SQUAREFREE DOUBLY PRIMITIVE DIVISORS IN DYNAMICAL SEQUENCES

D. GHIOCA, K. D. NGUYEN, AND T. J. TUCKER

Abstract. Let K be a number field or a function field of characteristic 0, let $\varphi \in K(z)$ with $\deg(\varphi) \geq 2$, and let $\alpha \in \mathbb{P}^1(K)$. Let S be a finite set of places of K containing all the archimedean ones and the primes where φ has bad reduction. After excluding all the natural counterexamples, we define a subset $\mathbf{A}(\varphi, \alpha)$ of $\mathbb{Z}_{\geq 0} \times \mathbb{Z}_{>0}$ and show that for all but finitely many $(m, n) \in \mathbf{A}(\varphi, \alpha)$ there is a prime $\mathfrak{p} \notin S$ such that $\operatorname{ord}_{\mathfrak{p}}(\varphi^{m+n}(\alpha) - \varphi^m(\alpha)) = 1$ and α has portrait (m, n) under the action of φ modulo $\mathfrak{p}$. This latter condition implies $\operatorname{ord}_{\mathfrak{p}}(\varphi^{u+v}(\alpha) - \varphi^u(\alpha)) \leq 0$ for $(u, v) \in \mathbb{Z}_{\geq 0} \times \mathbb{Z}_{>0}$ satisfying $u < m$ or $v < n$. Our proof assumes a conjecture of Vojta for $\mathbb{P}^1 \times \mathbb{P}^1$ in the number field case and is unconditional in the function field case thanks to a deep theorem of Yamanoi. This paper extends earlier work of Ingram-Silverman, Faber-Granville, and the authors.

1. Introduction

Let K be a number field or function field of transcendence degree 1 over an algebraically closed field of characteristic 0, let φ be a rational function of degree greater than one with coefficients in K, and let $\alpha \in K$. Suppose that α is not preperiodic. When $\mathfrak{p}$ is a nonarchimedean prime of K such that the reduction $\alpha_{\mathfrak{p}}$ of α is preperiodic under the reduction $\varphi_{\mathfrak{p}}$ of φ, we say that $(m, n) \in \mathbb{Z}_{\geq 0} \times \mathbb{Z}_{>0}$ is the portrait of α modulo $\mathfrak{p}$ if $\varphi_{\mathfrak{p}}^m(\alpha_{\mathfrak{p}})$ is periodic of minimum period n under $\varphi_{\mathfrak{p}}$, while m is the smallest nonnegative integer such that $\varphi_{\mathfrak{p}}^m(\alpha_{\mathfrak{p}})$ is periodic (as always in dynamics, we let f^k denote the k-th iterate of a map f). We call m the *preperiod* of α modulo $\mathfrak{p}$ and call n the *minimum* or *exact period* of α modulo $\mathfrak{p}$. Questions about the portraits that α achieves modulo $\mathfrak{p}$ have arisen in many contexts. For example, in their study of the Mandelbrot set, Douady and Hubbard [DH85] use an argument of Gleason to prove that if $\varphi(x) = x^2 + t$ over the function field $\mathbb{C}(t)$, then for every n there is λ such that 0 has exact period n modulo $(t - \lambda)$ and with the further property that $(t - \lambda)$ is a squarefree factor of the polynomial (in t) $\varphi^n(0)$; they then use these facts to prove that the Mandelbrot set has hyperbolic components of every period and that these components are all isomorphic to the unit disc. In the context of arithmetic dynamics, Ingram and Silverman [IS09] conjectured that if φ is defined over a number field K and $\alpha \in K$ is not preperiodic, then for all but finitely many possible portraits (m, n), there is a prime $\mathfrak{p}$ of K such that α has portrait (m, n) modulo $\mathfrak{p}$. In this paper, we will treat questions about portraits of

2010 *Mathematics Subject Classification.* Primary 11G50; Secondary 14G99.

Key words and phrases. write keywords.

The first author was partially supported by an NSERC Discovery Grant. The second author thanks the Pacific Institute of Mathematical Sciences for its generous support. The third author was partially supported by an NSF grant.

points modulo primes over both function fields and number fields, with an emphasis on obtaining factors that are squarefree.

From now on, let K be either a number field or a function field of transcendence degree 1 over a field κ of characteristic 0. Furthermore, unless otherwise noted, we also assume that κ is algebraically closed.

By a place $\mathfrak{p}$ of K, we mean an equivalence class of absolute values on K that are trivial on the constant field κ if K is a function field. Let M_K denote the set of places of K. Each nonarchimedean place $\mathfrak{p}$ gives rise to a valuation ring $\mathfrak{o}_\mathfrak{p}$ and a maximal ideal denoted (by an abuse of notation) by $\mathfrak{p}$; we let M_K^0 be the set of all nonarchimedean places of K (also called *finite* places). We denote by $k_\mathfrak{p}$ the residue field of K at the place $\mathfrak{p} \in M_K^0$; if K is a function field, then $k_\mathfrak{p}$ is canonically isomorphic to κ. For $\mathfrak{p} \in M_K^0$, let $\mathrm{ord}_\mathfrak{p}$ denote the additive valuation on K normalized so that $\mathrm{ord}_\mathfrak{p}(K) = \mathbb{Z} \cup \{\infty\}$. For every $\mathfrak{p} \in M_K^0$, we have a well-defined reduction map $r_\mathfrak{p} : \mathbb{P}^1(K) \longrightarrow \mathbb{P}^1(k_\mathfrak{p})$. Given a non-constant function $\varphi(x) \in K(x)$, for all but finitely many $\mathfrak{p} \in M_K^0$, by "reducing the coefficients of φ modulo $\mathfrak{p}$", the morphism $\varphi : \mathbb{P}^1_K \to \mathbb{P}^1_K$ induces a morphism $\overline{\varphi} : \mathbb{P}^1_{k_\mathfrak{p}} \to \mathbb{P}^1_{k_\mathfrak{p}}$ of the same degree such that $\overline{\varphi}(r_\mathfrak{p}(a)) = r_\mathfrak{p}(\varphi(a))$ for every $a \in \mathbb{P}^1(K)$ and we say that φ has good reduction modulo $\mathfrak{p}$ (see [Sil07, Chapter 2]). For $\mathfrak{p} \in M_K^0$, if K is a number field, let $N_\mathfrak{p} = \log(\#k_\mathfrak{p})$; otherwise, let $N_\mathfrak{p} = 1$. For every finite subset S of M_K, let $N_S := \sum_{\mathfrak{p} \in S \cap M_K^0} N_\mathfrak{p}$. Let h_K denote the Weil height (over K) on $\mathbb{P}^1(\overline{K})$ and for every $\varphi(x) \in K(x)$ having degree at least 2, we can define the canonical height $\widehat{h}_{\varphi,K}$ on $\mathbb{P}^1(\overline{K})$. The readers are referred to Section 3 or [Sil07, Chapter 3] for more details.

Given a sequence $(a_n)_{n \geq 0}$ of elements of K, we may ask if for every (sufficiently large) n there exists a prime $\mathfrak{p}$ such that $\mathrm{ord}_\mathfrak{p}(a_n) > 0$ while $\mathrm{ord}_\mathfrak{p}(a_m) \leq 0$ for every $m < n$. Such primes are called primitive divisors of the sequence (a_n). This well-studied question has a long history starting from work of Bang [Ban86], Zsigmondy [Zsi92], and Schinzel [Sch74] in the context of the multiplicative group to further work in the setting of elliptic curves (for examples, see [EMW06] and [Ing07]). First results in the context of arithmetic dynamics where $a_n = \varphi^n(\alpha)$ for a given $\varphi(x) \in K(x)$ and $\alpha \in \mathbb{P}^1(K)$ are obtained by Ingram and Silverman [IS09]. After [IS09], there are various papers on primitive divisors in dynamical sequences [FG11], [DH12], [Kri13], and especially [GNT13] in which the existence of primitive divisors is established for the function field case and conditionally on ABC for the number field case. Analogous results for the arithmetic dynamics of higher dimensional varieties are obtained by Silverman [Sil13] assuming Vojta's conjecture for projective spaces.

A harder question asked by Ingram-Silverman is the existence of a prime $\mathfrak{p}$ such that $\mathrm{ord}_\mathfrak{p}(\varphi^{m+n}(\alpha) - \varphi^m(\alpha)) > 0$ while $\mathrm{ord}_\mathfrak{p}(\varphi^{u+v}(\alpha) - \varphi^v(\alpha)) \leq 0$ if $u < m$ or $v < n$. Such primes are called doubly primitive divisors (for the double sequence $a_{m,n} = \varphi^{m+n}(\alpha) - \varphi^n(\alpha)$) by Faber and Granville [FG11] who discovered certain counter-examples to the question by Ingram-Silverman and proposed a modified question. In [GNT15], we answer a variant of the Ingram-Silverman-Faber-Granville question for function fields (and the proof in [GNT15] can be adapted to settle the number field case assuming ABC). More explicit results for the special case of unicritical polynomials are obtained in recent work of Doyle [Doy16], [Doy].

In number theory, whenever one has $\mathrm{ord}_{\mathfrak{p}}(a) > 0$, one could ask whether $\mathrm{ord}_{\mathfrak{p}}(a) = 1$ (i.e. whether $\mathfrak{p}$ is a squarefree factor of a). In fact, the existence of *squarefree* primitive divisors in the sequence $(a_n := \varphi^n(\alpha))_{n\geq 0}$ is also proved in [GNT13] and has an interesting application to the structure of certain iterated Galois groups [GNT13, Section 6]. The aim of this paper is to study the existence of the so-called squarefree doubly primitive divisors:

Definition 1.1. *Let $\varphi(x) \in K(x)$ with $\deg(\varphi) \geq 2$ and let $\alpha \in \mathbb{P}^1(K)$ which is not φ-periodic. Let $\mathfrak{p}$ be a prime of good reduction. We say that α has portrait (m,n) modulo $\mathfrak{p}$ if $r_{\mathfrak{p}}(\alpha)$ has portrait (m,n) under the reduction $\overline{\varphi}$ of φ. If, in addition, $\infty \notin \{\varphi^{m+n}(\alpha), \varphi^m(\alpha)\}$ and $\mathrm{ord}_{\mathfrak{p}}(\varphi^{m+n}(\alpha) - \varphi^m(\alpha)) = 1$ then we say that α has* squarefree *portrait (m,n) modulo $\mathfrak{p}$.*

If α has portrait (m,n) modulo $\mathfrak{p}$ then $\mathrm{ord}_{\mathfrak{p}}(\varphi^{u+v}(\alpha) - \varphi^u(\alpha)) \leq 0$ when $u < m$ or $v < n$; this explains the connection to the concept of doubly primitive divisors in Faber-Granville [FG11]. Given (m,n), the existence of $\mathfrak{p}$ such that α has squarefree portrait (m,n) modulo $\mathfrak{p}$ is also of interest in complex dynamics. To illustrate the kind of results proved in this paper without introducing several technical definitions, we state the following theorem:

Theorem 1.2. *Let K be a number field or a function field over a field of characteristic 0. In the number field case, assume Vojta's conjecture for $\mathbb{P}^1 \times \mathbb{P}^1$ (see Conjecture 4.1). Let $\varphi(x) \in K(x)$ with $d := \deg(\varphi) \geq 2$, let S be a finite set of places of K containing the archimedean ones and all primes of bad reduction of φ, and let τ be a positive number. Then there is a constant $C_1 = C_1(K, \varphi, N_S, \tau)$ depending only on K, φ, N_S, and τ such that the following holds. For every $\alpha \in \mathbb{P}^1(K)$ such that $\widehat{h}_{\varphi,K}(\alpha) \geq \tau$, for all positive integers $m > C_1$ and $n > C_1$, there is a prime $\mathfrak{p} \in M_K \setminus S$ such that α has squarefree portrait (m,n) modulo $\mathfrak{p}$.*

Remark 1.3. We emphasize the fact that C_1 depends on a lower bound τ of $\widehat{h}_{\varphi,K}(\alpha)$ instead of α itself. This means our results (Theorem 1.2 and Theorem 1.8) are essentially uniform in α. Indeed, if K is a number field, Northcott's principle gives a positive lower bound on the canonical height of wandering points in $\mathbb{P}^1(K)$. This also holds in the function field case as long as φ is not isotrivial thanks to a result of Baker [Bak09].

While Theorem 1.2 is effective in the function field case, its effectiveness in the number field case depends on the effectiveness of Vojta's conjecture for $\mathbb{P}^1 \times \mathbb{P}^1$ (Conjecture 4.1). Nevertheless, even if Theorem 1.2 is effective, the resulting C_1 should be large and the theorem does not say anything about small values of m or n. For example, fix $m = 2017$, we cannot conclude from Theorem 1.2 that for all sufficiently large n, there is $\mathfrak{p}$ such that α has squarefree portrait $(2017, n)$. *The ultimate goal of this paper* is to identify a subset $\mathbf{A}(\varphi, \alpha)$ of $\mathbb{Z}_{\geq 0} \times \mathbb{Z}_{>0}$ by excluding all the natural counter-examples and prove that for all but finitely many $(m,n) \in \mathbf{A}(\varphi, \alpha)$, there is $\mathfrak{p} \in M_K^0 \setminus S$ such that α has squarefree portrait (m,n) modulo $\mathfrak{p}$. First, we need the following definition taken from [GNT13]:

Definition 1.4. *Let $\varphi(x) \in K(x)$ and $a \in \mathbb{P}^1(\overline{K})$. We say that φ is dynamically unramified over a if for each $i \in \mathbb{N}$, there exists $a_i \in \mathbb{P}^1(\overline{K})$ such that $\varphi^i(a_i) = a$ and φ is unramified at a_i. In other words, a has an infinite backward orbit consisting of unramified points of φ.*

We are now able to define the set of "admissible" (m,n) which could possibly become a squarefree portrait after reducing modulo some prime $\mathfrak{p}$:

Definition 1.5. *Let $\varphi \in K(x)$ with $\deg(\alpha) \geq 2$ and let $\alpha \in \mathbb{P}^1(K)$ that is not φ-preperiodic.*

(i) *Let $A_1(\varphi,\alpha)$ be the set of $m \in \mathbb{Z}_{\geq 0}$ satisfying the following condition. If $m = 0$, we require that φ is dynamically unramified over α; if $m \geq 1$, we require that there exists $\eta \in \mathbb{P}^1(\overline{K}) \setminus \{\varphi^{m-1}(\alpha)\}$ such that $\varphi(\eta) = \varphi^m(\alpha)$, φ is unramified at η, and dynamically unramified over η.*

(ii) *Let $A_2(\varphi)$ be the set of $n \in \mathbb{Z}_{>0}$ satisfying the following condition. There is a φ-periodic point $\beta \in \overline{K}$ with exact period n such that $x - \beta$ is a squarefree factor of $\varphi^n(x) - x$ and there is $\eta \in \mathbb{P}^1(\overline{K}) \setminus \{\varphi^{n-1}(\beta)\}$ such that $\varphi(\eta) = \beta$, φ is unramified at η, and dynamically unramified over η.*

(iii) *Define $\mathbf{A}(\varphi,\alpha) := A_1(\varphi,\alpha) \times A_2(\varphi)$.*

Note that this definition makes sense over any field (i.e. not necessarily a number field or function field). When $m \geq 1$, the condition in Definition 1.5(i) says that $\varphi^m(\alpha)$ has an infinite backward orbit that starts from $\eta \neq \varphi^{m-1}(\alpha)$ and consists of unramified points. The condition on η in Definition 1.5(ii) says that β has an infinite backward orbit that starts from $\eta \neq \varphi^{n-1}(\beta)$ and consists of unramified points. Roughly speaking, the "bad" set $\mathbb{Z}_{\geq 0} \setminus A_1(\varphi,\alpha)$ (respectively $\mathbb{Z}_{>0} \setminus A_2(\varphi)$) is essentially the set of m (respectively n) that either belongs to the "bad" set $Y(\varphi,\alpha)$ (respectively $X(\varphi)$) defined in [GNT15, Definition 1.2] or fails a certain dynamical unramifiedness condition. Although Definition 1.5 looks slightly complicated, we briefly explain, through counter-examples, why $\mathbf{A}(\varphi,\alpha)$ is the largest set (up to subtracting *finitely many* elements of $\mathbb{Z}_{\geq 0} \times \mathbb{Z}_{>0}$) where we can hope for the existence of squarefree doubly primitive divisors.

Example 1.6. Consider $\varphi(x) = (x-\alpha)(x-\delta)^2$ (with $\delta \neq \alpha$) so that $1 \notin A_1(\varphi,\alpha)$. The only pre-image of $\varphi(\alpha) = 0$ that is not α is δ where φ is ramified. Now $\varphi^{n+1}(x) = (\varphi^n(x)-\alpha)(\varphi^n(x)-\delta)^2$. Therefore every squarefree divisor of $\varphi^{n+1}(\alpha) - \varphi(\alpha) = \varphi^{n+1}(\alpha)$ must be a divisor of $\varphi^n(\alpha) - \alpha$. Hence $(1,n)$ is not a squarefree portrait after reducing modulo any prime $\mathfrak{p}$.

Example 1.7. For simplicity, assume φ is a polynomial, and let $n \notin A_2(\varphi)$.

(a) If $\varphi^n(x) - x$ does not have a squarefree factor (for instance, $n = 1$ and $\varphi(x) = x + x^2$), then obviously $\varphi^{m+n}(\alpha) - \varphi^m(\alpha)$ does not have a squarefree factor.

(b) Now assume $\varphi^n(x) - x$ has a squarefree factor, but every such factor is of the form $x - \beta'$ where the exact period of β' is strictly smaller than n. Then every squarefree prime factor $\mathfrak{p}$ of $\varphi^{m+n}(\alpha) - \varphi^m(\alpha)$ must be a factor of $\varphi^m(\alpha) - \beta'$, and hence $r_{\mathfrak{p}}(\varphi^m(\alpha)) = r_{\mathfrak{p}}(\beta')$ has exact period less than n. Therefore (m,n) cannot be a squarefree portrait.

(c) Let $\beta_1, \ldots, \beta_k$ be all the points of exact period n such that $x - \beta_i$ is a squarefree factor of $\varphi^n(x) - x$. Assume that for each β_i, we fail to have an η as described in Definition 1.5(ii). So there is $M \geq 1$ such that for every $i \in \{1, \ldots, k\}$, every squarefree factor of $\varphi^M(x) - \beta_i$, if it exists, must have the form $x - \delta$ where $\varphi^{M-1}(\delta) = \varphi^{n-1}(\beta_i)$. Let $m \geq M$, assume that $\mathfrak{p}$ is a squarefree prime factor of $\varphi^{m+n}(\alpha) - \varphi^m(\alpha)$ and $r_{\mathfrak{p}}(\varphi^m(\alpha))$ has exact period n. By using the factorization of $\varphi^{M+n}(x) - \varphi^M(x)$ induced from the

factorization of $\varphi^n(x)-x$, we have that $\mathfrak{p}$ is a factor of some $\varphi^{m-M}(\alpha)-\delta$ with $\varphi^{M-1}(\delta) = \varphi^{n-1}(\beta_i)$ for some $i \in \{1,\dots,k\}$ as mentioned above. However, this implies $r_{\mathfrak{p}}(\varphi^{m-1}(\alpha)) = r_{\mathfrak{p}}(\varphi^{M-1}(\delta)) = r_{\mathfrak{p}}(\beta_i)$ which is also periodic. Hence (m,n) cannot be the portrait of α modulo $\mathfrak{p}$.

Having explained why the set $\mathbf{A}(\varphi,\alpha)$ is essentially best possible, we now state the main result of this paper:

Theorem 1.8. *Let K, φ, d, S, and τ be as in Theorem 1.2. In the number field case, assume Vojta's conjecture for $\mathbb{P}^1\times\mathbb{P}^1$ (see Conjecture 4.1). Then there is a finite subset $\Delta = \Delta(K,\varphi,N_S,\tau)$ of $\mathbb{Z}_{\geq 0}\times\mathbb{Z}_{>0}$ such that for every $\alpha\in\mathbb{P}^1(K)$ with $\widehat{h}_{\varphi,K}(\alpha)\geq\tau$, the following holds. Write $\mathbf{A} = \mathbf{A}(\varphi,\alpha)$; for every $(m,n)\in\mathbf{A}\setminus\Delta$ satisfying $\infty\notin\{\varphi^{m+n}(\alpha),\varphi^n(\alpha)\}$, there is a prime $\mathfrak{p}\in M_K\setminus S$ such that α has squarefree portrait (m,n) modulo $\mathfrak{p}$.*

We refer the readers to Section 2 where explicit examples are given to illustrate Theorem 1.8. We can also prove that the sets $A_1(\varphi,\alpha)$ and $A_2(\varphi)$ have finite complement in $\mathbb{Z}_{\geq 0}$, see Proposition 7.10. In fact, for the examples in Section 2, the set $\mathbf{A}(\varphi,\alpha)$ is often the whole $\mathbb{Z}_{\geq 0}\times\mathbb{Z}_{>0}$. Therefore, Theorem 1.8 subsumes Theorem 1.2. However, since Theorem 1.2 is needed to prove Theorem 1.8 and its simple statement does not involve the definition of $\mathbf{A}(\varphi,\alpha)$, we believe presenting it as a separate theorem will benefit the readers.

One of the motivations for studying the questions considered in this paper is possible applications to generalizations of iterated Galois groups. To explain, we need a little notation. For φ a rational function over a number field K and $\alpha\in K$, we let G_n be the Galois group of $K(\varphi^{-n}(\alpha))$ over K and let G_∞ be the inverse limit of the G_n as n goes to infinity. There has been a good deal of work done on classifying the G_∞ that arise in this manner (see [Juu15, GNT13, Odo85, Sto92]); in particular, there are various finite index conjectures analogous to the Serre open image theorem for ℓ-adic Galois representations (see [Jon13] for a nice survey). One of the main tools for treating these problems is finding square-free factors of $\varphi^n(\beta)-\alpha$ for β a critical point of φ, as these give rise to ramification groups in G_n (see [BIJ+15]). Richard Pink has asked what one can say about the Galois group that comes from taking inverse images of iterates of points. More specifically consider the two-parameter family of Galois groups given by letting $G_{m,n} = \mathrm{Gal}(K(\varphi^{-n}(\varphi^m(\alpha))/K)$ for $\alpha\in K$; one might hope for some sort of finite index theorem describing the group that arises as m and n go to infinity. It should be possible to use the techniques of this paper to treat this problem in some cases.

The organization of this paper is as follows. After giving examples in Section 2 and basic results on absolute values and heights in Section 3, we introduce Vojta's conjecture for $\mathbb{P}^1\times\mathbb{P}^1$ in Section 4. Assuming this conjecture, we prove Corollary 4.20 which is the key ingredient for the proof of our main theorems in the number field case. In Section 5, Corollary 5.11 which is the function field counterpart of Corollary 4.20 is proved thanks to a deep theorem of Yamanoi. The proof of Theorem 1.2 is given in Section 6 and we finish the paper with the proof of Theorem 1.8 in Section 7.

Acknowledgments. We thank Paul Vojta for useful suggestions. We also thank the referee for many useful comments and suggestions which improved our presentation.

2. Examples

Let $\varphi(x) \in K(x)$ with $d := \deg(\varphi) \geq 2$. We will use the simple observation that if $a \in \mathbb{P}^1(K)$ is not contained in the orbit of any critical point then φ is unramified at a as well as any point in the backward orbit of a.

2.1. **Number field case.** Let K be a number field and $\varphi(x) = x^2 + 1$. We have $A_2(\varphi) = \mathbb{Z}_{>0}$ thanks to the following:

- For every $n \in \mathbb{Z}_{>0}$, the polynomial $P_n(x) := \varphi^n(x) - x$ has only simple factors. In fact, every root r of P_n is an algebraic integer and this implies:

$$P_n'(r) = \varphi'(r)\varphi'(\varphi(r)) \cdots \varphi'(\varphi^{n-1}(r)) - 1 = 2^n r\varphi(r) \cdots \varphi^{n-1}(r) - 1 \neq 0.$$

- For every $n \in \mathbb{Z}_{>0}$, every root r of $P_n(x)$ whose period is strictly smaller than n must be a root of $P_{n/p}(x)$ for a prime divisor p of n. From

$$\sum_{\text{prime } p|n} 2^{n/p} < 2^n,$$

  there exists $\beta \in \overline{\mathbb{Q}}$ having exact period n.
- Since the critical point 0 is not preperiodic, the existence of η as in Definition 1.5(ii) is guaranteed.

For $\alpha \in K$ that is not φ-preperiodic, there are three (mutually exclusive) cases:

(1) There is $M \in \mathbb{Z}_{\geq 0}$ such that $\varphi^M(\alpha) = 1$. Then $A_1(\varphi, \alpha) = \mathbb{Z}_{\geq 0} \setminus \{M\}$.
(2) There is $M \in \mathbb{Z}_{\geq 0}$ such that $\varphi^M(\alpha) = -1$. Then $\varphi^{M+1}(\alpha) = 2$, the only pre-image of 2 that is not -1 is 1, and φ is not dynamically unramified over 1. Hence $A_1(\varphi, \alpha) = \mathbb{Z}_{\geq 0} \setminus \{M + 1\}$.
(3) $\{1, -1\} \cap \{\varphi^m(\alpha) : \ m \geq 0\} = \emptyset$. Then $A_1(\varphi, \alpha) = \mathbb{Z}_{\geq 0}$.

There is $\tau > 0$ depending only on φ and K such that $\widehat{h}(\alpha) \geq \tau$ for every $\alpha \in K$ that is not φ-preperiodic (see Section 3). Theorem 1.8 shows that there is a finite subset Δ of $\mathbb{Z}_{\geq 0} \times \mathbb{Z}_{>0}$ depending only on φ and K satisfying the following. For every $\alpha \in K$ that is not φ-preperiodic (hence $\widehat{h}(\alpha) \geq \tau$), for every $(m, n) \in \mathbb{A}(\varphi, \alpha) \setminus \Delta$, there exists $\mathfrak{p} \in M_K^0$ such that α has squarefree portrait (m, n) modulo $\mathfrak{p}$.

2.2. **Function field case.** Let K be a finite extension of $\mathbb{C}(t)$ and $\varphi(x) = x^2 + t$. By similar arguments to the previous example, we have that $A_2(\varphi) = \mathbb{Z}_{>0}$. To prove that $P_n'(r) \neq 0$ for every root r of $P_n(x)$, use the fact that if $\mathfrak{p}$ is the place of $\mathbb{C}(t)$ corresponding to the point at infinity of $\mathbb{P}^1(\mathbb{C})$ then (after extending $\mathrm{ord}_{\mathfrak{p}}$ to $\overline{\mathbb{C}(t)}$) we have $\mathrm{ord}_{\mathfrak{p}}(2^n r\varphi(r) \cdots \varphi^{n-1}(r)) < 0$.

Since φ is not isotrivial, by a result of Baker [Bak09], there is a positive lower bound τ (depending only on φ and K) on $\widehat{h}_{\varphi,K}(\alpha)$ for every $\alpha \in \mathbb{P}^1(K)$ that is not φ-preperiodic.

For $\alpha \in K$ that is not φ-preperiodic, there are three (mutually exclusive) cases:

(1) There is $M \in \mathbb{Z}_{\geq 0}$ such that $\varphi^M(\alpha) = t$. Then $A_1(\varphi, \alpha) = \mathbb{Z}_{\geq 0} \setminus \{M\}$.
(2) There is $M \in \mathbb{Z}_{\geq 0}$ such that $\varphi^M(\alpha) = -t$. Then $\varphi^{M+1}(\alpha) = t^2 + t$, the only pre-image of $t^2 + t$ that is not $-t$ is t, and φ is not dynamically unramified over t. Hence $A_1(\varphi, \alpha) = \mathbb{Z}_{\geq 0} \setminus \{M + 1\}$.
(3) $\{t, -t\} \cap \{\varphi^m(\alpha) : \ m \geq 0\} = \emptyset$. Then $A_1(\varphi, \alpha) = \mathbb{Z}_{\geq 0}$.

Theorem 1.8 shows that there is a finite subset Δ of $\mathbb{Z}_{\geq 0} \times \mathbb{Z}_{>0}$ depending only on φ and K satisfying the following. For every $\alpha \in K$ that is not φ-preperiodic,

for every $(m,n) \in \mathbf{A}(\varphi,\alpha) \setminus \Delta$, there exists a prime of good reduction $\mathfrak{p} \in M_K^0$ such that α has squarefree portrait (m,n) modulo $\mathfrak{p}$.

3. Absolute values and heights

3.1. **Absolute values.** When K is a function field, $M_K = M_K^0$. When K is a number field, the set $M_K \setminus M_K^0$ is finite and corresponds to the collection of real embeddings $K \to \mathbb{R}$ and pairs of complex conjugate embeddings $K \to \mathbb{C}$. For every place $v \in M_K$, define:

$$\|x\|_v = \begin{cases} e^{-N_{\mathfrak{p}} \operatorname{ord}_{\mathfrak{p}}(x)} & \text{if } v \in M_K^0 \text{ and it corresponds to the prime ideal } \mathfrak{p} \\ |\sigma(x)| & \text{if } v \in M_K^\infty \text{ is real and it corresponds to } \sigma:\ K \to \mathbb{R} \\ |\sigma(x)|^2 & \text{if } v \in M_K^\infty \text{ is complex and it corresponds to } \sigma:\ K \to \mathbb{C} \end{cases}$$

We also define $|x|_v = \|x\|_v^{1/2}$ if v is complex, and $|x|_v = \|x\|_v$ otherwise. This way, $|\cdot|_v$ becomes an absolute value on K (note that $\|\cdot\|_v$ does not satisfy the triangle inequality when v is complex).

3.2. **Heights.** For every real number y, define $\log^+(y) = \log \max\{1, y\}$. We define the Weil height h_K on $\mathbb{P}^1(\overline{K})$ as follows:

$$h_K(x) = \frac{1}{[K(x):K]} \sum_{\mathfrak{q} \in M_{K(x)}} \log^+ \|x\|_{\mathfrak{q}},$$

for every $x \in \overline{K}$, and $h_K(\infty) = 0$. If L/K is a finite extension then $h_L = [L:K] h_K$. When K is a number field, Northcott's principle states that there are only finitely many elements of $\mathbb{P}^1(\overline{K})$ whose height and degree are bounded above by a given constant. For the more general Weil height associated to a Cartier divisor on a projective variety, we refer the readers to [BG06].

Let x and y be distinct elements of $\mathbb{P}^1(K)$. Let $\mathcal{E} := \{\mathfrak{p} \in M_K^0 :\ r_{\mathfrak{p}}(x) = r_{\mathfrak{p}}(y)\}$, we have the following inequality:

$$\sum_{\mathfrak{p} \in \mathcal{E}} N_{\mathfrak{p}} \le \min\{h_K(x), h_K(y)\} + h_K(x) + h_K(y) + c_K, \tag{3.1}$$

where $c_K = 0$ in the function field case and $c_K = [K:\mathbb{Q}] \log 2$ in the number field case. To prove this, we assume that $x, y \in K$ since the case $x = \infty$ or $y = \infty$ is easy. Without loss of generality, assume $h_K(x) \le h_K(y)$. For every $\mathfrak{p} \in \mathcal{E}$, either $|x|_{\mathfrak{p}} > 1$ or $|x-y|_{\mathfrak{p}} < 1$. Therefore $\sum_{\mathfrak{p} \in \mathcal{E}} N_{\mathfrak{p}} \le h_K(x) + h_K(x-y)$. Then (3.1) follows from the well-known inequality $h_K(x-y) \le h_K(x) + h_K(y) + c_K$ [BG06, Proposition 1.5.15].

If $\varphi(z) \in \overline{K}(z)$ is a rational function of degree $d \ge 2$, then for each point $x \in \mathbb{P}^1(\overline{K})$, following [CS93] we define the canonical height (over K) of x under the action of φ by:

$$\widehat{h}_{\varphi,K}(x) = \lim_{n \to \infty} \frac{h_K(\varphi^n(x))}{d^n}.$$

According to [CS93], there is a constant $C_{\varphi,K}$ depending only on K and φ such that $|h_K(x) - \widehat{h}_\varphi(x)| < C_{\varphi,K}$ for all $x \in \mathbb{P}^1(\overline{K})$. When K is a number field, Northcott's principle implies that $\widehat{h}_{\varphi,K}(x) = 0$ if and only if x is φ-preperiodic. Moreover, there is a positive lower bound depending only on K and φ for $\widehat{h}_{\varphi,K}(x)$ for every $x \in \mathbb{P}^1(K)$ that is not φ-preperiodic. Baker [Bak09] proves that the same result holds in the function field case if φ is not isotrivial.

4. A conjecture of Vojta and its consequences

Throughout this section, let K be a number field. An M_K-constant is a collection of real numbers $(c_v)_{v\in M_K}$ such that $c_v = 0$ for all but finitely many v. Let X be a smooth projective variety and D a (Weil or Cartier) divisor defined over K. For each $v \in M_K$, we can define Weil functions:

$$\lambda_{X,D,v} : (X \setminus \operatorname{Supp} D)(\mathbb{C}_v) \to \mathbb{R}$$

satisfying certain functorial properties (see [Voj11, Chapter 8] for more details). If $D = \sum_{i=1}^{k} m_i[a]$ is a divisor on $\mathbb{P}^1_K$ where $k \in \mathbb{Z}_{>0}$ and $m_i \in \mathbb{Z}$ for every i, we *always* use the definition:

$$\lambda_{\mathbb{P}^1_K,D,\mathfrak{p}}(x) = \sum_{i=1}^{k} m_i \log^+ \frac{1}{\|x - a_i\|_{\mathfrak{p}}}$$

for $x \notin \{a_1, \dots, a_k\}$. Note that when $a_i = \infty$, the formula $\log^+ \dfrac{1}{\|x - a_i\|_{\mathfrak{p}}}$ is interpreted as $\log^+ \|x\|_v$.

Define the truncated counting function (see [Voj11, Chapter 22]):

$$N^{(1)}(X, D, x) := \sum_{\mathfrak{p}\in M_K^0} \min\{\lambda_{X,D,\mathfrak{p}}(x), N_{\mathfrak{p}}\}$$

for $x \in X(K)$ not lying in the support of D.

From now on, we work over the ambient variety $X = \mathbb{P}^1 \times \mathbb{P}^1$. The following is a special case of Vojta's conjecture (see [Voj11, Conjecture 22.5(b)]):

Conjecture 4.1. *Let K be a number field, let D be a normal crossing divisor on $X = (\mathbb{P}^1_K)^2$, let $\mathcal{K} = \mathcal{O}(-2,-2)$ be the canonical sheaf on X, and let $h_{\mathcal{K}(D),K}$ be a Weil height on $X(\overline{K})$ with respect to $\mathcal{K}(D)$. Then for any $\epsilon > 0$ there is a proper Zariski closed subset Z of X, depending on K, D, and ϵ, such that for all $C \in \mathbb{R}$, the inequality*

$$N^{(1)}(X, D, (a, b)) \geq h_{\mathcal{K}(D),K}(a, b) - \epsilon(h_K(a) + h_K(b)) - C$$

holds for all but finitely many $(a, b) \in (X \setminus Z)(K)$.

Remark 4.2. Note that if $D \cong \mathcal{O}(q, r)$ then $\mathcal{K}(D) \cong \mathcal{O}(q - 2, r - 2)$ and we can choose the definition:

$$h_{\mathcal{K}(D),K}(a, b) = (q - 2)h_K(a) + (r - 2)h_K(b)$$

for $(a, b) \in (\mathbb{P}^1)^2(K)$.

Lemma 4.3. *Let K be a number field, let $f(x) \in K(x) \setminus K$ be a non-constant rational function. Let $\mathcal{Z}$ and $\mathcal{P}$ respectively denote the effective divisors of zeros and poles of f (hence $(f) = \mathcal{Z} - \mathcal{P}$). There is a finite set of places $S(K, f) \subseteq M_K$ depending only on K and f such that the following holds. For every prime $\mathfrak{p} \in M_K^0 \setminus S(K, f)$, for every $a \in P^1(K)$ that is not a zero or pole of f, we have:*

(a) *If $\lambda_{\mathbb{P}^1_K,\mathcal{P},\mathfrak{p}}(a) > 0$ then $\log \|f(a)\|_{\mathfrak{p}} = \lambda_{\mathbb{P}^1_K,\mathcal{P},\mathfrak{p}}(a)$,*
(b) *if $\lambda_{\mathbb{P}^1_K,\mathcal{P},\mathfrak{p}}(a) = 0$ then $\log \|f(a)\|_{\mathfrak{p}} = -\lambda_{\mathbb{P}^1_K,\mathcal{Z},\mathfrak{p}}(a)$.*

Proof. There is a finite set of places $S_1(K, f)$ such that for every $\mathfrak{p} \in M_K^0 \setminus S(K, f)$ and for every $a \in \mathbb{P}^1(K)$ that is not a zero or pole of f, the following hold:

(i) $\lambda_{\mathbb{P}^1_K,\mathcal{Z},\mathfrak{p}}(a) = \lambda_{\mathbb{P}^1_K,(f),\mathfrak{p}}(a) + \lambda_{\mathbb{P}^1_K,\mathcal{P},\mathfrak{p}}(a) = -\log\|f(a)\|_{\mathfrak{p}} + \lambda_{\mathbb{P}^1_K,\mathcal{P},\mathfrak{p}}(a)$.
(ii) If $\lambda_{\mathbb{P}^1_K,\mathcal{Z},\mathfrak{p}}(a) > 0$ then a and some zero of f have the same reduction modulo $\mathfrak{p}$.
(iii) If $\lambda_{\mathbb{P}^1_K,\mathcal{P},\mathfrak{p}}(a) > 0$ then a and some pole of f have the same reduction modulo $\mathfrak{p}$.

Extend $S_1(K,f)$ to $S(K,f)$ such that for every $\mathfrak{p} \in M_K^0 \setminus S(K,f)$, any pole of f and any zero of f have different reduction modulo $\mathfrak{p}$. □

Let $f(x) \in K(x)$, $a \in \mathbb{P}^1(K)$ that is not a pole of f, and $b \in K$ such that $f(a) \neq b$, let $\mathcal{Z}(f,a,b) := \mathcal{Z}_K(f,a,b)$ be the set of primes $\mathfrak{p}$ of K such that $\mathrm{ord}_{\mathfrak{p}}(f(a)-b) \geq 1$ or, equivalently, $\|f(a)-b\|_{\mathfrak{p}} < 1$. We have:

Proposition 4.4. *Assume Conjecture 4.1 holds. Let K be a number field, let $f(x) \in K(x)$ be a rational function of degree $d > 0$. For every $\epsilon > 0$, there exist a proper Zariski closed subset Z of $X := (\mathbb{P}^1_K)^2$ and a constant $C_1 := C_1(K,f,\epsilon)$ such that*

$$\sum_{\mathfrak{p} \in \mathcal{Z}(f,a,b)} N_{\mathfrak{p}} \geq (d-2-\epsilon)h_K(a) - (2+\epsilon)h_K(b) - C_1 \tag{4.5}$$

for every $(a,b) \in (X \setminus Z)(K)$ such that a is not a pole of f and $b \in K$ satisfying $f(a) \neq b$.

Proof. Let D be the effective divisor defined by the equation $y = f(x)$ in X. Let v be a place of K, we now define $\lambda_{X,D,v}$. Let $\mathcal{P}$ denote the effective divisor of $\mathbb{P}^1_K$ corresponding to the poles (counted with multiplicity) of f, then write $D_{\mathcal{P}} := \mathcal{P} \times \mathbb{P}^1_K$ to denote the pull-back to X. Let D_∞ be the divisor $\mathbb{P}^1_K \times \{\infty\}$. Write $R = (f(x) - y)$ to denote the principal divisor generated by the rational function $f(x) - y$. From $R = D - D_{\mathcal{P}} - D_\infty$ we can take

$$\lambda_{X,D,v} := \lambda_{X,R,v} + \lambda_{X,D_{\mathcal{P}},v} + \lambda_{X,D_\infty,v}.$$

We define $\lambda_{X,R,v}$, $\lambda_{X,D_{\mathcal{P}},v}$, and $\lambda_{X,D_\infty,v}$ as follows. For every $(a,b) \in X(K)$ such that a is not a pole of f, $b \neq \infty$, and $f(a) \neq b$, we have:

$$\lambda_{X,R,v}(a,b) = -\log\|f(a)-b\|_v,$$
$$\lambda_{X,D_{\mathcal{P}},v}(a,b) = \lambda_{\mathbb{P}^1_K,\mathcal{P},v}(a)$$
$$\lambda_{X,D_\infty,v}(a,b) = \lambda_{\mathbb{P}^1_K,[\infty],v}(b) = \log^+\|b\|_v.$$

Therefore, we can define:

$$\lambda_{X,D,v}(a,b) = -\log\|f(a)-b\|_v + \lambda_{\mathbb{P}^1_K,\mathcal{P},v}(a) + \log^+\|b\|_v. \tag{4.6}$$

By Conjecture 4.1, given $\epsilon > 0$, there exist a proper Zariski closed subset Z of X and a constant C_2 depending on K, f, and ϵ such that:

$$N^{(1)}(X,D,(a,b)) \geq (d-2)h_K(a) - h_K(b) - \epsilon(h_K(a)+h_K(b)) - C_2 \tag{4.7}$$

for $(a,b) \in (X \setminus Z)(K)$. If a is not a pole of f, $b \neq \infty$, and $f(a) \neq b$, from (4.6) we have:

(4.8)

$$N^{(1)}(X,D,(a,b)) = \sum_{\mathfrak{p} \in M_K^0} \min\{-\log\|f(a)-b\|_{\mathfrak{p}} + \lambda_{\mathbb{P}^1_K,\mathcal{P},\mathfrak{p}}(a) + \log^+\|b\|_{\mathfrak{p}}, N_{\mathfrak{p}}\}.$$

By choosing $C_1 > |d-2-\epsilon| \cdot \max\{h_K(z) : f(z) = 0\}$, inequality (4.5) holds when a is zero of f. From now on, we assume the extra condition that a is not a

zero of f. Let $S(K,f)$ be a set of places of K as in the conclusion of Lemma 4.3. We partition M_K^0 into three sets $M_K^0(1)$, $M_K^0(2)$, and $M_K^0(3)$ (depending on K, f, a, and b) as follows.

$$M_K^0(1) := \{\mathfrak{p} \in M_K^0 : \ \log^+ \|b\|_p > 0 \text{ or } \mathfrak{p} \in S(K,f)\} \tag{4.9}$$

$$M_K^0(2) := \{\mathfrak{p} \in M_K^0 : \ \log^+ \|b\|_{\mathfrak{p}} = 0, \ \mathfrak{p} \notin S(K,f), \text{ and } \lambda_{\mathbb{P}^1_K,\mathcal{P},\mathfrak{p}}(a) > 0\} \tag{4.10}$$

$$\mathcal{M}_K^0(3) := \{\mathfrak{p} \in M_K^0 : \ \log^+ \|b\|_{\mathfrak{p}} = 0, \ \mathfrak{p} \notin S(K,f), \text{ and } \lambda_{\mathbb{P}^1_K,\mathcal{P},\mathfrak{p}}(a) = 0\} \tag{4.11}$$

Using (4.9), we then have:

$$\begin{aligned}\sum_{\mathfrak{p}\in M_K^0(1)} \min\{-\log\|f(a)-b\|_{\mathfrak{p}} + \lambda_{\mathbb{P}^1_K,\mathcal{P},\mathfrak{p}}(a) + \log^+\|b\|_{\mathfrak{p}}, N_{\mathfrak{p}}\} &\le \sum_{\mathfrak{p}\in M_K^0(1)} N_{\mathfrak{p}} \\ &\le h_K(b) + C_3\end{aligned} \tag{4.12}$$

where $C_3 := \displaystyle\sum_{\mathfrak{p}\in S(K,f)} N_{\mathfrak{p}}$.

For every $\mathfrak{p} \in M_K^0(2)$ (see (4.10)), Lemma 4.3 gives $\log\|f(a)\|_{\mathfrak{p}} = \lambda_{\mathbb{P}^1_K,\mathcal{P},\mathfrak{p}}(a) > 0$. Since $\|b\|_{\mathfrak{p}} \le 1$, we have $\log\|f(a)-b\|_{\mathfrak{p}} = \log\|f(a)\|_{\mathfrak{p}} = \lambda_{\mathbb{P}^1_K,\mathcal{P},\mathfrak{p}}(a)$. Therefore:

$$\sum_{\mathfrak{p}\in M_K^0(2)} \min\{-\log\|f(a)-b\|_{\mathfrak{p}} + \lambda_{\mathbb{P}^1_K,\mathcal{P},\mathfrak{p}}(a) + \log^+\|b\|_{\mathfrak{p}}, N_{\mathfrak{p}}\} = 0. \tag{4.13}$$

For every $\mathfrak{p} \in \mathcal{M}_K^0(3)$ (see (4.11)), we have:

$$\min\{-\log\|f(a)-b\|_{\mathfrak{p}} + \lambda_{\mathbb{P}^1_K,\mathcal{P},\mathfrak{p}}(a) + \log^+\|b\|_{\mathfrak{p}}, N_{\mathfrak{p}}\} = \min\{-\log\|f(a)-b\|_{\mathfrak{p}}, N_{\mathfrak{p}}\}.$$

Moreover, letting $\mathcal{Z}$ denote the divisor of zeros of f, Lemma 4.3 yields $0 \le \lambda_{\mathbb{P}^1,\mathcal{Z},\mathfrak{p}}(a) = -\log\|f(a)\|_{\mathfrak{p}}$; hence $\|f(a)\|_{\mathfrak{p}} \le 1$. Since $\|b\|_{\mathfrak{p}} \le 1$, we have $\|f(a)-b\|_{\mathfrak{p}} \le 1$. Therefore:

$$\begin{aligned}&\sum_{\mathfrak{p}\in M_K^0(3)} \min\{-\log\|f(a)-b\|_{\mathfrak{p}} + \lambda_{\mathbb{P}^1_K,\mathcal{P},\mathfrak{p}}(a) + \log^+\|b\|_{\mathfrak{p}}, N_{\mathfrak{p}}\} \\ &= \sum_{\mathfrak{p}\in M_K^0(3)} \min\{\operatorname{ord}_{\mathfrak{p}}(f(a)-b), 1\} N_{\mathfrak{p}} \le \sum_{\mathfrak{p}\in\mathcal{Z}(f,a,b)} N_{\mathfrak{p}}.\end{aligned} \tag{4.14}$$

Combining (4.7), (4.8), (4.12), (4.13), and (4.14), we have:

$$\sum_{\mathfrak{p}\in\mathcal{Z}(f,a,b)} N_{\mathfrak{p}} + h_K(b) + C_3 \ge (d-2-\epsilon)h_K(a) - (1+\epsilon)h_K(b) - C_2 \tag{4.15}$$

for $(a,b) \in (X \setminus Z)(K)$ such that a is not a zero or pole of f, $b \ne \infty$, and $f(a) \ne b$. This finishes the proof. □

We will also use the following complementary result to Proposition 4.4.

Proposition 4.16. *Assume Conjecture 4.1 holds. Let K, f, and ϵ be as in Proposition 4.4. Let $b \in K$ and let d_b be the number of zeroes of $f(x) - b$ counted without multiplicities(i.e. the cardinality of $f^{-1}(b)$). Then there is a constant $C_4 := C_4(K,f,\epsilon,b)$ such that*

$$\sum_{\mathfrak{p}\in\mathcal{Z}(f,a,b)} N_{\mathfrak{p}} \ge (d_b - 2 - \epsilon)h_K(a) - C_4 \tag{4.17}$$

for every $a \in \mathbb{P}^1(K)$ with $f(a) \notin \{\infty, b\}$.

Proof. Let δ be the divisor of zeroes counted without multiplicities of $f(x) - b$ in $\mathbb{P}^1_K$. In other words, over $\overline{K}$, the divisor δ is reduced and consists of the d_b points in the set $f^{-1}(b)$. Let $D = \delta \times \mathbb{P}^1_K$ be a divisor of $X := (\mathbb{P}^1_K)^2$, we have $D \cong \mathcal{O}(d_b, 0)$.

There is a finite set of places $S' \subset M^0_K$ depending only on K and f such that for every $\mathfrak{p} \in M^0_K \setminus S'$ and for every $a \in \mathbb{P}^1(K)$ with $f(a) \notin \{\infty, b\}$, we have $|f(a) - b|_\mathfrak{p} < 1$ if and only if $|a - z_0|_\mathfrak{p} < 1$ for some $z_0 \in f^{-1}(b)$ (as always, if $z_0 = \infty$ we interpret $|a - z_0|_\mathfrak{p}$ as $|1/a|_\mathfrak{p}$). Hence, for every such a and for every $\beta \in \mathbb{P}^1(K)$, we have:

$$\sum_{\mathfrak{p} \in \mathcal{Z}(f,a,b)} N_\mathfrak{p} + \sum_{\mathfrak{p} \in S'} N_\mathfrak{p} \geq N^{(1)}(\mathbb{P}^1_K, \delta, a) = N^{(1)}(X, D, (a, \beta)). \tag{4.18}$$

By Conjecture 4.1, there is a proper Zariski closed subset Z of X depending on K, f, ϵ, and b such that the inequality

$$N^{(1)}(X, D, (a, \beta)) \geq (d_b - 2 - \epsilon) h_K(a) - \epsilon h_K(\beta) \tag{4.19}$$

holds for all but finitely many $(a, \beta) \in (X \setminus Z)(K)$. We now *fix* a β_0 such that $\mathbb{P}^1_K \times \{\beta_0\}$ is not a horizontal component of Z. Hence there are only finitely many $a \in \mathbb{P}^1(K)$ such that $(a, \beta_0) \in Z(K)$. This together with (4.18) and (4.19) finish the proof. □

The goal of this section is the following application to arithmetic dynamics:

Corollary 4.20. *Assume Conjecture 4.1 holds. Let K be a number field, let $\varphi \in K(z)$ be a rational function of degree $d \geq 2$, let ℓ be a positive integer, and write $\widehat{h} = \widehat{h}_{\varphi,K}$. For every $\epsilon > 0$, there exist constants C_5 and $N \geq \ell$ depending only on K, φ, ℓ, and ϵ such that the following holds. For every $a \in \mathbb{P}^1(K)$ that is not φ-preperiodic, $b \in K$, and $n \in \mathbb{Z}_{\geq 0}$ satisfying $\widehat{h}(b) \leq \widehat{h}(a)$, $n > N$, and $\varphi^n(a) \neq \infty$, the set $\mathcal{D} := \{\mathfrak{p} \in M^0_K : \operatorname{ord}_\mathfrak{p}(\varphi^n(a) - b) \geq 1\}$ satisfies the inequality:*

$$\sum_{\mathfrak{p} \in \mathcal{D}} N_\mathfrak{p} \geq (d_{\ell,b} - \epsilon - 2) h_K(\varphi^{n-\ell}(a)) - (2 + \epsilon) h_K(b) - C_5 \tag{4.21}$$

where $d_{\ell,b}$ is the number of zeroes counted without multiplicities of $\varphi^\ell(z) - b$.

Proof. We apply Proposition 4.4 for $f = \varphi^\ell$ and get a proper Zariski closed subset Z of $X := (\mathbb{P}^1_K)^2$ and a constant C_6 such that:

$$\sum_{\mathfrak{p} \in \mathcal{Z}(f,\alpha,\beta)} N_\mathfrak{p} \geq (d^\ell - 2 - \epsilon) h_K(\alpha) - (2 + \epsilon) h_K(\beta) - C_6 \tag{4.22}$$

for every $(\alpha, \beta) \in (X \setminus Z)(K)$ such that α is not a pole of f and $\beta \in K$ satisfying $f(\alpha) \neq \beta$. If some irreducible components of Z are points, we simply increase C_6 to take care of them. Hence we may assume that every irreducible component of Z is a curve. Let $\{\beta_1, \ldots, \beta_s\}$ be the (possibly empty) set of $\beta \in \mathbb{P}^1(K)$ such that $\mathbb{P}^1 \times \{\beta\}$ is a component of Z. Let $n \in \mathbb{Z}_{\geq 0}$ with $n > \ell$ and $\varphi^n(a) \neq \infty$. From the condition $\widehat{h}(b) \leq \widehat{h}(a)$, we have that $\varphi^n(a) \neq b$. There are two cases.

First, if $b = \beta_i$ for some $1 \leq i \leq s$, then Proposition 4.16 (for $f = \varphi^\ell$ and $b = \beta_i$) gives the desired inequality. It remains to consider the case $b \notin \{\beta_1, \ldots, \beta_s\}$. Therefore when n is sufficiently large, the point $(\varphi^{n-\ell}(a), b)$ does not belong to a vertical or horizontal component of Z. Once we can prove that $(\varphi^{n-\ell}(a), b)$ does not belong to a "non-trivial" (i.e. neither vertical nor horizontal) component of Z

then (4.22) with $\alpha = \varphi^{n-\ell}(a)$ and $\beta = b$ and the fact that $d^\ell \geq d_{\ell,b}$ yield the desired inequality.

Note that there exist positive constants C_7 and C_8 (depending on K and Z) such that for every point $(s,t) \in (\mathbb{P}^1)^2(K)$, if (s,t) lies in a non-trivial component of Z then:

$$C_7 h_K(t) + C_8 > h_K(s). \tag{4.23}$$

In order to justify inequality (4.23), we note that any component W of Z, which is neither horizontal, nor vertical corresponds to a divisor of type (a,b) with $a,b>0$. If we let D be a divisor of $\mathbb{P}^1 \times \mathbb{P}^1$ of type $(-1,q)$, then $D|_W$ has degree $aq-b>0$ for q sufficiently large. So the height function $h_{D|_W}$ is bounded below, and for $(s,t) \in W$, we have

$$-h_K(s) + q h_K(t) = h_{D|_W}(s,t) + O(1) \geq O(1),$$

as claimed in (4.23).

Since $|\widehat{h} - h_K| = O(1)$ on $\mathbb{P}^1(\overline{K})$ where the constants in $O(1)$ depend only on K and φ, inequality (4.23) implies that there are positive constants C_9 and C_{10} such that if $(\varphi^{n-\ell}(a), b)$ is in a non-trivial component of Z then:

$$C_9 \widehat{h}(b) + C_{10} > \widehat{h}(\varphi^{n-\ell}(a)). \tag{4.24}$$

When $d^{n-\ell} > C_9$, the inequalities $\widehat{h}(a) \geq \widehat{h}(b)$ and (4.24) imply:

$$\widehat{h}(a) < \frac{C_{10}}{d^{n-\ell} - C_9}. \tag{4.25}$$

Since K is a number field and a is not φ-preperiodic, there is a positive constant C_{11} depending only on K and φ such that $\widehat{h}(a) \geq C_{11}$. Hence when n is sufficiently large so that $C_{11} > \dfrac{C_{10}}{d^{n-\ell} - C_9}$, the point $(\varphi^{n-\ell}(a), b)$ cannot belong to a non-trivial component of Z. This finishes the proof. □

5. A theorem of Yamanoi and its consequences

The goal of this section is to prove *unconditionally* a variant of Corollary 4.20 for the function field case. Throughout this section, let K be a function field over the ground field κ; we recall that this means κ is an algebraically closed field of characteristic 0 and K is the function field of a curve over κ.

When B is a curve over κ with function field $\kappa(B)$, elements of $\mathbb{P}^1(\kappa(B)) = \kappa(B) \cup \{\infty\}$ are viewed as functions on B by regarding ∞ as the constant function mapping B to $\infty \in \mathbb{P}^1(\kappa)$. The main technical ingredient of this section is the theorem of Yamanoi [Yam04, Theorem 2] reformulated as follows:

Theorem 5.1 (Yamanoi)**.** *Let $q \in \mathbb{Z}_{>0}$. For all $\epsilon > 0$, there exists a positive constant $C_{12}(q,\epsilon)$ with the following property. Let Y and B be smooth projective curves over κ with a non-constant κ-morphism $\pi : Y \to B$. Let $R \in \kappa(Y)$ be a rational function on Y. Let $r_1, \ldots, r_q \in \mathbb{P}^1(\kappa(B))$ be distinct functions on B. Assume that $R \neq r_i \circ \pi$ for every i. Then we have:*

$$\begin{aligned}(q - 2 - \epsilon)\deg R \leq &\sum_{1 \leq i \leq q} \overline{n}(r_i \circ \pi, R, Y) + 2g(Y) \\ &+ C_{12}(q,\epsilon)(\deg \pi)(\max_{1 \leq i \leq q}(\deg r_i) + g(B) + 1)\end{aligned}$$

Here $g(Y)$ (resp. $g(B)$) denotes the genus of Y (resp. B), and $\overline{n}(r_i \circ \pi, R, Y)$ is the cardinality of $\{z \in Y : R(z) = r_i \circ \pi(z)\}$.

For the rest of this section, fix a smooth projective curve $\mathcal{C}$ over κ satisfying $K = \kappa(\mathcal{C})$. For $r \in \mathbb{P}^1(\overline{K})$, if $r \neq \infty$ (respectively $r = \infty$) express r in homogeneous coordinate $[r_0 : 1]$ (respectively $[1 : 0]$) with $r_0 \in \overline{K}$ and let $K(r)$ be the field $K(r_0)$ (respectively K).

Lemma 5.2. *Let $f(x) \in K(x) \setminus K$. There are constants C_{13} and C_{14} depending on K and f such that the following holds. For every $b \in \mathbb{P}^1(K)$ and $r \in \mathbb{P}^1(\overline{K})$ satisfying $f(r) = b$, the κ-morphism of smooth projective curves $\mathcal{B} \to \mathcal{C}$ which corresponds to the extension $K(r)/K$ is ramified over at most $C_{13}h_K(b) + C_{14}$ points of $\mathcal{C}$.*

Proof. The conclusion is trivial when $r = \infty$, we may assume $r \in \overline{K}$. Let $P(x)$ be the minimal polynomial of r over K. By the inequality $\deg(P) \leq \deg(f)$ and $\deg(f)h_K(r) = h_K(b) + O(1)$ where the constants in $O(1)$ depend only on K and f, there exist C_{13} and C_{14} depending on K and f such that for every place $\mathfrak{p}$ of $\mathcal{C}$ that lies outside a set of at most $C_{13}h_K(b) + C_{14}$ places of $\mathcal{C}$, the polynomial $P(x)$ has $\mathfrak{p}$-adic integral coefficients and its discriminant is a $\mathfrak{p}$-adic unit; in this case we know that $\mathcal{B}/\mathcal{C}$ is unramified over such $\mathfrak{p}$. □

As in the previous section, for $f(x) \in K(x)$, $a \in \mathbb{P}^1(K)$ that is not a pole of f, and $b \in K$ such that $f(a) \neq b$, let $\mathcal{Z}(f, a, b)$ be the set of primes $\mathfrak{p}$ of K such that $\mathrm{ord}_{\mathfrak{p}}(f(a) - b) \geq 1$. We have the following unconditional counterpart of Proposition 4.4:

Proposition 5.3. *Let K be a function field of the curve $\mathcal{C}$ over κ as above. Let $f(x) \in K(x)$ be a rational function of degree $d > 0$. For every $\epsilon > 0$, there exist positive constants C_{15} and C_{16} depending on K, ϵ, and f such that the following holds. For every $a \in \mathbb{P}^1(K)$ that is not a pole of f and $b \in K$ with $f(a) \neq b$, we have:*

$$\sum_{\mathfrak{p} \in \mathcal{Z}(f,a,b)} N_{\mathfrak{p}} \geq (d_{f,b} - 2 - \epsilon)h_K(a) - C_{15}h_K(b) - C_{16} \tag{5.4}$$

where $d_{f,b}$ is the number (counted without multiplicities) of the solutions of $f(x) = b$ in $\mathbb{P}^1(\overline{K})$.

Remark 5.5. In down-to-earth terms, the quantity $\sum_{\mathfrak{p} \in \mathcal{Z}(f,a,b)} N_{\mathfrak{p}}$ is the number of zeros (counted *without* multiplicities) of the function $f(a) - b$ on the curve $\mathcal{C}$. The quantities $h_K(a)$ and $h_K(b)$ are, respectively, the degree of the functions a and b.

Proof of Proposition 5.3. We may assume $3 \leq d_{f,b}$. Note that $d_{f,b} \leq d$ (equality occurs when f is unramified over b), hence we may restrict to $b \in K \setminus \{f(a)\}$ with a *fixed* $q := d_{f,b} \in \{3, \ldots, d\}$. We have distinct elements $r_1, \ldots, r_q \in \mathbb{P}^1(\overline{K})$ such that $f(r_i) = b$ for every i. Let $\mathcal{Y} = \mathcal{B}$ be the smooth projective curve over κ with function field $L := K(r_1, \ldots, r_q)$ and let $\pi = \mathrm{id} : \mathcal{Y} \to \mathcal{B}$. By Theorem 5.1, there exists a constant $C_{17} = C_{17}(q, \epsilon)$ such that:

$$(q-2-\epsilon)h_L(a) \leq \sum_{1 \leq i \leq q} \overline{n}(r_i, a, \mathcal{Y}) + 2g(\mathcal{Y}) + C_{17}\left(\max_{1 \leq i \leq q} h_L(r_i) + g(\mathcal{B}) + 1\right) \tag{5.6}$$

By Lemma 5.2, the Riemann-Hurwitz theorem for the extension L/K, and the equation $\deg(f)h_K(r_i) = h_K(b)+O(1)$, there exist constants C_{18} and C_{19} depending only on K and f such that:

$$\frac{1}{[L:K]}\left(2g(\mathcal{Y}) + C_{17}\left(\max_{1\le i\le q} h_L(r_i) + g(\mathcal{B}) + 1\right)\right) \le C_{18}h_K(b) + C_{19}. \tag{5.7}$$

Recall that for every finite extension F of K and for every place $\mathfrak{p}$ of F, the notation $r_{\mathfrak{p}}$ denotes the reduction map from $\mathbb{P}^1(F)$ to $\mathbb{P}^1(\kappa)$. By identifying points of Y to places of L, for $1 \le i \le q$, the set $\{z \in Y : \ a(z) = r_i(z)\}$ is exactly the set of places $\mathfrak{q}$ of L satisfying $r_{\mathfrak{q}}(a) = r_{\mathfrak{q}}(r_i)$; this latter set of places of L is denoted by S_i. Let $S_{i,K}$ be the set of places of K lying below S_i. Let $\mathcal{S}$ be the set of places $\mathfrak{p}$ of K satisfying one of the following conditions:

(i) f has bad reduction over $\mathfrak{p}$.
(ii) $r_{\mathfrak{p}}(r_i) = r_{\mathfrak{p}}(r_j)$ for some $i \ne j$.
(iii) $\mathrm{ord}_{\mathfrak{p}}(b) < 0$.

There exist C_{20} and C_{21} depending only on K and f such that

$$|\mathcal{S}| \le C_{20}h_K(b) + C_{21}. \tag{5.8}$$

By condition (ii), we have that the sets $S_{i,K} \cap (M_K \setminus \mathcal{S})$ for $1 \le i \le q$ are pairwise disjoint. If $\mathfrak{p} \in S_{i,K} \cap (M_K \setminus \mathcal{S})$, then we have $r_{\mathfrak{p}}(f(a)) = r_{\mathfrak{p}}(f(r_i)) = r_{\mathfrak{p}}(b)$, and hence $\mathrm{ord}_{\mathfrak{p}}(f(a) - b) \ge 1$ since $\mathrm{ord}_{\mathfrak{p}}(b) \ge 0$. Therefore, we have:

$$\frac{1}{[L:K]}\sum_{i=1}^{q}\overline{n}(r_i, a, \mathcal{Y}) = \frac{1}{[L:K]}\sum_{i=1}^{q}|S_i| \le \sum_{i=1}^{q}|S_{i,k}| \le |\mathcal{S}| + \sum_{\mathfrak{p}\in\mathcal{Z}(f,a,b)} N_{\mathfrak{p}}. \tag{5.9}$$

which, together with (5.8), imply

$$\frac{1}{[L:K]}\sum_{i=1}^{q}\overline{n}(r_i, a, \mathcal{Y}) \le C_{20}h_K(b) + C_{21} + \sum_{\mathfrak{p}\in\mathcal{Z}(f,a,b)} N_{\mathfrak{p}}. \tag{5.10}$$

We now divide both sides of (5.6) by $[L : K]$ and apply inequalities (5.7) and (5.10) to obtain the desired inequality. □

We have the following counterpart of Corollary 4.20:

Corollary 5.11. *Let K, $\mathcal{C}$, and κ be as in Proposition 5.3. Let $\varphi(x) \in K(x)$ be a rational function of degree $d > 0$, let ℓ be a positive integer. For every $\epsilon > 0$, there exist positive constants C_{22} and C_{23} depending only on K, φ, ℓ, and ϵ such that the following hold. For every $a \in \mathbb{P}^1(K)$, $b \in K$, and $n \in \mathbb{Z}_{\ge 0}$ satisfying $n \ge \ell$ and $\varphi^n(a) \notin \{b, \infty\}$ the set $\mathcal{D} := \{\mathfrak{p} \in M_K^0 : \ \mathrm{ord}_{\mathfrak{p}}(\varphi^n(a) - b) \ge 1\}$ satisfies:*

$$|\mathcal{D}| = \sum_{\mathfrak{p}\in\mathcal{D}} N_{\mathfrak{p}} \ge (d_{\ell,b} - 2 - \epsilon)h_K(\varphi^{n-\ell}(a)) - C_{22}h_K(b) - C_{23}$$

where $d_{\ell,b}$ is the number (counted without multiplicities) of the solutions of $\varphi^\ell(x) = b$ in $\mathbb{P}^1(\overline{K})$.

Proof. This follows immediately from Proposition 5.3 for $f = \varphi^\ell$ and the point $(\varphi^{n-\ell}(a), b)$. □

6. Proof of Theorem 1.2

Throughout this section, let K be a number field or a function field over the ground field κ. We have:

Lemma 6.1. *Let $f(x) \in K(x)$ having degree $d > 1$ and let $\mathfrak{p} \in M_K^0$ be a prime of good reduction of f. Let $\gamma_1, \gamma_2 \in \mathbb{P}^1(K)$ such that $r_\mathfrak{p}(f(\gamma_1)) = r_\mathfrak{p}(f(\gamma_2))$ but $r_\mathfrak{p}(\gamma_1) \neq r_\mathfrak{p}(\gamma_2)$. If γ_1 is f-periodic modulo $\mathfrak{p}$ then γ_2 is not f-periodic modulo $\mathfrak{p}$.*

Proof. This is proved in [GNT15, Lemma 4.22, pp. 176]. □

Lemma 6.2. *Let $f(x) \in K(x)$ having degree $d > 1$. There exist constants C_{24} and C_{25} depending only on K and f such that the following hold. For every $b \in K$ that is not a critical value of f, write $f^{-1}(b) = \{r_1, \dots, r_d\} \subset \mathbb{P}^1(\overline{K})$, let $L_b := K(r_1, \dots, r_d)$. Let $\mathcal{S}_b$ be the subset of M_K^0 consisting of primes $\mathfrak{p}$ satisfying one of the following two conditions:*

(i) *f has bad reduction modulo $\mathfrak{p}$.*
(ii) *f has good reduction modulo $\mathfrak{p}$ and for some prime $\mathfrak{q}$ of L_b lying above $\mathfrak{p}$, we have $r_\mathfrak{q}(r_i) = r_\mathfrak{q}(r_j)$ for some $1 \leq i \neq j \leq d$.*

Then we have:

(a) $\displaystyle\sum_{\mathfrak{p} \in \mathcal{S}_b} N_\mathfrak{p} \leq C_{24} h_K(b) + C_{25}$.
(b) *If $\mathfrak{p} \in M_K^0 \setminus \mathcal{S}_b$, $a \in \mathbb{P}^1(K)$ that is not a pole of f such that $\operatorname{ord}_\mathfrak{p}(f(a) - b) > 0$, then there is $i \in \{1, \dots, d\}$ and a place $\mathfrak{q}$ of L_b lying above $\mathfrak{p}$ such that $r_\mathfrak{q}(a) = r_\mathfrak{q}(r_i)$.*

Proof. Let T be the set of prime $\mathfrak{q}$ of L_b such that there exist $1 \leq i \neq j \leq d$ satisfying $r_\mathfrak{q}(r_i) = r_\mathfrak{q}(r_j)$. There exist constants C_{26} and C_{27} depending only on K and f such that:

$$\sum_{\mathfrak{q} \in T} N_\mathfrak{q} \leq C_{26} \max_{1 \leq i \leq d} h_{L_b}(r_i) + C_{27}.$$

This implies part (a).

For part (b), we have $\operatorname{ord}_\mathfrak{q}(f(a) - b) > 0$ for some place $\mathfrak{q}$ of L lying above $\mathfrak{p}$. This implies $r_\mathfrak{q}(f(a)) = r_\mathfrak{q}(b)$. Since the $r_\mathfrak{q}(r_i)$'s are distinct and the map f mod $\mathfrak{q}$ has degree d, the elements $r_\mathfrak{q}(r_i)$'s are exactly the preimages of $r_\mathfrak{q}(b)$ under the map f modulo $\mathfrak{q}$. Hence there is some r_i such that $r_\mathfrak{q}(a) = r_\mathfrak{q}(r_i)$. □

We now spend the rest of this section to prove Theorem 1.2. Let K, $\varphi(x)$, d, τ, S, and N_S be as in the statement of Theorem 1.2, write $\widehat{h} = \widehat{h}_{\varphi,K}$. We use the facts that $\widehat{h} - h_K = O(1)$ and $\widehat{h} \circ \varphi = d \cdot \widehat{h}$ repeatedly. To simplify the exposition, the notations $C_{28}, C_{29}, \dots$ denote positive constants that always depend on K and φ. For instance, the expression $C_{28} := C_{28}(A, b, \gamma)$ indicates that C_{28} depends on the quantities A, b, γ, *and* depends, as always, on K and φ. When K is a number field, we assume Conjecture 4.1.

Let $C_{29}(\tau)$ be such that $d^{C_{29}(\tau)-4}\tau$ is greater than the canonical height of any ramification point of φ^4. For $\alpha \in \mathbb{P}^1(K)$ with $\widehat{h}(\alpha) \geq \tau$, for every $m \geq C_{29}(\tau)$, we have:

$$\varphi^4 \text{ is unramified over } \varphi^m(\alpha). \tag{6.3}$$

Hence Theorem 1.2 follows from the following slightly more precise result:

Theorem 6.4. *Let K, $\varphi(x)$, d, τ, S, and N_S be as in Theorem 1.2. If K is a number field, assume Conjecture 4.1. Then there exists a constant $C_{30}(N_S, \tau)$ depending on K, φ, N_S, and τ such that the following holds. For every $\alpha \in \mathbb{P}^1(K)$ such that $\widehat{h}(\alpha) \geq \tau$, for every $m \in \mathbb{Z}_{\geq 0}$ such that $\varphi^m(\alpha) \neq \infty$ and φ^4 is unramified over $\varphi^m(\alpha)$, if $n > C_{30}(N_S, \tau)$ and $\varphi^{m+n}(\alpha) \neq \infty$ then there exists $\mathfrak{p} \in M_K \setminus S$ such that α has squarefree portrait (m, n) modulo $\mathfrak{p}$.*

Proof. Applying Corollary 4.20 and Corollary 5.11 (for $\ell = 4$, $\epsilon = 1$, and $a = b = \varphi^m(\alpha)$), there exist $C_{31}(\tau)$, C_{32}, and C_{33} such that for $n \geq C_{31}(\tau)$, we have:

$$\sum_{\mathfrak{p} \in \mathcal{D}} N_{\mathfrak{p}} \geq (d^4 - 3) h_K(\varphi^{m+n-4}(\alpha)) - C_{32} h_K(\varphi^m(\alpha)) - C_{33} \tag{6.5}$$

where $\mathcal{D} := \{\mathfrak{p} \in M_K^0 : \ \operatorname{ord}_{\mathfrak{p}}(\varphi^{m+n}(\alpha) - \varphi^m(\alpha)) \geq 1\}$. In equation (6.5), we note that if K is a number field, then we may take $C_{32} = 3$ (see Corollary 4.20). On the other hand, if K is a function field, then Corollary 5.11 (see also Proposition 5.3) yields that C_{32} is a constant independent of m.

Let $\mathcal{D}_{(1)} := \{\mathfrak{p} \in M_K^0 : \ \operatorname{ord}_{\mathfrak{p}}(\varphi^{m+n}(\alpha) - \varphi^m(\alpha)) = 1\}$. After rewriting inequality (6.5) and using $|\widehat{h}_\varphi - h_K| = O(1)$ and $\widehat{h}_\varphi \circ \varphi = d \cdot \widehat{h}_\varphi$, we have:

$$\sum_{\mathfrak{p} \in \mathcal{D}_{(1)}} N_{\mathfrak{p}} + \sum_{\mathfrak{p} \in \mathcal{D} \setminus \mathcal{D}_{(1)}} N_{\mathfrak{p}} \geq (d^4 - 3) d^{m+n-4} \widehat{h}(\alpha) - C_{32} d^m \widehat{h}(\alpha) - C_{34}. \tag{6.6}$$

From the definition of h_K, we have:

$$h_K(\varphi^{m+n}(\alpha) - \varphi^m(\alpha)) \geq \sum_{\mathfrak{p} \in \mathcal{D}_{(1)}} N_{\mathfrak{p}} + 2 \left(\sum_{\mathfrak{p} \in \mathcal{D} \setminus \mathcal{D}_{(1)}} N_{\mathfrak{p}} \right) \tag{6.7}$$

which implies:

$$d^{m+n} \widehat{h}(\alpha) + d^m \widehat{h}(\alpha) + C_{35} \geq \sum_{\mathfrak{p} \in \mathcal{D}_{(1)}} N_{\mathfrak{p}} + 2 \left(\sum_{\mathfrak{p} \in \mathcal{D} \setminus \mathcal{D}_{(1)}} N_{\mathfrak{p}} \right). \tag{6.8}$$

We combine inequalities (6.6) and (6.8) to obtain:

$$\begin{aligned} \sum_{\mathfrak{p} \in \mathcal{D}_{(1)}} N_{\mathfrak{p}} &\geq 2(d^4 - 3) d^{m+n-4} \widehat{h}(\alpha) - d^{m+n} \widehat{h}(\alpha) - C_{36} d^m \widehat{h}(\alpha) - C_{37} \\ &= (d^4 - 6) d^{m+n-4} \widehat{h}(\alpha) - C_{36} d^m \widehat{h}(\alpha) - C_{37}. \end{aligned} \tag{6.9}$$

Let $\mathcal{E}_1 := \{\mathfrak{p} \in M_K^0 : \ r_{\mathfrak{p}}(\varphi^{m+n-1}(\alpha)) = r_{\mathfrak{p}}(\varphi^{m-1}(\alpha))\}$. By (3.1), we have:

$$\begin{aligned} \sum_{\mathfrak{p} \in \mathcal{E}_1} N_{\mathfrak{p}} &\leq h_K(\varphi^{m-1}(\alpha)) + h_K(\varphi^{m+n-1}(\alpha)) + h_K(\varphi^{m-1}(\alpha)) + C_{38} \\ &\leq d^{m+n-1} \widehat{h}(\alpha) + 2 d^{m-1} \widehat{h}(\alpha) + C_{39} \end{aligned} \tag{6.10}$$

Let $\mathcal{E}_2$ be the set of primes $\mathfrak{p} \in M_K^0$ of good reduction such that $r_{\mathfrak{p}}(\varphi^{m+n'}(\alpha)) = r_{\mathfrak{p}}(\varphi^m(\alpha))$ for some $1 \leq n' < n$ and $n' \mid n$. In other words, after reduction modulo $\mathfrak{p}$, $\varphi^m(\alpha)$ is periodic and its minimum period strictly divides n. By (3.1), we have:

$$\sum_{\mathfrak{p} \in \mathcal{E}_2} N_{\mathfrak{p}} \leq \sum_{\text{prime } p \mid n} (2 h_K(\varphi^m(\alpha)) + h_K(\varphi^{m+n/p}(\alpha)) + C_{38}). \tag{6.11}$$

Since there are at most $\log_2 n$ such p, we have:

(6.12)
$$\sum_{\mathfrak{p}\in\mathcal{E}_2} N_{\mathfrak{p}} \le (\log_2 n)d^{m+n/2}\widehat{h}(\alpha) + 2(\log_2 n)d^m\widehat{h}(\alpha) + C_{40}\log_2 n \le d^{m+2n/3}\widehat{h}(\alpha)$$

when n is larger than some constant $C_{41}(\tau)$. Here we need the inequality $\widehat{h}(\alpha) \ge \tau$ so that $\dfrac{C_{40}\log_2 n}{d^m\widehat{h}(\alpha)} \le \dfrac{C_{40}\log_2 n}{\tau} = o(d^{2n/3})$. Applying Lemma 6.2 for $f = \varphi^4$ and $b = \varphi^m(\alpha)$, we get the resulting constants C_{42} and C_{43} as in the conclusion of Lemma 6.2. We also use the notation $\mathcal{S}_{\varphi^m(\alpha)}$ as in the statement of Lemma 6.2. Combining (6.9), (6.10), (6.12), and the observation that $1 - \dfrac{6}{d^4} - \dfrac{1}{d} \ge \dfrac{1}{8}$, we have:

(6.13)
$$\begin{aligned}\sum_{\mathfrak{p}\in\mathcal{D}_{(1)}} N_{\mathfrak{p}} - \sum_{\mathfrak{p}\in\mathcal{E}_1} N_{\mathfrak{p}} - \sum_{\mathfrak{p}\in\mathcal{E}_2} N_{\mathfrak{p}} &\ge \frac{1}{8}d^{m+n}\widehat{h}(\alpha) - d^{m+2n/3}\widehat{h}(\alpha) - C_{44}d^m\alpha - C_{45}\\ &> N_S + C_{42}h_K(\varphi^m(\alpha)) + C_{43}\end{aligned}$$

when $n > C_{46}(\tau, N_S)$. Hence there is a prime $\mathfrak{p} \in \mathcal{D}_{(1)}$ such that $\mathfrak{p} \notin \mathcal{E}_1 \cup \mathcal{E}_2 \cup S \cup \mathcal{S}_{\varphi^m(\alpha)}$. We have the following properties of $\mathfrak{p}$:

(i) φ has good reduction modulo $\mathfrak{p}$.
(ii) Let L be the field obtained by adjoining the solutions of $\varphi^4(x) = \varphi^m(\alpha)$ to K. There exist a prime $\mathfrak{q}$ of L lying above $\mathfrak{p}$ and $r \in L$ with $\varphi^4(r) = \varphi^m(\alpha)$ and $r_{\mathfrak{q}}(r) = r_{\mathfrak{q}}(\varphi^{m+n-4}(\alpha))$. Consequently, $r_{\mathfrak{p}}(\varphi^{m+n}(\alpha)) = r_{\mathfrak{p}}(\varphi^m(\alpha))$.
(iii) $r_{\mathfrak{p}}(\varphi^{m+n-1}(\alpha)) \ne r_{\mathfrak{p}}(\varphi^{m-1}(\alpha)))$ since $\mathfrak{p} \notin \mathcal{E}_1$.
(iv) $r_{\mathfrak{p}}(\varphi^{m+n'}(\alpha)) \ne r_{\mathfrak{p}}(\varphi^m(\alpha))$ for any proper divisor n' of n.

Lemma 6.1 together with Properties (ii), (iii), (iv) give that α has portrait (m, n) modulo $\mathfrak{p}$. And since $\mathfrak{p} \in \mathcal{D}_{(1)}$, we finish the proof. □

7. Proof of Theorem 1.8

We prove Theorem 1.8 by considering 3 cases:

(a) the case when both m and n are sufficiently large which has been treated in Theorem 1.2,
(b) the case when m is small (hence, we can fix m), and
(c) the case when n is small (hence, we can fix n).

We will use the following simple result repeatedly for the proof of Theorem 1.8. It plays the role of the condition (6.3) in the proof of Theorem 1.2.

Lemma 7.1. *Assume φ is dynamically unramified over $t \in \mathbb{P}^1(\overline{K})$. Then there is a positive integer $i \le 2d^3$ and $\gamma \in \overline{K}$ such that:*

- $\varphi^i(\gamma) = t$,
- *φ^i is unramified at γ, and*
- *φ^3 is unramified over γ.*

Proof. Since φ is dynamically unramified over t, there is a backward orbit of distinct elements $t_0 = t, t_1, t_2, \ldots, t_{2d^3} \in \mathbb{P}^1(\overline{K})$ such that $\varphi(t_j) = t_{j-1}$ and φ is unramified at t_j for $1 \le j \le 2d^3$. Since φ^3 has at most $2d^3 - 2$ critical values, there are at least 2 elements in $\{t_1, \ldots, t_{2d^3}\}$ that are not critical value of φ^3. Let t_i be such an element that is not ∞. This t_i is our desired γ. □

7.1. **The case of Theorem 1.8 when m is small.** We *fix* m such that $m \in A_1(\varphi, \alpha)$ and $\varphi^m(\alpha) \neq \infty$. Then we prove that for all sufficiently large n, there is $\mathfrak{p}$ such that α has squarefree portrait (m, n) modulo $\mathfrak{p}$.

Proposition 7.2. *In the number field case, assume Conjecture 4.1. Let φ, d, S, $\widehat{h}$, $\tau > 0$, $\alpha \in \mathbb{P}^1(K)$ be as in Theorem 1.8. Let $m \in A_1(\varphi, \alpha)$ such that $\varphi^m(\alpha) \neq \infty$. We have the following:*

(a) *If $m = 0$, there exists $C_{47}(\tau, N_S)$ such that for every $n > C_{47}(\tau, N_S)$, there is a prime $\mathfrak{p} \notin S$ such that α is periodic modulo $\mathfrak{p}$ with exact period n and $\operatorname{ord}_{\mathfrak{p}}(\varphi^n(\alpha) - \alpha) = 1$ (i.e. α has squarefree portrait $(0, n)$ modulo $\mathfrak{p}$).*

(b) *If $m \geq 1$, there exists $C_{48}(\tau, N_S, m)$ such that for every $n > C_{48}(\tau, N_S, m)$, there is a prime $\mathfrak{p} \notin S$ such that α has squarefree portrait (m, n) modulo $\mathfrak{p}$.*

Proof. If φ^4 is unramified over $\varphi^m(\alpha)$, Theorem 6.4 gives the desired conclusion. Let $\{b_1, \dots, b_k\}$ denote the (possibly empty) set of critical values of φ^4 in K; this set depends only on φ and K. It remains to treat the case $\varphi^m(\alpha) \in \{b_1, \dots, b_k\}$.

Let $n \in \mathbb{Z}_{>0}$ such that $\varphi^{m+n}(\alpha) \neq \infty$. If $m \geq 1$, there is $\eta \in \mathbb{P}^1(\overline{K})$ such that $\eta \neq \varphi^{m-1}(\alpha)$, $\varphi(\eta) = \varphi^m(\alpha) = b_1$, φ is unramified at η and dynamically unramified over η. By Lemma 7.1, there exist an integer i such that $1 \leq i - 1 \leq 2d^3$ and $\gamma \in \overline{K}$ satisfying the following: $\varphi^{i-1}(\gamma) = \eta$, φ^{i-1} is unramified at γ, and φ^3 is unramified over γ. This last condition means the function $\varphi^3(x) - \gamma$ has d^3 distinct zeros.

Similarly, if $m = 0$, by Lemma 7.1 and the fact that φ is dynamically unramified over α, there exists a positive integer i such that $i \leq 2d^3$ and an element $\gamma \in \overline{K}$ satisfying the following: $\varphi^i(\gamma) = \alpha$, φ^i is unramified at γ, and φ^3 is unramified over γ.

In both cases ($m = 0$ and $m \geq 1$), we have that $i \leq 2d^3 + 1$. We recall that $\varphi^m(\alpha)$ belongs to the list $\{b_1, \dots, b_k\}$ which depends only on φ and K. Hence when $m \geq 1$ (respectively $m = 0$) the triple (i, η, γ) (respectively, the pair (i, γ)) belongs to a finite set that depends only on K and φ. Hence we may replace K by $K(\gamma)$ since every constant that depends on φ, $K(\gamma)$, and other data (such as S, τ,...) will ultimately depend on φ, K, and the exact same data. In other words, we may assume $\gamma \in K$. Then we can write:

$$\varphi^i(x) - \varphi^m(\alpha) = \frac{(x - \gamma)F(x)}{G(x)}$$

where $F(x), G(x) \in K[x]$ with $F(\gamma)G(\gamma) \neq 0$ and $\gcd(F(x), G(x)) = 1$. We also require that $G(x)$ is monic; hence the pair (F, G) is determined uniquely.

Write $F(x) = c\prod_{j=1}^{r}(x - f_j)$ and $G(x) = \prod_{k=1}^{s}(x - g_k)$. Let $S' \subset M_K^0$ be the finite set of primes $\mathfrak{p}$ satisfying one of the following conditions:

- $|c|_{\mathfrak{p}} \neq 1$
- $|\gamma - f_j|_{\mathfrak{p}} \neq 1$ for some j.
- $|\gamma - g_k|_{\mathfrak{p}} \neq 1$ for some k.

The point is that for every $z \in K$ that is not a zero or pole of $\varphi^i(x) - \varphi^m(\alpha)$ and for every $\mathfrak{p} \in M_K^0 \setminus S'$, if $\operatorname{ord}_{\mathfrak{p}}(z - \gamma) > 0$ then $\operatorname{ord}_{\mathfrak{p}}(\varphi^i(z) - \varphi^m(\alpha)) = \operatorname{ord}_{\mathfrak{p}}(z - \gamma)$. As argued before, the list of possibilities for S' depends only on φ and K. Hence there is C_{49} such that:

$$\sum_{\mathfrak{p} \in S'} N_{\mathfrak{p}} \leq C_{49} \tag{7.3}$$

Applying Corollary 4.20 and Corollary 5.11 (for $\ell = 3$, $\epsilon = 1$, $b = \gamma$, and $a = \varphi^{m+n-i-3}(\alpha)$), there exist positive constants C_{50}, C_{51}, and C_{52} such that when $m+n-i-3 \geq C_{50}$, we have $\varphi^{m+n-i-3}(\alpha) \neq \infty$ and the set $\mathcal{D} := \{\mathfrak{p} \in M_K^0 : \operatorname{ord}_{\mathfrak{p}}(\varphi^{m+n-i}(\alpha) - \gamma) \geq 1\}$ satisfies:

$$\sum_{\mathfrak{p}\in\mathcal{D}} N_{\mathfrak{p}} \geq (d^3-3)h_K(\varphi^{m+n-i-3}(\alpha)) - C_{51}h_K(\gamma) - C_{52}. \tag{7.4}$$

Let $\mathcal{D}_{(1)} := \{\mathfrak{p} \in M_K^0 : \operatorname{ord}_{\mathfrak{p}}(\varphi^{m+n-i}(\alpha)-\gamma) = 1\}$. After rewriting inequality (7.4) and using $\widehat{h}(\gamma) = \dfrac{\widehat{h}(\alpha)}{d^i}$, we have:

$$\sum_{\mathfrak{p}\in\mathcal{D}_{(1)}} N_{\mathfrak{p}} + \sum_{\mathfrak{p}\in\mathcal{D}\setminus\mathcal{D}_{(1)}} N_{\mathfrak{p}} \geq (d^3-3)d^{m+n-i-3}\widehat{h}(\alpha) - C_{53}\widehat{h}(\alpha) - C_{54}. \tag{7.5}$$

On the other hand, we have:

$$\sum_{\mathfrak{p}\in\mathcal{D}_{(1)}} N_{\mathfrak{p}} + 2\sum_{\mathfrak{p}\in\mathcal{D}\setminus\mathcal{D}_{(1)}} N_{\mathfrak{p}} \leq h_K(\varphi^{m+n-i}(\alpha)-\gamma) \leq d^{m+n-i}\widehat{h}(\alpha) + \widehat{h}(\alpha) + C_{55} \tag{7.6}$$

Inequalities (7.5) and (7.6) imply:

$$\sum_{\mathfrak{p}\in\mathcal{D}_{(1)}} N_{\mathfrak{p}} \geq (d^3-6)d^{m+n-i-3}\widehat{h}(\alpha) - C_{56}\widehat{h}(\alpha) - C_{57}. \tag{7.7}$$

Let $\mathcal{E}$ be the set of primes $\mathfrak{p} \in M_K^0$ of good reduction such that $r_{\mathfrak{p}}(\varphi^m(\alpha)) = r_{\mathfrak{p}}(\varphi^{m+n'}(\alpha))$ for some $1 \leq n' < n$ with $n' \mid n$. By the same arguments giving (6.11) and (6.12), we have:

$$\begin{aligned}\sum_{\mathfrak{p}\in\mathcal{E}} N_{\mathfrak{p}} &\leq \sum_{\text{prime } p\mid n} (2h_K(\varphi^m(\alpha)) + h_K(\varphi^{m+\frac{n}{p}}(\alpha)) + C_{58}) \\ &\leq (2d^m\widehat{h}(\alpha) + d^{m+\frac{n}{2}}\widehat{h}(\alpha) + C_{59})\log_2 n \leq d^{m+\frac{2n}{3}}\widehat{h}(\alpha)\end{aligned} \tag{7.8}$$

when n is larger than some constant $C_{60}(\tau)$. Since $i \leq 2d^3+1$, the term $(d^3-6)d^{m+n-i-3}$ dominates the term $d^{m+\frac{2n}{3}}$ when n is sufficiently large.

If $m = 0$, from (7.3),(7.7), and (7.8), there exists $C_{61}(\tau, N_S)$ such that

$$\sum_{\mathfrak{p}\in\mathcal{D}_{(1)}} N_{\mathfrak{p}} - \sum_{\mathfrak{p}\in\mathcal{E}} N_{\mathfrak{p}} - \sum_{\mathfrak{p}\in S'} N_{\mathfrak{p}} - N_S > 0$$

when $n > C_{61}(\tau, N_S)$. Consequently, there is $\mathfrak{p} \in \mathcal{D}_{(1)} \setminus (\mathcal{E} \cup S' \cup S)$. Since $\mathfrak{p} \in \mathcal{D}_{(1)} \setminus S'$, we have:

$$\operatorname{ord}_{\mathfrak{p}}(\varphi^n(\alpha) - \alpha) = \operatorname{ord}_{\mathfrak{p}}(\varphi^{n-i}(\alpha) - \gamma) = 1.$$

Since $\mathfrak{p} \notin S'$, we have that when reducing modulo $\mathfrak{p}$, the period of α must be exactly n. This proves part (a).

If $m \geq 1$, let $\mathcal{E}_1 := \{\mathfrak{p} \in M_K^0 : r_{\mathfrak{p}}(\eta) = r_{\mathfrak{p}}(\varphi^{m-1}(\alpha))\}$. Since $\eta \neq \varphi^{m-1}(\alpha)$ and $\varphi(\eta) = \varphi^m(\alpha)$, inequality (3.1) gives:

$$\sum_{\mathfrak{p}\in\mathcal{E}_1} N_{\mathfrak{p}} \leq 3d^{m-1}\widehat{h}(\alpha) + C_{62}. \tag{7.9}$$

From (7.3),(7.7),(7.8), and (7.9), there exists $C_{63}(\tau, N_S, m)$ such that

$$\sum_{\mathfrak{p}\in\mathcal{D}_{(1)}} N_{\mathfrak{p}} - \sum_{\mathfrak{p}\in\mathcal{E}} N_{\mathfrak{p}} - \sum_{\mathfrak{p}\in\mathcal{E}_1} N_{\mathfrak{p}} - \sum_{\mathfrak{p}\in S'} N_{\mathfrak{p}} - N_S > 0$$

when $n > C_{63}(\tau, N_S, m)$. Consequently, there is $\mathfrak{p} \in \mathcal{D}_{(1)} \setminus (\mathcal{E} \cup \mathcal{E}_1 \cup S' \cup S)$. By similar arguments in the case $m = 0$, we have $\operatorname{ord}_{\mathfrak{p}}(\varphi^{m+n}(\alpha) - \varphi^m(\alpha)) = 1$ and $\varphi^m(\alpha)$ is periodic with exact period n modulo $\mathfrak{p}$. It remains to show that $\varphi^{m-1}(\alpha)$ is not periodic modulo $\mathfrak{p}$. Since $\mathfrak{p} \notin \mathcal{E}_1$ and $r_{\mathfrak{p}}(\varphi^{m+n-i}(\alpha)) = r_{\mathfrak{p}}(\gamma)$, we have $r_{\mathfrak{p}}(\varphi^{m+n-1}(\alpha)) = r_{\mathfrak{p}}(\eta) \neq r_{\mathfrak{p}}(\varphi^{m-1}(\alpha))$. This finishes the proof. □

As an application of Proposition 7.2, we can now prove that the set $\mathbb{Z}_{>0} \setminus A_2(\varphi)$ is finite:

Proposition 7.10. *Let F be a field of characteristic 0, let $\varphi(x) \in F(x)$ with $d := \deg(\varphi) \geq 2$, and let $\alpha \in \mathbb{P}^1(F)$ that is not φ-preperiodic. Then the sets $\mathbb{Z}_{\geq 0} \setminus A_1(\varphi, \alpha)$ and $\mathbb{Z}_{>0} \setminus A_2(\varphi)$ are finite.*

Proof. Since replacing F by $\overline{F}$ does not change $A_1(\varphi, \alpha)$ and $A_2(\varphi)$, we may assume $F = \overline{F}$.

It is easy to show that $\mathbb{Z}_{>0} \setminus A_1(\varphi, \alpha)$ is finite, as follows. Let $c_1, \ldots, c_k$ be the distinct critical values of φ; we have $k \leq 2d - 2$. Let $\mathcal{O}_i := \{\varphi^n(c_i) : n \geq 0\}$ for $1 \leq i \leq k$. If $\varphi^m(\alpha)$ is not a critical value of φ^3 then the set

$$A := (\varphi^3)^{-1}(\varphi^m(\alpha)) \setminus (\varphi^2)^{-1}(\varphi^{m-1}(\alpha))$$

has $d^3 - d^2$ elements. Since α is not preperiodic, $\mathcal{O}_i \cap A$ has at most one element for each $1 \leq i \leq k$. And since $k \leq 2d - 2 < d^3 - d^2$, there is $\gamma \in A$ that does not belong to any $\mathcal{O}_i$. By choosing $\eta = \varphi^2(\gamma) \neq \varphi^{m-1}(\alpha)$, we have verified that $m \in A_1(\varphi, \alpha)$.

Now we prove that $\mathbb{Z}_{>0} \setminus A_2(\varphi)$ is finite. We consider the function field $K = F(t)$, the isotrivial function $\varphi(t) \in K(t)$, and the starting point $\alpha = t \in K$. By a direct computation, we have $\widehat{h}_{\varphi,K}(\alpha) = 1$. Let $\tau = 1$ and let S be the singleton whose element is the place at infinity of $K = F(t)$ (i.e. the place corresponding the point ∞ in $\mathbb{P}^1(F)$). Fix $m = 0$, then Proposition 7.2 gives that for all sufficiently large n, there is $\mathfrak{p} \in M_K \setminus S$ such that α has squarefree portrait (m, n) modulo $\mathfrak{p}$. In other words, if $\beta \in F$ is the point on $\mathbb{P}^1(F)$ corresponding $\mathfrak{p}$ then we have:

- β is period of exact period n under the function φ, and
- $t - \beta$ is a squarefree factor of $\varphi^n(t) - t$.

As above, $\mathcal{O}_i$ for $1 \leq i \leq k$ denotes the critical orbits. Among all (possibly none) of the $\mathcal{O}_i$'s that are finite (equivalently, c_i is preperiodic), let N be the maximum of the sizes of the periodic cycles. If we require further that $n > N$ then β is not contained in any $\mathcal{O}_i$. This implies $n \in A_2(\varphi)$. □

7.2. **The case of Theorem 1.8 when n is small.** Fix $n \in A_2(\varphi)$. Then we prove that for all sufficiently large m, there is $\mathfrak{p} \in M_K \setminus S$ such that α has squarefree portrait (m, n) modulo $\mathfrak{p}$.

Proposition 7.11. *In the number field case, assume Conjecture 4.1. Let φ, d, S, $\widehat{h}$, τ, and $\alpha \in \mathbb{P}^1(K)$ be as in Theorem 1.8. Let $n \in A_2(\varphi)$. There exist a positive constant $C_{64}(\tau, N_S, n)$ such that the following holds. For every $m > C_{64}(\tau, N_S, n)$, if $\infty \notin \{\varphi^m(\alpha), \varphi^{m+n}(\alpha)\}$ then there is $\mathfrak{p} \in M_K \setminus S$ such that α has squarefree portrait (m, n) modulo $\mathfrak{p}$.*

Proof. The proof uses similar arguments in the proof of Proposition 7.2 so we will be brief. Let β and η be as in Definition 1.5(ii). By Lemma 7.1, there is an integer i with $1 \leq i - 1 \leq 2d^3$ and $\gamma \in \overline{K}$ such that $\varphi^{i-1}(\gamma) = \eta$, φ^{i-1} is unramified at

γ and φ^3 is unramified over γ. As in the proof of Proposition 7.2, since the data (β, η, i, γ) belong to a finite set depending only on φ, n, and K, after extending K if necessary, we may assume that $\gamma \in K$.

Now $x - \gamma$ is a squarefree factor of $\varphi^i(x) - \beta$. Since $x - \beta$ is a squarefree factor of $\varphi^n(x) - x$, we have:

$$\varphi^{n+i}(x) - \varphi^i(x) = \frac{(x-\gamma)F(x)}{G(x)}$$

with $F(x), G(x) \in K[x]$, $F(\gamma)G(\gamma) \neq 0$, and $\gcd(F, G) = 1$. As before, choose G to be monic so that the pair (F, G) is uniquely determined.

As in the proof of Proposition 7.2, we have a finite subset S' of M_K^0 depending on K, φ, n, and i such that for every $\mathfrak{p} \in M_K^0 \setminus S'$ and every $z \in K$ that is not a zero of $(x-\gamma)F(x)G(x)$, if $\mathrm{ord}_{\mathfrak{p}}(z-\gamma) > 0$ then $\mathrm{ord}_{\mathfrak{p}}(\varphi^{n+i}(z) - \varphi^i(z)) = \mathrm{ord}_{\mathfrak{p}}(z-\gamma)$.

Let $m \in \mathbb{Z}_{\geq 0}$ such that $m \geq i+3$ and $\infty \neq \varphi^{m-i}(\alpha)$. As in the proof of Proposition 7.2, we can define the following sets:

$$\mathcal{D}_{(1)} := \{\mathfrak{p} \in M_K^0 : \ \mathrm{ord}_{\mathfrak{p}}(\varphi^{m-i}(\alpha) - \gamma) = 1\},$$

$$\mathcal{E} := \{\mathfrak{p} \in M_K^0 : \ r_{\mathfrak{p}}(\beta) = r_{\mathfrak{p}}(\varphi^{n'}(\beta)) \text{ for some } 1 \leq n' < n\},$$

$$\mathcal{E}_1 := \{\mathfrak{p} \in M_K^0 : \ r_{\mathfrak{p}}(\eta) = r_{\mathfrak{p}}(\varphi^{n-1}(\beta))\}.$$

Then we can prove that when m is sufficiently large, there is $\mathfrak{p} \in \mathcal{D}_{(1)} \setminus (\mathcal{E} \cup \mathcal{E}_1 \cup S' \cup S)$. This gives:

- $\mathrm{ord}_{\mathfrak{p}}(\varphi^{m+n}(\alpha) - \varphi^m(\alpha)) = 1$ since $\mathfrak{p} \in \mathcal{D}_{(1)} \setminus S'$.
- $r_{\mathfrak{p}}(\varphi^m(\alpha)) = r_{\mathfrak{p}}(\varphi^i(\gamma)) = r_{\mathfrak{p}}(\beta)$ which has exact period n since $\mathfrak{p} \notin \mathcal{E}$.
- $r_{\mathfrak{p}}(\varphi^{m-1}(\alpha)) = r_{\mathfrak{p}}(\varphi^{i-1}(\gamma)) = r_{\mathfrak{p}}(\eta) \neq r_{\mathfrak{p}}(\varphi^{n-1}(\beta))$, hence $\varphi^{m-1}(\alpha)$ is not periodic modulo $\mathfrak{p}$.

This finishes the proof. □

References

[Bak09] M. Baker, *A finiteness theorem for canonical heights attached to rational maps over function fields*, J. reine angew. Math **626** (2009), 205–233.

[Ban86] A. S. Bang, *Taltheoretiske Undersogelse*, Tidsshrift Mat. **4** (1886) 70–80, 130–137.

[BG06] E. Bombieri and W. Gubler, *Heights in Diophantine Geometry*, New Mathematical Monograph, Cambridge Univ. Press, Cambridge **3** (2006),

[BIJ+15] 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 postcritically finite morphisms*, to appear in Math. Res. Lett..

[CS93] G. S. Call and J. H. Silverman, *Canonical heights on varieties with morphisms*, Compositio Math. **89** (1993), 163–205.

[DH12] K. Doerksen and A. Haensch, *Primitive prime divisors in zero orbits of polynomials*, Integers **12** (2012), 7pp.

[DH85] A. Douady and J. H. Hubbard, *Étude dynamique des polynômes complexes. Partie II*, Publications Mathématiques d'Orsay [Mathematical Publications of Orsay], vol. 85, Université de Paris-Sud, Département de Mathématiques, Orsay, 1985, With the collaboration of P. Lavaurs, Tan Lei and P. Sentenac

[Doy] J. Doyle, *Preperiodic portraits for unicritical polynomials over a rational function field*, preprint, arXiv:1603.08138.

[Doy16] J. Doyle, *Preperiodic portraits for unicritical polynomials*, Proc. Amer. Math. Soc. **144** (2016), 2885–2899.

[EMW06] G. Everest, G. Mclaren, and T. Ward, *Primitive divisors of elliptic divisibility sequences*, J. Number Theory **118** (2006), 71–89.

[FG11] X. Faber and A. Granville, *Prime factors of dynamical sequences*, J. Reine Angew. Math. **661** (2011), 189–214.

[GNT15] D. Ghioca, K. Nguyen, and T. J. Tucker, *Portraits of preperiodic points for rational maps*, Math. Proc. Cambridge Philos. Soc. **159** (2015), 165–186.

[GNT13] C. Gratton, K. Nguyen, and T. J. Tucker, *ABC implies primitive prime divisors in arithmetic dynamics*, Bull. London Math. Soc. **45** (2013), 1194–1208.

[Ing07] P. Ingram, *Elliptic divisibility sequences over certain curves*, J. Number Theory **123** (2007), 473–486.

[IS09] P. Ingram and J. H. Silverman, *Primitive divisors in arithmetic dynamics*, Math. Proc. Cambridge Philos. Soc. **146** (2009), 289–302.

[Jon13] Rafe Jones, *Galois representations from pre-image trees: an arboreal survey*, Pub. Math. Besançon. (2013), 107–136.

[Juu15] J. Juul, *Iterates of generic polynomials and generic rational functions*, available at arXiv:1410.3814, 2015.

[Kri13] H. Krieger, *Primitive prime divisors in the critical orbit of* $z^d + c$, Int. Math. Res. Not. *IMRN* (2013), No. 23, 5498–5525.

[Odo85] R. W. K. Odoni, *The Galois theory of iterates and composites of polynomials*, Proc. London Math. Soc. (3) **51** (1985), no. 3, 385–414.

[Sch74] A. Schinzel, *Primitive divisors of the expression* $a^n - b^n$ *in algebraic number fields*, J. Reine Angew. Math. **268/269** (1974), 27–33.

[Sil07] J. H. Silverman, *The arithmetic of dynamical systems*, Graduate Texts in Mathematics **241**, Springer, New York, 2007, 511 pp.

[Sil13] J. H. Silverman, *Primitive divisors, dynamical Zsigmondy sets, and Vojta's conjecture*, J. Number Theory **133** (2013), 2948–2963.

[Sto92] M. Stoll, *Galois groups over* $\mathbf{Q}$ *of some iterated polynomials*, Arch. Math. (Basel) **59** (1992), no. 3, 239–244.

[Voj11] P. Vojta, *Diophantine approximation and Nevanlinna theory*, Arithmetic Geometry. Lectures given at the C.I.M.E. summer school held in Cetraro, Italy, September 10–15, 2007, Lecture Notes in Math., no. 2009, Springer-Verlag, 2011, pp. 111–230.

[Yam04] K. Yamanoi, *The second main theorem for small functions and related problems*, Acta Math. **192** (2004), 225–294.

[Zsi92] K. Zsigmondy, *Zur theorie der Potenzreste*, Monatsh. Math. Phys. **3** (1892), 265–284.

Dragos Ghioca, Department of Mathematics, University of British Columbia, Vancouver, BC V6T 1Z2, Canada

E-mail address: dghioca@math.ubc.ca

Khoa D. Nguyen Department of Mathematics, University of British Columbia, Vancouver, BC V6T 1Z2, Canada

E-mail address: dknguyen@math.ubc.ca

Thomas Tucker, Department of Mathematics, University of Rochester, Rochester, NY 14627, USA

E-mail address: thomas.tucker@rochester.edu