $f_p$, there is about a $1/\sqrt{p}$ chance that a given $\alpha$ is $f_p$-periodic, and that the proportion of $f_p$-periodic points in $\mathbb{F}_p$ is about $1/\sqrt{p}$.

Received October 27, 2014; Revised May 16, 2015; Accepted August 5, 2015

In particular, one would then have

$$\lim_{p\to\infty} \frac{\#\mathrm{Per}\left(f_p\right)}{p} = 0,$$

where $\mathrm{Per}(f_p)$ is the set of points in $\mathbb{F}_p$ that are $f_p$-periodic.

More generally, one might consider this problem for rational functions over number fields. Let $k$ be a number field and let $\varphi \in k(x)$ be a rational function of degree greater than 1. For all but finitely many primes $\mathfrak{p}$ in the ring of integers $\mathfrak{o}_k$ of $k$, reducing modulo $\mathfrak{p}$ gives rise to a well-defined map $\varphi_{\mathfrak{p}} : \mathbb{P}^1(\mathfrak{o}_k/\mathfrak{p}) \longrightarrow \mathbb{P}^1(\mathfrak{o}_k/\mathfrak{p})$. We let $N(\mathfrak{p})$ denote the number of elements in the residue field $\mathfrak{o}_k/\mathfrak{p}$. Then one might expect for a typical $\varphi$, taking the limit over the $\mathfrak{p}$ such that $\varphi_{\mathfrak{p}}$ is a well-defined map on $\mathbb{P}^1(\mathfrak{o}_k/\mathfrak{p})$, one should have

$$\lim_{N(\mathfrak{p})\to\infty} \frac{\#\mathrm{Per}(\varphi_{\mathfrak{p}})}{N(\mathfrak{p})+1} = 0. \tag{1}$$

Of course, this might not necessarily be the case. For example, if $f(x)$ is a powering map $f(x) = x^n$, then $f_p$ is a bijection for all $p \not\equiv 1 \pmod n$ and thus all points in $\mathbb{F}_p$ are $f_p$-periodic for all $p \not\equiv 1 \pmod n$. A more general family of examples comes from Dickson polynomials, which are defined by $f(x + a/x) = x^n + (a/x)^n$ (when $a = 0$, one has a powering map). Fried [5] showed that if $f$ is any polynomial over a number field $k$ such that $f_{\mathfrak{p}}$ is a bijection for infinitely many primes $\mathfrak{p}$ in $\mathfrak{o}_k$, then $f$ can be a written as a composition of Dickson polynomials and linear polynomials (polynomials of the form $ax + b$). More recently, Guralnick et al. [8] have given a classification of all indecomposable rational functions $\varphi$ over number fields such that $\varphi_{\mathfrak{p}}$ is a bijection for infinitely many primes $\mathfrak{p}$; the classification is substantially more complicated. The rational functions classified by Guralnick, Müller, and Saxl are often referred to as indecomposable *exceptional rational functions* (for a more general discussion of exceptional maps, see [9]).

**Question 1.1.** Let $k$ be a number field. Can one classify all rational functions $\varphi \in k(x)$ of degree greater than 1 over a number field $k$ such that (1) fails to hold? □

It is possible that all rational functions such that (1) fails to hold come from exceptional rational functions, but we are not able to prove it at the present time. However, we have some evidence that this may be the case. We can show that for "most" rational functions $\varphi$ of degree $d$, the proportion $\#\mathrm{Per}(\varphi_{\mathfrak{p}})/(N(\mathfrak{p})+1)$ becomes small for large $N(\mathfrak{p})$. To phrase this precisely, we need a bit more notation.

Let $k$ be a number field. Given a point $(a_0, \dots, a_d, b_0, \dots, b_d)$ in $\mathbb{A}^{2d+2}(\bar{k})$, we set $\vec{a} = (a_0, \dots, a_d)$, $\vec{b} = (b_0, \dots, b_d)$, $p_{\vec{a}} = a_d x^d + \cdots + a_0$, $q_{\vec{b}} = b_d x^d + \cdots + b_0$, and $\varphi_{\vec{a},\vec{b}} = p_{\vec{a}}/q_{\vec{b}}$. If the resultant of $p$ and $q$ is nonzero and either $a_d$ or $b_d$ is nonzero, then $\varphi_{\vec{a},\vec{b}} = p_{\vec{a}}/q_{\vec{b}}$ is a rational function of degree $d$ in $k(x)$. We denote the set of such $(\vec{a}, \vec{b})$ as $\mathrm{Rat}_d$. Thus, $\mathrm{Rat}_d$ is a Zariski-open subset of $\mathbb{A}^{2d+2}$.

**Theorem 1.2.** Let $\epsilon > 0$ and $d > 1$. With notation as above, there is a Zariski-dense open subset $U_{d,\epsilon}$ of $\mathrm{Rat}_d$ such that for any number field $k$ and any $(\vec{a}, \vec{b}) \in U_{d,\epsilon}(k)$, we have

$$\limsup_{\substack{N(\mathfrak{p})\to\infty \\ \text{primes } \mathfrak{p} \text{ of } \mathfrak{o}_k}} \frac{\#\mathrm{Per}\left(\varphi_{\vec{a},\vec{b}}\right)}{N(\mathfrak{p})+1} \leq \epsilon.$$

□

We are also able to prove the following.

**Theorem 1.3.** Let $\varphi$ be a rational function of degree $d > 1$ such that for any two distinct critical points $\alpha_1, \alpha_2$ of $\varphi$ and any positive integers $m$ and $n$, we have $\varphi^m(\alpha_1) \neq \varphi^n(\alpha_2)$ unless $m = n$ and $\alpha_1 = \alpha_2$. Then

(a)

$$\liminf_{\mathfrak{p}\to\infty} \frac{\#\mathrm{Per}(\varphi_{\mathfrak{p}})}{N(\mathfrak{p})+1} = 0;$$

(b) if $k$ is algebraically closed in the splitting field of $\varphi(x) - t$ over $k(t)$, then we have

$$\lim_{\mathfrak{p}\to\infty} \frac{\#\mathrm{Per}\left(\varphi_{\mathfrak{p}}\right)}{N(\mathfrak{p})+1} = 0.$$

□

Theorem 1.3 thus shows that there are essentially only two obstacles to showing that (1) holds for a given rational function $\varphi$: (i) intersections between the orbits of the critical points of $\varphi$ and (ii) nontrivial algebraic extensions of the ground field $k$ occurring in the splitting field for $\varphi(x) - t$ over $k(t)$. To some extent, one can overcome the second problem by passing to an extension of $k$ and asking instead that

$$\liminf_{N(\mathfrak{p})\to\infty} \frac{\#\mathrm{Per}\left(\varphi_{\mathfrak{p}}\right)}{N(\mathfrak{p})+1} = 0, \tag{2}$$

as we do in (a) above. Note, the condition that $k$ is algebraically closed in the splitting field of $\varphi(x) - t$ over $k(t)$ is the generic case. This condition holds whenever $\mathrm{Gal}((\varphi(x) - t)/\bar{k}(t)) \cong S_d$ which, by the proof of Theorem 1.2, holds for an open dense subset of $\mathrm{Rat}_d$.

**Question 1.4.** Let $k$ be a number field. Can one classify all rational functions $\varphi \in k(x)$ of degree greater than 1 over a number field $k$ such that (2) fails to hold? □

One interesting fact is that (2) holds for powering maps but not for all Dickson polynomials. While the powering map $f(x) = x^n$ induces a bijection $f_p : \mathbb{F}_p \longrightarrow \mathbb{F}_p$ when

$p \not\equiv 1 \pmod{n}$, it is easy to see that when $p \equiv 1 \pmod{n^r}$, we have $\frac{\#\mathrm{Per}(f_p)}{p} \le \frac{1}{n^r} + \frac{1}{p}$. Thus, in this case, we have $\liminf_{p\to\infty} \#\mathrm{Per}(f_p)/p = 0$ (see Example 7.1). However, as we shall see in Example 7.2, when $f$ is the Dickson polynomial $f(x+1/x) = x^d + (1/x)^d$ where $d$ is a power of an odd prime, we have

$$\liminf_{p\to\infty} \#\mathrm{Per}\left(f_p\right)/p = \frac{1}{2},$$

and if $f(x+1/x) = x^d + (1/x)^d$ for $d$ a power of 2, then

$$\liminf_{p\to\infty} \#\mathrm{Per}\left(f_p\right)/p = \frac{1}{4}.$$

(Dickson polynomials of the form $f(x+1/x) = x^n + (1/x)^n$ are called monic Chebyshev polynomials.)

In the case of quadratic polynomials, Chebyshev polynomials and their conjugates are the only polynomials such that (2) fails to hold.

**Theorem 1.5.** Let $k$ be a number field and let $f \in k[x]$ be a quadratic polynomial. Then

$$\liminf_{\mathfrak{p}\to\infty} \frac{\#\mathrm{Per}\left(f_{\mathfrak{p}}\right)}{N(\mathfrak{p})+1} = 0$$

unless there is a linear polynomial $\sigma = ax + b \in k[x]$ such that $\sigma^{-1} f \sigma$ is equal to the Chebyshev polynomial $x^2 - 2$. □

More generally, we are able to treat Question 1.4 for all maps of the form $f(x) = x^d + c$ (see Theorem 6.5). The fact that such maps can be treated is perhaps not surprising in light of related results of [10, 12].

Our approach follows that of Odoni [17], though with some differences. We begin with a definition.

**Definition 1.6.** If $H$ is a group acting on a set $S$, then we define $\mathrm{FPP}(H)$ to be the proportion of elements of $H$ fixing at least one $s \in S$. □

Let $\psi$ be a rational function defined over $\mathbb{F}_q$, let $K_n$ be the splitting field of $\psi^n(x) - t$ over $\mathbb{F}_q(t)$, and let $G_n = \mathrm{Gal}(K_n/\mathbb{F}_q(t))$; suppose that $\mathbb{F}_q$ is algebraically closed in $K_n$. Since $G_n$ acts on the set of roots of $\psi^n(x) - t$, it makes sense to consider $\mathrm{FPP}(G_n)$. The Chebotarev density theorem for function fields, due to Murty and Scherk [16], implies that when $\mathrm{FPP}(G_n)$ is small, then the image of $\mathbb{P}^1(\mathbb{F}_q)$ under $\psi^n$ is small provided that $q$ is sufficiently large. Since a periodic point is in the image of $\mathbb{P}^1(\mathbb{F}_q)$ under $\psi^n$ for every $n$ (see Lemma 5.2), this means that $\psi$ has few periodic points.

We will apply this idea to $\psi$ arising from the reduction $\varphi_{\mathfrak{p}}$ of a rational function over a number field $k$ modulo a prime $\mathfrak{p}$ in $k$. We will see, via Proposition 4.1, that for all but finitely many primes $\mathfrak{p}$, the Galois groups of the splitting fields of $\varphi_{\mathfrak{p}}^n(x) - t$ are the same as the Galois groups of the splitting fields of $\varphi^n(x) - t$ over $k(t)$; let us call this group $G_n$, as above. Then it suffices to show that $\mathrm{FPP}(G_n)$ is very small. This can be difficult to do in general, but Odoni [17, Lemma 4.3] has shown that if $G_n$ is the $n$-fold wreath product $[G]^n$ (see Section 6) of some transitive group $G$, then $\lim_{n\to\infty} \mathrm{FPP}(G_n) = 0$. In the "purely geometric" setting (i.e., extensions of $\mathbb{C}(t)$), we remark that Jones has shown [13] that $\lim_{n\to\infty} \mathrm{FPP}(G_n) = 0$ also holds for a large class of post-critically finite polynomials, and this will play an important part in the proof of Theorem 6.5.

We now give a brief outline of the paper. After some preliminaries in Section 2, we state and prove Theorem 3.1, which gives conditions guaranteeing that $G_n = [G]^n$. A key fact here is that primes in the critical orbit ramify "disjointly" in the sequence $K_n$ of splitting fields of $\varphi^n(x) - t$. That is, for each $n$ we can find primes that are unramified in the splitting field of $K_{n-1}$ and, in each of the subextensions of the splitting field of $K_n$ over $K_{n-1}$ that arise from adjoining to the splitting field of $K_{n-1}$ over $k$ the roots of $\varphi(x) - \alpha_i$ where $\alpha_i$ is a root of $\varphi^{n-1}(x) - t$, at least one such prime ramifies that ramifies in no other subextension. Following that, we show that Galois groups stay the same after almost all specializations, provided that the extensions are geometrically integral, in Section 4. Next, in Section 5, we use the Murty–Scherck effective Chebotarev theorem [16] to bound proportions of periodic points by proportions of fixed-point elements of Galois groups. We are then able to prove our main theorems on proportions of periodic points in Section 6. We conclude with an elementary discussion of periodic points of powering maps, Chebyshev maps, and Lattès maps.

We note that many of the results in this paper, Theorem 3.1 in particular, should generalize to higher dimensional situations. We plan to treat the case of higher dimensions in a future paper.

## 2 Preliminaries

Let $k$ be any field. We say that $F/k$ is a function field with field of constants $k$ if $F$ is a finite extension of $k(t)$ where $t$ is transcendental over $k$ and $k$ is algebraically closed in $F$ (i.e., $F$ contains no elements outside of $k$ that are algebraic over $k$). Define $\mathbb{P}_F$ to be the set of all $\mathfrak{p}$ such that $\mathfrak{p}$ is the maximal ideal of some valuation ring of $F/k$.

Let $\varphi \in k(x)$ be a rational function of degree $d$. We write $\varphi(x) = p(x)/q(x)$, where $p(x), q(x) \in k[x]$, and we let $P(X, Y)$ and $Q(X, Y)$ be the degree $d$ homogenizations of $p$

and $q$, respectively; that is, $P(X,Y)=Y^d p(X/Y)$ and $Q(X,Y)=Y^d q(X/Y)$. We set $P_0=P$ and $Q_0=Q$ and define $P_n$ and $Q_n$ recursively by $P_n(X,Y)=P(P_{n-1}(X,Y),Q_{n-1}(X,Y))$ and $Q_n(X,Y)=Q(P_{n-1}(X,Y),Q_{n-1}(X,Y))$ for $n\geq 1$. Then, defining $p_k=P_k(X,1)$ and $q_k=Q_k(X,1)$, any root of $\varphi^n(x)-t$ is a root of

$$p_n(x)-tq_n(x), \tag{3}$$

which is a polynomial with coefficients in $k(t)$. If $k$ is a number field and $\mathfrak{p}$ is a nonzero prime in its ring of integers $\mathfrak{o}_k$, we say that the rational function $\varphi(x)$, defined as above, has good reduction at $\mathfrak{p}$ if all of the coefficients of $p$ and $q$ have $\mathfrak{p}$-adic absolute value less than or equal to 1 and for all $\alpha\in\bar{k}$, we have $\max\{|P(\alpha,1)|_{\mathfrak{p}},|Q(\alpha,1)|_{\mathfrak{p}}\}=1$ and $\max\{|P(1,\alpha)|_{\mathfrak{p}},|Q(1,\alpha)|_{\mathfrak{p}}\}=1$.

Let $A$ be a Dedekind domain with fraction field $K$, let $P(x)\in K[x]$, and $L$ be the splitting field of $P(x)$ over $K$. It is a standard result that any prime of $A$ that ramifies in the integral closure of $A$ in $L$ must divide $\Delta(P(x))$, the usual polynomial discriminant of $P(x)$ (see, e.g., [11] or [14]). (Here and elsewhere in this paper, if a prime $\mathfrak{p}$ is said to *divide* an element $\alpha$ of $\mathcal{O}_K$, we mean that $v_{\mathfrak{p}}(\alpha)>0$.) Now consider the case where $L$ is the splitting field of $\psi(x)-t$ over $k(t)$, where $\psi(x)\in k(x)$. We can write $\psi(x)=\frac{p(x)}{q(x)}$ for some $p(x),q(x)\in k[x]$ and any prime of $k[t]$ that ramifies in $L$ must divide $\Delta(p(x)-tq(x))$. In [3], Cullinan and Hajir show that one may calculate the discriminant in terms of the critical points of $\psi(x)$.

**Lemma 2.1.** ([3, Proposition 1]) We have

$$\begin{aligned}\Delta\left(p(x)-tq(x)\right)&=C\,\mathrm{Res}\left(p'(x)q(x)-p(x)q'(x),\,p(x)-tq(x)\right)\\&=C'\prod_{a\in\psi_{\mathfrak{c}}}\left(\psi(a)-t\right)^{e(a/\psi(a))},\end{aligned}$$

where $C,C'\in k$ are constants, $\psi_{\mathfrak{c}}=\{a:\psi'(a)=0\}$, and $e(a/\psi(a))$ is the ramification index of $a$ over $\psi(a)$. □

Thus, we see that any prime $\mathfrak{p}$ of $k[t]$ that ramifies in a splitting field for $p(x)-tq(x)$ must divide $\prod_{a\in\psi_{\mathfrak{c}}}(\psi(a)-t)^{e(a/\psi(a))}$.

We now introduce wreath product actions on roots of iterates of polynomials. Since we are working with Galois groups that may not be the full symmetric group, we need slightly more technical definitions than those of [17].

**Definition 2.2.** Let $K$ be a field. Let $\psi(x),\gamma(x)$ be rational functions in $K(x)$ with $\deg(\psi)=\ell$, $\deg(\gamma)=d$, such that $\psi(\gamma(x))$ has $\ell d$ distinct roots in $\bar{K}$. A $\psi,\gamma$*-compatible* *numbering* on the roots of $\psi(\gamma(x))$ is a numbering that assigns to each root a unique ordered pair $(i, j) \in \{1, \ldots, \ell\} \times \{1, \ldots, d\}$ such that if $\alpha_1, \ldots, \alpha_\ell$ are the roots of $\psi$, then the set $\{i\} \times \{1, \ldots, d\}$ is assigned to the roots of $\gamma(x) - \alpha_i$. □

**Definition 2.3.** Let $G$ and $H$ be groups acting on the finite sets $\{1, \ldots, \ell\}$ and $\{1, \ldots, d\}$, respectively. We denote the *wreath product* of $G$ by $H$ as $G[H]$, and define it by its action on $\{1, \ldots, \ell\} \times \{1, \ldots, d\}$ as follows. We write $\sigma \in G[H]$ as $(\pi; \tau_1, \ldots, \tau_\ell)$ where $\pi \in G$, and $\tau_1, \ldots, \tau_\ell \in H$. Then $\sigma(i, j) = (\pi(i), \tau_i(j))$. □

**Definition 2.4.** Let $G$ be a group acting on the set $\{1, 2, \ldots, d\}$. The *nth wreath power* of $G$ is defined by $[G]^1 = G$ and $[G]^n = [G]^{n-1}[G]$ (note that $[G]^n$ then acts naturally on $\{1, 2, \ldots, d\}^n$.) □

The following lemma generalizes [17, Lemma 4.1].

**Lemma 2.5.** Let $\psi(x), \gamma(x) \in K(x)$ with $\deg(\psi) = \ell$, $\deg(\gamma) = d$, $\ell, d \geq 1$, such that $\psi(\gamma(x))$ has $\ell d$ distinct roots in $\bar{K}$. Assume that $\psi$ is irreducible over $K$. Let $\alpha_1, \ldots, \alpha_\ell$ be the roots of $\psi(x)$, $M_i$ be the splitting field of $\gamma(x) - \alpha_i$ over $K(\alpha_i)$, and $G := \mathrm{Gal}(\psi(x)/K)$. Let $H = \mathrm{Gal}(M_1/K(\alpha_1))$. As $\mathrm{Gal}(M_i/K(\alpha_i)) \cong H$ for all $i = 1, \ldots, \ell$, there is an embedding $\iota : \mathrm{Gal}(\psi(\gamma(x))/K) \hookrightarrow G[H]$. Furthermore, there is a $\psi, \gamma$-compatible numbering on the roots such that $\mathrm{Gal}(\psi(\gamma(x))/K) \leq G[H]$. □

**Proof.** We may write

$$\psi\left(\gamma(x)\right) = \prod_{i=1}^{\ell} \left(\gamma(x) - \alpha_i\right).$$

We will construct the desired numbering on the roots of $\psi(\gamma(x))$. First choose any numbering $(1, 1), \ldots, (1, d)$ on the roots of $\gamma(x) - \alpha_1$, so that each root is identified with an ordered pair $(1, j)$. For each $i = 2, \ldots, \ell$, choose $\theta_i \in \mathrm{Gal}(\psi(\gamma(x))/K)$ such that $\theta_i(\alpha_1) = \alpha_i$. Since $\theta_i$ acts on the splitting field of $\psi(\gamma(x))$, we can consider the action of $\theta_i$ on each of the roots $(1, 1), \ldots, (1, d)$ of $\gamma(x) - \alpha_1$. Note, $\theta_i(1, j)$ is a root of $\gamma(x) - \alpha_i$ for each $j$ since $\theta_i$ must commute with $\gamma$. Number the roots of $\gamma(x) - \alpha_i$ so that $\theta_i(1, j) = (i, j)$.

Let $\sigma \in \mathrm{Gal}(\psi(\gamma(x))/K)$. Then $\sigma$ induces a $K$-automorphism $\pi$ that permutes $\{\alpha_1, \ldots, \alpha_\ell\}$. Thus, $\pi \in G$. Now fix $i$ and note that $\sigma(i, j) = (\pi(i), s)$ for some $s \in \{1, \ldots, d\}$. This defines a map $\tau_i \in \mathrm{Perm}(1, \ldots, d)$ by $\tau_i(j) = s$. Then $\sigma(i, j) = (\pi(i), \tau_i(j))$ so, using the above wreath product notation, $\sigma = (\pi; \tau_1, \ldots, \tau_\ell) \in G[S_d]$. It remains to show $\tau_i \in H$ for each $i$. Consider $\theta_{\pi(i)}^{-1}\sigma\theta_i(1, j) = \theta_{\pi(i)}^{-1}\sigma(i, j) = \theta_{\pi(i)}^{-1}(\pi(i), \tau_i(j)) = (1, \tau_i(j))$. So $\theta_{\pi(i)}^{-1}\sigma\theta_i$ fixes $\alpha_1$ and $\theta_{\pi(i)}^{-1}\sigma\theta_i|_{M_1} = \tau_i$ and hence, $\tau_i \in H$. ■

## 3 Criteria for Wreath Product

Let $k$ be a general field and $\varphi(x) \in k(x)$ be a rational function with degree $d$, such that $\varphi'(x) \neq 0$. Note, the roots of $\varphi^n(x) - t$ are the roots of $p_n(x) - tq_n(x)$, and $p_n(x) - tq_n(x)$ is separable. To see this, note that since $p_n(x) - tq_n(x)$ is irreducible over $k(t)$, if it has a double root, we must have $p_n'(x) - tq_n'(x) = 0$ for all $x$. Then $(\varphi^n)' = \frac{q_n p_n' - p_n q_n'}{(q_n)^2} = 0$ for all $x$. But since we assumed $\varphi'(x) \neq 0$, $(\varphi^n)'(x) \neq 0$ by induction on $n$.

Let $K_n$ be the splitting field of $\varphi^n(x) - t$ over $k(t)$, $E = K_1 \cap \bar{k}$, and $G_n := \mathrm{Gal}(K_n/E(t))$. We let $G = G_1$. We let $\varphi_{\mathfrak{c}}$ denote the critical points of $\varphi$ in $\mathbb{P}^1(\bar{k})$. We also adopt some notation regarding extension of primes in finite extensions of function fields. Let $L_1 \subseteq L_2$ be a separable finite extension of function fields. If $\mathfrak{p}$ is a prime with discrete valuation ring $\mathcal{O}_{\mathfrak{p}}$, then we say that the prime $\mathfrak{q}$ of $L_2$ *extends* $\mathfrak{p}$ *in* $L_2/L_1$ if $\mathfrak{q}$ appears in the factorization of $\mathfrak{p}$ in the integral closure of $\mathcal{O}_{\mathfrak{p}}$ in $L_2$. (This terminology is fairly standard.) Likewise, in the language of points, we say that a point $\beta \in \mathbb{P}_{L_2}$ extends a point $\alpha \in \mathbb{P}_{L_1}$ in $L_2/L_1$ if the prime ideal corresponding to $\beta$ extends the prime ideal corresponding to $\alpha$ in $L_2/L_1$.

Our first main theorem gives conditions that ensure that $G_n \cong [G]^n$. This is similar to but more general than some recent work of Pink [18, Theorem 4.8.1] for quadratic maps, although Pink's criterion is both sufficient and necessary, whereas ours is only sufficient.

**Theorem 3.1.** Suppose that $\varphi(x) \in k(x)$ is a rational function of degree $d \geq 2$ such that $\varphi'(x) \neq 0$. Fix $N \in \mathbb{N}$ and suppose there is a subset $S \subseteq \varphi_{\mathfrak{c}}$ such that the following hold:

(1) for any $a \in S$, $b \in \varphi_{\mathfrak{c}}$, and $m, n \leq N$, we have $\varphi^m(a) \neq \varphi^n(b)$ unless $a = b$ and $m = n$ and

(2) the group $G$ is generated by the ramification groups of the $\varphi(a)$ for $a \in S$, that is,

$$\left\langle \bigcup_{a \in S} \bigcup_{\substack{z \text{ extends } \varphi(a) \\ \text{in } K_1/E(t)}} I\left(z/\varphi(a)\right) \right\rangle = G.$$

Then we have $G_N \cong [G]^N$. □

**Remark 3.2.** If $S$ is the set of *all* finite critical points of $\varphi$, then condition (2) of Theorem 3.1 follows automatically. To see this, let $I$ be the subgroup of $G$ generated by the ramification groups of all the critical points. Then the fixed field $K_1^I$ is unramified everywhere over $E(t)$, so $K_1^I = E(t)$ since $E(t)$ has no unramified extensions of degree greater than 1, by Riemann–Hurwitz. Thus, $I = G$ as desired. We use this fact in the proof of Theorem 1.3.

Also note, condition (2) depends only on information about the first extension $K_1/K$, and this information is enough to conclude that $G_N \cong [G]^N$ in the case that condition (1) is met. □

To illustrate the importance of considering the extension $K_1/E(t)$ rather than $K_1/k(t)$, we let $k = \mathbb{Q}$ and examine the example $\varphi(x) = x^d + c \in \mathbb{Q}[x]$ where $c$ is chosen so that 0 is not preperiodic. Then $E = \mathbb{Q}(\xi_d)$ where $\xi_d$ is a primitive $d$th root of unity and $I(\sqrt[d]{t-c}|(t-c)) \cong C_d \cong G$. The hypotheses of the theorem are satisfied for all $N$, thus, $G_N \cong [G]^N$ for all $N$.

On the other hand, if $d \neq 2$, then $\mathrm{Gal}(K_2/k(t))$ is not isomorphic to $[\mathrm{Gal}(K_1/k(t))]^2$. To see this, note that $E \subset K_1$ so $\mathrm{Gal}(x^d + c - \sqrt[d]{t-c}/K_1) \cong C_d$. Using a degree argument, this implies $\mathrm{Gal}(K_2/k(t)) \ncong [\mathrm{Gal}(K_1/k(t))]^2$ (in fact, one can show the index of $\mathrm{Gal}(K_N/k(t))$ in $[\mathrm{Gal}(K_1/k(t))]^N$ is unbounded as $N$ grows). In Proposition 3.6, we show that the first assertion holds more generally.

We use the following notation in the proof of Theorem 3.1. Let $\alpha_1, \ldots, \alpha_{d^n}$ be the distinct roots of $\varphi^n(x) - t$ in $\bar{k(t)}$. Let $M_i$ be the splitting field of $\varphi(x) - \alpha_i$ over $E(\alpha_i) := E(t, \alpha_i)$. Let $\hat{M}_i := K_n[\prod_{j \neq i} M_j]$.

**Lemma 3.3.** The group $\mathrm{Gal}(K_n/k(t))$ is isomorphic to a subgroup of $[H]^n$, where $H = \mathrm{Gal}(K_1/k(t))$. In particular, the group $G_n$ is isomorphic to a subgroup of $[G]^n$. □

**Proof.** Note that $k(\alpha_i) \cong k(t)$ so we have $\mathrm{Gal}(\varphi(x) - \alpha_i/k(\alpha_i)) \cong \mathrm{Gal}(K_1/k(t))$. The first assertion follows immediately from Lemma 2.5 and induction on $n$. The same proof, on replacing the constant field $k$ by $E$, yields the second assertion. ■

To make certain computations easier, we will work with discriminants in $E[t]$ rather than ramification divisors. In order to make this possible, we make a few reductions here. We note that, since for any extension $E'$ of $E$, we have $|\mathrm{Gal}(K_N \cdot E'/E'(t))| \leq |\mathrm{Gal}(K_N/E(t))|$, it will suffice to show that $\mathrm{Gal}(K_N \cdot E'/E'(t)) \cong [G]^N$ for some extension $E'$ of $E$. Hence, we may assume that $E$ is algebraically closed. Since $E$ is then infinite, and a change of variables on $\varphi$ does not affect $\mathrm{Gal}(K_N/E(t))$, we may therefore assume that

$$\text{if } a \in S \text{ and } m \leq N, \text{ then } \varphi^m(a) \text{ is not the point at infinity.} \tag{4}$$

Furthermore, we may assume that every prime in $E[t]$ is of the form $(z - t)$ for some $z \in E$, and that the prime at infinity in $E(t)$ does not ramify in $K_n$ for any $n \leq N$. Hence, in the next two lemmas, we assume that the conditions of Theorem 3.1 hold, that $E$ is algebraically closed, and that (4) holds.

**Lemma 3.4.** Let $n < N$. Every prime in $E(t)$ that ramifies in $K_n$ is of the form $(\varphi^m(a) - t)$ for $a \in \varphi_{\mathfrak{c}}$ and $m \leq n$. □

**Proof.** We have seen that the prime at infinity does not ramify in $K_n$. For any $i$, we see, by Lemma 2.1, that the primes of $E(t)$ that ramify in $K_n$ are those dividing

$$\Delta\left(p_n(x) - tq_n(x)\right) = \prod_{b \in \varphi_{\mathfrak{c}}} \left( (\varphi(b) - t)^{d^{n-1}} \left(\varphi^2(b) - t\right)^{d^{n-2}} \cdots \left(\varphi^n(b) - t\right) \right)^{e(b/\varphi(b))},$$

where the above equality follows from repeated application of the chain rule to iterates of $\varphi$. ■

Before continuing, we make a simple observation. Let $\alpha_i$ be a root of $\varphi^n(x) - t = 0$ as above. Under the inclusion of fields $E(t) \subseteq E(\alpha_i)$, any prime $(z - \alpha_i)$ extends the prime $(\varphi^n(z) - t)$ in $E(\alpha_i)/E(t)$, since $\alpha_i$ is a solution to $\varphi^n(x) = t$.

**Lemma 3.5.** Let $n < N$ and $a \in S$. The prime $(\varphi(a) - \alpha_i)$ in $E(\alpha_i)$ does not ramify in $\hat{M}_i$. □

**Proof.** We will show that $(\varphi(a) - \alpha_i)$ does not ramify in $K_n/E(\alpha_i)$ and that the primes extending it in $K_n/E(\alpha_i)$ do not ramify in $M_j K_n$ if $i \neq j$.

We have assumed that $\varphi^{n+1}(a) - t \neq \varphi^m(b) - t$ for any $m \leq n$, any $a \in S$, and $b \in \varphi_{\mathfrak{c}}$. Thus, by Lemma 3.4, we see that $(\varphi^{n+1}(a) - t)$ does not ramify in $K_n$. Since $(\varphi(a) - \alpha_i)$ extends $(\varphi^{n+1}(a) - t)$ in $E(\alpha_i)/E(t)$, it follows that $(\varphi(a) - \alpha_i)$ does not ramify in $K_n$.

To show that $(\varphi(a) - \alpha_i)$ does not ramify in $M_j K_n$ for $j \neq i$, first note that the primes of $K_n$ ramifying in $M_j K_n$ are those dividing

$$\Delta\left(\varphi(x) - \alpha_j\right) := \prod_{b \in \varphi_{\mathfrak{c}}} \left(\varphi(b) - \alpha_j\right)^{e(b/\varphi(b))},$$

by Lemma 2.1. If a prime $\mathfrak{p}$ of $K_n$ extending $(\varphi(a) - \alpha_i)$ in $K_n/E(\alpha_i)$ ramifies in $M_j$, then $\mathfrak{p}$ divides $\Delta(\varphi(x) - \alpha_j)$, so $\mathfrak{p} | (\varphi(b) - \alpha_j)$ for some $b \in \varphi_{\mathfrak{c}}$. Hence, $\mathfrak{p}$ extends the prime $(\varphi(a) - \alpha_i)$ in $K_n/E(\alpha_i)$ and extends the prime $(\varphi(b) - \alpha_j)$ in $K_n/E(\alpha_j)$. Now, the prime $\mathfrak{p}$ extends the prime $(\varphi^{n+1}(a) - t)$ in $E(\alpha_i)/E(t)$ and extends the prime $(\varphi^{n+1}(b) - t)$ in $K_n/E(t)$, so we must have $\varphi^{n+1}(a) = \varphi^{n+1}(b)$ (since $\mathfrak{p}$ can extend exactly one prime in $K_n/E(t)$). This means that $a = b$, by condition (1) of Theorem 3.1. Thus, $\mathfrak{p}$ divides both $(\varphi(a) - \alpha_i)$ and $(\varphi(a) - \alpha_j)$. This means that $(\alpha_i - \alpha_j) \in \mathfrak{p}$. Since $K_n$ is a splitting field for $\varphi^n(x) - t$, this implies that $\mathfrak{p}$ ramifies over $\mathfrak{p} \cap E(t) = (\varphi^{n+1}(a) - t)$, contradicting Lemma 3.4, since $\varphi^{n+1}(a) - t \neq \varphi^m(b) - t$ for any $m \leq n$, any $a \in S$, and $b \in \varphi_{\mathfrak{c}}$ by (3.4). ■

We now prove Theorem 3.1.

**Proof of Theorem 3.1.** We will use induction to prove that $G_n \cong [G]^n$ for all $n \leq N$. The case of $n = 1$ is clear. Let $n < N$ and suppose that $G_m \cong [G]^m$ for all $m \leq n$; we will show that $G_{n+1} \cong [G]^{n+1}$. First note that $E(\alpha_i) \cong E(t)$ so we have $\mathrm{Gal}(M_i/E(\alpha_i)) \cong \mathrm{Gal}(K_1/E(t)) \cong G$.

Elements of $\mathrm{Gal}(K_{n+1}/\hat{M}_i)$ and $\mathrm{Gal}(M_i/E(\alpha_i))$ are determined by their actions on the roots of $\varphi(x) - \alpha_i$. There is a natural injective homomorphism from $\mathrm{Gal}(K_{n+1}/\hat{M}_i)$ to $\mathrm{Gal}(M_i/E(\alpha_i))$ given by restriction of elements of $\mathrm{Gal}(K_{n+1}/\widehat{M}_i)$ to $M_i$. Let $\Psi : \mathrm{Gal}(K_{n+1}/\widehat{M}_i) \to \mathrm{Gal}(M_i/E(\alpha_i))$ be this map.

Let $\mathfrak{p}_1$ be any prime of $M_i$ dividing $\prod_{a \in S}(\varphi(a) - \alpha_i)$, let $\mathfrak{p} := \mathfrak{p}_1 \cap E[\alpha_i]$, let $\mathfrak{p}'$ be any extension of $\mathfrak{p}_1$ to $K_{n+1}$, and let $\mathfrak{p}_2 := \mathfrak{p}' \cap \hat{M}_i$. Then $\Psi|_{I(\mathfrak{p}'|\mathfrak{p}_2)} : I(\mathfrak{p}'|\mathfrak{p}_2) \to I(\mathfrak{p}_1|\mathfrak{p})$ is an injective homomorphism of the inertia group of $\mathfrak{p}'$ over $\mathfrak{p}_2$ to the inertia group of $\mathfrak{p}_1$ over $\mathfrak{p}$, so $e(\mathfrak{p}_1|\mathfrak{p}) \geq e(\mathfrak{p}'|\mathfrak{p}_2)$. Since $\mathfrak{p}_2$ is unramified over $E(\alpha_i)$, $e(\mathfrak{p}'|\mathfrak{p}_2) = e(\mathfrak{p}'|\mathfrak{p}) \geq e(\mathfrak{p}_1|\mathfrak{p})$. Hence, $|I(\mathfrak{p}'|\mathfrak{p}_2)| = |I(\mathfrak{p}_1|\mathfrak{p})|$ and $\Psi|_{I(\mathfrak{p}'|\mathfrak{p}_2)}$ must be an isomorphism.

Consider $I \subseteq \mathrm{Gal}(M_i/E(\alpha_i))$, the subgroup generated by

$$\left\{ I\left(\mathfrak{q}|\mathfrak{q} \cap E\left(\alpha_i\right)\right) : \mathfrak{q} \in \mathbb{P}_{M_i}, \mathfrak{q} \left| \prod_{a \in S} \left(\varphi(a) - \alpha_i\right) \right. \right\},$$

and $I' \subseteq \mathrm{Gal}(K_{n+1}/\hat{M}_i)$, the subgroup generated by

$$\left\{ I\left(\mathfrak{q}'|\mathfrak{q}' \cap \hat{M}_i\right) : \mathfrak{q}' \in \mathbb{P}_{K_{n+1}}, \mathfrak{q}' \left| \prod_{a \in S} \left(\varphi(a) - \alpha_i\right) \right. \right\}.$$

Then $\Psi|_{I'} : I' \to I$ is an isomorphism. So $\mathrm{Gal}(K_{n+1}/\hat{M}_i)$ contains an isomorphic copy of $I$. We have $I \cong G$ by hypothesis so $\mathrm{Gal}(K_{n+1}/\hat{M}_i)$ contains an isomorphic copy of $G$. We also know that $\mathrm{Gal}(K_{n+1}/\hat{M}_i)$ is isomorphic to a subgroup of $G$. It follows that $\mathrm{Gal}(K_{n+1}/\hat{M}_i) \cong G$.

Thus, we have

$$|G_{n+1}| = \prod_{i=0}^{n} |\, G \,|^{d^i} = |[G]^{n+1}|.$$

By Lemma 3.3, $G_{n+1}$ is isomorphic to a subgroup of $[G]^{n+1}$. Hence, $G_{n+1} \cong [G]^{n+1}$, as desired. ■

In Theorem 3.1, $E$ was taken to be the algebraic closure of $k$ in $K_1$. In the following proposition, we show that algebraic closure of this field is a necessary condition for the iterated Galois groups to be the full iterated wreath products.

**Proposition 3.6.** Let $H = \mathrm{Gal}(K_1/k(t))$. Suppose that $k$ is not algebraically closed in $K_1$. Then $\mathrm{Gal}(K_n/k(t))$ is a proper subgroup of $[H]^n$ for $n > 1$. □

**Proof.** If $k$ is not algebraically closed in $K_1$, then $k(t)$ is a proper subfield of $E(t)$ so $G$ is a proper subgroup of $H$. Thus, we have $|G| < |H|$. Now note that $E \subset K_n$ for $n \geq 1$ so $E(\alpha_i) \subset \hat{M}_i$. Then $\mathrm{Gal}(K_{n+1}/\hat{M}_i)$ is isomorphic to a subgroup of $\mathrm{Gal}(M_i/E(\alpha_i)) \cong G$. Therefore, $|\mathrm{Gal}(K_{n+1}/K_n)| < |H|^{d^n}$ and

$$|\mathrm{Gal}\,(K_{n+1}/k(t))\,| < |[H]^n|,$$

as desired. ■

## 4 Specializations of Galois Groups

Our main results will involve working over Galois extensions of function fields whose fields of constants are number fields and reducing modulo primes of the number fields. The notion of specializing Galois groups is most easily stated in a great deal of generality, so we work over Noetherian integral domains here, rather than merely over rings of integers in number fields.

Throughout out this section, we let $F(D)$ denote the field of fractions of $D$ for an integral domain $D$.

Let $R$ be a Noetherian integral domain of characteristic 0 and let $A$ be a finitely generated $R$-algebra that is an integrally closed domain. Let $h(x) = \sum_{i=1}^{d} a_i x^i \in A[x]$ be a nonconstant polynomial that is irreducible in $F(A)[x]$. Let $B = A[\theta_1, \ldots, \theta_n]$ where $\theta_i$ are the roots of $h$ in some splitting field for $h$ over $F(A)$. We let $X$ denote $\mathrm{Spec}\,A$ and let $Y$ denote $\mathrm{Spec}\,B$. For any prime $\mathfrak{p}$ of $R$, we let $X_{\mathfrak{p}}$ (respectively, $Y_{\mathfrak{p}}$) denote the fiber $X \times_{\mathrm{Spec}\,R} F(R/\mathfrak{p})$ (respectively, $Y \times_{\mathrm{Spec}\,R} F(R/\mathfrak{p})$). We let (0) denote the zero ideal in $R$. Note that since $R$ is an integral domain, (0) is Zariski-dense in $\mathrm{Spec}\,R$. In particular, any constructible subset of $\mathrm{Spec}\,R$ that contains (0) must be Zariski-dense and open. Recall that a subset $Z$ is said to be constructible if it is a finite union of locally closed sets; a locally closed set is the intersection of a closed set with an open set.

Suppose that $F(R)$ is algebraically closed in both $F(A)$ and $F(B)$ (this is a crucial assumption, see Remark 4.2). Then, since $A$ and $B$ have characteristic 0 we see that $X_{(0)}$ and $Y_{(0)}$ are both geometrically integral $F(R)$-schemes (see, e.g., [6, Proposition 5.5.1]); in other words, $A \otimes_{F(R)} k'$ and $B \otimes_{F(R)} k'$ are integral domains for any algebraic extension $k'$ of $F(R)$. Hence, by [7, Theorem 9.7.7], we see that the set of $\mathfrak{p} \in \operatorname{Spec} R$ such that $X_{\mathfrak{p}}$ and $Y_{\mathfrak{p}}$ are geometrically integral forms a Zariski-dense open subset of $\operatorname{Spec} R$. Thus, if we let $W_1$ denote the set of $\mathfrak{p} \in \operatorname{Spec} R$ such that $A/\mathfrak{p}A \otimes_R F(A/\mathfrak{p})$ and $B/\mathfrak{p}B \otimes_R F(B/\mathfrak{p})$ are integral domains, then $W_1$ is a Zariski-dense open subset of $\operatorname{Spec} R$.

Let $Z_2$ be the set of primes of $A$ that do not contain $a_d$, the leading coefficient of $h$. Then $Z_2$ is a Zariski-dense open subset of $\operatorname{Spec} A$. Let $\pi_{AR} : \operatorname{Spec} A \longrightarrow \operatorname{Spec} R$ be the map induced by the inclusion of $R$ into $A$ and let $W_2 = \pi_{AR}(Z_2)$. Then by Chevalley's theorem on images of constructible sets (see, e.g., [6, Theorem 10.70]), $W_2$ must be a constructible subset of $\operatorname{Spec} R$; since this subset contains the zero ideal, it must therefore be open and dense. Likewise, for each $i \neq j$, the set of primes $U_{ij}$ of $\mathfrak{p}$ in $\operatorname{Spec} B$ that do not contain $\theta_i - \theta_j$ form a Zariski-dense open subset of $\operatorname{Spec} B$. Chevalley's theorem thus implies that there is a Zariski-dense open subset $W_3 \subseteq \operatorname{Spec} R$ such that for all $\mathfrak{p} \in W_3$ and any $i \neq j$, we have $r_{\mathfrak{p}}(\theta_i) \neq r_{\mathfrak{p}}(\theta_j)$. Let $W = W_1 \cap W_2 \cap W_3$.

Now, let $\mathfrak{p} \in W$. We let $(A)_{\mathfrak{p}}$ and $(B)_{\mathfrak{p}}$ denote $A/\mathfrak{p}A \otimes_R F(A/\mathfrak{p})$ and $B/\mathfrak{p}B \otimes_R F(B/\mathfrak{p})$, respectively. We let $h_{\mathfrak{p}}$ denote the image of $h \in (A)_{\mathfrak{p}}[x]$ under the reduction map from $A$ to $(A)_{\mathfrak{p}}$. We let $r_{\mathfrak{p}}$ denote the reduction map from $B$ to $(B)_{\mathfrak{p}}$. Since $r_{\mathfrak{p}}$ is a homomorphism of rings, it is clear that if $\theta_i$ is a root of $h$, then $r_{\mathfrak{p}}(\theta_i)$ is root of $h_{\mathfrak{p}}$; furthermore, $h_{\mathfrak{p}}$ splits into distinct linear factors in $F(B/\mathfrak{p}B)[x]$, since $h$ splits into distinct factors in $B[x]$ and $r_{\mathfrak{p}}(\theta_i) \neq r_{\mathfrak{p}}(\theta_j)$ for all $i \neq j$. Thus, $F((B)_{\mathfrak{p}})$ is a splitting field for $h_{\mathfrak{p}}$ over $F((A)_{\mathfrak{p}})$ so $F((B)_{\mathfrak{p}})$ is a Galois extension of $F((A)_{\mathfrak{p}})$, and we have $[F((B)_{\mathfrak{p}}) : F((A)_{\mathfrak{p}})] = \#\mathrm{Gal}\,(h_{\mathfrak{p}}(x)/F((A)_{\mathfrak{p}}))$.

Now, given any $\sigma \in \mathrm{Gal}(h(x)/F(A))$, we see that $\sigma : B \longrightarrow B$ since $\sigma$ permutes the $\theta_i$, all of which are in $B$. Since $\sigma$ acts identically on $R$, and thus on $\mathfrak{p}$, we see that $\sigma$ is an automorphism of $R$-algebras and that $\sigma(\mathfrak{p}B) = \mathfrak{p}B$. Thus, $\sigma$ induces a homomorphism $\sigma_{\mathfrak{p}} : (B)_{\mathfrak{p}} \longrightarrow (B)_{\mathfrak{p}}$. If $\sigma\tau$ is the identity on $B$ for $\tau \in \mathrm{Gal}(F(B)/F(A))$, then clearly $\sigma_{\mathfrak{p}}\tau_{\mathfrak{p}}$ is the identity on $(B)_{\mathfrak{p}}$, so $\sigma_{\mathfrak{p}}$ is an automorphism of $(B)_{\mathfrak{p}}$. It extends to an automorphism of $F((B)_{\mathfrak{p}})$, because $(B)_{\mathfrak{p}}$ is an integral domain. Thus, we have a homomorphism

$$\rho_{\mathfrak{p}} : \mathrm{Gal}\,(h(x)/F(A)) \longrightarrow \mathrm{Gal}(h_{\mathfrak{p}}(x)/F((A)_{\mathfrak{p}}))$$

with the property that

$$\rho_{\mathfrak{p}}\,(\sigma)\left(r_{\mathfrak{p}}\,(\theta_i)\right) = r_{\mathfrak{p}}\,(\sigma\,(\theta_i))$$

for all $\sigma \in \mathrm{Gal}(h(x)/F(A))$ and all roots $\theta_i$ of $h$ in $B$.

**Proposition 4.1.** Let $R$ be a Noetherian integral domain of characteristic zero, and let $h$, $h_{\mathfrak{p}}$, $r_{\mathfrak{p}}$, and $\rho_{\mathfrak{p}}$ as defined above. For all $\mathfrak{p}$ in a Zariski-dense open set $W$ of primes of $R$, we have the following:

(i) $r_{\mathfrak{p}}$ induces a bijection between the roots of $h$ and the roots of $h_{\mathfrak{p}}$ and

(ii) $\rho_{\mathfrak{p}}$ is an isomorphism of groups. □

**Proof.** Let $\mathfrak{p} \in W$. Since $r_{\mathfrak{p}}(\theta_i) \neq r_{\mathfrak{p}}(\theta_j)$ for all $i \neq j$, we see that (i) follows immediately.

Let $\sigma$ be a nonidentity element of $\mathrm{Gal}(h(x)/F(A))$. Then, for some $\theta_i$ we have $\sigma(\theta_i) = \theta_j$ for some $\theta_j \neq \theta_i$. Since $r_{\mathfrak{p}}(\theta_i) \neq r_{\mathfrak{p}}(\theta_j)$ for any $\theta_i \neq \theta_j$, it follows that $\rho_{\mathfrak{p}}(\sigma)(r_{\mathfrak{p}}(\theta_i)) \neq r_{\mathfrak{p}}(\theta_i)$, so $\rho_{\mathfrak{p}}(\sigma)$ is not the identity. Thus, $\rho_{\mathfrak{p}}$ must be injective.

As before, we let $\pi_{AR} : \mathrm{Spec} A \longrightarrow \mathrm{Spec} R$ be the map induced by the inclusion of $R$ into $A$. Let $\mathrm{Spec} C$ be an open affine subset of $\pi_{AR}^{-1}(W)$ such that $\pi_{AR}(\mathrm{Spec} C)$ contains $\mathfrak{p}$. Then, since $h_{\mathfrak{p}}$ is separable (because the $r_{\mathfrak{p}}(\theta_i)$ are distinct) and $a_d$ is a unit in $C$, we have

$$\#\mathrm{Gal}(h_{\mathfrak{p}}(x)/F((A)_{\mathfrak{p}})) \leq \#\mathrm{Gal}\,(h(x)/F\,(A)) \tag{5}$$

by [17, Lemma 2.4]. It follows that $\rho_{\mathfrak{p}}$ is surjective and is therefore an isomorphism of groups. ■

**Remark 4.2.** When $F(R)$ is not algebraically closed in $F(B)$, many of the arguments in this section do not work. For example, if $R = \mathbb{Z}$, $A = \mathbb{Z}[t]$, and $B = \mathbb{Z}[\sqrt[3]{t}, \xi_3]$, for $\xi_3$ a cube root of unity, then the Galois group of $F(B)$ over $F(A)$ has order 6, but when one mods out by a prime $p \equiv 1 \pmod 3$, one does not obtain an integral domain. This explains why $\mathrm{Gal}((x^3 - t)/\mathbb{Q})$ can have order 6, even though there are infinitely many $p$ such that $\mathrm{Gal}((x^3 - t)/\mathbb{F}_p)$ has order 3. Note that we still have $\#\mathrm{Gal}((x^3 - t)/\mathbb{F}_p) \leq \#\mathrm{Gal}((x^3 - t)/\mathbb{Q})$ for all $p \neq 3$, as in [17, Lemma 2.4]. □

## 5 The Chebotarev Density Theorem for Function Fields

We begin by showing that if $\mathfrak{p}$ is a prime of good reduction for $\varphi$, then the number of periodic points for $\varphi_{\mathfrak{p}}$ is bounded above by $\#\varphi_{\mathfrak{p}}^n(\mathbb{P}^1(\mathbb{F}_q))$ for any $n$, where $\mathbb{F}_q$ is the residue field of $\mathfrak{p}$. This follows from a very general principle, which we now prove.

**Definition 5.1.** Let $T : \mathcal{U} \to \mathcal{U}$ be any map of a set $\mathcal{U}$ to itself. For $u \in \mathcal{U}$, define $T^0(u) = u$ and $T^n = T(T^{n-1}(u))$. We say that $u$ is *periodic* if $T^k(u) = u$ for some $k \in \mathbb{N}$ and we say $u$ is *preperiodic* if $T^k(u)$ is periodic for some $k \in \mathbb{Z}_{\geq 0}$. We denote the set of periodic points $\mathrm{Per}(T)$ if the set $\mathcal{U}$ is clear from the context. □

**Lemma 5.2.** If $\mathcal{U}$ is finite, then every point of $\mathcal{U}$ is preperiodic and $\mathrm{Per}(T) = \bigcap_{n=0}^{\infty} T^n(\mathcal{U})$. In particular, $\#\mathrm{Per}(T) \leq \#T^n(\mathcal{U})$ for any positive integer $n$. □

**Proof.** Suppose that $\mathcal{U}$ is finite and let $u \in \mathcal{U}$. Then by the pigeonhole principle, there exist $m, n \in \mathbb{N}$ such that $T^m(u) = T^n(u)$, so $u$ is preperiodic.

Suppose that $u \in \mathcal{U}$ is periodic. Write $T^i(u) = u$ for some $i > 0$. Then $u \in T^{ik}(\mathcal{U})$ for all $k > 0$. Since $T^{in}(\mathcal{U}) = T^n(T^{n(i-1)})$, we have that $T^{in}(\mathcal{U}) \subseteq T^n(\mathcal{U})$, so $u \in T^n(\mathcal{U})$ for every $n$.

Suppose that $u \in \bigcap_{n=0}^{\infty} T^n(\mathcal{U})$. Then we may form a sequence

$$\left\{T\left(a_1\right), T^2\left(a_2\right), T^3\left(a_3\right), \ldots\right\}$$

such that $T^i(a_i) = u$. Since $U$ is finite, the pigeonhole principle gives that there exist $i$, $j$ with $j > i$ such that $a_i = a_j$. Then $u$ is periodic, as

$$u = T^j\left(a_j\right) = T^{j-i}\left(T^i\left(a_j\right)\right) = T^{j-i}\left(T^i\left(a_i\right)\right) = T^{j-i}(u). \qquad \blacksquare$$

In order to apply the Chebotarev density theorem for function fields [16], we establish further notation. Let $L$ be a function field over a finite field $\mathbb{F}_q$, and let $M$ be a finite extension of $L$. Let $\alpha$ be a degree-1 prime in $L$, that is a prime whose residue field is $\mathbb{F}_q$. Suppose that $\alpha$ does not ramify in $M$. Then for each prime $\gamma$ in $M$ lying over $\alpha$, there is a unique Frobenius element $\mathrm{Frob}(\gamma/\alpha)$ such that $\mathrm{Frob}(\gamma/\alpha)$ fixes $\gamma$ and acts as $x \mapsto x^q$ on the residue field $\ell_\gamma$ of $\gamma$. We let $\mathrm{Frob}(\alpha)$ denote the conjugacy class of $\mathrm{Frob}(\gamma/\alpha)$ in $\mathrm{Gal}(M/L)$ (note that elements of this conjugacy class correspond to $\mathrm{Frob}(\gamma'/\alpha)$ as $\gamma'$ ranges over all primes of $M$ lying over $\alpha$).

**Proposition 5.3.** Let $k$ be a number field, let $K = k(t)$, and let $\varphi : \mathbb{P}^1_k \to \mathbb{P}^1_k$ be a rational function. Let $n \in \mathbb{Z}^+$ and $K_n$ be a splitting field of $\varphi^n(x) - t$ over $K$ for some $n$, and let $G_n$ be $\mathrm{Gal}(K_n/K)$. Suppose that $k$ is algebraically closed in $K_n$. Let $\delta > 0$. Then there is a constant $M_\delta$ such that for all $\mathfrak{p}$ with $N(\mathfrak{p}) > M_\delta$, we have

$$\frac{\#\mathrm{Per}\left(\varphi_{\mathfrak{p}}\right)}{N(\mathfrak{p}) + 1} \leq \mathrm{FPP}\left(G_n\right) + \delta. \tag{6}$$

□

**Proof.** Let $\mathfrak{p} \in \mathrm{Spec}\,\mathfrak{o}_k$ be a prime of good reduction for $\varphi$ such that we have $\mathrm{Gal}((K_n)_{\mathfrak{p}}/(K)_{\mathfrak{p}}) \cong G_n$ and let $\mathbb{F}_q$ denote its residue field $\mathfrak{o}_k/\mathfrak{p}$. We let $\varphi_{\mathfrak{p}}$ denote the reduction of $\varphi$ modulo $\mathfrak{p}$ and let $(K_n)_{\mathfrak{p}}$ denote the splitting field of $\varphi_{\mathfrak{p}}^n(x) - t$. Let $z$ be a root of $\varphi_{\mathfrak{p}}^n(x) - t$ in $(K_n)_{\mathfrak{p}}$ and let $\mathcal{S}$ denote the conjugates of $z$ in $(K_n)_{\mathfrak{p}}$. Then the map $\varphi_{\mathfrak{p}} : \mathbb{P}_{\mathbb{F}_q} \to \mathbb{P}_{\mathbb{F}_q}$ is induced by the inclusion of $(K)_{\mathfrak{p}}$ into $(K)_{\mathfrak{p}}(z)$. Let $A_n$ be the integral closure of $\mathbb{F}_q[t]$ in

$(K_n)_{\mathfrak{p}}$. Then $A_n^{G_n} = \mathbb{F}_q[t]$; that is, $\mathbb{F}_q[t]$ is the set of elements of $A_n$ that are fixed by every element of $G_n$. Now, let $(t-\xi)$ be a degree-1 prime in $F_q[t]$ that does not ramify in $(K_n)_{\mathfrak{p}}$, and let $D(\mathfrak{m}/(t-\xi))$ be the decomposition group of a prime $\mathfrak{m}$ in $(K_n)_{\mathfrak{p}}$ that lies over $(t-\xi)$. Then, by [9, Lemma 3.2], the number of degree-1 primes $\beta$ in $(K)_p(z)$ lying over $(t-\xi)$ is equal to the number of fixed points of $D(\mathfrak{m}/(t-\xi))$ acting on $\mathcal{S}$. Likewise, working with the integral closure $A'_n$ of $\mathbb{F}_q[\frac{1}{t}]$ in $(K_n)_{\mathfrak{p}}$, we see that if $\tau$ is the prime at infinity in $\mathbb{F}_q(t)$ (i.e., is the prime $(\frac{1}{t})$ in $\mathbb{F}_q[\frac{1}{t}]$) and $\tau$ does not ramify in $(K_n)_{\mathfrak{p}}$, then the number of degree-1 primes in $(K)_{\mathfrak{p}}(z)$ lying over $\tau$ is equal to the number of fixed points of $D(\mathfrak{m}/\tau)$ acting on $\mathcal{S}$, where $\mathfrak{m}$ is a prime of $A'_n$ lying over $\tau$. Since decomposition groups over unramified primes are generated by Frobenius elements, we see that for any $\alpha \in \mathbb{P}^1(\mathbb{F}_q)$ that does not ramify in $(K_n)_{\mathfrak{p}}$, we have

$$\exists \beta \in \mathbb{P}^1\left(\mathbb{F}_q\right) \text{ such that } \varphi_{\mathfrak{p}}^n(\beta) = \alpha \Leftrightarrow \operatorname{Frob}(\alpha) \text{ has a fixed point in } \mathcal{S}. \tag{7}$$

Since any dense open subset of $\operatorname{Spec}\mathfrak{o}_k$ contains all but finitely many primes in $\operatorname{Spec}\mathfrak{o}_k$, it thus follows from Proposition 4.1 that for all but finitely many $\mathfrak{p}$, the action of $\operatorname{Gal}((K_n)_{\mathfrak{p}}/(K)_{\mathfrak{p}})$ on $\mathcal{S}$ is isomorphic to the action of $G_n$ on the roots of $\varphi^n(x) - t$.

Let $\psi$ denote the number of degree-1 primes $\alpha$ of $\mathbb{P}^1_{\mathbb{F}_q}$ such that $\alpha$ does not ramify in $(K_n)_{\mathfrak{p}}$. For any conjugacy class $C$ of $G_n$, we let $\psi_C$ denote the number of degree-1 primes $\alpha$ of $\mathbb{P}^1_{\mathbb{F}_q}$ such that $\alpha$ does not ramify in $(K_n)_{\mathfrak{p}}$ and such that $\operatorname{Frob}(\alpha) = C$. Then [16, Theorem 1] states that

$$\left|\psi_C - \psi\frac{\#C}{\#G_n}\right| \le 2g_{(K_n)_{\mathfrak{p}}}\frac{\#C}{\#G_n}\sqrt{q} + \#R, \tag{8}$$

where $g_{(K_n)_{\mathfrak{p}}}$ is the genus of $(K_n)_{\mathfrak{p}}$ and $R$ is the set of primes of $\mathbb{P}^1_{\mathbb{F}_q}$ that ramify in $(K_n)_{\mathfrak{p}}$. Let $\operatorname{Fix}(G_n)$ be the set of elements of $G_n$ that fix an element of $\mathcal{S}$. Then $\frac{\#\operatorname{Fix}(G_n)}{\#G_n} = \operatorname{FPP}(G_n)$, and for any $\alpha$ outside of $R$, there is a $\beta$ in $\mathbb{P}^1(\mathbb{F}_q)$ such that $\varphi_{\mathfrak{p}}^n(\beta) = \alpha$ if and only if $\operatorname{Frob}(\alpha) \subseteq \operatorname{Fix}(G_n)$ by (7). There are at most $\#R$ ramified primes $\alpha$ of $\mathbb{F}_q$ such that $\alpha \in \varphi_{\mathfrak{p}}^n(\mathbb{P}^1(\mathbb{F}_q))$. Thus, summing the estimates in (8) over all conjugacy classes in $\operatorname{Fix}(G_n)$ and diving by $\psi = q+1$, we then obtain

$$\frac{\varphi_{\mathfrak{p}}^n\left(\mathbb{P}^1\left(\mathbb{F}_q\right)\right)}{q+1} \le \operatorname{FPP}\left(G_n\right) + 2g_{(K_n)_{\mathfrak{p}}}\frac{\sqrt{q}}{q+1} + \frac{(c+1)\#R}{q+1}, \tag{9}$$

where c is the number of conjugacy classes in $\operatorname{Fix}(G_n)$.

The set of primes over which $\varphi_{\mathfrak{p}}^n$ ramifies has size at most $n(2\deg\varphi - 2)$ since $\varphi_{\mathfrak{p}}$ ramifies over at most $(2\deg\varphi - 2)$ points and $\varphi_{\mathfrak{p}}^n$ can only ramify over these points and their first $n-1$ iterates under $\varphi_{\mathfrak{p}}$. (Note that $\deg\varphi_{\mathfrak{p}} = \deg\varphi$ since $\varphi$ has good reduction at $\mathfrak{p}$.) The size of $G_n$ can be bounded in terms of $n$ and $d$ only, since it is a subgroup of the symmetric group on $d^n$ elements.

Thus, for any $\mathfrak{p}$ of characteristic greater than $\deg \varphi$ (this guarantees that there is no wild ramification at for $\varphi_{\mathfrak{p}}$), we see that $g_{(K_n)_{\mathfrak{p}}}$ can be bounded in terms of $\deg \varphi_{\mathfrak{p}}$ and $n$ by Riemann–Hurwitz; for example,

$$g_{(K_n)_{\mathfrak{p}}} \leq |G_n| n \big(2 \deg \varphi_{\mathfrak{p}} - 2\big) .$$

Hence, by (9) there is an $M_\delta$ such that for all $\mathfrak{p}$ with $N(\mathfrak{p}) \geq M_\delta$, we have

$$\frac{\varphi_{\mathfrak{p}}^n \left(\mathbb{P}^1 \left(\mathbb{F}_q\right)\right)}{q+1} \leq \mathrm{FPP}\left(G_n\right) + \delta.$$

Applying Lemma 5.2 then finishes our proof. ■

We immediately deduce the following as a consequence Proposition 5.3.

**Corollary 5.4.** With notation as in Proposition 5.3, suppose that $k$ is algebraically closed in $K_n$ for all $n$. Then, if $\lim_{n\to\infty} \mathrm{FPP}(G_n) = 0$, we have

$$\lim_{N(\mathfrak{p})\to\infty} \frac{\#\mathrm{Per}\left(\varphi_{\mathfrak{p}}\right)}{N(\mathfrak{p})+1} = 0. \tag{10}$$

□

## 6 Proofs of Main Theorems

We will use the following lemma from [17].

**Lemma 6.1** ([17, Lemma 4.3]). Let $G$ be any transitive group acting faithfully on a finite set $S$, where $\#S > 1$. Then $[G]^n$ acts naturally on $S^n$ and $\lim_{n\to\infty} \mathrm{FPP}([G]^n) = 0$. □

We are now ready to prove our main theorems on proportions of periodic points.

**Proof of Theorem 1.2.** Fix $\epsilon > 0$. By Lemma 6.1, there is an $n$ such that $\mathrm{FPP}([S_d]^n) \leq \epsilon/2$. Let $R = k[a_0, \ldots, a_d, b_0, \ldots, b_d]$. Then, the general rational function

$$\varphi(x) = \frac{a_d x^d + \cdots + a_0}{b_d x^d + \cdots + b_0}$$

gives an equation $h_n(x) = \varphi^n(x) - t = 0$. Let $D$ be the ring $k[c_0, \ldots, c_{d-1}]$ and let $\psi : R[t] \longrightarrow D$ be the homomorphism given by $\psi(a_d) = 1$, $\psi(a_i) = c_i$ for $0 \leq i < d$, $\psi(b_0) = 1$, $\psi(b_j) = 0$ for $1 \leq j \leq d$, and $\psi(t) = 0$. Then $\psi$ extends to a map $\psi_1 : R[t][x] \longrightarrow D[x]$ such that $\psi_1(h(x)) = x^d + c_{d-1}x^{d-1} + \cdots + c_0$. By [17, Theorem 1], we have $\mathrm{Gal}(\psi_1(h_n)/F(D)) \cong [S_d]^n$. Since lemma [17, Lemma 2.4] gives

$$\#\mathrm{Gal}\left(\psi_1\left(h_n\right)/F\left(D\right)\right) \leq \#\mathrm{Gal}\left(h_n(x)/F\left(R[t]\right)\right),$$

and $\mathrm{Gal}(h_n(x)/F(R[t]))$ is isomorphic to a subgroup of $[S_d]^n$, this means that $\mathrm{Gal}(h_n(x)/F(R[t])) \cong [S_d]^n$. Proposition 3.6 then tells us that $F(R)$ is integrally closed in the splitting field of $h_n(x)$, since otherwise $\mathrm{Gal}(h_n(x)/F(R[t]))$ would be a proper subgroup of $[S_d]^n$ for all $n \geq 2$. Thus, by Proposition 4.1, if $V_{d,\epsilon}$ is the set of prime ideals $\mathfrak{m} \in \mathrm{Spec}R$ such that $\mathrm{Gal}((h_n)_{\mathfrak{p}}/(K)_{\mathfrak{p}}) \cong [S_d]^n$, then $V_{d,\epsilon}$ is Zariski-open in $\mathrm{Spec}R$.

Let $U_{d,\epsilon} = V_{d,\epsilon} \cap \mathrm{Rat}_d$ where $\mathrm{Rat}_d$ is as in the paragraph above the statement of Theorem 1.2. Let $\varphi_{\vec{a},\vec{b}} \in U_{d,\epsilon}(k)$. Then by Proposition 5.3, applied to $\delta = \epsilon/2$, we have

$$\frac{\#\mathrm{Per}\left(\varphi_{\vec{a},\vec{b}}\right)}{N(\mathfrak{p})+1} \leq \epsilon/2 + \epsilon/2 = \epsilon,$$

for all sufficiently large $N(\mathfrak{p})$, and our proof is complete. ■

**Lemma 6.2.** Let $k$ be a number field, let $\varphi \in k(x)$, let $\mathfrak{p}$ be a prime of good reduction for $\varphi$, and let $k'$ be a finite extension of $k$. Let $\mathfrak{q}$ be a prime of $k'$ such that $\mathfrak{q} \cap \mathfrak{o}_k = \mathfrak{p}$ and $[(\mathfrak{o}_{k'}/\mathfrak{q}) : (\mathfrak{o}_k/\mathfrak{p})] = 1$. Then $\varphi$ induces a map $\tilde{\varphi}$ over $k'$ such that $\tilde{\varphi}$ has good reduction at $\mathfrak{q}$ and we have $\#\mathrm{Per}(\tilde{\varphi}_{\mathfrak{q}}) = \#\mathrm{Per}(\varphi_{\mathfrak{p}})$. □

**Proof.** We let $\tilde{\varphi}$ be the image of $\varphi$ in $k'(x)$ under the inclusion $k(x) \subseteq k'(x)$. Then $\tilde{\varphi}$ has good reduction at $\mathfrak{q}$.

Since $[(\mathfrak{o}_{k'}/\mathfrak{q}) : (\mathfrak{o}_k/\mathfrak{p})] = 1$, for any $\beta \in \mathfrak{o}_{k'}$, there is an $\alpha \in \mathfrak{o}_k$ such that $\beta \equiv \alpha \pmod{\mathfrak{q}}$. Thus, there is a natural bijection $\sigma : \mathbb{P}^1(\mathfrak{o}_{k'}/\mathfrak{q}) \longrightarrow \mathbb{P}^1(\mathfrak{o}_k/\mathfrak{p})$ such that $\varphi_{\mathfrak{p}}(\sigma(z)) = \sigma(\tilde{\varphi}_{\mathfrak{q}}(z))$ for all $z \in \mathbb{P}^1(\mathfrak{o}_{k'}/\mathfrak{q})$. Thus, for each $z \in \mathbb{P}^1(\mathfrak{o}_{k'}/\mathfrak{q})$, we see that $z$ is periodic under $\varphi_{\mathfrak{q}}$ exactly when $\sigma(z)$ is periodic under $\varphi_{\mathfrak{p}}$. Hence, we have $\#\mathrm{Per}(\tilde{\varphi}_{\mathfrak{q}}) = \#\mathrm{Per}(\varphi_{\mathfrak{p}})$. ■

**Lemma 6.3.** Let $k$ be a number field, let $\varphi \in k[x]$, let $\mathfrak{p}$ be a prime of good reduction for $\varphi$, let $k'$ be a finite extension of $k$, and let $\tilde{\varphi}$ denote the extension of $\varphi$ to $\mathbb{P}^1_{k'}$. Then

$$\liminf_{\substack{N(\mathfrak{p})\to\infty \\ \text{primes } \mathfrak{p} \text{ of } k}} \frac{\#\mathrm{Per}\left(\varphi_{\mathfrak{p}}\right)}{N(\mathfrak{p})+1} \leq \limsup_{\substack{N(\mathfrak{q})\to\infty \\ \text{primes } \mathfrak{q} \text{ of } k'}} \frac{\#\mathrm{Per}\left(\tilde{\varphi}_{\mathfrak{q}}\right)}{N\left(\mathfrak{q}\right)+1}.$$ □

**Proof.** There is a positive proportion of primes $\mathfrak{p}$ in $k$ such that $\mathfrak{p}\mathfrak{o}_{k'}$ factors as a product of distinct primes $\mathfrak{q}$ such that $[(\mathfrak{o}_{k'}/\mathfrak{q}) : (\mathfrak{o}_k/\mathfrak{p})] = 1$, by the Chebotarev density theorem for number fields (see [22, 23]). Let $\mathcal{P}$ be the set of all such primes at which $\varphi$ has good reduction. Let $\mathcal{P}'$ be set of primes $\mathfrak{q}$ of $k'$ such that $\mathfrak{q}|\mathfrak{p}$ for some $\mathfrak{p} \in \mathcal{P}$. Then, by Lemma 6.2, we have

$$\begin{aligned}\liminf_{\substack{N(\mathfrak{p})\to\infty \\ \text{primes } \mathfrak{p} \text{ of } k}} \frac{\#\mathrm{Per}\left(\varphi_{\mathfrak{p}}\right)}{N(\mathfrak{p})+1} &\leq \liminf_{\substack{N(\mathfrak{p})\to\infty \\ \mathfrak{p}\in\mathcal{P}}} \frac{\#\mathrm{Per}\left(\varphi_{\mathfrak{p}}\right)}{N(\mathfrak{p})+1} \\ &\leq \limsup_{\substack{N(\mathfrak{q})\to\infty \\ \mathfrak{q}\in\mathcal{P}'}} \frac{\#\mathrm{Per}\left(\tilde{\varphi}_{\mathfrak{q}}\right)}{N(\mathfrak{q})+1} \\ &\leq \limsup_{\substack{N(\mathfrak{q})\to\infty \\ \text{primes } \mathfrak{q} \text{ of } k'}} \frac{\#\mathrm{Per}\left(\tilde{\varphi}_{\mathfrak{q}}\right)}{N(\mathfrak{q})+1},\end{aligned}$$

as desired. ■

We now prove Theorem 1.3. Recall that $K_n$ denotes the splitting field of $\varphi^n(x) - t$ over $k(t)$.

**Proof of Theorem 1.3.** Let $E$ denote the algebraic closure of $k$ in $K_1$ and let $G$ be the Galois group $\mathrm{Gal}((\varphi(x) - t)/E(t))$. Let $I$ be the subgroup of $G$ generated by the ramification groups of the critical points. Then $I = G$ by Remark 3.2. Thus, we have $\mathrm{Gal}((\varphi^n(x) - t)/E(t)) \cong [G]^n$ for all $n$ by Theorem 3.1. Thus, by Corollary 5.4,

$$\lim_{\substack{N(\mathfrak{q})\to\infty \\ \mathfrak{q} \text{ a prime of } E}} \frac{\#\mathrm{Per}\left(\tilde{\varphi}_{\mathfrak{q}}\right)}{N(\mathfrak{q})+1} = 0,$$

and Lemma 6.3 then implies (a). If $k$ is algebraically closed in $K_1$, then $k = E$ and (b) follows from Corollary 5.4. ■

**Proposition 6.4.** Let $k$ be a number field, let $d > 1$, and let $f(x) = x^d + c \in k[x]$ have the property that 0 is not preperiodic. Then

(a)

$$\liminf_{\mathfrak{p}\to\infty} \frac{\#\mathrm{Per}(f_{\mathfrak{p}})}{N(\mathfrak{p})+1} = 0;$$

(b) if $k$ contains a primitive $d$th root of unity, we have

$$\lim_{\mathfrak{p}\to\infty} \frac{\#\mathrm{Per}\left(f_{\mathfrak{p}}\right)}{N(\mathfrak{p})+1} = 0.$$ □

**Proof.** Let $k' = k(\xi_d)$ where $\xi_d$ is $d$th roof unity, and let $\tilde{f}$ denote the extension of $f$ to $\mathbb{P}^1_{k'}$. Then the splitting field of $\tilde{f}(x) - t$ over $k(t)$ is simply $k'(t)(\sqrt[d]{t-c})$, which has degree $d$ over $k'(t)$ and ramifies completely over $t-c$; thus, the Galois group is generated by the ramification group over $t-c$. Since the critical point 0 is not preperiodic, we see then that the conditions of Theorem 3.1 are met for all $N$. Thus, for any $n$, we have $\mathrm{Gal}((\tilde{f}^n(x)-t)/k'(t)) \cong [C_d]^n$, where $C_d$ is the cyclic group of order $d$. Thus, by Corollary 5.4 and Lemma 6.1, we have

$$\lim_{\substack{N(\mathfrak{q})\to\infty \\ \mathfrak{q} \text{ a prime of } k'}} \frac{\#\mathrm{Per}\left(\tilde{f}_{\mathfrak{q}}\right)}{N(\mathfrak{q})+1} = 0.$$

Since $k' = k$ if $k$ contains a primitive $d$th root of unity, (b) follows immediately from Corollary 5.4; likewise, (a) follows from Corollary 5.4 and Lemma 6.3. ■

**Theorem 6.5.** Let $k$ be a number field, let $d > 1$, and let $f(x) = x^d + c \in k[x]$. Then

$$\liminf_{\mathfrak{p}\to\infty} \frac{\#\mathrm{Per}\left(f_{\mathfrak{p}}\right)}{N(\mathfrak{p})+1} = 0$$

unless $f$ is the Chebyshev polynomial $x^2-2$. □

**Proof.** If 0 is not preperiodic under $f$, then the desired result follows immediately from Proposition 6.4.

If 0 is preperiodic for $f$, then $f$ is post-critically finite; that is, every critical point of $f$ is preperiodic. By [13, Theorem 1.1], we must then have $\lim_{n\to\infty} \mathrm{FPP}(\mathrm{Gal}((f^n(x)-t)/\mathbb{C}(t))) = 0$ unless either (a) $f$ is conjugate to $\pm T_d$, where $T_d$ is a Chebyshev polynomial of degree $d$ or (b) there is a fixed point $\alpha \in \mathbb{C}$ of $f$ such that $f^{-1}(\alpha) \setminus \{\alpha\}$ is a nonempty set of critical points of $f$. It is clear that (b) cannot happen for maps of the form $x^d + c$, since the inverse image of any point contains either a single critical point or more than one point that is not critical. Furthermore, when $d > 2$, no $\pm T_d$ can be conjugate to $x^d + c$, since the derivative of $\pm T_d$ cannot be a perfect $(d-1)$st power (since, e.g., $\pm T_d'$ has a nonzero term of degree $d-3$ but no term of degree $d-2$). In the case where $d = 2$, the only conjugate of $\pm T_d$ that has the form $x^2 + c$ is $x^2 - 2$ (see [13, Corollary 1.3]).

Now, assume that $f(x) \neq x^2 - 2$. Then, from above, we see that if $L_n$ is the splitting field of $f^n(x) - t$ over $\mathbb{C}(t)$ and $G_n = \mathrm{Gal}(L_n/\mathbb{C}(t))$, then $\mathrm{FPP}(G_n)$ goes to zero as $n$ goes to infinity. Now, let $K_n$ be the splitting field of $f^n(x) - t$ over $k(t)$ and let $k_n$ be the algebraic closure of $k$ in $K_n$. Since $K_n$ and $\mathbb{C}(t)$ are disjoint over $k_n(t)$ we see that every action of $G_n$ on the roots of $f^n(x) - t$ restricts to a unique action of $\mathrm{Gal}(K_n/k_n(t))$ on the roots of $f^n(x) - t$. For each $k_n$, there is a positive proportion of primes $\mathfrak{p}$ in $k$ such that $\mathfrak{p}\mathfrak{o}_{k_n}$ factors as a product of distinct primes $\mathfrak{q}$ such that $\mathfrak{o}_{k_n}/\mathfrak{q} = \mathfrak{o}_k/\mathfrak{p}$ by the Chebotarev density theorem for number fields (see [22, 23]). Let $U_n$ be the set of all such primes. Then there is some $n$ such that $\mathrm{FPP}(G_n) < \epsilon/2$. Then, using Proposition 5.3 with $\delta = \epsilon/2$, we see that for all sufficiently large $\mathfrak{q}$, the proportion of periodic points for $f_{\mathfrak{q}}$ is at most $\epsilon$. Thus, there is an element of $\mathfrak{q} \in U_n$ such that the proportion of periodic points for $f_{\mathfrak{q}}$ is at most $\epsilon$. Letting $\mathfrak{p} = \mathfrak{q} \cap \mathfrak{o}_k$, the proportion of periodic points for $f_{\mathfrak{p}}$ is at at most $\epsilon$, by Lemma 6.2. This proves the theorem. ■

We can now prove Theorem 1.5 quite easily.

**Proof of Theorem 1.5.** We choose a linear polynomial $\sigma = ax + b \in k[x]$ such that $(\sigma^{-1} f \sigma)(x) = x^2 + c$ for some $c \in k$. Since $\sigma$ is an automorphism of $\mathfrak{o}_k/\mathfrak{p}$ for all but at most finitely many primes $\mathfrak{p}$ of $\mathfrak{o}_k$, it follows that for all but at most finitely many primes $\mathfrak{p}$, we have $\#\mathrm{Per}(f_{\mathfrak{p}}) = \#\mathrm{Per}((\sigma^{-1} f \sigma)_{\mathfrak{p}})$. The result now follows immediately from Theorem 6.5. ■

**Remark 6.6.** We note that the techniques Jones [13] uses to control $\mathrm{Gal}((f^n(x) - t)/\mathbb{C}(t))$, for $f$ a post-critically finite polynomial, are completely different than the wreath product techniques used here. Whereas the wreath product techniques here are mostly algebraic (relying on disjointness of ramification in field extensions), Jones relies on the complex-analytic theory of iterated monodromy groups. □

## 7 Examples

We end with a discussion of how proportions of periodic points behave for powering, Chebyshev, and Lattès maps as we vary over primes in $\mathbb{Z}$. Note that Manes and Thompson [15] have previously analyzed periodic points for Chebyshev maps in $\mathbb{F}_{p^n}$ as $n$ goes to infinity. In these examples, we provide a mostly elementary analysis, with no estimates of proportions of fixed-point-free elements for iterated Galois groups; for a more Galois-theoretic discussion of related issues, see [13].

**Example 7.1.** Let $f(x) = x^d$. Let $k$ be a number field. By the Chebotarev density theorem for number fields, for any $m$ there are infinitely many primes $\mathfrak{q}$ of $\mathfrak{o}_k$ such that $d^m$ divides $q - 1$ where $\mathbb{F}_q$ is the residue field $\mathfrak{o}_k/\mathfrak{q}$. For each such prime, $f_{\mathfrak{q}}^m$ is a $d^m$-to-one map on $(\mathbb{F}_q)^*$ so the proportion of periodic points is at most $1/d^m + 2/(q+1)$ (the two comes from the fact that 0 and $\infty$ are periodic). Thus, we see that

$$\liminf_{N(\mathfrak{q}) \to \infty} \frac{\#\mathrm{Per}\left(f_{\mathfrak{q}}\right)}{N(\mathfrak{q}) + 1} = 0. \qquad \square$$

**Example 7.2.** Let $f$ be a monic Chebyshev polynomial satisfying $f(x+\frac{1}{x}) = x^d + \frac{1}{x^d}$. Here we work only over $\mathbb{Q}$. We can give an elementary description of the asymptotic behavior of the proportion of periodic points for $f_p$; it depends very much on whether or not $d$ is a prime power.

Define $\pi(x) = x + \frac{1}{x}$ and $g(x) = x^d$. Then we have

$$\begin{tikzcd}
\mathbb{P}^1 \arrow[r, "g"] \arrow[d, "\pi"'] & \mathbb{P}^1 \arrow[d, "\pi"'] \\
\mathbb{P}^1 \arrow[r, "f"] & \mathbb{P}^1
\end{tikzcd}$$

Take any $\alpha \in \mathbb{P}^1(\mathbb{F}_p)$. Let $\beta \in \mathbb{P}^1(\mathbb{F}_{p^2})$ such that $\pi(\beta) = \alpha$. We will show that $\beta$ is $g$-periodic if and only if $\alpha$ is $f$-periodic. If $\beta$ is $g$-periodic, then $g^m(\beta) = \beta$ so $f^m(\alpha) = \alpha$, so $\alpha$ must be $f$-periodic. Conversely, suppose that $\alpha$ is $f$-periodic. If $\beta$ equals 0 or $\infty$, then $\alpha$ is $\infty$ so both $\alpha$ and $\beta$ are periodic. Suppose $\beta \neq 0, \infty$. If $f^m(\alpha) = \alpha$ for some $m$, then $\pi(g^m(\beta)) = \alpha$ for some $m$, so $g^m(\beta) = \beta$ or $g^m(\beta) = 1/\beta$. If $g^m(\beta) = \beta$, then $\beta$ is obviously $g$-periodic; if $g^m(\beta) = 1/\beta$, then $\beta^{d^m} = 1/\beta$ so $(1/\beta)^{d^m} = \beta$, thus $g^{2m}(\beta) = \beta$ and hence $\beta$ is still periodic.

Let $U$ be the set of $z \in \mathbb{F}_{p^2}^*$ such that $\pi(z) \in \mathbb{F}_p$. We see that if $z \in U$ and $z \notin \mathbb{F}_p$, then $z$ and $1/z$ are the roots of the quadratic polynomial $T^2 - (z + 1/z)T + 1$, so $z$ and $1/z$ are conjugate over $\mathbb{F}_p$. Hence, we have $z^p = 1/z$ so $z^{p+1} = 1$. Thus, we see that $U = (\mathbb{F}_p)^* \cup U_{p+1}$ where $U_{p+1}$ is the set of points in $\mathbb{F}_{p^2}^*$ whose order divides $p+1$. The elements of $U$ that are $g$-periodic are simply the ones whose order is coprime to $d$.

When $d$ is a power of an odd prime, either $p+1$ or $p-1$ is prime to $d$, so we obtain at least $p-1$ $g$-periodic points. Since $\pi$ is two-to-one at all but two points of $U$, we see immediately that $\liminf_{p\to\infty} \#\mathrm{Per}(f_p)/p \geq \frac{1}{2}$. Now, there are $p$ such that $p \equiv 1 \pmod{d^r}$, for any positive integer $r$ by the Dirichlet theorem for primes in arithmetic progressions (which may be regarded as a special case of the Chebotarev density theorem for number fields), so the proportion of $g$-periodic points in $\mathbb{F}_p^*$ can be made as small as desired. Thus, we have

$$\liminf_{p\to\infty} \frac{\#\mathrm{Per}\left(f_p\right)}{p} = \frac{1}{2}.$$

Suppose that $d$ is a power of 2. Then at least one of $p-1$ and $p+1$ is not divisible by 4. Arguing as in the case of odd prime powers (only with 2 dividing both $p-1$ and $p+1$ for $p > 2$), we see that $\liminf_{p\to\infty} \#\mathrm{Per}(f_p)/p \geq \frac{1}{4}$. For any $r$, there are infinitely many $p$ such that $p \equiv 1 \pmod{2^r}$, again by Dirichlet's theorem on primes in arithmetic progressions. For such primes, half of the elements of $U_{p+1}$ are $g$-periodic and at most

$1/2^r$ points in $\mathbb{F}_p^*$ are $g$-periodic, so we thus obtain

$$\liminf_{p\to\infty} \frac{\#\mathrm{Per}\left(f_p\right)}{p} = \frac{1}{4}.$$

When $d$ has at least two distinct prime factors $\ell_1$ and $\ell_2$, things are very different. Using the Chinese Remainder Theorem together with Dirichlet's theorem for primes in arithmetic progressions we may, for any $r$, find a prime $p$ such that $p \equiv 1 \pmod{\ell_1^r}$ and $p \equiv -1 \pmod{\ell_2^r}$. The proportion of periodic points in $\mathbb{F}_p^*$ is then at most $1/\ell_1^r$, and the proportion of periodic points in $U_{p+1}$ is at most $1/\ell_2^r$. Hence, we see in this case that

$$\liminf_{p\to\infty} \frac{\#\mathrm{Per}\left(f_p\right)}{p} = 0. \qquad \square$$

**Example 7.3.** Let $\ell$ be a prime and let $\varphi(x)$ be a Lattès map induced by the multiplication-by-$\ell$ map on an elliptic curve $E$, say defined over $\mathbb{Q}$. We will show that in many cases, we must have

$$\liminf_{p\to\infty} \frac{\#\mathrm{Per}\left(\varphi_p\right)}{p} = 0.$$

The argument here is quite similar to that of Example 7.2, though the details are more complicated. Given the multiplication-by-$d$ map (which we denote as $[d]$) on an elliptic curve $E$, we have a Lattès map $\varphi$ that makes the following diagram commute:

$$\begin{tikzcd} E \arrow[r, "{[d]}"] \arrow[d, "\pi"'] & E \arrow[d, "\pi"'] \\ \mathbb{P}^1 \arrow[r, "\varphi"] & \mathbb{P}^1 \end{tikzcd}$$

The projection $\pi$ here comes from the inclusion of the fixed field of the elliptic involution $[-1]$ into the function field of $E$. When $E$ is in Weierstrass form $y^2 = g(x)$, we have simply $\pi(x, y) = x$.

We now assume that $d = \ell$ is a prime; letting $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ act on the Tate module $T_\ell(E)$ we obtain a homomorphism $\rho_\ell : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}_\ell)$. We further assume that $\ell$ is chosen so that $\rho_\ell$ surjects onto $\mathrm{GL}_2(\mathbb{Z}_\ell)$; for $E$ fixed (and without complex multiplication) this holds for all but finitely many primes $\ell$ by Serre's celebrated open image theorem (see [19]).

Given a prime $p$, let $F_p = \rho_\ell(\mathrm{Frob}_p)$ denote the image of the Frobenius conjugacy class $\mathrm{Frob}_p$ in $\mathrm{GL}_2(\mathbb{Z}_\ell)$. Given $k \in \mathbb{Z}^+$, the Chebotarev density theorem together with the surjectivity of $\rho_\ell$ implies that we have

$$\sigma_p \equiv \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \bmod \ell^k$$

for some $\sigma_p \in \rho_\ell(\mathrm{Frob}_p)$ for a positive proportion of primes $p$. For such $p$, the group $E(\mathbb{F}_p)$, viewed as an abelian group, contains a subgroup $H_1 \simeq \mathbb{Z}/\ell^k\mathbb{Z}$ on which the induced Frobenius action is trivial. Furthermore, since $\sigma_p^2$ is congruent to the identity matrix modulo $\ell^k$, there exists a subgroup $H_2 \simeq \mathbb{Z}/\ell^k\mathbb{Z}$ contained in $E(\mathbb{F}_{p^2})$ such that the induced Frobenius action on $H_2$ is given by multiplication by $-1$. In order to analyze the action of $\varphi_p$ on $\mathbb{P}^1(\mathbb{F}_p)$, let

$$S_1 = \left\{x \in \mathbb{F}_p : x^3 + ax + b \text{ is a quadratic residue mod } p\right\}$$

and let $S_2 = \mathbb{F}_p \setminus S_1$ denote the complement.

We begin with the $\varphi_p$-periodic points in $S_1$. With $G_1$ denoting the group of $\mathbb{F}_p$-points on $E$, we note that $\pi^{-1}(S_1) \cup \{\infty\} = G_1$. By [20, Proposition 6.52], $\mathrm{Per}_n(\varphi) = \pi(E[\ell^n - 1]) \cup \pi(E[\ell^n + 1])$ hence it is enough to show that $G_1$ has small intersection with the union of $E[\ell^n \pm 1]$ for all $n$. Let $H_1'$ denote the maximal cyclic group of order $\ell^{k_1}$ such that $H_1' \subset G_1$. Note that $H_1'$ contains $H_1$, so $k_1 \geq k$, and we also note that there is a natural surjection $G_1 \twoheadrightarrow H_1'$. Moreover, since $\ell$ is coprime to $\ell^n \pm 1$ for all $n$, the intersection

$$G_1 \cap \left(\bigcup_{n \geq 1} \left(\pi\left(E[\ell^n - 1]\right) \cup \pi\left(E[\ell^n + 1]\right)\right)\right)$$

is contained in the kernel of $G_1 \twoheadrightarrow H_1'$. Consequently, the proportion of $\varphi_p$-periodic point in $S_1$ is at most $(1 + o(1))/\ell^k$, as $p \to \infty$.

We next consider the proportion of $\varphi_p$-periodic points in $S_2$. Since $\pi^{-1}(S_2)$ is contained in the subgroup

$$G_2 := \left\{P \in E\left(\mathbb{F}_{p^2}\right) : P + \mathrm{Frob}_p(P) = 0\right\}$$

(if $x \in S_2$ and $y^2 = x^3 + ax + b$, then $\mathrm{Frob}_p(y) = -y$) and $\pi^{-1}(S_2) \cup E[2](\mathbb{F}_{p^2}) = G_2$ (i.e., they have essentially the same cardinality) we may argue as before by bounding the intersection $G_2 \cap (\bigcup_{n \geq 1}(\pi(E[\ell^n - 1]) \cup \pi(E[\ell^n + 1])))$. With $H_2'$ denoting the maximal cyclic group of order $\ell^{k_2}$ such that $H_2' \subset G_2$; we again have $k_2 \geq k$ and a projection $G_2 \twoheadrightarrow H_2'$.

Arguing as before, we find that the proportion of $\varphi_p$-periodic points in $S_2$ is also at most $(1 + o(1))/\ell^k$, as $p \to \infty$.

Thus, as both proportions of $\varphi_p$-periodic points in $S_1$ and $S_2$ is at most $(1 + o(1))/l^k$, as $p \to \infty$, the same bound holds for the proportion of $\varphi_p$-periodic points $x \in \mathbb{F}_p$

(recall that $\mathbb{F}_p$ is the disjoint union of $S_1$ and $S_2$). Since $k$ might be taken arbitrarily large, we find that

$$\liminf_{p\to\infty} \frac{\#\mathrm{Per}\left(\varphi_p\right)}{p+1} = 0.$$

We end by remarking that $\rho_\ell$ being surjective is a much stronger assumption than needed—we only require that the image contains a sequence of elements $g_i$ approaching (in the $\ell$-adic norm) some $h \in \mathrm{GL}_2(\mathbb{Z}_\ell)$ which is $\mathbb{Z}_\ell$-conjugate to $J := \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. For instance, if $\ell$ is odd and $\#(E[\ell] \cap E(\mathbb{Q})) = \ell$, the image of $\rho_\ell$ is much smaller than $\mathrm{GL}_2(\mathbb{Z}_\ell)$, but it still contains an element $M \in \mathrm{GL}_2(\mathbb{Z}_\ell)$ which, modulo $l$ is conjugate to $J$. (Since there is $\ell$-torsion defined over $\mathbb{Q}$, the reduction modulo $\ell$ fixes an $\mathbb{F}_\ell$-line, and the composition of $\rho_\ell$ with the determinant surjects onto $\mathbb{Z}_\ell^\times$.) Now, $M$ being conjugate (modulo $\ell$) to a diagonal matrix whose eigenvalues are distinct modulo $\ell$ implies a $\mathbb{Z}_\ell$-conjugacy $M \sim M' = \left(\begin{smallmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{smallmatrix}\right)$ where $\lambda_1 \equiv 1 \bmod \ell$ and $\lambda_2 \equiv -1 \bmod \ell$. Since $M$ is in the image, so is $M^{\ell^k}$, and we clearly have $(M')^{l^k} \to J$ as $k \to \infty$ (in the $\ell$-adic metric). □

**Acknowledgements**

We would like to thank Rafe Jones, Michelle Manes, and Joe Silverman for many useful conversations, suggestions, and corrections. We would also like to thank an anonymous referee for many thoughtful comments, which greatly improved the exposition in this paper.

**Funding**

This work was partially supported by NSF grant DMS-1200749 (to J.J. and T.J.T.) and by the Göran Gustafsson Foundation for Research in Natural Sciences and Medicine, and the Swedish Research Council (621-2011-5498) (to P.K.).

## References

[1] Bach, E. "Toward a theory of Pollard's rho method." *Information and Computation* 90, no. 2 (1991): 139–55.

[2] Benedetto, R. L., D. Ghioca, B. Hutz, P. Kurlberg, T. Scanlon, and T. J. Tucker. "Periods of rational maps modulo primes." *Mathematische Annalen* 355, no. 2 (2013): 637–60.

[3] Cullinan, J. and F. Hajir. "Ramification in iterated towers for rational functions." *Manuscripta Mathematica* 137, no. 3–4 (2012): 273–86.

[4] Flajolet, P. and A. M. Odlyzko. "Random Mapping Statistics." *Advances in Cryptology—EUROCRYPT '89 (Houthalen, 1989)*, 329–54. Lecture Notes in Computer Science 434. Berlin: Springer, 1990.

[5] Fried, M. "On a conjecture of Schur." *Michigan Mathematical Journal* 17 (1970): 41–55.

[6] Görtz, U. and T. Wedhorn. "Schemes with Examples and Exercises." *Algebraic Geometry I*. Advanced Lectures in Mathematics. Wiesbaden: Vieweg + Teubner, 2010.

[7] Grothendieck, A. "Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. III." *Institut de Hautes Études Scientifiques. Publications Mathématiques* 28 (1966): 255.

[8] Guralnick, R. M., P. Müller, and J. Saxl. "The rational function analogue of a question of Schur and exceptionality of permutation representations." *Memoirs of the American Mathematical Society* 162, no. 773 (2003): viii+79.

[9] Guralnick, R. M., T. J. Tucker, and M. E. Zieve. "Exceptional covers and bijections on rational points." *International Mathematics Research Notices* (2007), Art. ID rnm004, 20.

[10] Hamblen, S., R. Jones, and K. Madhu. "The density of primes in orbits of $z^d + c$." *International Mathematics Research Notices* 2015, no. 7 (2015): 1924–58.

[11] Janusz, G. J. *Algebraic Number Fields*. 2nd ed. Graduate Studies in Mathematics 7. Providence, RI: American Mathematical Society, 1996.

[12] Jones, R. "The density of prime divisors in the arithmetic dynamics of quadratic polynomials." *Journal of the London Mathematical Society. Second Series* 78, no. 2 (2008): 523–44.

[13] Jones, R. "Fixed-point-free elements of iterated monodromy groups." *Transactions of the American Mathematical Society* 367, no. 3 (2015): 2023–49.

[14] Lang, S. *Algebraic Numbers*. Reading, MA: Addison-Wesley Publishing, 1964.

[15] Manes, M. and B. Thompson. "Periodic points in towers of finite fields for polynomials associated to algebraic groups." (2013): preprint arXiv:1301.6158, 18 pp.

[16] Murty, V. K. and J. Scherk. "Effective versions of the Chebotarev density theorem for function fields." *Comptes Rendus de l'Académie des Sciences - Series I - Mathematics* 319, no. 6 (1994): 523–8.

[17] Odoni, R. W. K. "The Galois theory of iterates and composites of polynomials." *Proceedings of the London Mathematical Society. Third Series* 51, no. 3 (1985): 385–414.

[18] Pink, R. "Profinite iterated monodromy groups arising from quadratic morphisms with infinite postcritical orbits." (2013): preprint arXiv:1309.5804, 26 pp.

[19] Serre, J.-P. "Propriétés galoisiennes des points d'ordre fini des courbes elliptiques." *Inventiones Mathematicae* 15, no. 4 (1972): 259–331.

[20] Silverman, J. H. *The Arithmetic of Dynamical Systems*. Graduate Texts in Mathematics 241. New York: Springer, 2007.

[21] Silverman, J. H. "Variation of periods modulo $p$ in arithmetic dynamics." *New York Journal of Mathematics* 14 (2008): 601–16.

[22] Stevenhagen, P. and H. W. Lenstra Jr. "Chebotarëv and his density theorem." *The Mathematical Intelligencer* 18, no. 2 (1996): 26–37.

[23] Tschebotareff, N. "Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehören." *Mathematische Annalen* 95, no. 1 (1926): 191–228.