TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 370, Number 9, September 2018, Pages 6391–6410
http://dx.doi.org/10.1090/tran/7125
Article electronically published on March 20, 2018

AVERAGE ZSIGMONDY SETS, DYNAMICAL GALOIS GROUPS, AND THE KODAIRA-SPENCER MAP

WADE HINDES

Abstract. Let K be a global function field and let $\phi(x) \in K[x]$. For all wandering basepoints $b \in K$, we show that there is a bound on the size of the elements of the dynamical Zsigmondy set $\mathcal{Z}(\phi, b)$ that depends only on ϕ, the poles of the b, and K. Moreover, when we order $b \in \mathcal{O}_{K,S}$ by height, we show that $\mathcal{Z}(\phi, b)$ is empty on average. As an application, we prove that the inverse limit of the Galois groups of iterates of $\phi(x) = x^d + f$ is a finite index subgroup of an iterated wreath product of cyclic groups. In particular, since our methods translate to rational function fields in characteristic zero, we establish the inverse Galois problem for these groups via specialization.

1. Introduction

Given a rational map $\phi(x) \in K(x)$ over a global field K and a basepoint $b \in \mathbb{P}^1(K)$, we study the prime factors of $\phi^n(b)$ as we iterate ϕ. Specifically, we are interested in knowing whether or not $\phi^n(b)$ has a primitive prime factor, that is, whether or not there is a prime dividing $\phi^n(b)$ that does not divide any lower order iterates. This problem is analogous to a classical problem of Bang [2], Zsigmondy [49], and Schinzel [33] on the prime factorization of integer sequences defined dynamically on the multiplicative group.

Our motivation for studying primitive prime divisors comes from the Galois theory of iterates. For instance, in the family $\phi_f(x) = x^d + f$, the existence of d-power free primitive prime divisors in the orbit of zero implies a dynamical version of Serre's open image theorem ([8, Theorem 25], [17, Theorem 3.3] and [35]), and we prove this over global function fields.

To begin, we fix some notation. Let K be a global field and let V_K be a complete set of valuations on K (corresponding to prime ideals). We say that $v \in V_K$ is a *primitive prime divisor* of $\phi^n(b)$ if

$$v(\phi^n(b)) > 0 \ \text{ and } \ v(\phi^m(b)) = 0 \text{ for all } 1 \leq m \leq n-1$$

such that $\phi^m(b) \neq 0$. Likewise, we define the *Zsigmondy set* of ϕ and b to be

$$\mathcal{Z}(\phi, b) := \{n \mid \phi^n(b) \text{ has no primitive prime divisors}\}.$$

Over number fields, there are many results regarding the finiteness and size of $\mathcal{Z}(\phi, b)$ in special families; see for example [7, 14, 15, 24, 41]. However, it remains difficult to bound $\mathcal{Z}(\phi, b)$ in general. Nevertheless, over function fields $K/\mathbb{F}_q(t)$, we

---

Received by the editors May 11, 2016, and, in revised form, June 18, 2016 and November 15, 2016.

2010 *Mathematics Subject Classification.* Primary 37P15, 11R32; Secondary 11B37, 14G05, 11G99.

Key words and phrases. Arithmetic dynamics, rational points on curves, Galois theory.

show that there is a bound on $\#\mathcal{Z}(\phi,b)$ depending only on ϕ, the poles of b, and on K; see Theorem 1.1.

The main technique we use to prove this result is to associate to every element of $\mathcal{Z}(\phi,b)$ a rational point on some curve, and then use height bounds for points on curves to bound the size of the corresponding element of the Zsigmondy set. As one may expect, there are certain complications that arise in characteristic $p>0$ if the associated curve is defined over the field of constants. Therefore, we need the following geometric condition:

Definition 1. Let $K/\mathbb{F}_q(t)$ and $\ell\geq 2$ be an integer coprime to the characteristic of K. Then we say that ϕ is dynamically ℓ-power non-isotrivial if there exists an integer $m\geq 1$ such that

$$C_{\ell,m}(\phi): Y^\ell=\phi^m(X)=(\underbrace{\phi\circ\phi\circ\cdots\circ\phi}_{m})(X) \tag{1}$$

is a non-isotrivial curve (meaning that the associated Kodaira-Spencer map is non-zero on some open set [28]) of genus at least 2. As a motivating example, we show that $\phi_f(x)=x^d+f$ is dynamically 2-power and d-power non-isotrivial over $K=\mathbb{F}_p(t)$; see Theorem 1.5. Moreover, we show that most quadratic polynomials are dynamically 2-power non-isotrivial in Corollary 1.2.

In particular, if $S\subseteq V_K$ is any finite subset, $\mathcal{O}_{K,S}$ is the ring of S-integers of K, and ϕ is dynamically ℓ-power non-isotrivial for some $\ell\geq 2$, then we show that

$$\mathcal{Z}(\phi,S):=\big\{n\,|\,n\in\mathcal{Z}(\phi,b)\text{ for some }b\in\mathcal{O}_{K,S},\ \hat{h}_\phi(b)>0\big\} \tag{2}$$

is finite; in particular, $\#\mathcal{Z}(\phi,b)$ is uniformly bounded over all $b\in\mathcal{O}_{K,S}$. Moreover, we prove an analogous result when $K=\mathbb{Q}$ or K is an imaginary quadratic field, assuming the Vojta conjecture.

On the other hand, one expects that $\mathcal{Z}(\phi,b)$ is empty if we choose the basepoint $b\in K$ "at random". A reasonable interpretation of this statement can be formulated in terms of averages. To wit, for all $B\geq 0$, let $\mathcal{O}_{K,S}(B)$ be the set of points of $\mathcal{O}_{K,S}$ of height at most B, a finite set by the Northcott property [42, Theorem 3.7]. Then we study the average

$$\overline{\operatorname{Avg}}(\mathcal{Z}(\phi),S):=\limsup_{B\to\infty}\frac{\sum_{b\in\mathcal{O}_{K,S}(B)}\#\mathcal{Z}(\phi,b)}{\#\mathcal{O}_{K,S}(B)} \tag{3}$$

as we vary over all $b\in\mathcal{O}_{K,S}$. In particular, we show that $\overline{\operatorname{Avg}}(\mathcal{Z}(\phi),S)=0$ for all S; in other words, the naive heuristic is correct: one expects to see primitive prime divisors at every stage of iteration. Both the uniform bound and average-result are summarized below (in what follows, $\operatorname{Per}(\phi)$ and $\operatorname{PrePer}(\phi)$ denote the set of periodic and preperiodic points of ϕ, respectively):

Theorem 1.1. *Let $\phi(x)\in K[x]$ be such that $\deg(\phi)\geq 2$ and $0\notin\operatorname{Per}(\phi)$.*

(1) *If $K/\mathbb{F}_q(t)$ and ϕ is dynamically ℓ-power non-isotrivial for some $\ell\geq 2$, then $\mathcal{Z}(\phi,S)$ is finite and $\overline{\operatorname{Avg}}(\mathcal{Z}(\phi),S)=0$.*

(2) *When $K=\mathbb{Q}$ or K is a quadratic imaginary field, we have the following cases.*

(a) *If* $0 \in \mathrm{PrePer}(\phi)$, *then* $\mathcal{Z}(\phi, S)$ *is finite and* $\overline{\mathrm{Avg}}(\mathcal{Z}(\phi), S) = 0$.

(b) *If* $0 \notin \mathrm{PrePer}(\phi)$ *and the Vojta conjecture* [47, Conj. 25.1] *holds, then* $\mathcal{Z}(\phi, S)$ *is finite and* $\overline{\mathrm{Avg}}(\mathcal{Z}(\phi), S) = 0$.

In other words, there is a bound on the elements of $\mathcal{Z}(\phi, b)$ *depending only on* ϕ, *the poles of* b, *and* K. *Moreover, if we order* $\mathcal{O}_{K,S}$ *by height, then* $\mathcal{Z}(\phi, b)$ *is empty on average.*

For quadratic polynomials $\phi(x) = (x-\gamma)^2 + c \in K[x]$, the curve $C_{2,m}(\phi)$ for $m \geq 2$ maps to the elliptic curve

$$E_\phi : Y^2 = (X - c) \cdot \phi(X) \tag{4}$$

via $(X, Y) \to \big(\phi^{m-1}(X), Y \cdot (\phi^{m-2}(X) - \gamma)\big)$. In particular, if the j-invariant [39, III.1 Prop. 1.4] of E_ϕ is non-constant, then it follows from [11, Proposition 3.3] that $C_{2,m}(\phi)$ is non-isotrivial for all $m \geq 2$; see Remark 2.10 below. Therefore, we have an explicit form of Theorem 1.1 in the quadratic case:

Corollary 1.2. *Let* $K/\mathbb{F}_q(t)$ *be a finite extension of odd characteristic. For all monic, quadratic polynomials* $\phi(x) \in K[x]$, *write* $\phi(x) = (x-\gamma)^2 + c$ *by completing the square. If* $\phi(\gamma) \cdot \phi^2(\gamma) \neq 0$ *and the quantity*

$$\left(\frac{27}{1728}\right) \cdot j(E_\phi) = \frac{-\gamma^6 + 6\gamma^5 c - 15\gamma^4 c^2 + 9\gamma^4 c + 20\gamma^3 c^3 - 36\gamma^3 c^2 + \cdots + 27c^3}{\gamma^4 c - 4\gamma^3 c^2 + 6\gamma^2 c^3 + 2\gamma^2 c^2 - 4\gamma c^4 - 4\gamma c^3 + c^5 + 2c^4 + c^3}$$

is non-constant, then ϕ *is dynamically* 2*-power non-isotrivial. Hence,* $\mathcal{Z}(\phi, S)$ *is finite and* $\overline{\mathrm{Avg}}(\mathcal{Z}(\phi), S) = 0$ *for all* S.

By analogy with the function field case, we conjecture that Theorem 1.1 holds over all number fields without assuming the Vojta conjecture or that 0 is preperiodic.

Conjecture 1.3. *Let* $K/\mathbb{Q}$ *and* $\phi(x) \in K[x]$ *be a polynomial of degree* $d \geq 2$. *If* $\phi(x) \neq c \cdot x^d$, *then* $\mathcal{Z}(\phi, S)$ *is finite and* $\overline{\mathrm{Avg}}(\mathcal{Z}(\phi), S) = 0$ *for all finite subsets* $S \subseteq V_K$.

As for the key condition over function fields, we expect that most rational functions $\phi \in K(x)$ are dynamically ℓ-power non-isotrivial for some $\ell \geq 2$. In fact, it is likely that one can choose many such exponents.

Conjecture 1.4. *Suppose that* $\phi(x) \in K[x] \backslash \overline{\mathbb{F}}_p[x]$ *satisfies the following conditions:*

(1) $\deg(\phi) \geq 2$,

(2) $\gcd(\deg(\phi), p) = 1$,

(3) $\phi(x) \neq c \cdot x^d$ *for all* $c \in \overline{\mathbb{F}}_p$.

Then there exists $\ell \geq 2$ *and* $m \geq 1$, *such that* $\gcd(\ell, p) = 1$ *and* $C_{\ell,m}(\phi) : Y^\ell = \phi^m(X)$ *is a non-isotrivial curve of genus at least* 2.

As an application of Theorem 1.1, we study dynamical Galois groups. For $n \geq 1$, let $K_n(\phi)$ be the field obtained by adjoining all solutions of $\phi^n(x) = 0$ to K. Generically, the extension $K_n(\phi)/K$ is Galois, and we let $G_{K,n}(\phi) := \mathrm{Gal}_K(\phi^n)$ be the Galois group of $K_n(\phi)/K$. Since $K_{n-1}(\phi) \subseteq K_n(\phi)$ for all $n \geq 1$ (under some mild separability assumptions), we may define

$$G_K(\phi) = \varprojlim G_{K,n}(\phi) \tag{5}$$

with respect to the restriction maps. Dynamical analogs on $\mathbb{P}^1$ of the Galois representations attached to abelian varieties [35] (where one instead considers iterated preimages of multiplication maps), the groups $G_K(\phi)$ have obtained much attention in recent years; for instance, see [3, 12, 16, 29, 30, 45], among other places.

Of course, a key difference in this setting is the lack of group structure on projective space, and as such $G_K(\phi)$ may often only be viewed as a subgroup of a wreath product (or the automorphism group of a tree) and not inside a group of matrices. Explicitly, let $T(d)$ denote the infinite d-ary rooted tree. If we write $\phi^n = f_n/g_n$ for some $f_n, g_n \in K[x]$ such that $\operatorname{disc}(f_n) \neq 0$ for all $n \geq 1$, then we may identify $T(d)$ with the set of iterated preimages of zero (under ϕ) in $\overline{K}$ with the edge relation given by evaluation; see [3] for more details. In particular, $G_K(\phi) \leq \operatorname{Aut}(T(d))$, since Galois commutes with evaluation.

As in the case of abelian varieties, one expects that $G_K(\phi)$ is a large subgroup of $\operatorname{Aut}(T(d))$. However, given the unruly nature of $\operatorname{Aut}(T(d))$ and its subgroups, we focus our attention on polynomials of a special form. To do this, fix a faithful permutation representation of the cyclic group $C_d \leq \mathrm{S}_d$ and let $W(d)$ be the infinite iterated wreath product of C_d acting on $T(d)$; see [27] or [20, Defs. 2.3 and 2.4]. In particular, if μ_d is the group of d-th roots of unity in $\overline{K}$ and $\phi_f(x) = x^d + f$ for some $f \in K$, then we have the refinement $G_{K(\mu_d)}(\phi_f) \leq W(d) \leq \operatorname{Aut}(T(d))$; see [20, Lemma 2.5]. Moreover, it follows from Theorem 1.1 and some calculations involving the Kodaira-Spencer map of $C_{m,\ell}(\phi)$, that $G_{K(\mu_d)}(\phi_f) \leq W(d)$ is a finite index subgroup:

Theorem 1.5. *Let $K = \mathbb{F}_p(t)$, let $f \in K$ and let let $d \geq 2$ be coprime to p. If $f \notin K^p$ and $\phi(x) = x^d + f$, then ϕ is dynamically d-power non-isotrivial and:*

(1) *$\mathcal{Z}(\phi, S)$ is finite and $\overline{\operatorname{Avg}}(\mathcal{Z}(\phi), S) = 0$ for all finite subsets $S \subseteq V_K$.*

(2) *If d is an odd prime, $d \not\equiv 1 \pmod p$, $f \in \mathcal{O}_K$ and $f \notin K(\mu_d)^d$, then $G_{K(\mu_d)}(\phi) \leq W(d)$ is a finite index subgroup.*

In fact, it follows from Theorem 1.5 that $G_{K(\mu_d)}(\phi_f) \leq W(d)$ is a finite index subgroup for all non-constant $f \in \mathbb{F}_p(t)$ and $d \not\equiv 1 \pmod p$; see Remark 3.2 below. In particular, the number of irreducible factors of ϕ^n over $\mathbb{F}_p(t)$ is bounded independently of n (a phenomenon called eventual stability [16, §5]), and we recover a stronger version of [8, Corollary 7]. For applications of eventual stability to the study of integral points in reverse orbits, see [18, §3] and [43, Theorem 2.6]. As for characteristic zero function fields $K/k(t)$, a finite index statement for

$$G_{K(\mu_d)}(x^d + f) \leq W(d)$$

follows from [7] and [8, Theorem 25]. However, we can improve upon this result, making the index bounds explicit and uniform when $K = k(t)$ is a rational function field.

Theorem 1.6. *Let $K = k(t)$ be a rational function field of characteristic zero, let d be an odd prime, and let $\phi(x) = x^d + f$ for some non-constant $f \in k[t]$. Then the following statements hold:*

(1) *If $f \notin K(\mu_d)^d$, then we have the index bound*

$$\log_d [W(d) : G_{K(\mu_d)}] \leq \frac{d^{10} - 1}{d - 1} + 10.$$

(2) *If* $\mathrm{Gal}_{K(\mu_d)}(\phi^{10}) \cong [C_d]^{10}$, *then* $G_{K(\mu_d)}(\phi) \cong W(d)$.

(3) *If* $d \geq 367$ *and* $\mathrm{Gal}_{K(\mu_d)}(\phi^5) \cong [C_d]^5$, *then* $G_{K(\mu_d)}(\phi) \cong W(d)$.

Moreover, if $\phi(x) = x^d + t$, *then* $G_{K(\mu_d)}(\phi) \cong W(d)$ *for all* $d \geq 2$ (*not necessarily prime*). *In particular, if* $k/\mathbb{Q}$ *is a number field and* $\phi_c(x) = x^d + c$ *for some* $c \in k$, *then there are infinitely many values of* c *satisfying* $\mathrm{Gal}_{k(\mu_d)}(\phi_c^n) \cong [C_d]^n$.

Remark 1.7. In particular, Theorem 1.6 establishes the inverse Galois problem for iterated wreath products of cyclic groups.

2. Primitive prime divisors and averages

In this section, we make the following conventions:

- K is a number field or a finite extension $K/\mathbb{F}_q(t)$.
- If K is a function field, then k is its field of constants.
- $\mathfrak{p}$ is a finite prime of K.
- $k_\mathfrak{p}$ is the residue field of $\mathfrak{p}$.
- If K is a number field, then $\mathrm{N}_\mathfrak{p} := \frac{\log \# k_\mathfrak{p}}{[K:\mathbb{Q}]}$.
- If K is a function field, then $\mathrm{N}_\mathfrak{p} := [k_\mathfrak{p} : k]$.
- If K is a function field, then $\mathfrak{p}_0$ is a fixed prime of K.

We normalize $\mathrm{N}_\mathfrak{p}$ in the number field case, since it streamlines our proofs. Moreover, given a finite set of primes $S \subseteq V_K$, we let $\mathcal{O}_K := \{a \in K : v(a) \geq 0,\ v \in V_K\}$ be the ring of integers of K and $\mathcal{O}_{K,S} := \{a \in K : v(a) \geq 0,\ v \notin S\}$ be the ring of S-integers. Similarly, when K is a function field, we fix a prime $\mathfrak{p}_0$ and set $\mathcal{O}_K := \big\{\alpha \in K : v_\mathfrak{p}(\alpha) \geq 0,\ \mathfrak{p} \neq \mathfrak{p}_0\big\}$ and let $\mathcal{O}_{K,S} := \big\{\alpha \in K : v_\mathfrak{p}(\alpha) \geq 0,\ \mathfrak{p} \notin S\big\}$ for all S containing $\mathfrak{p}_0$. Moreover, we let $\mathcal{O}_K^*$ and $\mathcal{O}_{S,K}^*$ be the corresponding unit groups.

We now define the relevant global Weil-height functions; see [42, §3.1] and [44, Theorem 1.4.11] for more details. If K is a function field, then we define the height of $\alpha \in K$ to be

$$h(\alpha) = -\sum_{\mathfrak{p} \in V_K} \min(v_\mathfrak{p}(\alpha), 0) \cdot \mathrm{N}_\mathfrak{p} = \sum_{\mathfrak{p} \in V_K} \max(v_\mathfrak{p}(\alpha), 0) \cdot \mathrm{N}_\mathfrak{p}\,. \tag{6}$$

On the other hand, if K is a number field, the height of $\alpha \in K$ is

$$h(\alpha) = -\sum_{\mathfrak{p} \in V_K} \min(v_\mathfrak{p}(\alpha), 0) \cdot \mathrm{N}_\mathfrak{p} \ + \frac{1}{[K:\mathbb{Q}]} \sum_{\sigma : K \to \mathbb{C}} \max(\log|\sigma(\alpha)|, 0). \tag{7}$$

Remark 2.1. The key advantage in the function field setting when studying primitive prime divisors is that one can compute heights of integers by keeping track of positive valuations only.

As was mentioned in the introduction, the main technique we use to prove Theorem 1.1 comes from the theory of rational points on curves. However, over function fields, we must stipulate that our curve not be defined over the field of constants, otherwise certain results (such as the Mordell conjecture) are false. The most convenient way to achieve this is to define the Kodaira-Spencer map.

To do this, we think of a curve $X_{/K}$ as a surface over k. In particular, X is equipped with a map $f : X \to C$ to a curve $C_{/k}$ satisfying $K = k(C)$. Abstractly, the Kodaira-Spencer map (or KS) is constructed on any open set $U \subseteq C$ over which f is smooth from the exact sequence

$$0 \to f^*\Omega^1_U \to \Omega^1_{X_U} \to \Omega^1_{X_U/U} \to 0$$

by taking the coboundary map $KS : f_*(\Omega_{X_U/U}) \to \Omega^1_U \times R^1 f_*(\mathcal{O}_{X_U})$. Fortunately for us, the KS map has been made explicit for superelliptic curves in [22, §5.2], and we are therefore able to sidestep most of this abstraction when dealing with $C_{\ell,m}(\phi) : Y^\ell = \phi^m(X)$; see Section 3.

Proof of Theorem 1.1. To estimate the size of elements in $\mathcal{Z}(\phi, b)$, we refine our proof of the finiteness of $\mathcal{Z}(\phi, b)$ in [11, Theorem 1] and follow the conventions therein. Note that $S \subseteq S'$ implies $\mathcal{Z}(\phi, S) \subseteq \mathcal{Z}(\phi, S')$. Therefore, to prove that $\mathcal{Z}(\phi, S)$ is finite, we may enlarge S and assume that

$$\text{(a).}\quad b \in \mathcal{O}_{K,S}, \qquad \text{(b).}\quad \phi \in \mathcal{O}_{K,S}[x],$$
$$\text{(c).}\quad v(a_d) = 0 \ \text{ for all } v \notin S, \qquad \text{(d).}\quad \mathcal{O}_{K,S} \text{ is a UFD},$$

where a_d is the leading term of ϕ. Note that condition (d) is made possible by the finiteness of the class group; see [32, Prop. 14.2] over function fields. Likewise, we may assume that $\mathfrak{p}_0 \in S$.

We first bound $\mathcal{Z}(\phi, b)$ when 0 is not in the orbit of b, true of all but finitely many $b \in K$: this follows from the following stronger statement.

Lemma 2.2. *Let $B > 0$. There exists a positive integer $n_\phi(B)$ such that $h(\phi^n(b)) \leq B$ implies $n < n_\phi(B)$ for all $b \in K$ satisfying $\hat{h}_\phi(b) \neq 0$.*

To bound $\mathcal{Z}(\phi, b)$ when $\phi^n(b) \neq 0$ for all n, we use the following decomposition of $\phi^n(b)$ into an ℓ and ℓ-free part.

Lemma 2.3. *Let ϕ, K, and S be as above and let $\ell \geq 2$. Then we have a decomposition*

$$\phi^n(b) = u_n \cdot d_n \cdot y_n^\ell \quad \text{for some } d_n, y_n \in \mathcal{O}_{K,S},\ u_n \in \mathcal{O}^*_{K,S}, \tag{8}$$

satisfying the following properties:

1. *$0 \leq v_\mathfrak{p}(d_n) \leq \ell - 1$ for all $\mathfrak{p} \notin S$.*
2. *There is a constant $r(S)$ such that $0 \leq v_\mathfrak{p}(d_n) \leq r(S)$ for all $\mathfrak{p} \in S$ when $K/\mathbb{Q}$ and all $\mathfrak{p} \in S \setminus \{\mathfrak{p}_0\}$ when $K/\mathbb{F}_q(t)$.*
3. *The height $h(u_n)$ is bounded independently of n.*

Proof of Lemma 2.3. By assumptions (a) and (b) on $S = S(\phi, b)$, we see that $\phi^n(b) \in \mathcal{O}_{K,S}$ for all n. Hence, for any integer $\ell \leq 2$, we may write $\phi^n(b) = u_n \cdot d_n \cdot y_n^\ell$ as on (8) since $\mathcal{O}_{K,S}$ is a UFD. Furthermore, we can assume that $0 \leq v(d_n) \leq \ell - 1$ for all $v \notin S$. To see this, we use the correspondence $V_K \setminus S \longleftrightarrow \operatorname{Spec}(\mathcal{O}_{K,S})$ discussed in [32, Ch. 14] and write:

$$d_n = p_1^{e_1} \cdot p_2^{e_2} \cdots p_s^{e_s} \left(p_1^{q_1} \cdot p_2^{q_2} \cdots p_s^{q_s}\right)^\ell, \qquad p_i \in \operatorname{Spec}(\mathcal{O}_{K,S})$$

for some integers e_i, q_i satisfying $v_{p_i}(d_n) = q_i \cdot \ell + e_i$ and $0 \leq e_i < \ell$. In particular, by replacing d_n with $\left(p_1^{e_1} \cdot p_2^{e_2} \cdots p_s^{e_s}\right)$ and y_n with $\left(y_n \cdot p_1^{q_1} \cdot p_2^{q_2} \cdots p_s^{q_s}\right)$, we may assume that $0 \leq v(d_n) \leq \ell - 1$ for all $v \in V_K \setminus S$ as claimed.

On the other hand, let $\mathfrak{p}_i \in S$ when K is a number field and let $\mathfrak{p}_i \in S \setminus \{\mathfrak{p}_0\}$ when K is a function field. Since the class group of K is finite, there exists $a_i \in \mathcal{O}_K$ and

$n_i \geq 1$ such that $\mathfrak{p}_i^{n_i} = (a_i)$. In particular, $v_{\mathfrak{p}_i}(a_i) = n_i > 0$ and $v_{\mathfrak{p}}(a_i) = 0$ for all $\mathfrak{p} \in \operatorname{Spec}(\mathcal{O}_K)\setminus\{\mathfrak{p}_i\}$. Therefore, if we write $v_{\mathfrak{p}_i}(d_n) = q_i \cdot n_i + r_i$ for some $0 \leq r_i < n_i$ and set $d_n' := d_n/(\prod_i a_i^{q_i})$, then we have that $0 \leq v_{\mathfrak{p}}(d_n') = v_{\mathfrak{p}}(d_n) \leq \ell - 1$ for all $\mathfrak{p} \notin S$ and $v_{\mathfrak{p}_i}(d_n') = r_i$ for all $\mathfrak{p}_i$. Hence, after replacing d_n with d_n' and u_n with $u_n \cdot (\prod_i a_i^{q_i})$, we see that conditions (1) and (2) of Lemma 2.3 are satisfied for $r(S) := \max\{r_i\}$.

Finally, since $\mathcal{O}_{K,S}^*$ is a finitely generated group ([32, Prop. 14.2]), we can absorb ℓ-powers into y_n and write $u_n = \mathbf{u}_1^{r_1} \cdot \mathbf{u}_2^{r_2} \dots \mathbf{u}_t^{r_t}$ for some basis $\{\mathbf{u}_i\}$ of $\mathcal{O}_{K,S}^*$ and some integers $0 \leq r_i \leq \ell - 1$. In particular, we may assume that the u_n are in a finite set, independent of n, and this shows that the height $h(u_n)$ is uniformly bounded. $\square$

It is our goal to show that $\mathbf{d_n} \in \mathcal{O}_\mathbf{K}$ contains primitive prime divisors outside of S. To do this, first note that conditions (b) and (c) imply that ϕ has good reduction (see [42, Theorem. 2.15]) modulo the primes in $V_K \setminus S$. In particular, if $\mathfrak{p} \in V_K \setminus S$ is such that $v_{\mathfrak{p}}(d_n) > 0$ and $v_{\mathfrak{p}}(\phi^m(b)) > 0$ for some $1 \leq m \leq n-1$, then

$$\phi^{n-m}(0) \equiv \phi^{n-m}(\phi^m(b)) \equiv \phi^n(b) \equiv 0 \pmod{\mathfrak{p}}; \tag{9}$$

see [42, Theorem. 2.18]. Therefore, if $n \geq 1$ is such that d_n has no primitive prime divisors outside of S, then we have the refined factorization of ideals in $\mathcal{O}_{K,S}$:

$$(d_n) = \prod \mathfrak{p}_j^{e_j}, \ \text{ where } \ \mathfrak{p}_j \big| \phi^{t_j}(b) \text{ or } \mathfrak{p}_j \big| \phi^{t_j}(0) \ \text{ for some } 1 \leq t_j \leq \left\lfloor \frac{n}{2} \right\rfloor. \tag{10}$$

Moreover, we may assume that $0 \leq e_j \leq \ell - 1$ and $0 \leq v_{\mathfrak{p}}(d_n) \leq r(S)$ for $\mathfrak{p} \in S$ by Lemma 2.3. On the other hand, since $d_n \in \mathcal{O}_K$, we can calculate the height of d_n by computing positive valuations only:

Lemma 2.4. *If K is one of the global fields in Theorem 1.1, then*

$$\sum_{\mathfrak{p} \subseteq \mathcal{O}_K, v_{\mathfrak{p}}(\alpha) \geq 0} v_{\mathfrak{p}}(\alpha) \cdot \mathrm{N}_{\mathfrak{p}} = h(\alpha) \tag{11}$$

for all non-zero $\alpha \in \mathcal{O}_K$. On the other hand, $\sum_{v_{\mathfrak{p}}(\alpha) \geq 0} v_{\mathfrak{p}}(\alpha)\, \mathrm{N}_{\mathfrak{p}} \leq h(\alpha)$ for all $\alpha \in K^*$.

Remark 2.5. For number fields $K/\mathbb{Q}$, the height calculation in Lemma 2.4 fails whenever the group of units $\mathcal{O}_K^*$ is infinite. In particular, one cannot in general calculate heights of algebraic integers by solely keeping track of divisors. Therefore, in order to generalize Theorem 1.1 to all number fields, one would need to estimate $|\phi^n(b)|_\sigma$ for the archimedean places $\sigma : K \to \mathbb{C}$ as well.

Hence, Lemma 2.3, Lemma 2.4, and (10) imply that there is a constant $c(K,S)$ such that

$$\begin{aligned} h(d_n) &= \sum_{\mathfrak{p} \notin S} v_{\mathfrak{p}}(d_n)\, \mathrm{N}_{\mathfrak{p}} \ + \sum_{\mathfrak{p} \in S} v_{\mathfrak{p}}(d_n)\, \mathrm{N}_{\mathfrak{p}} \\ &\leq (\ell - 1) \cdot \sum_{\mathfrak{p} \notin S, v_{\mathfrak{p}}(d_n) \geq 0} \mathrm{N}_{\mathfrak{p}} \ + \ r(S) \cdot \sum_{\mathfrak{p} \in S} N_{\mathfrak{p}} \\ &\leq (\ell - 1) \Bigg(\sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} h(\phi^i(b)) + \sum_{j=1}^{\lfloor \frac{n}{2} \rfloor} h(\phi^j(0)) \Bigg) + c(K,S); \end{aligned} \tag{12}$$

here the last line follows from (10) and the lower bound in Lemma 2.4 applied to $\alpha = \phi^i(b)$ and $\alpha = \phi^j(0)$ for $1 \leq i, j \leq \lfloor \frac{n}{2} \rfloor$, valid since $\phi^i(b) \neq 0$ and $\phi^j(0) \neq 0$ for all $i, j \geq 1$. Now choose an integer $m = m_\phi$ and $\ell = \ell_\phi$ such that

$$C := C_{\ell,m}(\phi) : Y^\ell = \phi^m(X)$$

is a non-singular curve of genus at least 2. This is possible in the function field case since ϕ is dynamically ℓ-power non-isotrivial. As for the number field case, since zero is not periodic, the Riemann-Hurwitz formula implies that $\#\phi^{-m}(0) \geq d^{m-2}$ for all $m \geq 1$; see [42, Exercise 3.37]. Hence, we may choose m such that $\#\phi^{-m}(0) \geq 5$. Now choose ℓ coprime to the multiplicities of all roots of $\phi^m(x)$, and apply [4, Corollary 2.2] or [44, Proposition 3.7.3].

If $n \leq m_\phi$ for all $n \in \mathcal{Z}(\phi, b)$ with $b \in \mathcal{O}_{K,S}$ and $\hat{h}_\phi(b) > 0$, then we are done. Otherwise, we may assume that $n > m_\phi$ so that (8) implies that

$$P_n(b) := \left(\phi^{n-m_\phi}(b) \ , \ y_n \cdot \sqrt[\ell]{u_n \cdot d_n}\,\right) \in C(\overline{K})\,.$$

It follows from the Vojta conjecture [47, Conj. 24.1 or 25.1] for number fields or any of the bounds (suitable to positive characteristic) discussed in the introductions of [21,28] for function fields, that there are positive constants $A_1 = A_1(d, \ell_\phi, m_\phi)$ and $A_2 = A_2(\phi, d, \ell_\phi, m_\phi)$ such that

$$h_{\kappa(C)}(P_n(b)) \leq A_1 \cdot \mathfrak{d}(P_n(b)) + A_2; \tag{13}$$

here $\kappa(C)$ is a canonical divisor class of C with associated height function $h_{\kappa(C)} : C \to \mathbb{R}_{\geq 0}$ (see [22, §2.2]), $\mathfrak{d}(P_n(b))$ is the logarithmic discriminant of $K(P_n(b))/K$ relative to K (see [47, §23]) over number fields, and

$$\mathfrak{d}(P_n(b)) := \frac{2 \cdot \text{genus}\left(K_n(b)\right) - 2}{\left[K_n(b) : K\right]} \quad \text{for} \quad K_n(b) := K\left(\sqrt[\ell]{u_n \cdot d_n}\,\right)$$

over function fields. We note that the bounds on (13) have been made more explicit in [22, §2.2] over function fields, although we do not need them here.

On the other hand, if K is a function field, then it follows from [44, Prop. 3.7.3] and the remark [44, Remark 3.7.5] that there is a constant $B_1 = B_1(\mathfrak{g}_K)$, depending only on the genus $\mathfrak{g}_K$ of K, such that $\mathfrak{d}(P_n(b)) \leq h(u_n \cdot d_n) + B_1$. Likewise, $h(u_n \cdot d_n) \leq h(d_n) + B(K, S)$, since the height of u_n is absolutely bounded. Hence, there is a constant $B(K, S)$, depending only on K and S, such that $\mathfrak{d}(P_n(b)) \leq h(d_n) + B(K, S)$. Similarly, $\mathfrak{d}(P_n(b)) \leq h(d_n) + B(K, S)$ over number fields; see [47, §23]. In either case, we deduce from (13) that

$$h_{\kappa(C)}(P_n(b)) \leq A_1 \cdot h(d_n) + A_3, \tag{14}$$

where

$$A_3 = A_3(\phi, d, m_\phi, \ell_\phi, \mathfrak{g}_K, S) = (B_1(\mathfrak{g}_K) + B_2(K, S)) \cdot A_1(d, m_\phi) + A_2(\phi, d, \ell_\phi, m_\phi).$$

In particular, all of the constants appearing above are independent of the basepoint b. However, we want a bound relating $h(\phi^{n-m}(b))$ and $h(d_n)$ instead of one relating $h_{\kappa(C)}(P_n(b))$ and $h(d_n)$. To do this, we note that if $\mathcal{D}_1$ is any ample divisor on C and $\mathcal{D}_2$ is an arbitrary divisor, then

$$\lim_{h_{\mathcal{D}_1}(P) \to \infty} \frac{h_{\mathcal{D}_2}(P)}{h_{\mathcal{D}_1}(P)} = \frac{\deg \mathcal{D}_2}{\deg \mathcal{D}_1}, \qquad P \in C(\overline{K}); \tag{15}$$

see [38, Thm III.10.2]. In particular, if $\pi : C \to \mathbb{P}^1$ is the covering $\pi(X, Y) = X$, then a degree one divisor on $\mathbb{P}^1$ (giving the usual height h_K on projective space) pulls back to a $\deg(\pi)$ divisor $\mathcal{D}_2$ on C satisfying $h_{\mathcal{D}_2}(P) = h(\pi(P))$. Therefore, we deduce from (15) that there exists a constant $\delta = \delta(\phi, m, \ell)$ satisfying:

$$(16)\quad h_{\kappa(C)}(P) > \delta \quad \text{implies} \quad h(\pi(P)) \leq \frac{\ell}{2\mathfrak{g}_C - 2} \cdot h_{\kappa(C)}(P) + 1 \leq \frac{\ell}{2} \cdot h_{\kappa(C)}(P) + 1$$

for all $P \in C(\overline{K})$; here $\mathfrak{g}_C \geq 2$ is the genus of C and $\deg(\pi) \leq \ell$. As an alternative to the height ratio on (15) over function fields, we could use explicit calculations of $h_{\kappa(C)}$ in [22, §4]; however, we prefer a uniform approach over global fields when possible. On the other hand, we note that the set of points $\{P_n(b)\} \subseteq C(\overline{K})$ where (16) fails:

$$\begin{aligned} nT_C :=& \big\{ P_n(b) \;\big|\; h_{\kappa(C)}(P_n(b)) \leq \delta \big\} \\ &\subseteq \big\{ P \in C(\bar{K}) \;\big|\; h_{\kappa(C)}(P) \leq \beta \ \text{ and } \ [K(P):K] \leq \ell \big\}, \end{aligned}$$

is finite, since the canonical class $\kappa(C)$ is ample in genus at least 2; see [38, Thm. 10.3]. In particular, we deduce that $P_n(b) \in T_C$ implies $h(\phi^{n-m}(b))$ is bounded. Hence, Lemma 2.2 implies that n is bounded independently of b as claimed. Conversely, if $P_n(b) \notin T_C$, then (12), (14), and (16) imply that

$$(17)\qquad h(\phi^{n-m_\phi}(b)) \leq \frac{\ell(\ell-1)}{2} \cdot A_1 \cdot \left(\sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} h(\phi^i(b)) + \sum_{j=1}^{\lfloor \frac{n}{2} \rfloor} h(\phi^j(0)) \right) + A_4,$$

for $A_4 = A_4(\phi, d, \ell_\phi, m_\phi, \mathfrak{g}_K, K, S) = \ell/2 \cdot (A_1 \cdot c(K,S) + A_3) + 1$. However, for wandering basepoints the left hand side of (17) grows like d^{n-m} and the right hand side of (17) grows like $d^{\lfloor \frac{n}{2} \rfloor + 1}$. In particular, since m is fixed, it follows that n is bounded. To make this formal, we use properties of $\hat{h}_\phi$, the canonical height function attached to $\phi(x)$. Specifically, it is known that:

$$(18)\qquad \text{(a). } \hat{h}_\phi = h + O(1), \qquad \text{(b). } \hat{h}_\phi(\phi^s(\alpha)) = d^s \cdot \hat{h}_\phi(\alpha)$$

for all $\alpha \in \overline{K}$ and all integers $s \geq 0$; see [42, Thm. 3.20]. In particular, we deduce from (17) that

(19)

$$d^{n-m_\phi} \cdot \hat{h}_\phi(b) \leq \left(\frac{\ell(\ell-1)}{2} \big(\hat{h}_\phi(b) + \hat{h}_\phi(0)\big) A_1 \right) \frac{d^{\lfloor \frac{n}{2} \rfloor + 1} - 1}{d-1} + \left(\frac{\ell(\ell-1)}{2} A_1 B_\phi \right) n + A_5;$$

here $|\hat{h}_\phi - h| \leq B_\phi$ from (18) and $A_5(\phi, d, \ell_\phi, m_\phi, \mathfrak{g}_K, K, S) = A_4 + B_\phi$. Moreover, since $\hat{h}_\phi(b) \neq 0$ and $\hat{h}_{\phi,K}^{\min}$ is positive (see the proof Lemma 2.2), it follows that

$$(20)\qquad d^{n-m_\phi} \leq B_4 \cdot d^{\lfloor \frac{n}{2} \rfloor + 1} + B_5 \cdot n + B_6,$$

where the constants B_4, B_5, and B_6 are all independent of the basepoint $b \in \mathcal{O}_{K,S}$. However, such an inequality implies for instance that

$$(21)\qquad n \leq 5 + 2m_\phi + 2\log_d \big(B_{\max}\big),$$

where $B_{\max} := \max\{B_4, B_5, B_6\}$. Hence, we have shown that the elements of $\mathcal{Z}(\phi, b)$ are bounded by a constant that depends only on ϕ, S, and K whenever 0 is not in the orbit of b. On the other hand, suppose that $\phi^m(b) = 0$ for some $m \geq 1$. Lemma 2.2 implies that there exists n_ϕ (depending only on ϕ and K) such that $\phi^n(a) \neq 0$ for all $n \geq n_\phi$ and all $a \in K$. It follows that the set $\mathfrak{Z}_{\phi,K} := \big\{ a \in K : 0 \in \mathcal{O}_\phi(a) \big\}$ is finite. In particular, the set of primes

$$S_0 := \big\{ \text{primes } \mathfrak{p} \in V_K \,:\, v_\mathfrak{p}(\phi^n(a)) > 0 \text{ for some } a \in \mathfrak{Z}_{\phi,K},\ n \leq n_\phi,\ \phi^n(a) \neq 0 \big\}$$

is also finite. Let $S' = S_0 \cup S$, where S satisfies the conditions (a)-(d) above. We have already shown that there exists $N(\phi, S')$ such that $\phi^n(c)$ contains primitive prime divisors outside of S' for all $n \geq N(\phi, S')$ and all $c \in \mathcal{O}_{K,S} \setminus \mathfrak{Z}_{\phi,K}$. Hence, we may apply this to $c := \phi^{n_\phi}(b)$, from which it follows that all $n \in \mathcal{Z}(\phi, b)$ must satisfy $n \leq n_\phi + N(\phi, S')$. As in the previous case, the bound $n_\phi + N(\phi, S')$ only depends on ϕ, S, and K and not the basepoint. In particular, this completes the proof that $\mathcal{Z}(\phi, S)$ is finite.

We note that the use of the Vojta conjecture in the number field setting is not necessary to prove the finiteness of $\mathcal{Z}(\phi, S)$ when zero is preperiodic. To see this, note that Lemma 2.3 and (9) imply that $\{d_n\}_{n \in \mathcal{Z}(\phi,S)}$ is finite, since there are only finitely many primes not in S dividing elements of the orbit of zero (equivalently, d_n has bounded height by Lemma 2.4). Now define

$$K(\phi, S) := K\big(\sqrt[\ell]{u_n \cdot d_n}\ :\ n \in \mathcal{Z}(\phi, S)\big),$$

a finite extension of K. Hence, Faltings' Theorem [6] implies that the set of $K(\phi, S)$ rational points of C is finite. In particular, $\phi^{n-m_\phi}(b)$ has bounded height, and Lemma 2.2 implies that n is bounded as claimed.

As for statements about averages, we consider the set

$$T_{\phi,n,S} := \big\{b \in \mathcal{O}_{K,S} \mid n \in \mathcal{Z}(\phi, b),\ \hat{h}_\phi(b) \neq 0\big\}. \tag{22}$$

It follows from the fact that $\mathcal{Z}(\phi, S)$ is finite that $T_{\phi,n,S} = \varnothing$ for all n sufficiently large. Although it may be the case that $T_{\phi,n,S}$ is an infinite set for some n, we will show that $T_{\phi,n,S}$ is always a sparse subset of $\mathcal{O}_{K,S}$. With this in mind, for any subset $E \subseteq \mathcal{O}_{K,S}$ we define the (natural) upper density $\overline{\delta}_{\mathrm{Nat},S}(E)$ of E to be the quantity

$$\overline{\delta}_{\mathrm{Nat},S}(E) := \limsup_{B\to\infty} \frac{\#\{b \in E \mid h(b) \leq B\}}{\#\{b \in \mathcal{O}_{K,S} \mid h(b) \leq B\}} := \limsup_{B\to\infty} \frac{\#E(B)}{\#\mathcal{O}_{K,S}(B)}. \tag{23}$$

In particular, if we set $N(\phi, S) := \sup\{n : n \in \mathcal{Z}(\phi, S)\}$, then we see that

$$\overline{\mathrm{Avg}}(\mathcal{Z}(\phi), S) \leq N(\phi, S) \cdot \Bigg(\sum_{n=1}^{N(\phi,S)} \overline{\delta}_{\mathrm{Nat},S}\big(T_{\phi,n,S}\big)\Bigg). \tag{24}$$

Therefore, it suffices to prove that $\overline{\delta}_{\mathrm{Nat},S}(T_{\phi,n,S}) = 0$ for all $1 \leq n \leq N(\phi, S)$, to deduce that $\overline{\mathrm{Avg}}(\mathcal{Z}(\phi), S) = 0$. To do this, we make a few auxiliary definitions: for all rational functions $g(x) \in K(x)$ and all sets of primes $\mathcal{P} \subseteq V_K$, we define:

$$I_{g,S,\mathcal{P}} := \big\{b \in \mathcal{O}_{K,S}\ :\ \mathrm{Supp}(g(b)) \subseteq \mathcal{P}\big\}. \tag{25}$$

Here, for any $\alpha \in K$, the support $\mathrm{Supp}(\alpha)$ is the set of all primes $\mathfrak{p}$ such that $v_\mathfrak{p}(\alpha) > 0$. Furthermore, let $\mathcal{P}_0$ be the finite set of prime divisors of the first $N(\phi, S)$-elements of the orbit of zero, that is, $\mathcal{P}_0 := \{\mathrm{Supp}(\phi^n(0))\}_{n \leq N(\phi,S)}$. Finally, let $\mathcal{P}_g$ be the set of primes of bad reduction of $g(x)$.

In particular, it follows from (9) that

$$T_{\phi,n,S} \subseteq I_{\phi^n,S,\mathcal{P}} \quad \text{for } \mathcal{P} = S \cup \mathcal{P}_0 \cup \mathcal{P}_\phi\,. \tag{26}$$

Therefore, if we let $g(x) := \phi^n(x)$ for any $n \leq N(\phi, S)$, then our average-zero result follows from Lemma 2.6 below. However, because of its possible independent interest, we state Lemma 2.6 for subsets $\mathcal{P} \subseteq V_K$ of (Dirichlet) density zero, not just finite subsets; see [26] and [36, §3] for the relevant background and results on densities over global fields. Moreover, in what follows $\mathrm{N}(\mathfrak{p}) = \#k_{\mathfrak{p}}$ is the size of the residue field. $\square$

Lemma 2.6. *Let $g : \mathbb{P}^1 \to \mathbb{P}^1$ be a non-constant rational function, let $\mathcal{P} \subseteq V_K$, and let*

$$\overline{\delta}_{\mathrm{Dir}}(\mathcal{P}) := \lim_{s\to 1^+} \frac{\sum_{\mathfrak{q}\in\mathcal{P}} \mathrm{N}(\mathfrak{q})^{-s}}{\sum_{\mathfrak{q}\in V_K} \mathrm{N}(\mathfrak{q})^{-s}} = \lim_{s\to 1^+} \frac{\sum_{\mathfrak{q}\in\mathcal{P}} \mathrm{N}(\mathfrak{q})^{-s}}{\log(1/(s-1))} \tag{27}$$

be the Dirichlet density of $\mathcal{P}$. If $\overline{\delta}_{\mathrm{Dir}}(\mathcal{P}) = 0$, then $\overline{\delta}_{\mathrm{Nat},S}(I_{g,S,\mathcal{P}}) = 0$.

Proof of Lemma 2.6. Since $I_{g,S,\mathcal{P}_1} \subseteq I_{g,S,\mathcal{P}_2}$ whenever $\mathcal{P}_1 \subseteq \mathcal{P}_2$, we may enlarge $\mathcal{P}$ and assume that $\mathcal{P}$ contains both S and $\mathcal{P}_g$. Now let

$$\mathcal{P}' = \{\mathfrak{p} \notin \mathcal{P} : g(x) \text{ has a root } (\mathrm{mod}\ \mathfrak{p})\},$$

and for $\mathfrak{p} \in \mathcal{P}'$ let $a_{\mathfrak{p}}$ be such a root (mod $\mathfrak{p}$); note that this makes sense, i.e., $g : \mathbb{P}^1(\mathbb{F}_{\mathfrak{p}}) \to \mathbb{P}^1(\mathbb{F}_{\mathfrak{p}})$ is well defined, since $\mathfrak{p} \notin \mathcal{P}_g$. It follows from the Chebotarev Density Theorem, that $\delta_{\mathrm{Dir}}(\mathcal{P}')$ is positive. Let $\mathcal{P}''$ be any finite subset of $\mathcal{P}'$. By definition of $I_{g,S,\mathcal{P}}$ we see that

$$I_{g,S,\mathcal{P}} \subseteq \left\{b \in \mathcal{O}_{K,S} \,:\, b \not\equiv a_p \ (\mathrm{mod}\ \mathfrak{p}) \text{ for all } \mathfrak{p} \in \mathcal{P}''\right\}. \tag{28}$$

Fix $\mathfrak{p} \in \mathcal{P}''$. Since $\delta_{\mathrm{Nat},S}$ is translation invariant, $\delta_{\mathrm{Nat},S}(a + \mathfrak{p})$ is independent of $a \in \mathcal{O}_{K,S}$. In particular, we can add up $\delta_{\mathrm{Nat},S}(a + \mathfrak{p})$ over coset representatives $a \in \mathcal{O}_{K,S}/\mathfrak{p}\mathcal{O}_{K,S}$ and see that the natural density of $\{b \in \mathcal{O}_{K,S} \,:\, b \equiv a_p \ (\mathrm{mod}\ \mathfrak{p})\}$ is $1/\mathrm{N}(\mathfrak{p})$ as expected. In particular, one computes via the Chinese Remainder Theorem and the inclusion-exclusion principle that the natural density of the set displayed on the right hand side of (28) is $\prod_{\mathfrak{p}\in\mathcal{P}''}\left(1 - \frac{1}{\mathrm{N}(\mathfrak{p})}\right)$. On the other hand,

$$\overline{\delta}_{\mathrm{Nat},S}(I_{g,S,\mathcal{P}}) \leq \prod_{\mathfrak{p}\in\mathcal{P}',\ \mathrm{N}(\mathfrak{p})\leq B} \left(1 - \frac{1}{\mathrm{N}(\mathfrak{p})}\right) \sim \frac{c}{\log(B)^{\delta_{\mathrm{Dir}}(\mathcal{P}')}} \tag{29}$$

as $B \to \infty$ for some positive constant c; see [36, Exercise 3.3.2.2]. In particular, since the density $\delta_{\mathrm{Dir}}(\mathcal{P}') \neq 0$, we see that $\overline{\delta}_{\mathrm{Nat},S}(I_{g,S,\mathcal{P}}) = 0$ as claimed. $\square$

We conclude this section with the proofs of Lemmas 2.2 and 2.4 and some remarks on possible generalizations of Theorem 1.1.

Proof of Lemma 2.2. Suppose that $b \in K$ and $h(\phi^n(b)) \leq B$. Since $\hat{h}_\phi = h + O(1)$ and $\hat{h}_\phi(\phi^n(b)) = d^n \cdot \hat{h}_\phi(b)$, we see that $d^n \cdot \hat{h}_\phi(b) = \hat{h}_\phi(\phi^n(b)) \leq B'$ for some positive constant B' depending on ϕ and B. Moreover,

$$\hat{h}^{\min}_{\phi,K} := \inf\left\{\hat{h}_\phi(c) \mid c \in \mathbb{P}^1(K),\ \hat{h}_\phi(c) > 0\right\} \tag{30}$$

is strictly positive. To see this, choose an arbitrary wandering point $c_0 \in \mathbb{P}^1(K)$ for ϕ (possible, for instance, by the Northcott property [42, Theorem. 3.12]), and note that

$$\hat{h}^{\min}_{\phi,K} = \inf\left\{\hat{h}_\phi(c) \mid c \in \mathbb{P}^1(K) \text{ and } 0 < \hat{h}_\phi(c) < \hat{h}_\phi(c_0)\right\}.$$

However, this latter set is finite and consists of strictly positive numbers; hence $\hat{h}^{\min}_{\phi,K} > 0$. In particular, it follows that $h_K(\phi^n(b)) \leq B$ implies $n \leq \log_d\left(B'/\hat{h}^{\min}_{\phi,K}\right)$. Hence, n is bounded as claimed. $\square$

Proof of Lemma 2.4. Let K be a function field. If $\alpha \in \mathcal{O}_K = \mathcal{O}_{\mathfrak{p}_0}$ is non-constant, then $v_{\mathfrak{p}_0}(\alpha) < 0$ and the claim follows from (6), i.e., the number of zeros equals the number of poles when counted with the correct multiplicity. On the other hand, let $K/\mathbb{Q}$ be a number field. Then the product formula implies

$$h(\alpha) = \sum_{\mathfrak{p} \subseteq \mathcal{O}_K, v_{\mathfrak{p}}(\alpha) \geq 0} v_{\mathfrak{p}}(\alpha) \cdot \mathrm{N}_{\mathfrak{p}} - \frac{1}{[K:\mathbb{Q}]} \sum_{\sigma: K \to \mathbb{C}} \min(\log |\sigma(\alpha)|, 0). \tag{31}$$

In particular, if $K = \mathbb{Q}$ or $K/\mathbb{Q}$ is an imaginary quadratic extension, then one verifies directly that $|\sigma(\alpha)| > 1$ for all $\sigma : K \to \mathbb{C}$ and all non-zero $\alpha \in \mathcal{O}_K \setminus \mathcal{O}_K^*$. Therefore, (31) implies the claim for such integers. Conversely, if $\alpha \in \mathcal{O}_K^*$, then α is a root of unity and $h(\alpha) = 0$. On the other hand, if α is a unit, then $v_{\mathfrak{p}}(\alpha) = 0$ for all $\mathfrak{p}$ and (11) holds. In either setting, we see that the inequality, $\sum_{v_{\mathfrak{p}}(\alpha) \geq 0} v_{\mathfrak{p}}(\alpha)\, \mathrm{N}_{\mathfrak{p}} \leq h(\alpha)$ for all $\alpha \in K^*$, follows from the product formula. □

Remark 2.7. We note that Theorem 1.1 part 2(a) is a strengthening of the main result of [31]. Moreover, for results on $\mathcal{Z}(\phi, b)$ when $0 \in \mathrm{Per}(\phi)$, see [14].

Remark 2.8. In characteristic zero, the finiteness of $\mathcal{Z}(\phi, S)$ holds for $K = k(t)$ with essentially the same proof: use the fact that $\mathcal{O}_{K,S}$ is a unique factorization domain for all S and that $\hat{h}_{\phi,K}^{\min}$ is positive [1, Remark 1.7(ii)]. On the other hand, the proof of Theorem 1.1 breaks down when $K \neq k(t)$, since the class group of K is not finite. Note also that $\overline{\mathrm{Avg}}(\mathcal{Z}(\phi), S)$ does not make sense for characteristic zero function fields, since the Northcott property fails.

Remark 2.9. Of course, one would like to know whether Theorem 1.1 holds for rational functions. However, in Lemma 2.3 and elsewhere in the proof of Theorem 1.1, we used that $\phi^n(b) \in \mathcal{O}_{K,S}$ for all n, a property that will fail in general. For instance, over number fields Silverman has shown that $\phi^2(x) \notin \overline{K}[x]$ implies that $\mathcal{O}_\phi(b) \cap \mathcal{O}_{K,S}$ is finite for all $b \in K$; see [40] for Silverman's integral point theorem, and see [10] for an average-version.

At present, Conjecture 1.4 seems quite difficult. On the other hand, there are formulas for the relevant Kodaira-Spencer maps in [22] in terms of the iterated preimages of zero. It is therefore possible that one can exploit knowledge of $\mathrm{Gal}_K(\phi^m)$ for some (hopefully small) $m \geq 1$, to show that the KS map is non-zero.

We carry out these calculations for the polynomials $\phi(x) = x^d + f$, where the KS map computation becomes a sum over cyclotomic characters. Although special cases, these polynomials are important examples in several ways. First of all the curves $C_{\ell,1}(\phi)$, defined by the first iterate of $\phi(x)$, are isotrivial for all $\ell \geq 2$ while $C_{d,2}(\phi)$ and $C_{2,2}(\phi)$ are not (see Remark 3.3). This Illustrates that one must in general pass to a non-trivial iterate when studying primitive prime divisors. Secondly, we can use Theorem 1.1 to show that the Galois groups of iterates of $\phi(x) = x^d + f$ form a finite index subgroup of an infinite iterated wreath product of cyclic groups. In particular, they provide examples of a dynamical Serre-type open image theorem over global fields; compare to results for quadratic rational maps over number fields in [7, 19, 45].

Remark 2.10. It is worth pointing out that we could just as well use the more standard notion of isotriviality in Definition 1, Theorem 1.1, and Conjecture 1.4: a curve is said to be isotrivial (in the standard sense) if after a base extension it may be defined over a finite field; see the Appendix in [48]. Strictly speaking, the key bounds in [21, 28] are for curves with non-zero Kodaira-Spencer class. However, the general case follows from this one as follows: assuming that $C_{\ell,m}(\phi)_{/K}$ is a non-isotrivial curve (in the the standard sense), there is an r (a power of the characteristic of K) and a separable extension L/K such that $C_{\ell,m}(\phi)$ is defined over L^r and that the Kodaira-Spencer class of $C_{\ell,m}(\phi)$ over L^r is non-zero. Now, if we apply any of the bounds in [21, 28] to $C_{\ell,m}(\phi)$ over L^r, then we achieve the bounds on (13); the rest of the proof of Theorem 1.1 is the same. However, we prefer the more explicit (computational) condition that the Kodaira-Spencer map be non-zero.

3. Dynamical Galois groups and the Kodaira-Spencer map

We now use our results on dynamical Zsigmondy sets to study dynamical Galois groups. To do so, we first introduce the necessary background material on wreath products, following the presentation in [42, §3.9] and the results in [20].

Definition 2. Let G be a group acting on an index set A, and let H be an abelian group with its group law written additively. The set of maps $\mathrm{Map}(A, H)$ is naturally a group: for $i_1, i_2 \in \mathrm{Map}(A, H)$, define

$$(i_1 + 1_2) : H \to H, \quad (i_1 + i + 2)(a) = i_1(a) + i_2(a).$$

Since G acts on A, it comes equipped with an action on $\mathrm{Map}(A, H)$ as follows:

$$g : \mathrm{Map}(A, H) \to \mathrm{Map}(A, H), \quad g(i)(a) = i(g(a))$$

for all $g \in G$, $i \in \mathrm{Map}(A, H)$, and $a \in A$. The *wreath product* of G and H (relative to A) is the set $\mathrm{Map}(A, H) \times G$ with the group law

$$(g_1, i_1) * (g_2, i_2) = (g_2(i_1) + i_2\, ,\, g_1 g_2)$$

and is denoted $G[H]$.

Definition 3. If G acts on A, then $[G]^m$ acts on A^m (the cartesian product) for all $m \geq 1$. Therefore, we may define the *n-th iterated wreath power of G* inductively: $[G]^1 = G$ and $[G]^n = [G]^{n-1}[G]$.

Definition 4. Since $G[H] \to G$ via projection onto the second coordinate, we have a system of maps $[G]^n \to [G]^{n-1}$ allowing us to define an inverse limit. In the special case when $G = C_d$ is the cyclic group of order d (acting on itself by translation), we define

$$W(d) := \varprojlim [C_d]^n$$

to be the infinite iterated wreath product of C_d; for more on $W(d)$, see [27].

Our primary interest in wreath products comes from their relationship to the Galois groups of compositions of rational functions. We restate the following result from [20, Lemma 2.5].

Lemma 3.1. *Let K be a field and let $\psi, \gamma \in K[x]$ with $\deg(\psi) = \ell$ and $\deg(\gamma) = d$. We assume that $\psi \circ \gamma$ has ℓd distinct roots in $\overline{K}$ and that ψ is irreducible over K. Let $\alpha_1, \ldots, \alpha_\ell$ be the roots of ψ, let M_i be the splitting field of $\gamma(x) - \alpha_i$ over $K(\alpha_i)$, and $G = \mathrm{Gal}_K(\psi)$. If $H = \mathrm{Gal}(M_i/K(\alpha_i))$, then there is an embedding $\mathrm{Gal}_K(\psi \circ \gamma) \leq G[H]$.*

As in the introduction, for $\phi(x) \in K(x)$ and $n \geq 1$, we let $K_n(\phi)$ be the field obtained by adjoining all solutions of $\phi^n(x) = 0$ to K. Since ϕ has coefficients in K, the extension $K_n(\phi)/K$ is Galois, and we let $G_{K,n}(\phi) := \mathrm{Gal}_K(\phi^n)$ be the Galois group of $K_n(\phi)/K$. Since $K_{n-1}(\phi) \subseteq K_n(\phi)$ for all n (with some separability assumptions), we may define $G_K(\phi)$ to be the inverse limit of the $G_{K,n}(\phi)$. Eschewing the generic situation for reasons of complexity, we focus our attention on the family of iterates of $\phi(x) = x^d + f$ for $f \in \mathbb{F}_p[t]$. We now prove a Serre-type finite index theorem for $G_K(\phi) \leq W(d)$ from the introduction; this is the first unconditional finite index result over any global field in the non-quadratic case:

Proof of Theorem 1.5. To prove the first statement, it suffices to show that ϕ is dynamically 2-power non-isotrivial; see Definition 1 and Theorem 1.1 above. When $d = 2$, it suffices to calculate the j-invariant of the elliptic curve E_ϕ from (4) above. In particular, we compute that

$$\frac{1}{64}j(E_\phi) = \frac{-f^3 + 9f^2 - 27f + 27}{f^2 + 2f + 1},$$

which cannot be constant unless f is constant. Therefore, we may assume that $d \geq 3$. If d is odd, then $\{\frac{x^i dx}{y}\}$ for $0 \leq i \leq \frac{d^2-1}{2} - 1$ is a basis for the space of regular 1-forms [23, Theorem 3] on

$$C_{2,2}(\phi) : Y^2 = \phi^2(X) = (X^d + f)^d + f.$$

To see that $C_{2,2}(\phi)$ is non-singular, use the discriminant formula in [17, Lemma 2.6]; there we see that the discriminant of $\phi^2(x)$ is zero if and only if $\phi(0) \cdot \phi^2(0) = f \cdot (f^d + f) = 0$. This is impossible since f is non-constant.

We now calculate the Kodaira-Spencer map associated to the surface $C_{2,2}(\phi) \to \mathbb{P}^1$ using [22]. In keeping with the notation in [22, §5.2], let $\{P_s\}$ for $1 \leq s \leq d^2$ be the set of roots of $\phi^2(x)$, and let $\phi_x^2(x)$ and $\phi_t^2(x)$ denote the partial derivatives of $\phi^2(x)$ with respect to x and t, respectively. In [22, §5.2], it is shown that the Kodaira-Spencer matrix with respect to the standard basis above is

$$m_{i,j} = \sum_s \frac{P_s^{i+j}\phi_t^2(P_s)}{2\phi_x^2(P_s)^2} \tag{32}$$

using Serre duality. One computes that $\phi_x^2(x) = d^2 \cdot (\phi(x) \cdot x)^{d-1}$ and $\phi_t^2(x) = f' \cdot (d \cdot (\phi(x))^{d-1} + 1)$. On the other hand, since $0 = \phi^2(P_s) = \phi(\phi(P_s))$, we may write $\phi(P_s) = \zeta_s \cdot \alpha_f$ where $\alpha_f := \sqrt[d]{-f}$ is a fixed d-th root of $-f$ in $\overline{K}$ and ζ_s is a d-th root of unity. In particular, it follows from (32) that

$$m_{i,j} = \left(\frac{f'}{2d^4 f^2}\right) \cdot \sum_s P_s^{i+j-2d+2} \cdot \left(\zeta_s^2 \alpha_f^2 - d \cdot \alpha_f \cdot f \cdot \zeta_s\right). \tag{33}$$

To show that the Kodaira-Spencer map is non-zero, it suffices to find a single entry $m_{i,j} \neq 0$. To do this, let $i = d - 2$ and $j = 0$. In this case, we see from (33) that

$$m_{d-2,0} = \left(\frac{f'}{2d^4 f^2}\right) \cdot \sum_s \frac{1}{\zeta_s \alpha_f - f} \cdot \left(\zeta_s^2 \alpha_f^2 - d \cdot \alpha_f \cdot f \cdot \zeta_s\right).$$

On the other hand, the formal identity $x^n - y^n = (x-y)\cdot(x^{n-1} + yx^{n-2} + \cdots + y^{n-2}x + y^{n-1})$ applied to $n = d,\ x = \zeta_s \alpha_f$ and $y = f$ implies that

$$m_{d-2,0} = \left(\frac{f'}{2d^4 f^2}\right) \sum_s \left(\left(\frac{-\alpha_f^{d-1}}{f^d + f}\right)\zeta_s^{d-1} + \left(\frac{-\alpha_f^{d-2}\cdot f}{f^d+f}\right)\zeta_s^{d-2} + \cdots + \left(\frac{-f^{d-1}}{f^d+f}\right)\right) \cdot \left(\zeta_s^2 \alpha_f^2 - d\cdot \alpha_f \cdot f \cdot \zeta_s\right).$$

After regrouping terms and changing the order of summation, we see that

$$m_{d-2,0} = \left(\frac{f'}{2d^4 f^2}\right)\cdot\left(\frac{(1-d)\cdot f}{f^{d-1}+1} + \sum_{k=1}^{d-1}\sum_s c_k\, \zeta_s^k\right)$$

for some constants c_k depending only on $1 \le k \le d-1$ (not on s). However, because the function sending $P_s \to \zeta_s$ is a $d:1$ surjection onto μ_d (the group of d-th roots of unity), the sum $\sum_s c_k \zeta^k = (d^2 c_k)\sum_{\zeta\in\mu_d}\zeta^k = 0$ for all indices k. We deduce that

$$m_{d-2,0} = \frac{(1-d)\cdot f'}{2d^4(f^d+f)}. \tag{34}$$

In particular, $m_{d-2,0} \neq 0$ since $f \notin K^p$ and $d \not\equiv 1 \pmod p$. It follows that $C_{2,2}(\phi)$ is a non-isotrivial curve of genus at least 2, and Theorem 1.1 implies that $\mathcal{Z}(\phi, S)$ is finite and $\overline{\mathrm{Avg}}(\mathcal{Z}(\phi), S) = 0$ for all finite subsets $S \subseteq V_K$ as claimed.

On the other hand, essentially the same argument shows that $C_{d,2} : Y^d = \phi^2(x)$ is a non-isotrivial curve of genus at least 2, and we take this approach to prove Theorem 1.5 part (1) when $d \ge 4$ is even. To see that $C_{d,2}$ is non-isotrivial, we use the differentials $\frac{x^{d-2}dx}{y^{d-1}}$ and $\frac{dx}{y}$, which are both holomorphic by [23, Theorem 3], to compute a non-zero entry of the Kodaira-Spencer matrix. In particular, the same Serre duality argument in [22, §5.2] implies that

$$m_{(d-2,d-1),(0,1)} = \sum_s \mathrm{Res}_{P_s}\left(\frac{x^{d-2}\,\phi_t^2\,dx}{y^d\,\phi_x^2}\right)dt = \sum_s \frac{{P_s}^{d-2}\,\phi_t^2(P_s)\,dx}{d\cdot\phi_x^2(P_s)^2}dt, \tag{35}$$

since $y^d = \phi^2(x)$, so that $\phi^2(x)/(x-P_s)|_{P_s} = \phi_x^2(P_s)$ and $(x-P_s)$ is of degree d; here we use Res to denote the residue map on the differentials of a curve [9, Theorem 7.14.1]. Hence, $m_{(d-2,d-1),(0,1)}$ is nothing but $2/d \cdot m_{d-2,0}$ from the hyperelliptic case on (32). We deduce that

$$m_{(d-2,d-1),(0,1)} = \frac{(1-d)\,f'}{d^5\,(f^d+f)} \neq 0,$$

which completes the proof of the first statement.

Now for the proof of part (2). In what follows, we view $\phi(x)$ over $K(\mu_d)$. If d is a prime and $f \notin K(\mu_d)^d$, then we first show that ϕ^n is irreducible over $K(\mu_d)$ for all $n \ge 1$. To see this, we must rule out the presence of d-powers in the orbit of zero. Suppose that $\phi^n(0) \in K(\mu_d)^d$ for some $n \ge 2$. Since, $\phi^n(0) = (((f^d+f)^d+f)^d\cdots+f)^d+f$ and $\mathcal{O}_{K(\mu_d)}$ is a UFD, we may write $\phi^n(0) = f\cdot g_n$ for some $g_n \in \mathcal{O}_{K(\mu_d)}$ coprime to f. It follows that f and g_n must both be d-powers, a contradiction. Hence, $\phi^n(0) \notin K(\mu_d)^d$ for all $n \ge 1$, and [8, Theorem 8] implies that all iterates of ϕ are irreducible over $K(\mu_d)$.

As for the Galois groups of iterates of ϕ, note that Lemma 3.1 (applied inductively to $\psi = \phi$ and $\gamma = \phi$) implies that $G_{K(\mu_d)}(\phi) \le W(d)$. On the other hand, we see that the proofs of Theorem 1.1 and Theorem 1.5 part (1) imply that the d-free part of all but finitely many terms of the orbit $\mathcal{O}_\phi(b)$ contains primitive prime divisors whenever $\hat{h}_\phi(b) \neq 0$. In particular, since $\deg(\phi^n(0)) = d^n \cdot \deg(f)$ goes to infinity, this holds for $b = 0$. Hence, if $K_m(\phi)$ is a splitting field of $\phi^m(x)$ over $K(\mu_d)$, then $\mathrm{Gal}(K_n(\phi)/K_{n-1}(\phi)) \cong (\mathbb{Z}/d\mathbb{Z})^{d^n}$ for all but finitely many n; see [8, Theorem 25]. Therefore, $G_{K(\mu_d)}(\phi) \leq W(d)$ is a finite index subgroup as claimed. $\square$

Remark 3.2. It follows from Theorem 1.5 that $G_{K(\mu_d)}(\phi_f) \leq W(d)$ is a finite index subgroup for all non-constant $f \in K$. To see this, apply Theorem 1.5 to the field $K_0 = \mathbb{F}_p(f) \cong \mathbb{F}_p(t) = K$ and the polynomial $\phi(x) = x^2 + t$ and then use the fact that $[\mathbb{F}_p(t) : \mathbb{F}_p(f)] = \deg(f)$ to get the index bound

$$\left[W(d) : G_{K(\mu_d)}(\phi_f)\right] \leq \left[W(d) : G_{K(\mu_d)}(x^d + t)\right] \cdot \deg(f).$$

In particular, the number of irreducible factors of $\phi_f^n(x)$ over $K(\mu_d)$ (and hence over K) is bounded independently of n (cf. [8, Corollary 7]).

Remark 3.3. We note that $C_{\ell,1}(\phi) : Y^\ell = X^d + f$ is isotrivial for all $\ell \geq 2$: the map $(X, Y) \to \left(\frac{X}{\sqrt[d]{f}}, \frac{Y}{\sqrt[\ell]{f}}\right)$ is an isomorphism (defined over $\overline{K}$) onto the curve $Y^\ell = X^d + 1$. Alternatively, one can compute the Kodaira-Spencer map for the surface $C_{\ell,m}(\phi)$. For instance, when $\ell = 2$, it follows from the formulas in [22, §5.2] that

$$m_{i,j} = \frac{f' \sqrt[d]{-f}}{2d^2} \cdot \sum_{\zeta \in \mu_d} \zeta^{(y_{ij})}, \quad \text{for some } -2d + 2 \leq y_{ij} \leq -d - 1, \ y_{ij} \in \mathbb{Z}.$$

In particular, we see that $y_{ij} \not\equiv 0 \pmod{d}$, from which it follows that $m_{ij} = 0$ for all indices $0 \leq i, j \leq \frac{d-1}{2} - 1$; here again we use the standard basis $\{\frac{x^i dx}{y}\}$ of regular differentials on a hyperelliptic curve. In either case, the examples $\phi(x) = x^d + f$ underscore the importance of passing to an iterate (and its corresponding superelliptic curve) to study primitive prime divisors.

Remark 3.4. Although it was enough to show that certain KS maps were non-zero to prove Theorems 1.1 and 1.5, we believe that the KS maps for the curves $C_{2,2}(\phi) : Y^2 = (x^d + f)^d + f$ and $C_{d,2}(\phi) : Y^d = (x^d + f)^d + f$ have maximal rank, from which it follows that the best possible height bounds (involving a main term of $2 + \epsilon$) hold in these families; see [21]. If such a statement were true, then one could give relatively small bounds for the size of the elements of $\mathcal{Z}(\phi, S)$. In practice, one exploits the fact the KS matrix is symmetric (33) and the fact that the cyclotomic sums $\sum \zeta_s^m$ and power sums $\sum P^m$ vanish (a trace-zero fact), to prove that the KS map has maximal rank.

As for characteristic zero function fields, we can make the index bounds explicit and uniform when $K = k(t)$ is a rational function field; compare to uniform bounds in the quadratic case [12]. Here we use work of Schmidt [34] and Mason [25] on Thue Equations over function fields; conveniently, we need not worry about isotriviality, since it does not affect the height bounds in this setting.

Proof of Theorem 1.6. We work over the ground field $K(\mu_d)$. We have already seen that $f \notin K(\mu_d)^d$ implies all iterates of $\phi(x)$ are irreducible over $K(\mu_d)$; see the proof of Theorem 1.5 above. We show that for all $n \geq 11$, there is a place

$v_n \in V_{K(\mu_d)}$ such that: $v_n(\phi^n(0)) > 0$, $v(\phi^n(0)) \not\equiv 0 \pmod d$ and $v(\phi^m(0)) = 0$ for all $1 \leq m \leq n-1$.

If there is no such place for some $n \geq 2$, then $\phi^n(0) = d_n \cdot y_n^d$ for some (d-power free) d_n satisfying

$$\deg(d_n) \leq (d-1)\sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} \deg(\phi^i(0)) = (d-1)\cdot \sum_{i=1}^{\lfloor \frac{n}{2} \rfloor} \deg(f)\cdot d^{i-1} = \deg(f)\cdot (d^{\lfloor \frac{n}{2} \rfloor+1}-1);$$

see (10) in the proof of Theorem 1.1. Hence the twisted curve $C_\phi^{(d_n)} : Y^d = d_n^{d-1}\cdot(X^d+f)$ has an integral point $(\phi^{n-1}(0), d_n\cdot y_n)$. Let K_1 be a splitting field of ϕ over $K(\mu_d)$, let $\mathfrak{g}_{K_1}$ be the genus of K_1, and let $\mathfrak{r}_{K_1}$ be the number of infinite places of K_1. Then it follows from [25, Theorem 15] that

$$h_{K_1}(\phi^{n-1}(0)) \leq 18h_{K_1}(C_\phi^{(d_n)}) + 6\mathfrak{g}_{K_1} + 3\mathfrak{r}_{K_1} - 3;$$

here $h_{K_1}(C_\phi)$ is the maximum height (relative to K_1) of the coefficients defining $C_\phi^{(d_n)}$. However, [34, 2.11] implies that $h_{K_1}(\alpha) = d\cdot\deg(\alpha)$ for all $\alpha \in K(\mu_d)$ and [34, Lemma H] implies that $\mathfrak{g}_{K_1} \leq (d-1)(\deg(f)-1)$. In particular, we see that

$$d\cdot d^{n-2}\cdot\deg(f) \leq 18\cdot d\cdot\deg(f)\cdot d^{\lfloor \frac{n}{2} \rfloor+1} + 6(d-1)(\deg(f)-1)+3d-3.$$

Therefore,

$$d^{n-1} \leq 18d^{\lfloor \frac{n}{2} \rfloor+2} + (3d-3)\frac{2\deg(f)-1}{\deg(f)} \leq 18d^{\lfloor \frac{n}{2} \rfloor+2}+6d-6.$$

We deduce that $n \leq 2\log_d(19)+5 < 10.4$ since $d \geq 3$ and $n \geq 2$; statements (2) and (3) then follow from [8, Theorem 2.5].

As for the index bound in statement (1), let $K_n(\phi)$ be the splitting field of $\phi^n(x)$ over $K(\mu_d)$. One computes inductively via [5, §3.3 Theorem 19] that $[C_d]^n$ is a group of order $d^{\frac{d^n-1}{d-1}}$ for all $n \geq 1$. On the other hand, since the subextensions $K_n(\phi)/K_{n-1}(\phi)$ are Kummer extensions of degree $d^{d^{n-1}}$ for all $n \geq 11$ by [8, Theorem 2.5] and the first part of our proof, we have the index bound:

$$\log_d\big[\,[C_d]^n : \mathrm{Gal}_{K(\mu_d)}(\phi^n)\big] = \log_d \frac{d^{\frac{d^n-1}{d-1}}}{[K_{10}(\phi):K(\mu_d)]\cdot\prod_{j=10}^{n-1}[K_{j+1}(\phi):K_j(\phi)]}.$$

However, $[K_{10}(\phi):K(\mu_d)] \geq d^{10}$ since $\phi^{10}(x)$ is an irreducible polynomial, and we deduce that

$$\log_d\big[\,[C_d]^n : \mathrm{Gal}_{K(\mu_d)}(\phi^n)\big] \leq \frac{d^n-1}{d-1} - (d^{n-1}+d^{n-2}+\dots d^{10}+10) \leq \frac{d^{10}-1}{d-1}+10.$$

Finally, we consider the special case $\phi(x) = x^d+t$ for all $d \geq 2$ (not necessarily prime). We note that the discriminant of $\phi^n(0)$ (as an element of $k[t]$) is non-zero. In particular, $\phi^n(0)$ is square-free for all n. To see this, let $p|d$ be a prime. Then the quotient map $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ induces a ring homomorphism $\mathbb{Z}[t] \to (\mathbb{Z}/p\mathbb{Z})[t]$ given by reducing coefficients. Therefore, if $\phi^n(0)$ is not square-free in $\overline{\mathbb{Q}}[t]$ (hence not square-free in $\mathbb{Z}[t]$), then the image of $\phi^n(0) \in (\mathbb{Z}/p\mathbb{Z})[t]$ is not square-free. Hence, [5, §13.5 Prop. 33] implies that $\phi^n(0)$ and its formal derivative in $(\mathbb{Z}/p\mathbb{Z})[t]$ must share a root. However. one sees that the formal derivative of $\phi^n(0)$ is 1 in $\mathbb{F}_p[t]$ for all $n \geq 2$ by the power-rule. We deduce that $\phi^n(0)$ is square-free in $k[t]$ for all

$n \geq 1$. It terms of valuations, this means that $v_{\mathfrak{p}}(\phi^n(0)) = 1$ for all $\mathfrak{p} \in V_K$ such that $v_{\mathfrak{p}}(\phi^n(0)) > 0$. On the other hand, a simple degree computation shows

$$\begin{aligned}\deg(\phi^n(0)) = d^{n-1} &> \frac{d^{n-1}-1}{d-1}\\ &= d^{n-2} + d^{n-3} + \cdots + 1 = \deg(\phi^{n-1}(0)) + \cdots + \deg(\phi(0)).\end{aligned}$$

Therefore, it is impossible that all prime factors of $\phi^n(0)$ come from lower order iterates. Moreover, since $\phi^n(0)$ is square-free, it follows from [8, Theorem 8] that all iterates of ϕ are irreducible over $K(\mu_d)$. We deduce from [8, Theorem 25] that $G_{K(\mu_d)}(\phi) \cong W(d)$ as claimed. The statement about specializations follows from Hilbert's irreducibility theorem [37, Theorem 1, Theorem 3.4.1]. ☐

Remark 3.5. The proof of Theorem 1.6 implies that

$$\max\left\{\, n \;\middle|\; n \in \mathcal{Z}(x^d+f,0,d) \text{ for some } f \in k[t],\ \deg(f) \geq 1,\ d \geq 2 \,\right\} \leq 10;$$

here $\mathcal{Z}(x^d+f,0,d)$ is the d-th Zsigmondy set [11, Definition 2], representing terms which do not have d-power free primitive prime divisors. Equivalently, after the 10th stage of iteration, we always see d-power free primitive prime in the orbit of zero (independent of both $f \in k[t]$ and d) in characteristic zero (cf. [24, Theorem 1.1]).

Remark 3.6. It is tempting to think that the discriminant trick we used to prove $G_{K(\mu_d)}(\phi) \cong W(d)$ for $\phi(x) = x^d + t$ works for all $\phi(x) = x^d + f$ satisfying $f \notin K(\mu_d)^d$. However, surjectivity already fails for $d = 2$: when $\phi(x) = x^2 - (t^2+1)$, we show in [12] that $[W(2) : G_K(\phi)] = 2$, even though $-(t^2+1)$ is never a square in characteristic zero; this example is essentially due to Stoll [45]. Likewise, this discriminant trick does not work in prime characteristic: for $d = 5$, $p = 43$ and $\phi(x) = x^5 + t$, the discriminant of $\phi^6(0)$ is zero in $\mathbb{F}_p[t]$. Nevertheless, a finite index statement (not necessarily surjective) holds by Theorem 1.5.

Remark 3.7. To the author's knowledge, there is not a single pair (d, c) of values $d \geq 3$ and $c \in \mathbb{Q}$ for which $\mathrm{Gal}_{\mathbb{Q}(\mu_d)}(\phi_c^n)$ is known for large n. Therefore, Theorem 1.6 represents some progress and solves the inverse Galois problem for $[C_d]^n$.

Remark 3.8. To prove the surjectivity of the ℓ-adic Galois representation attached to an elliptic curve, it suffices to prove the surjectivity onto some finite quotient. Namely, if $G \leq \mathrm{GL}_2(\mathbb{Z}_\ell)$ is a closed subgroup that surjects onto $\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ for some small n, then G must be equal to $\mathrm{GL}_2(\mathbb{Z}_\ell)$; see, for instance, [46]. In particular, this is a fact from group theory. On the other hand, such a property will fail in general for closed subgroups of $W(d)$. Nevertheless, we have proven such rigidity for subgroups $G_K(\phi) \leq W(d)$ coming from dynamics in Theorem 1.6.

Acknowledgments

It is a pleasure to thank Rafe Jones, Brian Conrad, Bjorn Poonen, and Felipe Voloch for the useful discussions related to the work in this paper. The author also thanks the anonymous referees for their comments.

References

[1] Matthew Baker, *A finiteness theorem for canonical heights attached to rational maps over function fields*, J. Reine Angew. Math. **626** (2009), 205–233, DOI 10.1515/CRELLE.2009.008. MR2492995

[2] A. S. Bang, *Taltheoretiske Undersogelse*, Tidsskrift Mat., 4.5 (1886): 70-80, 130-137.

[3] Lizhen Ji, Kefeng Liu, and Shing-Tung Yau, *Preface to the Serre issues [Special issue: in honor of Jean-Pierre Serre, Part 1 of 2]*, Pure Appl. Math. Q. **4** (2008), no. 4, Special Issue: In honor of Jean-Pierre Serre., 1–2, DOI 10.4310/PAMQ.2008.v4.n1.a1. MR2440249

[4] J. Cahn, R. Jones, and J. Spear, *Powers in orbits of rational functions: cases of an arithmetic dynamical Mordell-Lang conjecture*, preprint arXiv:1512.03085

[5] David S. Dummit and Richard M. Foote, *Abstract algebra*, 3rd ed., John Wiley & Sons, Inc., Hoboken, NJ, 2004. MR2286236

[6] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern* (German), Invent. Math. **73** (1983), no. 3, 349–366, DOI 10.1007/BF01388432. MR718935

[7] C. Gratton, K. Nguyen, and T. J. Tucker, *ABC implies primitive prime divisors in arithmetic dynamics*, Bull. Lond. Math. Soc. **45** (2013), no. 6, 1194–1208, DOI 10.1112/blms/bdt049. MR3138487

[8] Spencer Hamblen, Rafe Jones, and Kalyani Madhu, *The density of primes in orbits of $z^d + c$*, Int. Math. Res. Not. IMRN **7** (2015), 1924–1958, DOI 10.1093/imrn/rnt349. MR3335237

[9] Robin Hartshorne, *Algebraic geometry*, Springer-Verlag, New York-Heidelberg, 1977. Graduate Texts in Mathematics, No. 52. MR0463157

[10] W. Hindes, *The average number of integral points in orbits*, preprint, arXiv:1509.00752 (2015).

[11] Wade Hindes, *Prime divisors in polynomial orbits over function fields*, Bull. Lond. Math. Soc. **48** (2016), no. 6, 1029–1036, DOI 10.1112/blms/bdw061. MR3608948

[12] Wade Hindes, *Galois uniformity in quadratic dynamics over $k(t)$*, J. Number Theory **148** (2015), 372–383, DOI 10.1016/j.jnt.2014.09.033. MR3283185

[13] Patrick Ingram, *Arboreal Galois representations and uniformization of polynomial dynamics*, Bull. Lond. Math. Soc. **45** (2013), no. 2, 301–308, DOI 10.1112/blms/bds088. MR3064415

[14] Patrick Ingram and Joseph H. Silverman, *Primitive divisors in arithmetic dynamics*, Math. Proc. Cambridge Philos. Soc. **146** (2009), no. 2, 289–302, DOI 10.1017/S0305004108001795. MR2475968

[15] Patrick Ingram and Joseph H. Silverman, *Uniform estimates for primitive divisors in elliptic divisibility sequences*, Number theory, analysis and geometry, Springer, New York, 2012, pp. 243–271, DOI 10.1007/978-1-4614-1260-1_12. MR2867920

[16] Rafe Jones, *Galois representations from pre-image trees: an arboreal survey* (English, with English and French summaries), Actes de la Conférence "Théorie des Nombres et Applications", Publ. Math. Besançon Algèbre Théorie Nr., vol. 2013, Presses Univ. Franche-Comté, Besançon, 2013, pp. 107–136. MR3220023

[17] Rafe Jones, *The density of prime divisors in the arithmetic dynamics of quadratic polynomials*, J. Lond. Math. Soc. (2) **78** (2008), no. 2, 523–544, DOI 10.1112/jlms/jdn034. MR2439638

[18] R. Jones and A. Levy, *Eventually stable rational functions*, preprint, arXiv:1603.00673.

[19] Rafe Jones and Michelle Manes, *Galois theory of quadratic rational functions*, Comment. Math. Helv. **89** (2014), no. 1, 173–213, DOI 10.4171/CMH/316. MR3177912

[20] Jamie Juul, Pär Kurlberg, Kalyani Madhu, and Tom J. Tucker, *Wreath products and proportions of periodic points*, Int. Math. Res. Not. IMRN **13** (2016), 3944–3969, DOI 10.1093/imrn/rnv273. MR3544625

[21] Minhyong Kim, *Geometric height inequalities and the Kodaira-Spencer map*, Compositio Math. **105** (1997), no. 1, 43–54, DOI 10.1023/A:1017995416618. MR1436743

[22] Minhyong Kim, Dinesh S. Thakur, and José Felipe Voloch, *Diophantine approximation and deformation* (English, with English and French summaries), Bull. Soc. Math. France **128** (2000), no. 4, 585–598. MR1815399

[23] Ja Kyung Koo, *On holomorphic differentials of some algebraic function field of one variable over* **C**, Bull. Austral. Math. Soc. **43** (1991), no. 3, 399–405, DOI 10.1017/S0004972700029245. MR1107394

[24] Holly Krieger, *Primitive prime divisors in the critical orbit of $z^d + c$*, Int. Math. Res. Not. IMRN **23** (2013), 5498–5525. MR3142262

[25] R. C. Mason, *Diophantine equations over function fields*, London Mathematical Society Lecture Note Series, vol. 96, Cambridge University Press, Cambridge, 1984. MR754559

[26] Vijaya Kumar Murty and John Scherk, *Effective versions of the Chebotarev density theorem for function fields* (English, with English and French summaries), C. R. Acad. Sci. Paris Sér. I Math. **319** (1994), no. 6, 523–528. MR1298275

[27] Miklós Abért and Bálint Virág, *Dimension and randomness in groups acting on rooted trees*, J. Amer. Math. Soc. **18** (2005), no. 1, 157–192, DOI 10.1090/S0894-0347-04-00467-9. MR2114819

[28] Atsushi Moriwaki, *Geometric height inequality on varieties with ample cotangent bundles*, J. Algebraic Geom. **4** (1995), no. 2, 385–396. MR1311357

[29] R. W. K. Odoni, *The Galois theory of iterates and composites of polynomials*, Proc. London Math. Soc. (3) **51** (1985), no. 3, 385–414, DOI 10.1112/plms/s3-51.3.385. MR805714

[30] R. Pink, *Profinite iterated monodromy groups arising from quadratic polynomials*, preprint arXiv:1307.5678.

[31] Brian Rice, *Primitive prime divisors in polynomial arithmetic dynamics*, Integers **7** (2007), A26, 16. MR2312276

[32] Michael Rosen, *Number theory in function fields*, Graduate Texts in Mathematics, vol. 210, Springer-Verlag, New York, 2002. MR1876657

[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, DOI 10.1515/crll.1974.268-269.27. Collection of articles dedicated to Helmut Hasse on his seventy-fifth birthday, II. MR0344221

[34] Wolfgang M. Schmidt, *Thue's equation over function fields*, J. Austral. Math. Soc. Ser. A **25** (1978), no. 4, 385–422. MR508466

[35] Jean-Pierre Serre, *Abelian l-adic representations and elliptic curves*, McGill University lecture notes written with the collaboration of Willem Kuyk and John Labute, W. A. Benjamin, Inc., New York-Amsterdam, 1968. MR0263823

[36] Jean-Pierre Serre, *Lectures on $N_X(p)$*, Chapman & Hall/CRC Research Notes in Mathematics, vol. 11, CRC Press, Boca Raton, FL, 2012. MR2920749

[37] Jean-Pierre Serre, *Topics in Galois theory*, 2nd ed., Research Notes in Mathematics, vol. 1, A K Peters, Ltd., Wellesley, MA, 2008. With notes by Henri Darmon. MR2363329

[38] Joseph H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994. MR1312368

[39] Joseph H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1986. MR817210

[40] Joseph H. Silverman, *Integer points, Diophantine approximation, and iteration of rational maps*, Duke Math. J. **71** (1993), no. 3, 793–829, DOI 10.1215/S0012-7094-93-07129-3. MR1240603

[41] Joseph H. Silverman, *Primitive divisors, dynamical Zsigmondy sets, and Vojta's conjecture*, J. Number Theory **133** (2013), no. 9, 2948–2963, DOI 10.1016/j.jnt.2013.03.005. MR3057058

[42] Joseph H. Silverman, *The arithmetic of dynamical systems*, Graduate Texts in Mathematics, vol. 241, Springer, New York, 2007. MR2316407

[43] Vijay A. Sookdeo, *Integer points in backward orbits*, J. Number Theory **131** (2011), no. 7, 1229–1239, DOI 10.1016/j.jnt.2011.01.005. MR2782838

[44] Henning Stichtenoth, *Algebraic function fields and codes*, Universitext, Springer-Verlag, Berlin, 1993. MR1251961

[45] Michael Stoll, *Galois groups over $\mathbf{Q}$ of some iterated polynomials*, Arch. Math. (Basel) **59** (1992), no. 3, 239–244, DOI 10.1007/BF01197321. MR1174401

[46] Adrian Vasiu, *Surjectivity criteria for p-adic representations. I*, Manuscripta Math. **112** (2003), no. 3, 325–355, DOI 10.1007/s00229-003-0402-4. MR2067042

[47] Paul Vojta, *Diophantine approximation and Nevanlinna theory*, Arithmetic geometry, Lecture Notes in Math., vol. 2009, Springer, Berlin, 2011, pp. 111–224, DOI 10.1007/978-3-642-15945-9_3. MR2757629

[48] José Felipe Voloch, *Diophantine geometry in characteristic p: a survey*, Arithmetic geometry (Cortona, 1994), Sympos. Math., XXXVII, Cambridge Univ. Press, Cambridge, 1997, pp. 260–278. MR1472501

[49] K. Zsigmondy, *Zur Theorie der Potenzreste* (German), Monatsh. Math. Phys. **3** (1892), no. 1, 265–284, DOI 10.1007/BF01692444. MR1546236

Department of Mathematics, CUNY Graduate Center, 365 Fifth Avenue, New York, New York 10016-4309

Email address: whindes@gc.cuny.edu