Algebra &
Number
Theory

Volume 17
2023
No. 9

Isotriviality, integral points, and primitive primes in orbits in characteristic p

Alexander Carney, Wade Hindes and Thomas J. Tucker

msp

ALGEBRA AND NUMBER THEORY 17:9 (2023)
https://doi.org/10.2140/ant.2023.17.1573

Isotriviality, integral points, and primitive primes in orbits in characteristic p

Alexander Carney, Wade Hindes and Thomas J. Tucker

We prove a characteristic p version of a theorem of Silverman on integral points in orbits over number fields and establish a primitive prime divisor theorem for polynomials in this setting. In characteristic p, the Thue–Siegel–Dyson–Roth theorem is false, so the proof requires new techniques from those used by Silverman. The problem is largely that isotriviality can arise in subtle ways, and we define and compare three different definitions of isotriviality for maps, sets, and curves. Using results of Favre and Rivera-Letelier on the structure of Julia sets, we prove that if φ is a nonisotrivial rational function and β is not exceptional for φ, then $\varphi^{-n}(\beta)$ is a nonisotrivial set for all sufficiently large n; we then apply diophantine results of Voloch and Wang that apply for all nonisotrivial sets. When φ is a polynomial, we use the nonisotriviality of $\varphi^{-n}(\beta)$ for large n along with a partial converse to a result of Grothendieck in descent theory to deduce the nonisotriviality of the curve $y^\ell = \varphi^n(x) - \beta$ for large n and small primes $\ell \neq p$ whenever β is not postcritical; this enables us to prove stronger results on Zsigmondy sets. We provide some applications of these results, including a finite index theorem for arboreal representations coming from quadratic polynomials over function fields of odd characteristic.

1. Introduction and Statement of Results

In [36, Theorem A], Silverman proved the following theorem.

Theorem 1.1 [36, Theorem A]. *Let $\varphi \in \mathbb{Q}(z)$ be rational function of degree at least 2, and let $\alpha \in \mathbb{P}^1(\mathbb{Q})$. If $\varphi^2 \notin \mathbb{Q}[z]$, then the set $\{\varphi^n(\alpha) \mid n \in \mathbb{Z}^+\}$ contains only finitely many points in $\mathbb{Z}$.*

We prove that the analogous theorem holds for nonisotrivial rational functions in $\mathbb{F}_p(t)$. Recall that a rational function $\varphi \in \mathbb{F}_p(t)(z)$ is said to be isotrivial if there is a $\sigma \in \overline{\mathbb{F}_p(t)}(z)$ of degree 1 such that $\sigma \circ \varphi \circ \sigma^{-1} \in \overline{\mathbb{F}}_p(z)$. We prove the following.

Theorem 1.2. *Let $\varphi \in \mathbb{F}_p(t)(z)$ be a nonisotrivial rational function of degree at least 2, and let $\alpha \in \mathbb{P}^1(\mathbb{F}_p(t))$. If $\varphi^2 \notin \mathbb{F}_p(t)[z]$, then $\{\varphi^n(\alpha) \mid n \in \mathbb{Z}^+\}$ contains only finitely many points in $\mathbb{F}_p[t]$.*

Silverman [36] also proves Theorem 1.1 over number fields; see [36, Theorem B]. Likewise, our most general form of Theorem 1.2 is stated in terms of S-integrality and isotriviality for rational functions defined over finite extensions of $\mathbb{F}_p(t)$. We will define S-integrality in the next section (see Definition 2.1). We give our more general definition of isotriviality for rational functions here.

MSC2020: primary 37P15; secondary 11G50, 11R32, 14G25, 37P05, 37P30.
Keywords: arithmetic dynamics, integral points, arboreal representations, Zsigmondy sets.

Definition 1.3. Let K be a finite extension of $\mathbb{F}_p(t)$ and let φ be a rational function in $K(z)$. We say that φ is an isotrivial rational function if there exists $\sigma \in \overline{K}(z)$ of degree 1 such that $\sigma \circ \varphi \circ \sigma^{-1} \in \overline{\mathbb{F}}_p(z)$.

Also recall that for a rational function $\varphi \in K(z)$, a point $\beta \in \mathbb{P}^1(K)$ is said to be *exceptional* for φ if its total orbit (both forward and backward) is finite. However, for the maps that we consider, this amounts to $\varphi^{-2}(\beta) = \{\beta\}$ by Riemann–Hurwitz. In particular, since totally inseparable maps are isotrivial (which may be seen by moving fixed points to 0 and ∞), we avoid the more exotic cases of exceptional points arising in positive characteristic; see, for instance, [38]. With this in place, we state our general form of Theorem 1.2.

Theorem 1.4. *Let K be a finite extension of $\mathbb{F}_p(t)$, let $\varphi \in K(z)$ be a nonisotrivial rational function with $\deg \varphi > 1$, let S be a finite set of places of K, and let $\alpha, \beta \in K$ where β is not exceptional for φ. Then $\{\varphi^n(\alpha) \mid n \in \mathbb{Z}^+\}$ contains only finitely many points that are S-integral relative to β.*

The main tools used in the proof of [36, Theorem A] are from diophantine approximation. Roughly, one takes an inverse image $\varphi^{-i}(\infty)$ that contains at least three points and applies Siegel's theorem on integral points for the projective line with at least three points deleted to conclude that there only finitely many n such that $\varphi^n(\alpha)$ are integral relative to $\varphi^{-i}(\infty)$ and thus only finitely many $n+i$ such that $\varphi^{n+i}(\alpha)$ is an integer. Over function fields in characteristic p, the problem is more complicated since Roth's theorem is false; in fact, no improvement on Liouville's theorem is possible in general. There is, however, a weaker version of Siegel's theorem, due to Wang [45, Theorem in $\mathbb{P}^1(K)$, page 337] and Voloch [44], which states that, for function fields in characteristic p, there are finitely many S-integral points on the projective line with a nonisotrivial set of points deleted. (Note that this is strictly weaker than Siegel's theorem, since any set of three points is automatically isotrivial, and there are isotrivial sets of every countable cardinality.) Basic functorial results on integral points thus imply that Theorem 1.4 will hold whenever $\varphi^{-n}(\beta)$ is a nonisotrivial set. In Theorem 3.1, we show that $\varphi^{-n}(\beta)$ is a nonisotrivial set for large n whenever φ is a nonisotrivial rational function and β is not exceptional, using results of Favre and Rivera-Letelier [14] on the structure of Julia sets at primes of genuinely bad reduction.

In the case where φ is a polynomial of separable degree greater than 1, we can prove a bit more than Theorem 1.4. To describe our result we need a bit of terminology. For a sequence $\{b_n\}_{n=1}^{\infty}$ of elements of a global field K, we say that a place $\mathfrak{p}$ of K is a *primitive divisor* of b_n if

$$v_{\mathfrak{p}}(b_n) > 0 \text{ and } v_{\mathfrak{p}}(b_m) \le 0 \quad \text{for all } m < n.$$

For a positive integer ℓ, we say that $\mathfrak{p}$ is a *primitive ℓ-divisor* of b_n if

$$\mathfrak{p} \text{ is a primitive divisor of } b_n \text{ and } \ell \nmid v_{\mathfrak{p}}(b_n).$$

Given a rational function $\varphi \in K(x)$ and points $\alpha, \beta \in K$, we obtain a sequence $\{\varphi^n(\alpha) - \beta\}_{n=1}^{\infty}$. We define the Zsigmondy set $\mathcal{Z}(\varphi, \alpha, \beta)$ (see [3; 47]) for φ, α, and β as

$$\mathcal{Z}(\varphi, \alpha, \beta) = \{n \mid \varphi^n(\alpha) - \beta \text{ has no primitive divisors}\}.$$

Likewise, for a positive integer ℓ and α, β, and φ as above, we define the ℓ-Zsigmondy set $\mathcal{Z}(\varphi, \alpha, \beta, \ell)$ for φ, α, β, and ℓ as

$$\mathcal{Z}(\varphi, \alpha, \beta, \ell) = \{n \mid \varphi^n(\alpha) - \beta \text{ has no primitive } \ell\text{-divisors}\}.$$

We will also need a precise definition of critical points to state our next theorem. Let φ be a rational function in $K(z)$. We let $\deg_s \varphi$ denote the degree of the maximal separable extension of $K(\varphi(z))$ in $K(z)$ and let $\deg_i \varphi = (\deg \varphi)/(\deg_s \varphi)$; note that $\deg_i \varphi$ is also the largest power p^r of p such that φ can be written as $\varphi(z) = g(x^{p^r})$ for some rational function $g \in K(z)$. For $\gamma \in \mathbb{P}^1$, there are degree one rational functions $\sigma, \theta \in K(z)$ such that $\theta(0) = \gamma$ and $\sigma \circ \varphi \circ \theta(0) = 0$. We may then write $\sigma \circ \varphi \circ \theta(z) = z^e g(z)$ for some rational function g such that $g(z) \neq 0$. We call e the *ramification degree* of φ at γ denote it as $e_\varphi(\gamma/\varphi(\gamma))$. We say that γ is a *critical point* of φ if $e_\varphi(\gamma/\varphi(\gamma)) > \deg_i \varphi$.

We let $O_\varphi^+(\alpha)$ denote the set $\{\varphi^n(\alpha) \mid n \in \mathbb{Z}^+\}$, called the forward orbit of α with respect to ϕ. Moreover, we say that a point β is postcritical if there is a critical point γ of φ such that $\beta \in O^+(\gamma)$.

With this terminology, we have the following two theorems for polynomials.

Theorem 1.5. *Let K be a finite extension of $\mathbb{F}_p(t)$, let $f \in K[z]$ be a nonisotrivial polynomial with $\deg f > 1$, and let α and β be elements of K such that α is not preperiodic, β is not postcritical, and $\beta \notin O_f^+(\alpha)$. Then for any prime $\ell \neq p$, the Zsigmondy set $\mathcal{Z}(f, \alpha, \beta, \ell)$ is finite.*

Theorem 1.6. *Let K be a finite extension of $\mathbb{F}_p(t)$, let $f \in K[z]$ be a nonisotrivial polynomial with $\deg f > 1$, and let α and β be elements of K such that α is not preperiodic, β is not exceptional for f, and $\beta \notin O_f^+(\alpha)$. Then the Zsigmondy set $\mathcal{Z}(f, \alpha, \beta)$ is finite.*

Theorem 1.4 is not true in general for isotrivial rational functions, and Theorems 1.5 and 1.6 are not true not in general for isotrivial polynomials; see [30]. There are some results in the isotrivial case, however (see [21]), and some of the techniques here do work for a wide class of isotrivial rational functions. We may address these questions in a future paper.

Theorem 1.4 is proved by using two different notions of isotriviality. The first is our Definition 1.3 for functions. We now define an isotrivial set. Here we use a simple, if inelegant, definition rather than a slightly more technical one that generalizes to varieties other than $\mathbb{P}^1$. Below we regard an element of $\overline{K}(z)$ as a map from $\overline{K} \cup \infty$ to itself.

Definition 1.7. Let K be a finite extension of $\mathbb{F}_p(t)$ and let $\mathcal{S}$ be a finite subset of $\overline{K} \cup \infty$. We say that $\mathcal{S}$ is a isotrivial set if there exists $\sigma \in \overline{K}(z)$ of degree 1 such that $\sigma(\mathcal{S}) \subseteq \overline{\mathbb{F}}_p \cup \infty$.

We note that if φ is a nonisotrivial rational function the set $\varphi^{-1}(\beta)$ may still be an isotrivial set; for example any set of three or fewer elements is an isotrivial set, but there are nonisotrivial rational functions of degree 2 and 3.

Theorem 1.5 is proved using a third notion of isotriviality, this time for curves.

Definition 1.8. Let K be a finite extension of $\mathbb{F}_p(t)$ and let C be a curve defined over K. We say that C is an isotrivial curve if there is a curve C' defined over a finite extension k' of $K \cap \overline{\mathbb{F}}_p$ and a finite extension K' of K such that

$$C \times_K K' \cong C' \times_{k'} K'.$$

An outline of the paper is as follows. Throughout this paper, K is a finite extension of $\mathbb{F}_p(t)$ as in Definitions 1.3 ,1.7, and 1.8. In Section 2, we introduce some basic facts about heights, integral points, and cross ratios that are used throughout the paper. Following that, we prove Theorem 3.1, which says that if φ is a nonisotrivial rational function of degree greater than 1 and β is not exceptional for φ, then $\varphi^{-n}(\beta)$ is a nonisotrivial set for all sufficiently large n. The proof uses work of Baker [1] and Favre and Rivera-Letelier [14] to produce elements in $\varphi^{-n}(\beta)$ whose v-adic cross ratio is not 1 at a place v of bad reduction. We then apply work of [45] (see also [44]) to give a quick proof of Theorem 1.4 in Section 4. In Section 5, we begin by proving Corollary 5.3, which states that if the roots of a polynomial F are distinct and form a nonisotrivial set, then the curve C given by $y^\ell = F(x)$ is a nonisotrivial curve when $\ell \neq p$ is a prime that is small relative to the degree of F. The techniques we use to do this build upon work in [19]; the idea is to use the adjunction formula to show that the projection map onto the x-coordinate is the unique map $\theta : C \to \mathbb{P}^1$ of degree ℓ up to change of coordinates on $\mathbb{P}^1$ (see Lemma 5.1). We then use Corollary 5.3 and Theorem 3.1 to show the nonisotriviality of curves associated to $\varphi^{-n}(\beta)$, where φ is a nonisotrivial rational function of degree greater than 1 and β is not exceptional for φ, in Theorem 5.5. In Section 6, we prove Proposition 6.1, which immediately implies Theorems 1.5 and 1.6; the proof uses Theorem 3.1 along with height bounds on nonisotrivial curves in characteristic p due to Szpiro [41] and Kim [25] (see Theorem 6.3). Finally, in Section 7, we present some applications of our results to other dynamical questions.

We note that the proof of Theorem 3.1 works the same for function fields in characteristic 0 as for function fields in characteristic p. Theorems 1.4, 1.5, and 1.6 all hold in stronger forms for function fields in characteristic 0, as proved in [16]; the main difference here is that Yamanoi [46] has proved the full Vojta conjecture for algebraic points on curves over function fields of characteristic 0 (see [43; 42]), whereas Theorem 6.3 is weaker than the full Vojta conjecture for algebraic points on curves over function fields of characteristic p. Analogs of Theorems 1.5 and 1.6 have not yet been proved over number fields, except in some very special cases (see [3; 47; 33; 31; 32]), but both theorems are implied by the *abc* conjecture (see [16]).

2. Preliminaries

In this section we will review some terminology and results on heights, integral points, and dynamics. For background on heights; see [20; 26; 6]. We set some notation below.

Throughout this paper, K will denote a finite extension of $\mathbb{F}_p(t)$ and k will denote the intersection $K \cap \overline{\mathbb{F}}_p$. Equivalently, K is the function field of a smooth, projective curve B defined over k.

2A. ***Places, heights, and reduction.*** Let M_K be the set of places of K, which corresponds to the set of closed points of B.

Since K is a function field, we choose a place $\mathfrak{p}_\infty$ of K, denote

$$\mathfrak{o}_K = \{z \in K \mid v_\mathfrak{p}(z) \geq 0 \text{ for all } \mathfrak{p} \neq \mathfrak{p}_\infty\},$$

and let $k_\mathfrak{p}$ be the residue field $\mathfrak{o}_K/\mathfrak{p}$. Also, define the local degree of $\mathfrak{p}$ to be

$$N_\mathfrak{p} = [k_\mathfrak{p} : k].$$

Likewise, for each $\mathfrak{p} \in M_K$ we let $|\cdot|_\mathfrak{p}$ be a normalized absolute value such that the product formula

$$\prod_{\mathfrak{p} \in M_K} |z|_\mathfrak{p} = 1$$

holds for all $z \in K^*$. Moreover, we define $K_\mathfrak{p}$ to be the completion of K with respect to $|\cdot|_\mathfrak{p}$ and define $\mathbb{C}_\mathfrak{p}$ to be the completion of the algebraic closure of $K_\mathfrak{p}$.

For $z \in K$, let $h(z)$ denote the logarithmic height of K. For $\varphi \in K(z)$ with $\deg \varphi = d \geq 2$, let $h_\varphi(z)$ denote the Call–Silverman canonical height of z relative to φ [13], defined by

$$h_\varphi(z) = \lim_{n \to \infty} \frac{h(\varphi^n(z))}{d^n}.$$

We will often write sums indexed by primes that satisfy some condition. These are taken to be primes of $\mathfrak{o}_K$. As an example of our indexing convention, observe that

$$\sum_{v_\mathfrak{p}(z) > 0} v_\mathfrak{p}(z) N_\mathfrak{p} \leq h(z).$$

We say that a rational function $\varphi \in K(z)$ has *good reduction* at a place $\mathfrak{p}$ of K if the map it induces on $\mathbb{P}^1$ is nonconstant and well-defined modulo $\mathfrak{p}$. More precisely, we write $\varphi(x) = f/g$, where all the coefficients of f and g are in $(\mathfrak{o}_K)_\mathfrak{p}$, and either f or g has at least one coefficient in $(\mathfrak{o}_K)_\mathfrak{p}^*$. We let $f_\mathfrak{p}$ and $g_\mathfrak{p}$ denote the reductions of f and g at $\mathfrak{p}$. We say that φ has good reduction at $\mathfrak{p}$ if $f_\mathfrak{p}$ and $g_\mathfrak{p}$ have no common root in the algebraic closure of the residue field of $\mathfrak{p}$ and $\deg(f_\mathfrak{p}/g_\mathfrak{p}) = \deg \varphi$. We say that φ has *bad reduction* at $\mathfrak{p}$ if it does not have good reduction at $\mathfrak{p}$. This notion is dependent on our choice of coordinates. We say that φ has *potentially good reduction* at $\mathfrak{p}$ if there is a finite extension K' of K, a prime $\mathfrak{q}$ of K' lying over $\mathfrak{p}$, and a degree one rational function $\sigma \in K'(z)$ such that $\sigma \circ \varphi \circ \sigma^{-1}$ has good reduction at $\mathfrak{q}$. We say that φ has *genuinely bad reduction* at $\mathfrak{p}$ if φ does not have potentially good reduction at $\mathfrak{p}$.

2B. ***Integral points.*** Let S be a nonempty finite subset of M_K. The ring of S-integers in K is defined to be

$$\mathfrak{o}_{K,S} := \{z \in K : |z|_\mathfrak{p} \leq 1 \text{ for all } \mathfrak{p} \notin S\}.$$

Given a place $\mathfrak{p}$ of K and two points $\alpha = [x_1 : y_1]$ and $\beta = [x_2, y_2]$ in $\mathbb{P}^1(\mathbb{C}_\mathfrak{p})$, define the $\mathfrak{p}$-*adic chordal metric* $\delta_\mathfrak{p}$ by

$$\delta_\mathfrak{p}(\alpha, \beta) = \frac{|x_1 y_2 - y_1 x_2|_\mathfrak{p}}{\max\{|x_1|_\mathfrak{p}, |y_1|_\mathfrak{p}\} \cdot \max\{|x_2|_\mathfrak{p}, |y_2|_\mathfrak{p}\}}.$$

Note that we always have $0 \le \delta_{\mathfrak{p}}(\alpha, \beta) \le 1$, and that $\delta_{\mathfrak{p}}(\alpha, \beta) = 0$ if and only if $\alpha = \beta$. Then the ring $\mathfrak{o}_{K,S}$ is equivalent to the set which is maximally distant from ∞ outside of S, i.e., the set of $z \in K$ such that

$$\delta_{\mathfrak{p}}(z, \infty) = \delta_{\mathfrak{p}}([z : 1], [1, 0]) = 1$$

for all $\mathfrak{p} \notin S$.

We can now extend our definition of S-integrality to any divisor D on $\mathbb{P}^1$ that is defined over K.

Definition 2.1. Fix a nonempty finite set of places $S \subset M_K$. Let D be an effective divisor on $\mathbb{P}^1$ that is defined over K. Then $\alpha \in \mathbb{P}^1(K)$ is S-integral relative to D provided that for all places $\mathfrak{p} \notin S$, all $\tau \in \mathrm{Gal}(\overline{K}/K)$, and all $\beta \in \operatorname{Supp} D$, we have

$$\delta_{\mathfrak{p}}(\alpha, \tau(\beta)) = 1.$$

For affine coordinates $[\alpha : 1] \in \mathbb{P}^1(K)$ and a divisor D defined over K that does not contain the point at infinity in its support, the statement that $[\alpha : 1]$ is S-integral relative to D is equivalent to

$$\begin{aligned} |\alpha - \tau(\beta)|_{\mathfrak{p}} \ge 1 \quad &\text{if } |\tau(\beta)|_{\mathfrak{p}} \le 1, \text{ and} \\ |\alpha|_{\mathfrak{p}} \le 1 \quad &\text{if } |\tau(\beta)|_{\mathfrak{p}} > 1 \end{aligned}$$

for all $\mathfrak{p} \notin S$, all $\tau \in \mathrm{Gal}(\overline{K}/K)$, and all $[1 : \beta] \in \operatorname{Supp} D$.

Let θ be a linear fractional change of coordinate on $\mathbb{P}^1(\overline{K})$. Then α is S-integral relative to β if and only if $\theta(\alpha)$ is S-integral relative to $\theta(\beta)$ provided we allow an enlargement of S depending only on θ. We prove a variant of this statement for any $\theta \in K[x]$ later in the paper. The following is a simple and standard consequence of our definition of S-integrality (see [39, Corollary 2.4], for example). Recall that for a point $\alpha \in \mathbb{P}^1(K)$, the divisor $\varphi^*(\alpha)$ is defined as $\sum_{\varphi(\beta)=\alpha} e_{\varphi}(\beta/\alpha)\beta$.

Lemma 2.2. *Let $\varphi \in K(x)$ and S be a set of primes containing all the primes of bad reduction for φ. Then, for any $\alpha, \gamma \in \mathbb{P}^1(K)$, we have that $\varphi(\gamma)$ is S-integral relative to α if and only if γ is S-integral relative to $\varphi^*(\alpha)$.*

2C. *The cross ratio.* Let $|\cdot|$ be a non-Archimedean absolute value on a field L. For any distinct $x_1, x_2, y_1, y_2 \in L$ we define

$$(x_1, x_2; y_1, y_2) = \frac{|x_1 - y_2||x_2 - y_1|}{|x_1 - y_1||x_2 - y_2|}.$$

We may extend this to points in $x_1, x_2, y_1, y_2 \in L \cup \infty$ by eliminating the terms involving ∞; for example,

$$(\infty, x_2; y_1, y_2) = \frac{|x_2 - y_1|}{|x_2 - y_2|}.$$

Importantly, for $\sigma \in \mathrm{PGL}_2(L)$, we have $(z_1, z_2; z_3, z_4) = (\sigma z_1, \sigma z_2; \sigma z_3, \sigma z_4)$. This is easily seen by noting that an element of $\mathrm{PGL}_2(L)$ is a composition of translations, scaling maps, and the map sending every element to its multiplicative inverse, and that $(z_1, z_2; z_3, z_4)$ is invariant under all these types of maps.

We will use the following two lemmas for points $x_1, x_2, y_1, y_2 \in L$. The first lemma is immediate.

Lemma 2.3. *Suppose that $|x_1| < |y_1| < |x_2| < |y_2|$. Then*

$$(x_1, x_2; y_1, y_2) = \frac{|y_2||x_2|}{|y_1||y_2|} > 1.$$

Lemma 2.4. *Suppose that there are points $a_1, a_2 \in L$ such that $|x_1 - a_1|, |y_1 - a_1| < |a_1 - a_2|$ and $|x_2 - a_2|, |y_2 - a_2| < |a_1 - a_2|$. Then*

$$(x_1, x_2; y_1, y_2) > 1.$$

Proof. After a translation, we may assume that $a_1 = 0$. Then $|x_1|, |y_1| < |a_2|$ and $|x_2|, |y_2| = |a_2|$. Thus, we have

$$(x_1, x_2; y_1, y_2) = \frac{|a_2||a_2|}{|x_1 - y_1||x_2 - y_2|} > 1. \qquad \square$$

Remark 2.5. The cross ratio of x_1, x_2, y_1, y_2 is often defined without taking absolute values, i.e., as

$$\frac{(x_1 - y_2)(x_2 - y_1)}{(x_1 - y_1)(x_2 - y_2)}.$$

The advantage of the definition we use is that it extends to points in Berkovich space; see [14]. While we do not use this extension, it can be used to give a quick proof of our Proposition 3.2. We give a slightly longer proof that we think may be more accessible for some readers.

3. Nonisotriviality of inverse images

In this section, we will prove the following theorem.

Theorem 3.1. *Let $\varphi \in K(z)$ have $\deg \varphi > 1$. Suppose that φ is not isotrivial and that β is not exceptional for φ. Then for all sufficiently large n the set $\varphi^{-n}(\beta)$ is not an isotrivial set.*

We will derive Theorem 3.1 from the following proposition.

Proposition 3.2. *Suppose $\varphi \in K(z)$ has genuinely bad reduction at the prime $\mathfrak{p}$. Let $|\cdot|$ be an extension of $|\cdot|_{\mathfrak{p}}$ to $\mathbb{C}_{\mathfrak{p}}$. Then for any nonexceptional $\alpha \in K$, and for all sufficiently large n, there are elements $z_1, z_2, z_3, z_4 \in \varphi^{-n}(\alpha)$ such that*

$$(z_1, z_2; z_3, z_4) > 1.$$

Proof. We work over the non-Archimedean complete field $\mathbb{C}_{\mathfrak{p}}$, and consider the dynamical system induced by φ on the Berkovich projective line $\mathbb{P}^{1,an}$. We will use some basic facts about the topology of the Berkovich projective line, including the classification of points as Type I, II, III, or IV; see [2] or [4] for a detailed description of the topology of the Berkovich projective line.

By [14, Théorème E] (see also [4, Theorem 8.15]), bad reduction implies that the equilibrium measure ρ_φ is nonatomic. Thus, there are four or more points all of the same type (I, II, III, or IV) in the support of ρ_φ.

Since ρ_φ is nonatomic and the inverse images of a nonexceptional point equidistribute with respect to ρ_φ we have the following fact.

Fact 3.3. For any γ in the support of ρ_φ, any open subset U containing γ, and any positive integer m, there is an N such that $U \cap \varphi^{-n}(\beta)$ contains m or more points for all $n \geq N$.

We also have the following basic facts about the topology of $\mathbb{P}^{1,an}$.

Fact 3.4. Let $\xi(a, r)$, where $a \in K$ and $r > 0$, be a point of Type II or Type III corresponding to the disc $\{x \in K \mid |x - a| \leq r\}$. Then for any $\epsilon > 0$, there is an open set $U \subset \mathbb{P}^{1,an}$ with $\xi(a, r) \in U$ such that every point x of Type I in U satisfies $r - \epsilon < |x - a| < r + \epsilon$.

Fact 3.5. Let a_1 and a_2 be any two points of the same type in $\mathbb{P}^{1,an}$, which are not concentric Type II or III points. Then there exist open sets U_1 and U_2 with $a_1 \in U_1$ and $a_2 \in U_2$ such that $U_1 \cap \mathbb{P}^1(\mathbb{C}_\mathfrak{p})$ and $U_2 \cap \mathbb{P}^1(\mathbb{C}_\mathfrak{p})$ are disjoint open discs.

Proof. Since a_1 and a_2 are not concentric, $a_1 \wedge a_2$, the unique point such that $[a_1, \infty] \cap [a_2, \infty] = [a_1 \wedge a_2, \infty]$, is not equal to a_1 or a_2; see [14]. Now let D_i be the open disc corresponding to any Type II point in the open interval $(a_i, a_1 \wedge a_2)$, for $i = 1, 2$. Then there are open sets U_i such that $U_i \cap \mathbb{P}^1(\mathbb{C}_\mathfrak{p}) = D_i$. □

Now suppose that the support of ρ_φ contains two nonconcentric points z_1, z_2 of the same type. Then, by Facts 3.3 and 3.5, for all sufficiently large n there must be open discs $D(a_1, r_1)$ and $D(a_2, r_2)$ with $|a_1 - a_2| > \max\{r_1, r_2\}$ and points $x_1, x_2, y_1, y_2 \in \varphi^{-n}(\beta)$ with $x_1, y_1 \in D(a_1, r_1)$ and $x_2, y_2 \in D(a_2, r_2)$. By Lemma 2.4, we have

$$(x_1, x_2; y_1, y_2) > 1,$$

proving the proposition.

Now suppose that ρ_φ contains four concentric points of Type II or Type III, corresponding to closed discs $\overline{D}(a, r_i)$, for $i = 1, 2, 3, 4$, for some fixed a. We suppose that $r_1 < r_2 < r_3 < r_4$, and after an affine change of coordinates, we may suppose that $a = 0$. By Facts 3.3 and 3.4, for any $\epsilon > 0$, there must be an n such that $\varphi^{-n}(\beta)$ contains points z_1, z_2, z_3, z_4 with $|z_i|$ within ϵ of r_i for each i. Choosing ϵ appropriately, we will then have $|z_1| < |z_2| < |z_3| < |z_4|$. Then $(z_1, z_3; z_2, z_4) > 1$ by Lemma 2.3. □

Proof of Theorem 3.1. By [1, Theorem 1.9], since φ is nonisotrivial, it must have genuine bad reduction over some prime $\mathfrak{p}$. Then we may apply Proposition 3.2 to obtain four points in $\varphi^{-n}(\beta)$ with cross ratio greater than one for any sufficiently large n. Since the cross ratio of four points in $\overline{\mathbb{F}}_p \cup \infty$ is always 1 and the cross ratio is invariant under change of coordinate, we see then that $\varphi^{-n}(\beta)$ is a nonisotrivial set for all sufficiently large n. □

4. Proof of Theorem 1.4

We will use the following theorem due to Wang [45, Theorem in $\mathbb{P}^1(K)$, page 337] and Voloch [44].

Theorem 4.1. *Let D be an effective divisor on $\mathbb{P}^1$ that is defined over K. If the points in* Supp D *form a nonisotrivial set, then the set of points in $\mathbb{P}^1(K)$ that are S-integral relative to D is finite.*

The corollary below follows easily.

Corollary 4.2. *Let $\varphi \in K(z)$, let $\beta \in K$. Suppose that there is some i such that $\varphi^{-i}(\beta)$ is not an isotrivial set. Then for any $\alpha \in K$, the forward orbit $O_{\varphi}^{+}(\alpha)$ contains only finitely many points that are S-integral relative to β.*

Proof. We may extend S to contain all the primes of bad reduction for φ. The set of iterates $\varphi^{n-i}(\alpha)$ that are S-integral relative to $(\varphi^i)^*(\beta)$ is finite by Theorem 4.1, so by Lemma 2.2, the set of points $\varphi^n(\alpha)$ that are S-integral relative to β must be finite. □

The proof of Theorem 1.4 is now easy.

Proof of Theorem 1.4. By Theorem 3.1, there is some i such that $\varphi^{-i}(\beta)$ is not an isotrivial set. Applying Corollary 4.2 then gives the desired conclusion. □

5. Nonisotriviality of certain curves

Let $\pi : C \to \mathbb{P}^1$ be a separable nonconstant morphism defined over K. We define the *ramification locus* of π to be the support of $\pi(R_\pi)$, where R_π is the ramification divisor of π. If the ramification locus of π is an isotrivial set, then it follows from descent theory (see [34], for example) that C must be isotrivial. On the other hand, given any finite subset $\mathcal{U}$ of $\mathbb{P}^1$, one can use interpolation to construct a nonconstant separable morphism $f : \mathbb{P}^1 \to \mathbb{P}^1$ such that the ramification locus of f contains $\mathcal{U}$; thus, there are isotrivial curves that admit nonconstant separable morphisms $\pi : C \to \mathbb{P}^1$ such that the ramification locus of π is a nonisotrivial set. We can show, however, that if the degree of $\pi : C \to \mathbb{P}^1$ is a prime $\ell \neq p$ that is small relative to the genus of C and the ramification locus of π is a nonisotrivial set, then C must indeed be a nonisotrivial curve. This enables us to prove Theorem 5.5, which gives rise to diophantine estimates used in the proofs of Theorems 1.5 and 1.6. The technique here is similar to that of [19]. We begin with a lemma about uniqueness of low prime degree maps on curves of high genus.

Lemma 5.1. *Let C be a curve of genus g over K and let ℓ be a prime such that $(\ell - 1)^2 < g$ and $\ell \neq p$. Suppose there is morphism $\theta_1 : C \to \mathbb{P}^1$ of degree ℓ. Then for any morphism $\theta_2 : C \to \mathbb{P}^1$ of degree ℓ, there is an automorphism $\lambda : \mathbb{P}^1 \to \mathbb{P}^1$ such that $\theta_2 = \lambda \circ \theta_1$.*

Proof. Suppose that $g > (\ell - 1)^2$ and that $\theta_2 : C \to \mathbb{P}^1$ is another map of degree ℓ on C. Then we have a map $(\theta_1, \theta_2) : C \to \mathbb{P}^1 \times \mathbb{P}^1$; let $\widetilde{C}$ be the image of this map. If (θ_1, θ_2) is injective, then $\widetilde{C}$ also has genus g; see [17, Theorem II.8.19]. On the other hand, $\widetilde{C}$ is a curve of bidegree (d_1, d_2) in $\mathbb{P}^1 \times \mathbb{P}^1$ for some $d_i \leq \ell$. Hence, the Adjunction Formula implies that $g \leq (d_1 - 1)(d_2 - 1) \leq (\ell - 1)^2$, a contradiction; see

[17, Example V.1.5.2]. Therefore, (θ_1, θ_2) is not an injection. However, we have a commutative diagram

$$\begin{tikzcd}
& C \arrow[ld, "\theta_1"'] \arrow[d, "(\theta_1,\theta_2)"] \arrow[rd, "\theta_2"] & \\
\mathbb{P}^1 & \widetilde{C} \arrow[l, "\pi_1"'] \arrow[r, "\pi_2"] & \mathbb{P}^1
\end{tikzcd}$$

where the π_i are the restrictions of the natural projections $\pi_i : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^1$ to $\widetilde{C}$. Therefore,

$$\deg(\pi_1) \cdot \deg((\theta_1, \theta_2)) = \deg(\theta_1) = \ell = \deg(\theta_2) = \deg(\pi_2) \cdot \deg((\theta_1, \theta_2)).$$

However, (θ_1, θ_2) is not injective, so that $\deg((\theta_1, \theta_2)) > 1$. Therefore, $\deg((\theta_1, \theta_2)) = \ell$, since ℓ is prime. Hence, $\deg(\pi_1) = 1 = \deg(\pi_2)$, and both π_i are isomorphisms [35, Corollary 2.4.1]. In particular, $\pi_2 \circ \pi_1^{-1} = \lambda$ is a linear fractional transformation, and $\theta_2 = \lambda \circ \theta_1$ as claimed. □

Theorem 5.2. *Let C be a curve of genus g over K and let ℓ be a prime such that $(\ell - 1)^2 < g$ and $\ell \neq p$. Suppose there is morphism $\theta : C \to \mathbb{P}^1$ of degree ℓ such that the ramification locus of θ is a nonisotrivial set. Then C is a nonisotrivial curve.*

Proof. Suppose that C is isotrivial; we will prove that this implies that the ramification locus of θ must be isotrivial. Then for some finite extensions K' of K and k' of k there is a model $\mathcal{C}$ for $C \times_K K'$ over the k'-curve X corresponding to the function field K' such that for any place $t \in X(\bar{k}')$, the curve $\mathcal{C}_t \times_{k(t)} L$ is isomorphic to $C \times_K L$, where $k(t)$ is the field of definition of t and $L = K' \cdot k(t)$. Let $\mathcal{P}$ be a model for $\mathbb{P}^1$ over X. Then, for all but finitely many places $t \in X(\bar{k}')$, the morphism θ specializes to a degree ℓ morphism $\theta_t : \mathcal{C}_t \to \mathbb{P}^1_{k(t)}$ defined over $k(t)$. Let $\theta_2 = \theta_t \times_{k(t)} L$. Since $\theta_2 : C \to \mathbb{P}^1$ has degree ℓ, and $(\ell - 1)^2 < g$, there is a $\lambda \in \mathrm{PGL}_2(\bar{K})$ such that $\theta_2 = \lambda \circ \theta$, by Lemma 5.1. But λ must take the ramification locus of θ to the ramification locus of θ_2, which is defined over k'. Hence, the ramification locus of θ must be isotrivial. □

Corollary 5.3. *Let F be a polynomial over K without repeated roots such that the roots of F form a nonisotrivial set. Let ℓ be a prime number such that $\ell \neq p$ and $\ell - 1 < \deg F/2 - 1$. Then the curve C given by $y^\ell = F(x)$ is not isotrivial.*

Proof. Let $\theta : C \to \mathbb{P}^1$ be the map coming from projection onto the x-coordinate. Then $\deg \theta = \ell$. Since the genus of C is at least $(\ell - 1) \deg F/2 - (\ell - 1)$ by Riemann–Hurwitz and the ramification locus of θ includes the roots of F (note: it will be larger than that if θ also ramifies over the point at infinity), applying Theorem 5.2 shows that C is not isotrivial. □

As mentioned above, there are obvious examples of maps $\pi : C \to \mathbb{P}^1$, where C is isotrivial but the ramification locus of π is not, but we have not found examples of isotrivial curves of the specific form $y^m = F(x)$, for F a polynomial with distinct roots that form a nonisotrivial set and m is an integer greater than 1 that is not a power of p.

Question 5.4. Does there exist an isotrivial curve of the form $y^m = F(x)$, where F is a polynomial with distinct roots that form a nonisotrivial set and m is an integer greater than 1 that is not a power of p?

Corollary 5.3 and the techniques of [18] can be used to show that when p is odd and m is even, the answer to Question 5.4 is "no"; we cannot however rule out examples where m is odd or $p = 2$.

We are now ready to prove a theorem guaranteeing the nonisotriviality of certain curves obtained by taking inverse images of points under iterates of a nonisotrivial rational function.

Theorem 5.5. *Let $\varphi \in K(x)$ be a nonisotrivial rational function. Let $\beta \in K$ be nonexceptional for φ. Then for any prime $\ell \neq p$, there is an n such that the curve given by*

$$y^\ell = \prod_{\substack{\gamma \in \overline{K} \\ \varphi^n(\gamma)=\beta}} (x - \gamma)$$

(*where the product $\prod_{\substack{\gamma \in \overline{K} \\ \varphi^n(\gamma)=\beta}} (x - \gamma)$ is taken without multiplicities*) *is not an isotrivial curve.*

Proof. If $\infty \notin \varphi^{-n}(\beta)$ for any n, then this is immediate from Corollary 5.3 and Theorem 3.1. Otherwise, since $\deg_s \varphi > 1$ (because purely inseparable rational functions are isotrivial) and β is not exceptional for φ, there is some m such that $\varphi^{-m}(\beta)$ contains at least three points. Thus, there is some point $\beta' \in \varphi^{-m}(\beta)$ such that $\infty \notin \varphi^{-n}(\beta')$ for any n. Then there is some m' such that $\varphi^{-m'}(\beta')$ is not isotrivial by Theorem 3.1, and since the set of points other than ∞ in $\varphi^{-(m+m')}(\beta)$ contains $\varphi^{-m'}(\beta')$, this set is nonisotrivial as well, so the curve given by

$$y^\ell = \prod_{\substack{\gamma \in \overline{K} \\ \varphi^{m+m'}(\gamma)=\beta}} (x - \gamma)$$

is not an isotrivial curve for all m large enough so that $\varphi^{-(m+m')}(\beta)$ contains more than $2\ell + 1$ points, by Corollary 5.3. □

Hindes conjectured [18, Conjecture 3.1] that when φ is a nonisotrivial polynomial of degree prime to p and β is not postcritical for φ, then for some n and some ℓ prime to p, the curve

$$y^\ell = \prod_{\substack{\gamma \in \overline{K} \\ \varphi^n(\gamma)=\beta}} (x - \gamma)$$

is not isotrivial. Theorem 5.5 answers this with many of the hypotheses removed. Note that by taking the product without multiplicities, we essentially remove the issue of β being postcritical. We note that Ferraguti and Pagano have proved Theorem 5.5 in the special case where φ is a quadratic polynomial, $\ell = 2$, and $p \neq 2$; see [15, Theorem 2.4].

6. Proof of Theorems 1.5 and 1.6

Theorems 1.5 and 1.6 will both follow from the following more general statement.

Proposition 6.1. *Let $f \in K[x]$ be nonisotrivial with $\deg f > 1$ and let $\ell \neq p$ be a prime number. Let $\alpha, \beta \in K$ where $\beta \notin O_\varphi^+(\alpha)$ and α is not preperiodic. Suppose that for some r, there is a $\gamma \in f^{-r}(\beta)$ such that γ is neither postcritical nor periodic and such that $e_{f^r}(\gamma/\beta)$ is prime to ℓ. Then $\mathcal{Z}(f, \alpha, \beta, \ell)$ is finite.*

We will prove Proposition 6.1 by combining effective forms of the Mordell Conjecture over function fields (see 6.3) with Theorem 5.5 and the following lemma from [10, Lemma 5.2]; see also [16, Proposition 5.1]. Note that while this lemma is stated in characteristic 0 in [10], the proof is the same word-for-word for finite extensions of $\mathbb{F}_p(t)$.

Lemma 6.2. *Let $f \in K[x]$ with $d = \deg(f) \geq 2$. Let $\alpha \in K$ with $h_f(\alpha) > 0$. Let $\gamma_1, \gamma_2 \in K$ such that $\gamma_2 \notin \mathcal{O}_f(\gamma_1)$ and $\gamma_1 \notin O_f(\alpha)$. For $n > 0$, let $\mathcal{X}(n)$ denote the set of primes $\mathfrak{p}$ of $\mathfrak{o}_K$ such that*

$$\min(v_{\mathfrak{p}}(f^m(\alpha) - \gamma_1), v_{\mathfrak{p}}(f^n(\alpha) - \gamma_2)) > 0$$

for some $0 < m < n$. Then for any $\epsilon > 0$, we have

$$\sum_{\mathfrak{p} \in \mathcal{X}(n)} N_{\mathfrak{p}} \leq \epsilon d^n h_f(\alpha) + O_\epsilon(1).$$

for all n.

The next result we use follows from (any of the) effective forms of the Mordell Conjecture over function fields [25; 27; 41]. To make this precise, we need some terminology. Let C be a curve over K and let $P \in C$ be a point on C defined over some finite extension $K(P)/K$. Then we let $h_{\mathcal{K}_C}(P)$ denote the logarithmic height of P with respect to the canonical divisor $\mathcal{K}_C$ of C and let

$$d_K(P) = \frac{2g(K(P)) - 2}{[K(P) : K]}$$

denote the logarithmic discriminant of P; here $g(K(P))$ is the genus of $K(P)$. Then we have the following height bounds for rational points on nonisotrivial curves due to Szpiro [41] and Kim [25].

Theorem 6.3. *Let C be a nonisotrivial curve of genus at least two over a finite extension K of $\mathbb{F}_p(t)$. Then there are constants $B_1 > 0$ and B_2 (depending only on C) such that*

$$h_{\mathcal{K}_C}(P) \leq B_1 d_K(P) + B_2 \tag{6.3.1}$$

holds for all $P \in C$.

Remark 6.4. The first of these bounds (with explicit B_1 and B_2 in the semistable case) are due to Szpiro [41, Section 3], and the best possible bounds (i.e., with smallest possible B_1) are due to Kim [25]. Strictly speaking, the bound in [41, Section 3] is stated for semistable curves. However, one may always pass to a finite extension L/K over which C is semistable [41, Section 1] and thus obtain bounds of the form in (6.3.1). Likewise, the bound in [25] is stated for curves with nonzero Kodaira–Spencer class. However, the general nonisotrivial case follows from this one as follows. Assuming that C/K is nonisotrivial and $\text{char}(K) = p$, there is an inseparability degree $r = p^e$ and a separable extension L/K such that C is defined over L^r and that the Kodaira–Spencer class of C over L^r is nonzero; see [41, pages 51–53]. Now apply Kim's theorem to C/L^r. In either case, Castelnuovo's inequality [40, Theorem 3.11.3] applied to the composite extensions $L(P) = LK(P)$ or $L^r(P) = L^rK(P)$ may be used to appropriately alter B_1 and B_2 to go from bounds with d_L or d_{L^r} back to those with d_K.

Before we apply the height bounds for points on curves from Theorem 6.3 to dynamics, we need the following elementary observation about valuations and powers.

Lemma 6.5. *Let $K/\mathbb{F}_p(t)$ be finite extension and let $\ell \neq p$ be a prime. Then there is a finite extension L of K such that if u is any element of K with the property that $\ell \mid v_{\mathfrak{p}}(u)$ for all primes $\mathfrak{p}$ of K, then u is an ℓ-th power in L.*

Proof. Suppose that $u \in K$ is such that $\ell \mid v_{\mathfrak{p}}(u)$ for all primes $\mathfrak{p}$ of K. Then the divisor $(u) = \ell D_u$ for some divisor $D_u \in \operatorname{Div}^0(K)$ of degree 0. Hence, the linear equivalence class of D_u is an ℓ-torsion class in $\operatorname{Cl}^0(K)$, the group of divisor classes of degree 0. In particular, there are only finitely many possible linear equivalence classes for D_u by [40, Proposition 5.1.3]. Thus, there is a finite set $\mathcal{S}$ of $u \in K$, each satisfying $(u) = \ell D_u$ for some $D_u \in \operatorname{Div}^0(K)$, such that for any $u' \in K$ with $(u') = \ell D_{u'}$ for a divisor $D_u \in \operatorname{Div}^0(K)$, the divisor $D_{u'}$ is linearly equivalent to D_u for some $u \in \mathcal{S}$. Let L' be the finite extension of K generated by the ℓ-th roots of the elements of $\mathcal{S}$. Now if u and u' are two such elements of K as above such that D_u and $D_{u'}$ are linearly equivalent, then $D_u - D_{u'} = (w_{u,u'})$ for some $w_{u,u'} \in K$. Hence, $u/u' = c_{u,u'}w_{u,u'}^{\ell}$ for some $c_{u,u'}$ in the field of constants of K. In particular, there are only finitely many possible such $c_{u,u'}$ since the field of constants of K is finite. Adjoining the ℓ-th roots of these $c_{u,u'}$ to L' gives a finite extension L of K. □

Lemma 6.6. *Let $\mathcal{S}$ be a finite set of primes of K, let $F \in \mathfrak{o}_{K,\mathcal{S}}[z]$ be a polynomial without repeated roots and let $\ell \neq p$ be a prime such that $C : y^\ell = F(x)$ is a nonisotrivial curve of genus $g(C) > 1$. Then there are constants $r_1 > 0$ and r_2 (depending on F, ℓ, K, and $\mathcal{S}$) such that*

$$\sum_{\substack{v_{\mathfrak{p}}(F(a))>0 \\ \ell \nmid v_{\mathfrak{p}}(F(a))}} N_{\mathfrak{p}} \geq r_1 h(a) + r_2 \tag{6.6.1}$$

holds for all $a \in \mathfrak{o}_{K,\mathcal{S}}$.

Proof. Suppose that $C : y^\ell = F(x)$ is a nonisotrivial curve of genus $g(C) > 1$. Then given $a \in \mathfrak{o}_{K,\mathcal{S}}$, we let $u_a := F(a)$ and choose a corresponding point $P_a = (a, \sqrt[\ell]{u_a})$ on C. From here, we proceed in cases.

Suppose first that $\ell \mid v_{\mathfrak{p}}(u_a)$ for all primes $\mathfrak{p}$ of K. Then by Lemma 6.5 there exists a finite extension L/K (independent of a) such that u_a is an ℓ-th power in L. In particular, since we may assume that L contains a primitive ℓ-th root of unity, $K(P_a) \subseteq L$. Therefore, (6.3.1) implies that $h_{\mathcal{K}_C}(P_a)$ is absolutely bounded. However, the canonical divisor class is ample in genus at least 2, so that the set of possible points P_a is finite in this case. Therefore, $h(a)$ is bounded and (6.6.1) holds trivially (take $r_1 = 1$ and choose r_2 to be sufficiently negative).

Now suppose that there exists a prime $\mathfrak{p}$ of K such that $\ell \nmid v_{\mathfrak{p}}(u_a)$. Then we may apply the genus formula in [40, Corollary 3.7.4] to deduce that

$$\begin{aligned} d_K(P_a) &= 2g(K) - 2 + \tfrac{1}{\ell}\sum_{\mathfrak{p}}(\ell - \gcd(\ell, v_{\mathfrak{p}}(u_a)))N_{\mathfrak{p}} \\ &= 2g(K) - 2 + \left(\frac{\ell-1}{\ell}\right) \sum_{\substack{v_{\mathfrak{p}}(u_a)>0 \\ \ell \nmid v_{\mathfrak{p}}(u_a)}} N_{\mathfrak{p}} + \left(\frac{\ell-1}{\ell}\right) \sum_{\substack{v_{\mathfrak{p}}(u_a)<0 \\ \ell \nmid v_{\mathfrak{p}}(u_a)}} N_{\mathfrak{p}} \\ &\le 2g(K) - 2 + \left(\frac{\ell-1}{\ell}\right) \sum_{\substack{v_{\mathfrak{p}}(u_a)>0 \\ \ell \nmid v_{\mathfrak{p}}(u_a)}} N_{\mathfrak{p}} + \left(\frac{\ell-1}{\ell}\right) \sum_{\mathfrak{p} \in \mathcal{S}} N_{\mathfrak{p}}, \end{aligned} \tag{6.6.2}$$

since the only way that $u_a := F(a)$ can have negative valuation at $\mathfrak{p}$ is if $\mathfrak{p} \in \mathcal{S}$. However, this is a finite set of primes. Therefore, (6.6.2) implies that

$$d_K(P_a) \le \left(\frac{\ell-1}{\ell}\right) \sum_{\substack{v_{\mathfrak{p}}(F(a))>0 \\ \ell \nmid v_{\mathfrak{p}}(F(a))}} N_{\mathfrak{p}} + O_{K,\mathcal{S}}(1). \tag{6.6.3}$$

On the other hand, if $\pi : C \to \mathbb{P}^1$ is the map given by projection onto the x-coordinate, then π pulls back a degree one divisor on $\mathbb{P}^1$ (yielding the Weil height on $\mathbb{P}^1$) to a degree ℓ divisor on C. Hence, the algebraic equivalence of divisors and [37, Theorem III.10.2] (see also [26, Section 4.3]) together imply that

$$\lim_{h_{\mathcal{K}_C}(P)\to\infty} \frac{h(\pi(P))}{h_{\mathcal{K}_C}(P)} = \frac{\ell}{2g(C)-2}.$$

In particular, we may deduce that

$$h(a) \le \frac{(1+\epsilon)\ell}{(2g(C)-2)} h_{\mathcal{K}_C}(P_a) + O_{K,F,\ell,\epsilon}(1) \tag{6.6.4}$$

for all $\epsilon > 0$ and all $a \in K$ (not just $a \in \mathfrak{o}_{K,S}$). Finally, by choosing $\epsilon = 1$ and combining (6.3.1), (6.6.3), and (6.6.4), we see that there are constants $r_1 > 0$ and r_2 (depending on F, ℓ, K, and $\mathcal{S}$) such that

$$\sum_{\substack{v_{\mathfrak{p}}(F(a))>0 \\ \ell \nmid v_{\mathfrak{p}}(F(a))}} N_{\mathfrak{p}} \ge r_1 h(a) + r_2$$

holds for all $a \in \mathfrak{o}_{K,S}$. In particular, after replacing r_1 and r_2 with the minimum of the corresponding constants from the first and second cases above, we prove Lemma 6.6. □

Lemma 6.7. *Let $f \in K[z]$ be a nonisotrivial polynomial with* $\deg f = d > 1$ *and let $\alpha, \gamma \in K$ where γ is not postcritical. Then for any prime $\ell \neq p$, there is a $\delta > 0$ such that for all sufficiently large n, we have*

$$\sum_{\substack{v_{\mathfrak{p}}(f^n(\alpha)-\gamma)>0 \\ \ell \nmid v_{\mathfrak{p}}(f^n(\alpha)-\gamma)}} N_{\mathfrak{p}} \ge \delta d^n h_f(\alpha). \tag{6.7.1}$$

Proof. Let $\mathcal{S}$ be finite set of primes such that α, γ, and all the coefficients of f are in $\mathfrak{o}_{K,\mathcal{S}}$. Then $f^n(\alpha) \in \mathfrak{o}_{K,\mathcal{S}}$ for all m. By Theorem 5.5, there is an m such that the curve given by

$$y^\ell = \prod_{\substack{\beta \in \overline{K} \\ f^m(\beta)=\gamma}} (x-\beta)$$

is not an isotrivial curve. There is an $\omega \in K$ (the leading term of $f^m(z)-\gamma$) and an e (coming from the degree of inseparability of f^ℓ) such that

$$f^m(z)-\gamma = \omega \prod_{\substack{\beta \in \overline{K} \\ f^m(\beta)=\gamma}} (z-\beta)^{p^e}.$$

Let

$$F(z) = \prod_{\substack{\beta \in \overline{K} \\ f^m(\beta)=\gamma}} (z-\beta).$$

Applying Lemma 6.6 with $a = f^{n-m}(\alpha)$ we see that since $\ell \neq p$, we have constants r_1, r_2 such that

$$\sum_{\substack{v_\mathfrak{p}(f^n(\alpha)-\gamma)>0 \\ \ell \nmid v_\mathfrak{p}(f^n(\alpha)-\gamma)}} N_\mathfrak{p} \geq \Bigg(\sum_{\substack{v_\mathfrak{p}(F(a))>0 \\ \ell \nmid v_\mathfrak{p}(F(a))}} N_\mathfrak{p} \Bigg) - h(\omega) \geq r_1 h(f^{n-m}(\alpha)) + r_2 - h(\omega).$$

Since $|h_f - h| \leq O(1)$ and $h_f(f^{n-m}(\alpha)) = d^{n-m} h_f(\alpha)$, we see that there is a constant r_3 such that

$$\sum_{\substack{v_\mathfrak{p}(f^n(\alpha)-\gamma)>0 \\ \ell \nmid v_\mathfrak{p}(f^n(\alpha)-\gamma)}} N_\mathfrak{p} \geq r_1 d^{n-m} h_f(\alpha) + r_3$$

for all n. Choosing a δ such that $0 < \delta < r_1/d^m$ then gives

$$\sum_{\substack{v_\mathfrak{p}(f^n(\alpha)-\gamma)>0 \\ \ell \nmid v_\mathfrak{p}(f^n(\alpha)-\gamma)}} N_\mathfrak{p} \geq \delta d^n h_f(\alpha)$$

for all sufficiently large n, as desired. □

We are now ready to prove Proposition 6.1.

Proof of Proposition 6.1. We first note it suffices to prove this after passing to a finite extension of K since $\ell \neq p$. To see this, let L be a finite extension of K, let L^s denote the separable closure of K in L, and let $\mathfrak{q}$ be a prime in L lying over a prime $\mathfrak{p}$ of K. Then $v_\mathfrak{q}(f^n(\alpha)-\beta) = [L : L^s] v_\mathfrak{p}(f^n(\alpha)-\beta)$ unless $\mathfrak{p}$ is in the finite set of primes of K that ramify in L^s. We also note that $h_f(\alpha) > 0$ since α is not preperiodic and f is not isotrivial, by [1, Corollary 1.8].

We change coordinates so that $\beta = 0$. Let r be the smallest positive integer such that $f^r(\gamma) = 0$. After passing to a finite extension we may assume that all the roots of $f^r(z)$ are in K. Let $e = e_{f^r}(\gamma/\beta)$ and write

$$f^r(z) = (z-\gamma)^e g(z).$$

Then for all but finitely many primes $\mathfrak{p}$ of K we have

$$v_{\mathfrak{p}}(f^{n+r}(\alpha)) = e v_{\mathfrak{p}}(f^n(\alpha) - \gamma) \tag{6.7.2}$$

for all n.

Since γ is not postcritical, by Lemma 6.7, there exists $\delta > 0$ such that for all sufficiently large n, we have

$$\sum_{\substack{v_{\mathfrak{p}}(f^n(\alpha)-\gamma)>0 \\ \ell \nmid v_{\mathfrak{p}}(f^n(\alpha)-\gamma)}} N_{\mathfrak{p}} \geq \delta d^n h_f(\alpha). \tag{6.7.3}$$

Let $\mathcal{W}$ be the roots of $f^r(z)$ that are not roots of $f^{r'}(z)$ for any $r' < r$. Let $\mathcal{S}_1$ be the set of primes of bad reduction for f and let $\mathcal{S}_2$ be the set of primes such that $v_{\mathfrak{p}}(f^{r'}(w)) > 0$ for some $r' < r$ and some $w \in \mathcal{W} \cup \{\alpha\}$. Now, for each n, let $\mathcal{Y}(n)$ be the set of primes $\mathfrak{p}$ such that $v_{\mathfrak{p}}(f^n(\alpha) - \gamma) > 0$ and $v_{\mathfrak{p}}(f^{n'}(\alpha)) > 0$ for some $n' < n + r$. If $\mathfrak{p} \notin \mathcal{S}_1 \cup \mathcal{S}_2$ for $\mathfrak{p} \in \mathcal{Y}(n)$, then $v_{\mathfrak{p}}(f^m(\alpha)) - \gamma') > 0$ for some $\gamma' \in \mathcal{W}$ and some $m < n$; this follows from the fact that if $s \geq r$ is the smallest integer such that $v_{\mathfrak{p}}(f^s(\alpha)) > 0$, then $v_{\mathfrak{p}}(f^{s-r}(\alpha) - \gamma') > 0$ for some $\gamma' \in \mathcal{W}$. Thus, since γ is not in the forward orbit of α (since $\beta \notin O_{\varphi}^{+}(\alpha)$ by assumption) or of any element of $\mathcal{W}$ (since it is not periodic) and the sets $\mathcal{W}$, $\mathcal{S}_1$, and $\mathcal{S}_2$ are all finite, we may apply Lemma 6.2 to each element of $\mathcal{W}$. We obtain

$$\sum_{\mathfrak{p} \in \mathcal{Y}(n)} N_{\mathfrak{p}} \leq \frac{\delta}{2} d^n h_f(\alpha) \tag{6.7.4}$$

for all sufficiently large n. Combining (6.7.4) with (6.7.2) and (6.7.3), we see that for all sufficiently large n, there is a prime $\mathfrak{p}$ such that

- $v_{\mathfrak{p}}(f^n(\alpha) - \gamma) > 0$;
- $\ell \nmid v_{\mathfrak{p}}(f^n(\alpha) - \gamma)$;
- $v_{\mathfrak{p}}(f^{n'}(\alpha)) = 0$ for all $0 < n' < n$; and
- $v_{\mathfrak{p}}(f^{n+r}(\alpha)) = e v_{\mathfrak{p}}(f^n(\alpha) - \gamma)$.

Since e is prime to ℓ, it follows that the Zsigmondy set $\mathcal{Z}(f, \alpha, \beta, \ell)$ is finite. □

7. Applications

The original Zsigmondy theorem [3; 47] had to do with orders of algebraic numbers modulo primes. We can treat a related dynamical problem; here we will not assume nonisotriviality. We begin with some notation and terminology. If $\alpha \in K$ is an integer at a prime $\mathfrak{p}$, we let $\alpha_{\mathfrak{p}} \in k_{\mathfrak{p}}$ be its reduction at $\mathfrak{p}$. If $f \in K[x]$, and all of the coefficients of f are integers at $\mathfrak{p}$, we let $f_{\mathfrak{p}} \in k_{\mathfrak{p}}[x]$ be the reduction of f at $\mathfrak{p}$ obtained by reducing each coefficient of f at $\mathfrak{p}$. If $g : \mathcal{U} \to \mathcal{U}$ is any map from a set to itself and $u \in \mathcal{U}$ is periodic under g, then the *prime period* of u for g is the smallest positive integer m such that $g^m(u) = u$. We say that a polynomial $f \in K[x]$ is additive if $f(\alpha + \beta) = f(\alpha) + f(\beta)$ for all $\alpha, \beta \in \overline{K}$.

Theorem 7.1. *Let f be a polynomial of degree greater than 1 and let $\alpha \in K$ be a point that is not preperiodic for f. If f is not both isotrivial and additive, then for all but finitely many positive integers n, there is a prime $\mathfrak{p}$ such that the prime period of $\alpha_{\mathfrak{p}}$ for $f_{\mathfrak{p}}$ is equal to n. If f is isotrivial and additive, then for all but finitely many positive integers n that are not a power of p, there is a $\mathfrak{p}$ such that the prime period of $\alpha_{\mathfrak{p}}$ for $f_{\mathfrak{p}}$ is equal to n.*

Proof. If f is not isotrivial, this follows immediately from Theorem 1.6 by letting $\alpha = \beta$. If f is isotrivial, then after a change of coordinates, we may assume that $f \in k[x]$ and $\alpha \in K \setminus k$ for some finite extension k of $\mathbb{F}_p$. If f is not additive then for all but finitely many positive integers n, there exists $\beta_n \in \bar{k}$ having prime period n for f, by [30, Theorem]. For each such β_n, there exists $\mathfrak{p}_n$ such that $\alpha_{\mathfrak{p}_n} = \beta_n$, so we see that for all but all but finitely many positive integers n, there exists $\mathfrak{p}$ such that the prime period of $\alpha_{\mathfrak{p}}$ for $f_{\mathfrak{p}}$ is equal to n. If f is additive, then for all but finitely many positive integers n that are not a power of p, there exists $\beta_n \in \bar{k}$ having prime period n for f, by [30, Theorem]. Then, as in the nonadditive case, we may choose $\mathfrak{p}_n$ such that $\alpha_{\mathfrak{p}_n} = \beta_n$. □

Theorem 1.4 allows one to prove characteristic p analogs of various results that rely on the results of [36]. For example, the proofs of Theorems 4 and 5 of [5] extend easily to the case of nonisotrivial rational functions over a function field in characteristic p, using Theorem 1.4. Similarly, one can use Theorem 1.4 to prove Theorem 4 of [11] with the additional hypothesis that at least one of the wandering critical points of φ has a ramification degree that is not a power of p.

We will now prove a few results about unicritical polynomials that rely on Theorem 1.5, which is not available over number fields.

The following lemma is very similar to [9, Proposition 3.1]; we include the proof for a sake of completeness.

Lemma 7.2. *Let $f(x) = x^d + c$ where d is an integer greater than 1 that is not divisible by p, let $\beta \in K$, and let n be a positive integer. Let $\mathfrak{p}$ be any prime of K such that*

(i) $|c|_{\mathfrak{p}} \le 1$;

(ii) $|\beta|_{\mathfrak{p}} \le 1$; *and*

(iii) $|f^m(0) - \beta|_{\mathfrak{p}} = 1$ *for all* $0 \le m \le n$.

Then $\mathfrak{p}$ does not ramify in $K(f^{-n}(\beta))$.

Proof. We proceed by induction. The case where $n = 1$ follows immediately from taking the discriminant of $x^d + (c - \beta)$. Now, let $\mathfrak{p}$ be a prime satisfying (i)–(iii) for some $n \ge 2$. Then it also satisfies them for $n - 1$, so by the inductive hypothesis, the prime $\mathfrak{p}$ does not ramify in $K(f^{-(n-1)}(\beta))$. Now, $K(f^{-n}(\beta))$ is obtained from $K(f^{-(n-1)}(\beta))$ by adjoining elements of the form $\sqrt[d]{\gamma_i - c}$ for $f^{n-1}(\gamma_i) = \beta$. For any prime $\mathfrak{q}$ in $K(f^{-(n-1)}(\beta))$ lying over $\mathfrak{p}$, we see that $|\gamma_i|_{\mathfrak{q}} \le 1$ by (i) and (ii). We also have $|\gamma_i|_{\mathfrak{q}} \ge 1$ since otherwise γ would be in the same residue class as 0, which contradicts (iii). Thus, each $\mathfrak{q}$ in $K(f^{-(n-1)}(\beta))$ lying over $\mathfrak{p}$ does not ramify in any $K(f^{-(n-1)}(\beta))(\sqrt[d]{\gamma_i - c}) = K(f^{-n}(\beta))$. Since each such $\mathfrak{q}$ does not ramify over $\mathfrak{p}$ by the inductive hypothesis, it follows that $\mathfrak{p}$ does not ramify in $K(f^{-n}(\beta))$, as desired. □

The next lemma follows a proof that is similar to that of [9, Proposition 3.2] and [11, Theorem 5].

Lemma 7.3. *Let $f(x) = x^d + c$ where $c \in K \setminus k$ where d is an integer greater than 1 that is not divisible by p. Let $\beta \in K$, let $\ell \neq p$ be a prime number, and let e be a positive integer such that ℓ^e divides d. Suppose that $\mathfrak{p}$ is a primitive ℓ-divisor of $f^n(0) - \beta$ such that $|c|_{\mathfrak{p}} = |\beta|_{\mathfrak{p}} = 1$. Then for any prime $\mathfrak{p}'$ in $K(f^{-(n-1)}(\beta))$ that lies over $\mathfrak{p}$, there is a prime $\mathfrak{q}$ in $K(f^{-n}(\beta))$ such that ℓ^e divides $e(\mathfrak{q}/\mathfrak{p}')$.*

Proof. Let $\mathfrak{p}'$ be a prime in $K(f^{-(n-1)}(\beta))$ lying over $\mathfrak{p}$. By Lemma 7.2, the prime $\mathfrak{p}$ does not ramify in $K(f^{-(n-1)}(\beta))$, so $v_{\mathfrak{p}'}(z) = v_{\mathfrak{p}}(z)$ for all $z \in K$. Since $f^n(0) - \beta = \prod_{f^{n-1}(\gamma)=\beta}(f(0) - \gamma)$, we see that there is some $\gamma \in f^{-(n-1)}(\beta)$ such that $\ell \nmid v_{\mathfrak{p}'}(c - \gamma)$. Thus, if $\mathfrak{q}$ is a prime of $K(f^{-(n-1)}(\beta))(\sqrt[d]{c - \gamma})$ lying over $\mathfrak{p}'$, we see that $\ell^e \mid e(\mathfrak{q}/\mathfrak{p}')$. □

Using the Lemmas above, we can prove a result for separable nonisotrivial polynomials of the form $x^d + c$ that is a special case of a characteristic p analog of [9, Theorem 1.1]. Note that if $f(x) = x^d + c$ and d is not divisible by p, then f is isotrivial if and only if $c \in \overline{\mathbb{F}}_p$. To see this, note that $h_f(0) = \frac{h(c)}{d} > 0$ when $c \notin \overline{\mathbb{F}}_p$, as can be seen by simply considering the orbit of f at the places v where $|c|_v > 1$. Therefore, if $c \notin \overline{\mathbb{F}}_p$, then f has a critical point that is not preperiodic, and hence f cannot be isotrivial. We note also that a polynomial of the form $x^d + c$ is separable if and only if $p \nmid d$.

Theorem 7.4. *Let $f(x) = x^d + c$ be a separable nonisotrivial polynomial of degree $d > 1$. Let $\beta \in K$. Then for all sufficiently large n, there is a prime $\mathfrak{p}$ of K such that $\mathfrak{p}$ ramifies in $K(f^{-n}(\beta))$ but not in $K(f^{-(n-1)}(\beta))$.*

Proof. Since 0 is not periodic and every point in K other than $\beta = c$ has $d > 1$ distinct preimages under f, we see that for any $\beta \neq c$, there is a $\gamma \in f^{-1}(\beta)$ meeting the conditions of Proposition 6.1. Furthermore, we note that if $\beta = c$, then $f^{-n}(\beta) = f^{-(n-1)}(0)$ for all $n > 0$, so it suffices to prove the result for $\beta = 0$; thus, we need only treat the case where $\beta \neq c$.

Let $\ell \neq p$ be a prime dividing d. By Proposition 6.1, for all sufficiently large n, there is a prime $\mathfrak{p}$ such that $v_{\mathfrak{p}}(f^n(0) - \beta) > 0$ with $\ell \nmid v_{\mathfrak{p}}(f^n(0) - \beta)$ and $v_{\mathfrak{p}}(f^m(0) - \beta) = 0$ for all $0 < m < n$. Since $|c|_{\mathfrak{p}} = |\beta|_{\mathfrak{p}} = 1$ for all but finitely many $\mathfrak{p}$ we may also suppose that $|c|_{\mathfrak{p}} = |\beta|_{\mathfrak{p}} = 1$. Then, by Lemma 7.2, the prime $\mathfrak{p}$ does not ramify in $K(f^{-(n-1)}(\beta))$. By Lemma 7.3, it does ramify in $K(f^{-n}(\beta))$. □

The next result is a characteristic p analog of a theorem of Pagano [29, Theorem 1.3] for number fields (see also [8] for a similar result); the growth condition here is stronger than what Pagano obtains over number fields.

Theorem 7.5. *Let $f(x) = x^d + c$ be a separable nonisotrivial polynomial of degree $d > 1$. Let $\beta \in K$. Then there is a constant $C(n, \beta) > 0$ such that $[K(f^{-n}(\beta)) : K] > C(n, \beta)d^n$ for all positive integers n.*

Proof. It will suffice to show that d divides $[K(f^{-n}(\beta)) : K(f^{-(n-1)}(\beta))]$ for all sufficiently large n. Let ℓ be a prime such that $\ell^e \mid d$ for some $e > 0$. Applying Proposition 6.1 as in Theorem 7.4, we see that for all sufficiently large n, there is a prime $\mathfrak{p}$ with the property $|c|_{\mathfrak{p}} = |\beta|_{\mathfrak{p}} = 1$ such that $v_{\mathfrak{p}}(f^n(0) - \beta) > 0$ with $\ell \nmid v_{\mathfrak{p}}(f^n(0) - \beta)$ and $v_{\mathfrak{p}}(f^m(0) - \beta) = 0$ for all $0 < m < n$. Then Lemma 7.3 implies that for any prime $\mathfrak{p}'$ in $K(f^{-(n-1)}(\beta))$ that lies over $\mathfrak{p}$, there is a prime $\mathfrak{q}$ in $K(f^{-n}(\beta))$ such that ℓ^e divides $e(\mathfrak{q}/\mathfrak{p}')$. Hence $\ell^e \mid [K(f^{-n}(\beta)) : K(f^{-(n-1)}(\beta))]$. Since this holds for any prime $\ell \neq p$ such that $\ell^e \mid d$ for some $e > 0$, it follows that $d \mid [K(f^{-n}(\beta)) : K(f^{-(n-1)}(\beta))]$ for all sufficiently large n, and our proof is complete. □

We can now prove a finite index result for iterated monodromy groups of quadratic polynomials. We need a little terminology to state our result.

Let L be a field, let f be a quadratic polynomial, and let $\beta \in \bar{L}$. For $n \in \mathbb{N}$, let $L_n(f, \beta) = L(f^{-n}(\beta))$ be the field obtained by adjoining the n-th preimages of β under f to $L(\beta)$, and let $L_\infty(f, \beta) = \bigcup_{n=1}^{\infty} L_n(f, \beta)$. We let $G_\infty(\beta) = \mathrm{Gal}(L_\infty(f, \beta)/L)$. The group $G_\infty(\beta)$ embeds into $\mathrm{Aut}(T_\infty^2)$, the automorphism group of an infinite 2-ary rooted tree T_∞^2 (note that all of the definitions here generalize to rational functions of any degree — see [28] or [23], for example). Boston and Jones [7] asked if $G_\infty(\beta)$ had finite index in $\mathrm{Aut}(T_\infty^2)$ whenever f is not postcritically finite in the case where L is a number field. It was later shown [24] that this is true if the pair (f, β) is eventually stable (see below), assuming the *abc* conjecture. This was also shown to be true unconditionally for nonisotrivial quadratic polynomials over function fields of characteristic 0 in [12].

For $\beta \in \bar{L}$ and a polynomial $f \in L[x]$, the pair (f, β) is said to be *eventually stable* if the number of irreducible factors of $f^n(x) - \beta$ over $L(\beta)$ is bounded independently of n as $n \to \infty$ (stability and eventual stability can also be defined for rational functions as in [22]). We will prove a finite index result for nonisotrivial quadratic polynomials over function fields of odd positive characteristic under an eventual stability assumption.

The technique we use is the same as that used in [12]; see also [24; 10; 19]. We make use of [12, Proposition 7.7], which is stated in characteristic 0 but is true with no changes in the proof in characteristic p provided that $K(f^{-n}(\beta))$ is separable over K for all n, which is automatic here when $p > 2$; the following result is a strengthening of [18, Corollary 1].

Theorem 7.6. *Let f be a nonisotrivial quadratic polynomial defined over a field K that is a finite extension of $\mathbb{F}_p(t)$. Suppose that $p > 2$ and that β is not postcritical or periodic for f. Suppose furthermore that the pair (f, β) is eventually stable. Then $G_\infty(\beta)$ has finite index in* $\mathrm{Aut}(T_\infty^2)$.

Proof. As in [12], it will suffice to show that for all sufficiently large N, we have

$$\mathrm{Gal}(K_N/K_{N-1}) \cong C_2^{2^N},$$

where C_2 is the cyclic group with two elements. After a change of variables, we may assume that $f(x) = x^2 + c$ for some $c \in K \setminus k$.

Since (f, β) is eventually stable, there is an m such that $f^m(x) - \beta = (x - \gamma_1) \cdots (x - \gamma_{2^m})$ for γ_i with the property that $f^n(x) - \gamma_i$ is irreducible over $K(\gamma_i)$ for all n for $i = 1, \dots, 2^m$, by [10, Proposition 4.2]. Let $L = K(\gamma_1, \dots, \gamma_{2^m})$. It follows from [12, Proposition 7.7] and Lemma 7.3 (see Remark 7.7) that we must have $\mathrm{Gal}(K_{n+m}/K_{n+m-1}) \cong [C_2]^{2^{m+n}}$ whenever there are primes $\mathfrak{p}_i$ of L, for $i = 1, \dots, 2^m$, such that

(i) $v_{\mathfrak{p}_i}(c) = v_{\mathfrak{p}_i}(\gamma_j) = 0$ for $j = 1, \dots, 2^m$;

(ii) $2 \nmid v_{\mathfrak{p}_i}(f^n(0) - \gamma_i)$;

(iii) $v_{\mathfrak{p}_i}(f^{n'}(0) - \gamma_i) = 0$ for all $n' < n$;

(iv) $v_{\mathfrak{p}_i}(f^{n'}(0) - \gamma_j) = 0$ for all $n' \le n$ and $j \ne i$; and

(v) $\mathfrak{p}_i$ does not ramify over $\mathfrak{p}_i \cap K$.

Note that conditions (i) clearly holds for all but finitely many primes $\mathfrak{p}_i$. Likewise, (v) holds for all but finitely many primes due to the separability of L over K, which follows from the fact that f is quadratics and $p \ne 2$. Hence, we will be done if we can show that for all sufficiently large n, there are $\mathfrak{p}_i$, for $i = 1, \dots, 2^m$, that satisfy conditions (ii), (iii), and (iv).

Now, fix a γ_i. By Lemma 6.7, there exists $\delta > 0$ such that for all sufficiently large n, we have

$$\sum_{\substack{v_{\mathfrak{p}}(f^n(0)-\gamma_i)>0 \\ 2 \nmid v_{\mathfrak{p}}(f^n(0)-\gamma_i)}} N_{\mathfrak{p}} \ge \delta d^n h_f(0). \tag{7.6.1}$$

For any n, let $\mathcal{X}(n)$ be the set of primes $\mathfrak{p}$ such that $v_{\mathfrak{p}}(f^n(0) - \gamma_i) > 0$ and $v_{\mathfrak{p}}(f^{n'}(0) - \gamma_i) > 0$ for some $n' < n$. Since γ_i is neither periodic nor postcritical and $h_f(0) > 0$, we may apply Lemma 6.2. We see then that for all sufficiently large n, we have

$$\sum_{\mathfrak{p} \in \mathcal{X}(n)} N_{\mathfrak{p}} \le \frac{\delta}{3} d^n h_f(0). \tag{7.6.2}$$

For any n and $j \ne i$, we let $\mathcal{Y}_j(n)$ be the set of primes $v_{\mathfrak{p}}(f^n(0) - \gamma_i) > 0$ and $v_{\mathfrak{p}}(f^{n'}(0) - \gamma_j) > 0$ for some $n' \le n$. Since $f^{n'}(\gamma_j) \ne \gamma_i$ for all n' and $i \ne j$, we may apply Lemma 6.2 again. Since in addition we have $v_{\mathfrak{p}}(\gamma_i - \gamma_j) \ne 0$ for all but finitely many $\mathfrak{p}$ when $i \ne j$, we see that for all sufficiently large n, we have

$$\sum_{j \ne i} \sum_{\mathfrak{p} \in \mathcal{Y}_j(n)} N_{\mathfrak{p}} \le \frac{\delta}{3} d^n h_f(0). \tag{7.6.3}$$

Since $\delta h_f(0) > 0$, Equations (7.6.1), (7.6.2), and (7.6.3) imply that for any sufficiently large n, there is a prime $\mathfrak{p}_i$ satisfying conditions (ii), (iii), and (iv), and our proof is complete. □

Remark 7.7. We note that while conditions (i) and (ii) above are weaker as stated than Condition R from [12, Definition 7.2], they do imply that the prime $\mathfrak{p}_i$ ramifies in $K(f^{-n}(\gamma_i))$ (by Lemma 7.3), which is what [12, Proposition 7.7] requires.

It should also be possible to prove a finite index result along the lines of Theorem 7.6 more generally for nonisotrivial polynomials of the form $x^d + c$, where $d > 2$ and $p \nmid d$ by modifying techniques in [12] and combining them with our argument for Theorem 7.5 above.

Acknowledgements

Benedetto, Dragos Ghioca, Minhyong Kim, Carlo Pagano, Joe Silverman, Dinesh Thakur, Felipe Voloch, and Julie Wang for many helpful conversations. We give special thanks to Juan Rivera-Letelier, who provided us with the argument for Proposition 3.2 and without whose help this paper likely would not have been possible. Finally, we thank the anonymous referee for their many helpful suggestions.

References

[1] M. Baker, "A finiteness theorem for canonical heights attached to rational maps over function fields", *J. Reine Angew. Math.* **626** (2009), 205–233. MR Zbl

[2] M. Baker and R. Rumely, *Potential theory and dynamics on the Berkovich projective line*, Math. Surv. Monogr. **159**, Amer. Math. Soc., Providence, RI, 2010. MR Zbl

[3] A. S. Bang, "Taltheoretiske Undersøgelser", *Tidsskrift Mat.* **4**:5 (1886), 70–80, 130–137.

[4] R. L. Benedetto, *Dynamics in one non-archimedean variable*, Grad. Stud. in Math. **198**, Amer. Math. Soc., Providence, RI, 2019. MR Zbl

[5] R. L. Benedetto, D. Ghioca, B. Hutz, P. Kurlberg, T. Scanlon, and T. J. Tucker, "Periods of rational maps modulo primes", *Math. Ann.* **355**:2 (2013), 637–660. MR Zbl

[6] E. Bombieri and W. Gubler, *Heights in Diophantine geometry*, New Math. Monogr. **4**, Cambridge Univ. Press, 2006. MR Zbl

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

[8] G. Boxall, G. Jones, and H. Schmidt, "Rational values of transcendental functions and arithmetic dynamics", *J. Eur. Math. Soc.* **24**:5 (2022), 1567–1592. MR Zbl

[9] A. Bridy and T. J. Tucker, "ABC implies a Zsigmondy principle for ramification", *J. Number Theory* **182** (2018), 296–310. MR Zbl

[10] A. Bridy and T. J. Tucker, "Finite index theorems for iterated Galois groups of cubic polynomials", *Math. Ann.* **373**:1-2 (2019), 37–72. MR Zbl

[11] A. Bridy, P. Ingram, R. Jones, J. Juul, A. Levy, M. Manes, S. Rubinstein-Salzedo, and J. H. Silverman, "Finite ramification for preimage fields of post-critically finite morphisms", *Math. Res. Lett.* **24**:6 (2017), 1633–1647. MR Zbl

[12] A. Bridy, J. R. Doyle, D. Ghioca, L.-C. Hsia, and T. J. Tucker, "Finite index theorems for iterated Galois groups of unicritical polynomials", *Trans. Amer. Math. Soc.* **374**:1 (2021), 733–752. MR Zbl

[13] G. S. Call and J. H. Silverman, "Canonical heights on varieties with morphisms", *Compos. Math.* **89**:2 (1993), 163–205. MR Zbl

[14] C. Favre and J. Rivera-Letelier, "Théorie ergodique des fractions rationnelles sur un corps ultramétrique", *Proc. Lond. Math. Soc.* (3) **100**:1 (2010), 116–154. MR Zbl

[15] A. Ferraguti and C. Pagano, "Constraining images of quadratic arboreal representations", *Int. Math. Res. Not.* **2020**:22 (2020), 8486–8510. MR Zbl

[16] C. Gratton, K. Nguyen, and T. J. Tucker, "ABC implies primitive prime divisors in arithmetic dynamics", *Bull. Lond. Math. Soc.* **45**:6 (2013), 1194–1208. MR Zbl

[17] R. Hartshorne, *Algebraic geometry*, Grad. Texts in Math. **52**, Springer, 1977. MR Zbl

[18] W. Hindes, "Prime divisors in polynomial orbits over function fields", *Bull. Lond. Math. Soc.* **48**:6 (2016), 1029–1036. MR Zbl

[19] W. Hindes and R. Jones, "Riccati equations and polynomial dynamics over function fields", *Trans. Amer. Math. Soc.* **373**:3 (2020), 1555–1575. MR Zbl

[20] M. Hindry and J. H. Silverman, *Diophantine geometry: an introduction*, Grad. Texts in Math. **201**, Springer, 2000. MR Zbl

[21] H.-L. Huang, C.-L. Sun, and J. T.-Y. Wang, "Integral orbits over function fields", *Int. J. Number Theory* **10**:8 (2014), 2187–2204. MR Zbl

[22] R. Jones and A. Levy, "Eventually stable rational functions", *Int. J. Number Theory* **13**:9 (2017), 2299–2318. MR Zbl

[23] J. Juul, P. Kurlberg, K. Madhu, and T. J. Tucker, "Wreath products and proportions of periodic points", *Int. Math. Res. Not.* **2016**:13 (2016), 3944–3969. MR Zbl

[24] J. Juul, H. Krieger, N. Looper, M. Manes, B. Thompson, and L. Walton, "Arboreal representations for rational maps with few critical points", pp. 133–151 in *Research directions in number theory* (Banff, AB, 2017), edited by J. S. Balakrishnan et al., Assoc. Women Math. Ser. **19**, Springer, 2019. MR Zbl

[25] M. Kim, "Geometric height inequalities and the Kodaira–Spencer map", *Compos. Math.* **105**:1 (1997), 43–54. MR Zbl

[26] S. Lang, *Fundamentals of Diophantine geometry*, Springer, 1983. MR Zbl

[27] A. Moriwaki, "Height inequality of nonisotrivial curves over function fields", *J. Algebraic Geom.* **3**:2 (1994), 249–263. MR Zbl

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

[29] C. Pagano, "The size of arboreal images, I: Exponential lower bounds for PCF and unicritical polynomials", preprint, 2021. arXiv 2104.11175

[30] T. Pezda, "Cycles of polynomials in algebraically closed fields of positive characteristic", *Colloq. Math.* **67**:2 (1994), 187–195. MR Zbl

[31] L. P. Postnikova and A. Schinzel, "Primitive divisors of the expression $a^n - b^n$ in algebraic number fields", *Mat. Sb.* (*N.S.*) **75 (117)** (1968), 171–177. In Russian; translated in *Math. USSR-Sb.* **4**:2 (1968), 153–159. MR

[32] B. Rice, "Primitive prime divisors in polynomial arithmetic dynamics", *Integers* **7** (2007), art. id. A26. MR Zbl

[33] A. Schinzel, "Primitive divisors of the expression $A^n - B^n$ in algebraic number fields", *J. Reine Angew. Math.* **268/269** (1974), 27–33. MR Zbl

[34] A. Grothendieck, *Revêtements étales et groupe fondamental, Fasc. II: Exposés VI, VIII–XI* (Séminaire de Géométrie Algébrique du Bois Marie 1960–1961), Inst. des Hautes Études Sci., Paris, 1963. MR

[35] J. H. Silverman, *The arithmetic of elliptic curves*, Grad. Texts in Math. **106**, Springer, 1986. MR Zbl

[36] J. H. Silverman, "Integer points, Diophantine approximation, and iteration of rational maps", *Duke Math. J.* **71**:3 (1993), 793–829. MR Zbl

[37] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Grad. Texts in Math. **151**, Springer, 1994. MR Zbl

[38] J. H. Silverman, "Rational functions with a polynomial iterate", *J. Algebra* **180**:1 (1996), 102–110. MR Zbl

[39] V. A. Sookdeo, "Integer points in backward orbits", *J. Number Theory* **131**:7 (2011), 1229–1239. MR Zbl

[40] H. Stichtenoth, *Algebraic function fields and codes*, 2nd ed., Grad. Texts in Math. **254**, Springer, 2009. MR Zbl

[41] L. Szpiro, "Propriétés numériques du faisceau dualisant relatif", pp. 44–78 in *Séminaire sur les pinceaux de courbes de genre au moins deux*, Astérisque **86**, Soc. Math. France, Paris, 1981. MR Zbl

[42] P. Vojta, *Diophantine approximations and value distribution theory*, Lecture Notes in Math. **1239**, Springer, 1987. MR Zbl

[43] P. Vojta, "A more general *abc* conjecture", *Int. Math. Res. Not.* **1998**:21 (1998), 1103–1116. MR Zbl

[44] J. F. Voloch, "Diophantine approximation in characteristic p", *Monatsh. Math.* **119**:4 (1995), 321–325. MR Zbl

[45] J. T.-Y. Wang, "Integral points of projective spaces omitting hyperplanes over function fields of positive characteristic", *J. Number Theory* **77**:2 (1999), 336–346. MR Zbl

[46] K. Yamanoi, "The second main theorem for small functions and related problems", *Acta Math.* **192**:2 (2004), 225–294. MR Zbl

[47] K. Zsigmondy, "Zur Theorie der Potenzreste", *Monatsh. Math. Phys.* **3**:1 (1892), 265–284. MR Zbl

Communicated by Jason P. Bell
Received 2021-12-31 Revised 2022-09-02 Accepted 2022-10-04

alexanderjcarney@gmail.com *Department of Mathematics, University of Rochester, Rochester, NY, United States*

wmh33@txstate.edu *Department of Mathematics, Texas State University, San Marcos, TX, United States*

thomas.tucker@rochester.edu *Department of Mathematics, University of Rochester, Rochester, NY, United States*

mathematical sciences publishers msp

Algebra & Number Theory

msp.org/ant

PRODUCTION
production@msp.org
Silvio Levy, Scientific Editor

See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2023 is US $485/year for the electronic version, and $705/year (+$65, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online.

ANT peer review and production are managed by EditFLOW® from MSP.

PUBLISHED BY
mathematical sciences publishers
nonprofit scientific publishing
http://msp.org/

Algebra & Number Theory

Volume 17 No. 9 2023