Bulletin of the London Mathematical Society Advance Access published July 29, 2013

Bull. London Math. Soc. Page 1 of 15
doi:10.1112/blms/bdt049

ABC implies primitive prime divisors in arithmetic dynamics

C. Gratton, K. Nguyen and T. J. Tucker

Abstract

Let K be a number field, let $\varphi(x) \in K(x)$ be a rational function of degree $d > 1$, and let $\alpha \in K$ be a wandering point such that $\varphi^n(\alpha) \neq 0$ for all $n > 0$. We prove that if the *abc*-conjecture holds for K, then for all but finitely many positive integers n, there is a prime $\mathfrak{p}$ of K such that $v_\mathfrak{p}(\varphi^n(\alpha)) > 0$ and $v_\mathfrak{p}(\varphi^m(\alpha)) \leqslant 0$ for all positive integers $m < n$. Under appropriate ramification hypotheses, we can replace the condition $v_\mathfrak{p}(\varphi^n(\alpha)) > 0$ with the stronger condition $v_\mathfrak{p}(\varphi^n(\alpha)) = 1$. We prove the same result unconditionally for function fields of characteristic 0 when φ is not isotrivial.

1. *Introduction*

Let K be a number field or function field, let $\varphi(x) \in K(x)$ be a rational function of degree $d > 1$, and let $\alpha \in K$. We denote the n-iterate of φ as φ^n. It is often the case that for all but finitely many n, there is a prime that is a divisor of $\varphi^n(\alpha)$, but is not a divisor of $\varphi^m(\alpha)$ for any $m < n$. This problem was considered by Bang [**2**], Zsigmondy [**38**], and Schinzel [**27**] in the context of the multiplicative group. More recently, many authors have considered the problem in other cases. Most of these results apply either when 0 is preperiodic under φ (see [**11**, **16**], for example) or when 0 is a ramification point of φ (see [**8**, **20**, **25**]). Much work has been done on this problem in the setting of elliptic curves (refer to [**10**, **15**], for example). However, here we do not have an underlying algebraic group. In this paper, we show that similar results will hold in close to full generality, assuming the *abc*-conjecture of Masser–Oesterlé–Szpiro for number fields. Our result also holds unconditionally over characteristic 0 function fields, where the *abc*-conjecture is a theorem of Stothers [**33**]. Note that Mason [**21**] (and Silverman [**29**]) proved it independently a few years later without knowing about Stother's result. We are not, however, able to derive our result directly from the *abc*-conjecture in this case, because of the absence of Belyi maps (see Lemma 3.2) over function fields; our proof requires a more difficult theorem of Yamanoi [**37**] conjectured by Vojta [**35**].

We will say that a field K is an *abc-field* if K is a number field satisfying the *abc*-conjecture [**34**] or a characteristic zero function field of transcendence degree 1. We define the *orbit* $\mathrm{Orb}_\varphi(\alpha)$ of a point α under a map φ to be $\mathrm{Orb}_\varphi(\alpha) = \bigcup_{i=1}^{\infty}\{\varphi^i(\alpha)\}$. Observe that this definition of orbit is non-standard, as typically $\varphi^0(\alpha) = \alpha$ is included in the orbit. But this non-standard definition of orbit will make it easier to state the main theorems of this paper. We say that a point γ is *exceptional* if $\varphi^{-2}(\gamma) = \{\gamma\}$. The most general results here are most naturally stated in terms of the canonical height h_φ of Call and Silverman [**7**] (see Section 2 for its definition and a few of its basic properties).

In keeping with the terminology of [**16**, **27**], we say that $\mathfrak{p}$ is a *primitive prime factor* of $\varphi^n(\alpha) - \beta$ if $v_\mathfrak{p}(\varphi^n(\alpha) - \beta) > 0$ and $v_\mathfrak{p}(\varphi^m(\alpha) - \beta) \leqslant 0$ for all $m < n$. We say that $\mathfrak{p}$ is a *square-free primitive prime factor* if $v_\mathfrak{p}(\varphi^n(\alpha) - \beta) = 1$ and $v_\mathfrak{p}(\varphi^m(\alpha) - \beta) \leqslant 0$ for all $m < n$.

Received 7 November 2012; revised 9 March 2013.

2010 *Mathematics Subject Classification* 37P05, 11G50, 14G25.

The first and third authors were partially supported by NSF Grants DMS-0854839 and DMS-1200749. The second author was partially supported by NSF Grant DMS-0901149.

With this notation and terminology, the main theorem of our paper is the following.

Theorem 1.1. *Let K be an abc-field, let $\varphi \in K(x)$ have degree $d > 1$, and let $\alpha, \beta \in K$, where $h_\varphi(\alpha) > 0$ and $\beta \notin \mathrm{Orb}_\varphi(\alpha)$. Suppose that β is not exceptional for φ. Then for all but finitely many positive integers n, there is a prime $\mathfrak{p}$ of K such that $\mathfrak{p}$ is a primitive prime factor of $\varphi^n(\alpha) - \beta$.*

We will say that φ is *dynamically unramified* over β if there are infinitely many $\tau \in \bar{K}$ such that $\varphi^n(\tau) = \beta$ and $e_{\varphi^n}(\tau/\beta) = 1$ for some n, where $e_{\varphi^n}(\tau/\beta)$ is the ramification index of φ^n at τ over β. Since φ has only finitely many critical points, saying φ is dynamically unramified over β means that there is at least one infinite backward orbit that contains no critical points.

Theorem 1.2. *Let K be an abc-field, let $\varphi \in K(x)$ have degree $d > 1$, and let $\alpha, \beta \in K$, where $h_\varphi(\alpha) > 0$ and $\beta \notin \mathrm{Orb}_\varphi(\alpha)$. Suppose that φ is dynamically unramified over β. Then for all but finitely many positive integers n, there is a prime $\mathfrak{p}$ of K such that $\mathfrak{p}$ is a square-free primitive prime factor of $\varphi^n(\alpha) - \beta$.*

In fact, the conclusion of Theorem 1.2 is false for any φ that *fails* to be dynamically unramified over β; see Remark 5.5. This is most easily seen in the case of maps such as $\varphi(x) = (x - a)^2$, which have the property that $\varphi^n(\alpha)$ is always a perfect square because φ^n itself is a perfect square in the field of rational functions.

Theorem 1.2 shows that the *abc*-conjecture implies what Jones and Boston call the 'Strong Dynamical Wieferich Prime Conjecture' [**6**, Conjecture 4.5]. Silverman [**30**] had earlier shown that the *abc*-conjecture implies a logarithmic lower bound on the growth of the number of Wieferich primes; a Wieferich prime is a prime p for which $2^{p-1} \not\equiv 1 \pmod{p^2}$.

Theorems 1.1 and 1.2 may also be stated in terms of *wandering* α. We say that α is wandering if $\varphi^n(\alpha) \neq \varphi^m(\alpha)$ for all $n > m > 0$; this is equivalent to saying that $\mathrm{Orb}_\varphi(\alpha)$ is infinite. It follows immediately from Northcott's theorem (as stated on [**31**, p. 94]) that $h_\varphi(\alpha) \neq 0$ if and only if $\alpha \in K$ is wandering for $\varphi \in K(x)$, where K is a number field and $\deg \varphi > 1$ (see [**7**]). By works of Benedetto [**4**] and Baker [**1**], one has the same result for non-isotrivial rational functions over a function field. A rational function over a function field K is said to be *isotrivial* if it cannot be defined over a finite extension of the field of constants of K, up to change of coordinates; more precisely, we say that φ is isotrivial if there exists $\psi \in \bar{K}(x)$ of degree 1 such that $(\psi^{-1} \circ \varphi \circ \psi) \in \bar{k}(x)$, where ψ^{-1} is the compositional inverse of ψ (that is, $\psi^{-1}(\psi(x)) = x$ in $\bar{K}(x)$).

Baker's result says that if K is a function field and $\varphi \in K(x)$ is a non-isotrivial map with $\deg \varphi > 1$, then $\alpha \in K$ is wandering if and only if $h_\varphi(\alpha) \neq 0$.

Thus, the following are immediate corollaries of Theorems 1.1 and 1.2.

Corollary 1.3. *Let K be an abc-field, let $\varphi \in K(x)$ have degree $d > 1$, and let $\alpha, \beta \in K$, where α is wandering and $\beta \notin \mathrm{Orb}_\varphi(\alpha)$. Suppose that β is not exceptional for φ. Furthermore, assume that φ is non-isotrivial if K is a function field. Then for all but finitely many positive integers n, there is a prime $\mathfrak{p}$ of K such that $\mathfrak{p}$ is a primitive prime factor of $\varphi^n(\alpha) - \beta$.*

Corollary 1.4. *Let K be an abc-field, let $\varphi \in K(x)$ have degree $d > 1$, and let $\alpha, \beta \in K$, where α is wandering and $\beta \notin \mathrm{Orb}_\varphi(\alpha)$. Suppose that φ is dynamically unramified over β and that φ is non-isotrivial if K is a function field. Then for all but finitely many positive integers n, there is a prime $\mathfrak{p}$ of K such that $\mathfrak{p}$ is a square-free primitive prime factor of $\varphi^n(\alpha) - \beta$.*

The strategy of the proofs of Theorems 1.1 and 1.2 is fairly simple. First, we show, in Propositions 3.4 and 4.2, that if F is a polynomial of reasonably high degree without repeated roots, then for any τ of large height, the product of the distinct prime factors of $F(\tau)$ is large, assuming the *abc*-conjecture in the number field case (following Granville [**13**], we call these 'Roth-*abc*' theorems). We then apply this to an appropriate factor F of the numerator of a power φ^i of φ, after proving, in Proposition 5.1, that the product of the distinct factors of $\prod_{\ell=1}^{n-1}\varphi^\ell(\alpha)$ that are also factors of $F(\varphi^{n-i}(\alpha))$ must be very small. With at most finitely many exceptions, any prime that divides $F(\varphi^{n-i}(\alpha))$ also divides $\varphi^n(\alpha)$, so $\varphi^n(\alpha)$ must then have a factor that is not a factor of $\varphi^m(\alpha)$ for any $m < n$. This completes the proof when $\beta = 0$, and a simple coordinate change argument, Lemma 5.3, gives the case of arbitrary $\beta \in K$.

An outline of the paper is as follows. We begin by setting our notation and terminology in Section 2. In Section 3, we modify a result of Granville [**13**] that enables us to say, roughly, that polynomials without repeated factors take on 'reasonably square-free' values in general, assuming the *abc*-conjecture; this is Proposition 3.4. Then, in Section 4, we derive the same result for function fields, unconditionally, using recent work of Yamanoi [**37**]; this is Proposition 4.2. This enables us to give a proof of our main results in Section 5, using Proposition 5.1. We end with some applications of Theorem 1.2 to iterated Galois groups, in Section 6.

REMARK 1.5. When $\beta \in \mathrm{Orb}_\varphi(\alpha)$ and α is wandering, there is a unique M such that $\varphi^M(\alpha) = \beta$. Hence, Theorems 1.1 and 1.2 still hold if we impose the additional condition $m \neq M$ on the positive integers $m < n$ in the statements of these theorems.

2. *Preliminaries*

We set the following:

(1) K is a number field or one-dimensional function field of characteristic 0;
(2) if K is a function field, then we let k denote its field of constants;
(3) $\mathfrak{p}$ is a finite prime of K;
(4) $k_\mathfrak{p}$ is the residue field of $\mathfrak{p}$;
(5) if K is a number field, then we let $N_\mathfrak{p} = \log(\#k_\mathfrak{p})/[K:\mathbb{Q}]$;
(6) if K is a function field, then we let $N_\mathfrak{p} = [k_\mathfrak{p} : k]$;
(7) $\varphi \in K(x)$ is a rational function of degree $d > 1$.

All of this is completely standard with one exception: the quantity $N_\mathfrak{p}$ has been normalized in the case of number fields. We divide by $[K:\mathbb{Q}]$ in our definition so that we can use the same proofs (without reference to possible normalization factors) for number fields and function fields in Section 5.

When K is a number field, we let $\mathfrak{o}_K$ denote the ring of algebraic integers of K as usual. When K is a function field, we choose a prime $\mathfrak{r}$, and let $\mathfrak{o}_K$ denote the set $\{z \in K \mid v_\mathfrak{p}(z) \geqslant 0 \text{ for all primes } \mathfrak{p} \neq \mathfrak{r} \text{ in } K\}$.

If K is a number field, then the height of $\alpha \in K$ is

$$h(\alpha) = -\sum_{\text{primes } \mathfrak{p} \text{ of } \mathfrak{o}_K} \min(v_\mathfrak{p}(\alpha), 0)\, N_\mathfrak{p} + \frac{1}{[K:\mathbb{Q}]}\sum_{\sigma : K \hookrightarrow \mathbb{C}} \max(\log|\sigma(\alpha)|, 0). \tag{2.1}$$

(Note that the $\sigma : K \hookrightarrow \mathbb{C}$ is simply all maps from K to $\mathbb{C}$; in particular, we do not identify complex conjugate embeddings in any way.) We extend our definition of $h(\alpha)$ to the point at infinity by setting $h(\infty) = 0$.

If K is a function field, then the height of $\alpha \in K$ is

$$h(\alpha) = -\sum_{\text{primes } \mathfrak{p} \text{ of } K} \min(v_\mathfrak{p}(\alpha), 0)\, N_\mathfrak{p}\,.$$

In either case, for $\alpha \neq 0$ the product formula gives the inequality

$$\sum_{v_{\mathfrak{p}}(\alpha)>0} v_{\mathfrak{p}}(\alpha)\, N_{\mathfrak{p}} \leqslant h(\alpha). \tag{2.2}$$

We will work with the canonical height h_φ, which is defined as

$$h_\varphi(z) = \lim_{n\to\infty} \frac{h(\varphi^n(z))}{d^n}. \tag{2.3}$$

The convergence of the right-hand side follows from a telescoping series argument due to Tate. The canonical height has the following important properties:

$$h_\varphi(\varphi(z)) = d h_\varphi(z) \quad \text{for all } z \in K; \tag{2.4}$$

$$\text{there is a constant } C_\varphi \text{ such that } |h(z) - h_\varphi(z)| < C_\varphi \quad \text{for all } z \in K. \tag{2.5}$$

It follows immediately from (2.4) and (2.5) that

$$h_\varphi(\alpha) \neq 0 \iff \lim_{s\to\infty} h(\varphi^s(\alpha)) = \infty. \tag{2.6}$$

We refer the readers to the work of Call and Silverman [7] for details on the proofs of the various properties of h_φ.

We say that a point α is *preperiodic* if there exist $n > m > 0$ such that $\varphi^m(\alpha) = \varphi^n(\alpha)$; we will say that α is *periodic* if there is an $n > 0$ such that $\varphi^n(\alpha) = \alpha$. Note that a point is wandering if and only if it is not preperiodic.

We write $\varphi(x) = P(x)/Q(x)$ for $P, Q \in \mathfrak{o}_K[x]$ having no common roots in $\bar{K}$. Then we may write $\varphi^i(x) = P_i(x)/Q_i(x)$, where P_i and Q_i are defined recursively in terms of P and Q. This is most easily explained by passing to homogeneous coordinates. We let $p(x, y)$ and $q(x, y)$ be the degree d homogenizations of P and Q, respectively. Set $p_0(x, y) = x$ and $q_0(x, y) = y$. Then we define recursively

$$p_i(x, y) = p(p_{i-1}(x, y), q_{i-1}(x, y))$$

and

$$q_i(x, y) = q(p_{i-1}(x, y), q_{i-1}(x, y)),$$

for all $i \geqslant 1$. Letting $P_i = p_i(x, 1)$ and $Q_i = q_i(x, 1)$ then gives our P_i and Q_i. We will say that $\mathfrak{p}$ is a prime of *weak good reduction* if $P(x)$ and $Q(x)$ have no common root modulo $\mathfrak{p}$ and the polynomials $p(1, y)$ and $q(1, y)$ have no common roots modulo $\mathfrak{p}$. The reason this notion is called *weak* good reduction is because we are ruling out common roots only in the residue field $k_{\mathfrak{p}}$. Note that we are allowing common roots in $\overline{k_{\mathfrak{p}}}$. When $\mathfrak{p}$ is a prime of weak good reduction, φ induces a well-defined map from $k_{\mathfrak{p}} \cup \infty$ to itself. To describe this, let $r_{\mathfrak{p}}$ be the reduction map $r_{\mathfrak{p}} : K \longrightarrow k_{\mathfrak{p}} \cup \infty$ given by $r_{\mathfrak{p}}(z) = z \pmod{\mathfrak{p}}$ if $v_{\mathfrak{p}}(z) \geqslant 0$ and $r_{\mathfrak{p}}(z) = \infty$ if $v_{\mathfrak{p}}(z) < 0$. Then letting $\varphi(r_{\mathfrak{p}}(z)) = r_{\mathfrak{p}}(\varphi(z))$ defines a well-defined map on residue classes and thus gives the desired map. So if $r_{\mathfrak{p}}(z_1) = r_{\mathfrak{p}}(z_2)$, then $r_{\mathfrak{p}}(\varphi(z_1)) = r_{\mathfrak{p}}(\varphi(z_2))$. Thus, φ takes residue classes to residue classes. We will make use of this in Proposition 5.1.

When K is a function field, we say that φ is isotrivial if $\varphi = \sigma^{-1}\psi\sigma$ for some $\sigma \in \bar{K}(x)$ with $\deg \sigma = 1$ and some $\psi \in \bar{k}(x)$, where k is the field of constants in K. Here σ^{-1} is the compositional inverse of σ; we have $\sigma(\sigma^{-1}(x)) = \sigma^{-1}(\sigma(x)) = x$ in the field $\bar{K}(x)$.

Finally, a few words on notation and conventions. The zeroth iterate of any map is taken to be the identity. Since our maps φ are rational, rather than polynomials, they induce maps from $K \cup \{\infty\}$ to $K \cup \{\infty\}$. When $\varphi^n(\alpha) = \infty$ and $\beta \in K$, we say that for any prime $\mathfrak{p}$, we have $v_{\mathfrak{p}}(\infty - \beta) = 0$ if $v_{\mathfrak{p}}(\beta) \geqslant 0$ and $v_{\mathfrak{p}}(\infty - \beta) = -v_{\mathfrak{p}}(\beta)$ if $v_{\mathfrak{p}}(\beta) < 0$. When $\varphi^n(\tau) = \beta$, we let $e_{\varphi^n}(\tau/\beta)$ denote the ramification index of φ^n at τ over β.

3. *Roth-abc for number fields*

The main result of this section, Proposition 3.4, is a direct translation of [**13**, Theorem 5] into the more general setting of number fields. Following Granville, we refer to this as a 'Roth-*abc*' type result, because it can be interpreted as a strengthening of Roth's theorem [**26**] (in particular, the $-2-\epsilon$ here plays the same role as the $2+\epsilon$ in Roth's theorem). The techniques are the same as those of [**13**]. We include a full proof for the sake of completeness. The methods here are also quite similar to those of [**9**] (see especially p. 105) and [**5**, Theorem 14.4.16].

Let K be a number field. We will be using a version of the '*abc*-Conjecture for Number Fields'. Recall our definition of $h(z)$ for $z \in K$ from (2.1). For $n \geqslant 2$, we may extend this definition to an n-tuple $(z_1, \ldots, z_n) \in K^n \setminus \{(0, \ldots, 0)\}$ by letting

$$h(z_1, \ldots, z_n) = -\sum_{\text{primes } \mathfrak{p} \text{ of } \mathfrak{o}_K} \min(v_{\mathfrak{p}}(z_1), \ldots, v_{\mathfrak{p}}(z_n))\, N_{\mathfrak{p}} + \frac{1}{[K:\mathbb{Q}]} \sum_{\sigma: K \hookrightarrow \mathbb{C}} \max(\log|\sigma(z_1)|, \ldots, \log|\sigma(z_n)|). \tag{3.1}$$

Note that when $z_2 \neq 0$, we have $h(z_1, z_2) = h(z_1/z_2, 1) = h(z_1/z_2)$.

For any $(z_1, \ldots, z_n) \in (K^*)^n$, we define

$$I(z_1, \ldots, z_n) = \{\text{primes } \mathfrak{p} \text{ of } \mathfrak{o}_K \mid v_{\mathfrak{p}}(z_i) \neq v_{\mathfrak{p}}(z_j) \text{ for some } 1 \leqslant i, j \leqslant n\},$$

and let

$$\operatorname{rad}(z_1, \ldots, z_n) = \sum_{\mathfrak{p} \in I(z_1, \ldots, z_n)} N_{\mathfrak{p}}\,.$$

With all of this notation set, the *abc*-conjecture for number fields says the following.

Conjecture 3.1. For any $\epsilon > 0$, there exists a constant $C_{K,\epsilon} > 0$ such that for all $a, b, c \in K^*$ satisfying $a + b = c$, we have $h(a, b, c) < (1 + \epsilon) \operatorname{rad}(a, b, c) + C_{K,\epsilon}$.

Following Granville [**13**], we start by proving a homogeneous form of Roth-*abc*. Let S be a finite set of finite primes of K. We will say that a pair $(z_1, z_2) \in \mathfrak{o}_K$ is in *S-reduced form* if they have no common prime factors outside of S, that is, $\min(v_{\mathfrak{p}}(z_1), v_{\mathfrak{p}}(z_2)) = 0$ for all $\mathfrak{p} \notin S$. We will use a well-known result of Belyi [**3**].

Lemma 3.2. *Given any homogeneous $f(x, y) \in K[x, y]$, we can determine homogeneous polynomials $a(x, y), b(x, y), c(x, y) \in \mathfrak{o}_K[x, y]$ satisfying $a(x, y) + b(x, y) = c(x, y)$, all of degree $D \geqslant 1$, with no common linear factors, where $a(x, y)b(x, y)c(x, y)$ has exactly $D + 2$ non-proportional linear factors (over $\bar{K}$), which include all the factors of $f(x, y)$.*

The conclusion of Lemma 3.2 [**3**] can be more cleanly stated as follows: The divisor of *abc* in $\mathbf{P}^1(\bar{K})$ is a sum of $D + 2$ points, each having multiplicity 1. Now let $Q(\mathfrak{p})$ be a condition involving the prime $\mathfrak{p}$. Then when a sum of the following form appears, $\sum_{Q(\mathfrak{p})}$, interpret this to mean that the indicated sum is being taken over all (finite) primes $\mathfrak{p}$ satisfying the condition $Q(\mathfrak{p})$. We may then prove the following.

Proposition 3.3. *Let $f(x, y) \in \mathfrak{o}_K[x, y]$ be a homogeneous polynomial of degree 3 or more without repeated factors. Let $\epsilon > 0$ and let S be a finite set of finite places of K. Suppose that*

K is a number field satisfying the abc-conjecture. Then

$$(\deg f - 2 - \epsilon)h(z_1, z_2) \leqslant \left(\sum_{v_{\mathfrak{p}}(f(z_1,z_2))>0} N_{\mathfrak{p}} \right) + O_{K,S,\epsilon,f}(1),$$

for all $(z_1, z_2) \in \mathfrak{o}_K$ in S-reduced form.

Proof. We begin by applying Lemma 3.2 to obtain $a(x,y), b(x,y), c(x,y) \in \mathfrak{o}_K[x,y]$ of degree D where $a(x,y)b(x,y)c(x,y)$ has exactly $D+2$ non-proportional linear factors (over $\bar{K}$), which include all the factors of $f(x,y)$, and $a(x,y)+b(x,y) = c(x,y)$. Write the product of the factors of $a(x,y)b(x,y)c(x,y)$ as $f(x,y)g(x,y)$.

Then applying the *abc*-conjecture for number fields, we obtain

$$(1 - \epsilon/D)h(a(z_1, z_2), b(z_1, z_2)) \leqslant \left(\sum_{\mathfrak{p} \in I(a(z_1,z_2),b(z_1,z_2),c(z_1,z_2))} N_{\mathfrak{p}} \right) + O_{K,S,\epsilon,f}(1).$$

Now, a, b, and c have no common linear factors and (z_1, z_2) is in S-reduced form, so, possibly after enlarging S, we have a finite set S of primes, depending only on a, b, c, and K. Note that

$$I(a(z_1, z_2), b(z_1, z_2), c(z_1, z_2)) \backslash S = \{\mathfrak{p} : v_{\mathfrak{p}}(a(z_1, z_2)b(z_1, z_2)c(z_1, z_2)) > 0\} \backslash S.$$

Since $a(x,y)b(x,y)c(x,y)$ has the same prime factors as $f(x,y)g(x,y)$, we therefore have

$$\left(\sum_{\mathfrak{p} \in I(a(z_1,z_2),b(z_1,z_2),c(z_1,z_2))} N_{\mathfrak{p}} \right) \leqslant \left(\sum_{v_{\mathfrak{p}}(f(z_1,z_2))>0} N_{\mathfrak{p}} \right) + \left(\sum_{v_{\mathfrak{p}}(g(z_1,z_2))>0} N_{\mathfrak{p}} \right) + O_{K,S,\epsilon,f}(1),$$

so

$$(1 - \epsilon/D)h(a(z_1, z_2), b(z_1, z_2)) \leqslant \left(\sum_{v_{\mathfrak{p}}(f(z_1,z_2))>0} N_{\mathfrak{p}} \right) + \left(\sum_{v_{\mathfrak{p}}(g(z_1,z_2))>0} N_{\mathfrak{p}} \right) + O_{K,S,\epsilon,f}(1). \tag{3.2}$$

By basic properties of height functions, we have

$$\sum_{v_{\mathfrak{p}}(g(z_1,z_2))>0} N_{\mathfrak{p}} \leqslant h(g(z_1, z_2)) \leqslant (D + 2 - \deg f)h(z_1, z_2) + O_{K,S,\epsilon,f}(1),$$

since g has degree $D + 2 - \deg f$. Similarly, using the assumption at $a(x,y)$ and $b(x,y)$ have no common factors, we have

$$h(a(z_1, z_2), b(z_1, z_2)) + O_{K,S,\epsilon,f}(1) \geqslant D(h(z_1, z_2)).$$

Substituting these inequalities into (3.2) gives

$$(\deg f - 2 - \epsilon)h(z_1, z_2) \leqslant \left(\sum_{v_{\mathfrak{p}}(f(z_1,z_2))>0} N_{\mathfrak{p}} \right) + O_{K,S,\epsilon,f}(1),$$

as desired. □

PROPOSITION 3.4. *Let $F(x) \in \mathfrak{o}_K[x]$ be a polynomial of degree 3 or more without repeated factors. Suppose that K is a number field satisfying the abc-conjecture. Then, for any $\epsilon > 0$, there is a constant $C_{F,\epsilon}$ such that*

$$\sum_{v_{\mathfrak{p}}(F(z))>0} N_{\mathfrak{p}} \geqslant (\deg F - 2 - \epsilon)h(z) + C_{F,\epsilon},$$

for all $z \in K$.

Proof. For any finite set S of finite primes, let $\mathfrak{o}_{K,S}$ denote as usual the ring of S-integers of K. By the finiteness of the class group, we can (effectively) find an S, depending only on K, so that $\mathfrak{o}_{K,S}$ is a principal ideal domain. Then we may write any $z \in K$ as $z = z_1/z_2$ with (z_1, z_2) in S-reduced form.

Let $g(x, y)$ be the homogenization of $F(x)$ so that $g(x, 1) = F(x)$ and $g(z_1, z_2) = z_2^{\deg f} F(z_1)$. Let $f(x, y) = yg(x, y)$. Let

$$T_1 = \{\text{primes } \mathfrak{p} : \min(v_\mathfrak{p}(z_1), v_\mathfrak{p}(z_2)) > 0\}.$$

Note that we can take $S = T_1$. Let T_2 be the set of primes such that $|a_n|_\mathfrak{p} \neq 1$ for some non-zero coefficient a_n of F (note that T_1 and T_2 are finite and depend only on K and F). Then for all $\mathfrak{p} \notin T_1 \cup T_2$, we have $v_\mathfrak{p}(F(z)) \neq 0$ if and only if $v_\mathfrak{p}(f(z_1, z_2)) > 0$. Thus, we have

$$\left(\sum_{v_\mathfrak{p}(F(z)) \neq 0} N_\mathfrak{p} \right) + O_{F,\epsilon}(1) \geqslant \sum_{v_\mathfrak{p}(f(z_1,z_2))>0} N_\mathfrak{p} \,.$$

Since $h(z) = h(z_1, z_2)$ and $\deg f = \deg F + 1$, applying Proposition 3.3 gives

$$\left(\sum_{v_\mathfrak{p}(f(z_1,z_2))>0} N_\mathfrak{p} \right) + O_{F,\epsilon}(1) \geqslant (\deg F - 1 - \epsilon) h(z_1, z_2). \tag{3.3}$$

For $\mathfrak{p} \notin T_1 \cup T_2$, we have $v_\mathfrak{p}(F(z)) < 0$ exactly when $v_\mathfrak{p}(z) < 0$, so

$$\sum_{v_\mathfrak{p}(F(z))<0} N_\mathfrak{p} \leqslant h(z) + O_{F,\epsilon}(1).$$

Thus, we have a constant $C_{F,\epsilon}$ such that $\sum_{v_\mathfrak{p}(F(z))>0} N_\mathfrak{p} \geqslant (\deg F - 2 - \epsilon) h(z) + C_{F,\epsilon}$, as desired. □

4. *Roth-abc for function fields*

Using Yamanoi's theorem [**37**, Theorem 5] which establishes a conjecture of Vojta for function fields (see also [**12**, **22**]), we obtain a function field analog of Proposition 3.4. Note that a more general implication is proved by Vojta [**35**], see also [**36**, p. 202]. In the special case needed here, we include a short proof for the sake of completeness.

Let V be a curve over a function field K, and let $\gamma \in V(\bar{K})$. Then we define

$$d(\gamma) = \frac{1}{[K(\gamma) : K]} \sum_{\text{primes } \mathfrak{p} \text{ of } K} (v_\mathfrak{p}(\Delta_{K(\gamma)/K})),$$

where $\Delta_{K(\gamma)/K}$ is the relative discriminant of the extension $K(\gamma)/K$.

Since we are working over a function field of characteristic 0 (so that all ramification is tame), we may use the definition

$$d(\gamma) = \frac{1}{[K(\gamma) : K]} \sum_{\text{primes } \mathfrak{q} \text{ of } K(\gamma)} (e(\mathfrak{q}/(\mathfrak{q} \cap \mathfrak{o}_K)) - 1)\, N_\mathfrak{q}\,,$$

where $e(\mathfrak{q}/(\mathfrak{q} \cap \mathfrak{o}_K))$ is the ramification index of $\mathfrak{q}$ over $\mathfrak{q} \cap \mathfrak{o}_K$.

Let $\mathcal{K}_V$ be a canonical divisor on V, and let $h_{\mathcal{K}_V}$ be a height function for $\mathcal{K}_V$. Yamanoi [**37**] proves the following result, sometimes called the Vojta $(1 + \epsilon)$-conjecture.

THEOREM 4.1 (Yamanoi). *Let K be a function field, let V be a curve over K, let M be a positive integer, and let $\epsilon > 0$. Then there is a constant $C_{M,\epsilon}$ such that for all $\gamma \in V(\bar{K})$ with*

$[K(\gamma):K] \leqslant M$, *we have*

$$h_{\mathcal{K}_V}(\gamma) \leqslant (1+\epsilon)d(\gamma) + C_{M,\epsilon}. \tag{4.1}$$

We will use Theorem 4.1 to prove Proposition 4.2, the function field analog of Proposition 3.4. To do this, we first introduce a little information about height functions and divisors.

The divisor $\mathcal{K}_V$ has degree $2g_V - 2$ where g_V is the genus of V. By the standard theory of heights on curves (see [**34**, Proposition 1.2.9], for example), if D is any ample divisor, and D' is an arbitrary divisor, we have

$$\lim_{h_D(z)\to\infty} \frac{h_{D'}(z)}{h_D(z)} = \frac{\deg D'}{\deg D}. \tag{4.2}$$

Now, let $\pi : V \longrightarrow \mathbb{P}^1$ be a non-constant map on a curve. Suppose that $\pi(\gamma) = z$ for $z \in \mathbb{P}^1(\bar{K})$. The usual height $h(z)$ comes from a degree 1 divisor on $\mathbb{P}^1$ which pulls back to a degree $\deg\pi$ divisor on V. Furthermore, if $\pi(\gamma) \in \mathbb{P}^1(K)$, then $[K(\gamma):K] \leqslant \deg\pi$. Thus, Theorem 4.1 and (4.2) imply that for any $\epsilon' > 0$, we have

$$(1-\epsilon')\frac{2g_V - 2}{\deg\pi} h(\pi(\gamma)) \leqslant d(\gamma) + O_{\epsilon'}(1), \tag{4.3}$$

for all $\gamma \in V(\bar{K})$ such that $\pi(\gamma) \in \mathbb{P}^1(K)$.

We will use this to prove a function field analog of Proposition 3.4.

PROPOSITION 4.2. *Let K be a function field and let $F(x) \in K[x]$ be a polynomial of degree 3 or more without repeated factors. Then, for any $\epsilon > 0$, there is a constant $C_{F,\epsilon}$ such that*

$$\sum_{v_{\mathfrak{p}}(F(z))>0} N_{\mathfrak{p}} \geqslant (\deg F - 2 - \epsilon)h(z) + C_{F,\epsilon}, \tag{4.4}$$

for all $z \in K$.

Proof. For each $n > 0$, let V_n be a non-singular projective model over K of $y^n = F(x)$. We obtain this by taking plane curve in $\mathbb{P}^2$ obtained by taking the homogenization of $y^n - F(x) = 0$, and the blowing up repeatedly over the point at infinity. Following [**14**, Chapter V, Section 3], one sees that we obtain a single point at infinity in this way, since $\gcd(n, \deg F) = 1$.

To calculate the genus g_n of V_n, we use the morphism $\pi : V_n \longrightarrow \mathbb{P}^1$ given by projection onto the x-coordinate; that is, $\pi(x,y) = x$.

From now on, we choose n such that it is relatively prime to $\deg F$. This makes the above morphism totally ramified at zeroes and poles of F and unramified everywhere else. Since F has a single pole at the point at infinity along with $\deg F$ zeros, and π has degree n, the Riemann–Hurwitz theorem gives

$$2g_n - 2 = (n-1)(\deg F + 1) - 2n = n(\deg F - 1) - (\deg F + 1). \tag{4.5}$$

Suppose that $\pi(\gamma) = z \in K$. Then (4.3) and (4.5) together give

$$(1-\epsilon')\left(\deg F - 1 - \frac{\deg F + 1}{n}\right) h(z) \leqslant d(\gamma) + O_{\epsilon',n}(1).$$

Let $\epsilon > 0$. Choosing sufficiently large n and sufficiently small ϵ' yields

$$(\deg F - 1 - \epsilon)h(z) \leqslant d(\gamma) + O_{n,\epsilon}(1). \tag{4.6}$$

Now, $K(\gamma) = K(\sqrt[n]{F(z)})$, which can ramify only over a prime $\mathfrak{p}$ when $v_\mathfrak{p}(F(z)) \neq 0$. Since $e(\mathfrak{q}/(\mathfrak{q} \cap \mathfrak{o}_K)) \leqslant n-1$, where $e(\mathfrak{q}/\mathfrak{q} \cap \mathfrak{o}_K)$ is the ramification index of $\mathfrak{q}$ over $\mathfrak{q} \cap \mathfrak{o}_K$, we have

$$d(\gamma) \leqslant \sum_{v_\mathfrak{p}(F(z)) \neq 0} N_\mathfrak{p}\,.$$

When $v_\mathfrak{p}(F(z)) < 0$, either $v_\mathfrak{p}(z) < 0$ or $v_\mathfrak{p}(a_i) < 0$ for some coefficient a_i of $F(z)$. Since F has only finitely many coefficients and each has negative valuation at only finitely many primes, this means that

$$\sum_{v_\mathfrak{p}(F(z)) < 0} N_\mathfrak{p} \leqslant h(z) + O_F(1).$$

Hence, we have

$$d(\gamma) \leqslant \sum_{v_\mathfrak{p}(F(z)) > 0} N_\mathfrak{p} + h(z) + O_F(1).$$

Combining this inequality with (4.6) then gives (4.4). □

5. *Proofs of main theorems*

We begin with a proposition that allows us to control the size of certain non-primitive factors of $\varphi^n(\alpha)$. We choose a polynomial factor F of the numerator P_i of $\varphi^i(z)$ and use the fact that, outside a finite set of primes, we have $v_\mathfrak{p}(\varphi^n(\alpha)) > 0$ whenever $v_\mathfrak{p}(F(\varphi^{n-i}(\alpha))) > 0$. If $m < n$, then the condition

$$\min(v_\mathfrak{p}(F(\varphi^{n-i}(\alpha))), v_\mathfrak{p}(\varphi^m(\alpha))) > 0,$$

forces some root of F to be periodic modulo $\mathfrak{p}$, with period at most $n-m$. If all of the roots of F are non-periodic, then, for bounded $n-m$, there are at most finitely many such $\mathfrak{p}$. Thus, any $\mathfrak{p}$ such that $\min(v_\mathfrak{p}(F(\varphi^{n-i}(\alpha))), v_\mathfrak{p}(\varphi^m(\alpha))) > 0$ comes from either a bounded set or from a relatively low order iterate $\varphi^\ell(\alpha)$ of α. Since $h(\varphi^\ell(\alpha))$ is very small relative to $h(\varphi^n(\alpha))$ when ℓ is small relative to n, this allows for a strong lower bound on the product of all such $\mathfrak{p}$.

Proposition 5.1. *Let $\delta > 0$, let K be an abc-field, let $\alpha \in K$ such that $h_\varphi(\alpha) > 0$, and let F be a factor of the numerator of φ^i such that every root γ_j of F is non-periodic and satisfies $\varphi^\ell(\gamma_j) \neq 0$ for $\ell = 0, \dots, i-1$. Let Z be the set of primes $\mathfrak{p}$ such that $\min(v_\mathfrak{p}(\varphi^m(\alpha)), v_\mathfrak{p}(F(\varphi^{n-i}(\alpha)))) > 0$ for some positive integer $m < n$. Then there is a constant C_δ such that for all positive integers n, we have*

$$\sum_{\mathfrak{p} \in Z} N_\mathfrak{p} \leqslant \delta h(\varphi^n(\alpha)) + C_\delta. \tag{5.1}$$

Proof. Let L be a finite extension of K over which F splits completely as $F(x) = a(x - \gamma_1)\dots(x-\gamma_s)$, for $\gamma_j \in L$. Then, for all but finitely many primes $\mathfrak{p}$ of K, we have $v_\mathfrak{p}(F(z)) > 0$ if and only if $v_\mathfrak{q}(z - \gamma_j) > 0$ for some prime $\mathfrak{q}$ of L with $\mathfrak{q} \mid \mathfrak{p}$. Thus, it suffices to show that for each γ_j, there is a C_δ such that for all n we have

$$\sum_{\mathfrak{p} \in Y} N_\mathfrak{p} \leqslant \delta h(\varphi^n(\alpha)) + C_\delta, \tag{5.2}$$

where Y is the set of primes $\mathfrak{p}$ such that $\min(v_\mathfrak{q}(\varphi^m(\alpha)), v_\mathfrak{q}(\varphi^{n-i}(\alpha) - \gamma_j)) > 0$ for some positive integer $m < n$ and some prime $\mathfrak{q}$ of L with $\mathfrak{q} \mid \mathfrak{p}$.

Let Y_1 be the set of primes of L at which φ does not have weak good reduction, as defined in Section 2. Write $P_i = FR$, and let Y_2 be the finite set of primes $\mathfrak{q}$ at which some $|b_s|_\mathfrak{q} \neq 1$

for some non-zero coefficient of F or R. Then, for all $\mathfrak{q}$ outside of $Y_1 \cup Y_2$, we have $\varphi(z) \equiv 0 \pmod{\mathfrak{q}}$ whenever $F(z) \equiv 0 \pmod{\mathfrak{q}}$.

If $\min(v_{\mathfrak{q}}(\varphi^m(\alpha)), v_{\mathfrak{q}}(\varphi^{n-i}(\alpha) - \gamma_j)) > 0$ for $n - i \leqslant m < n$, then $v_{\mathfrak{q}}(\varphi^{m-(n-i)}(\gamma_j)) > 0$. The set Y_3 of primes for which this can happen is therefore finite since $\varphi^\ell(\gamma_j) \neq 0$ for $\ell = 0, \dots, i-1$.

For any B, let W_B be the set of primes outside $Y_1 \cup Y_2 \cup Y_3$ such that $\min(v_{\mathfrak{q}}(\varphi^m(\alpha)), v_{\mathfrak{q}}(\varphi^{n-i}(\alpha) - \gamma_j)) > 0$ for some positive integers m and n with $n - i > m > n - i - B$. If $\mathfrak{q} \in W_B$, then $\varphi^m(\alpha) \equiv \varphi^n(\alpha) \equiv 0 \pmod{\mathfrak{q}}$, so 0 is in a cycle of period at most $n - m$ modulo $\mathfrak{q}$. Since $\gamma_j \equiv \varphi^{n-i}(\alpha) \equiv \varphi^{(n-i)-m}(0) \pmod{\mathfrak{q}}$, we see that γ_j is in the same cycle modulo $\mathfrak{q}$. This implies that γ_j has period $n - m < B + i$ modulo $\mathfrak{q}$. Since γ_j is not periodic, there are only finitely many such $\mathfrak{q}$, so W_B must be finite. (Note that φ induces a well-defined map from $k_{\mathfrak{q}} \cup \infty$ to itself, because $\mathfrak{q}$ is a prime of weak good reduction for φ.)

Note that $v_{\mathfrak{p}}(\varphi^l(\alpha)) > 0$ if and only if $v_{\mathfrak{q}}(\varphi^l(\alpha)) > 0$ for some $\mathfrak{q} \mid \mathfrak{p}$. Let Z_B be the set $\{\text{primes } \mathfrak{p} \in \mathfrak{o}_K \mid \mathfrak{q} \mid \mathfrak{p} \text{ for some } \mathfrak{q} \in W_B\}$. Let Y_i' (for $i = 1, 2, 3$) be the set $\{\text{primes } \mathfrak{p} \in \mathfrak{o}_K \mid \mathfrak{q} \mid \mathfrak{p} \text{ for some } \mathfrak{q} \in Y_i\}$. When $\mathfrak{p} \notin Z_B \cup Y_1' \cup Y_2' \cup Y_3'$, we see then that if $\min(v_{\mathfrak{p}}(F(\varphi^{n-i}(\alpha))), v_{\mathfrak{p}}(\varphi^n(\alpha))) > 0$, then $v_{\mathfrak{p}}(\varphi^m(\alpha)) > 0$ for some positive integer $m \leqslant n - i - B$. Since Y_1', Y_2', and Y_3' are finite, and Z_B is finite for any positive integer B, see that for any B, there is a constant C_B such that

$$\sum_{\mathfrak{p} \in Y} N_{\mathfrak{p}} \leqslant \sum_{\ell=1}^{n-i-B} \sum_{v_{\mathfrak{p}}(\varphi^\ell(\alpha))>0} N_{\mathfrak{p}} + C_B \leqslant \sum_{\ell=1}^{n-B-i} h(\varphi^\ell(\alpha)) + C_B, \tag{5.3}$$

where Y is the set of primes $\mathfrak{p}$ where $\min(v_{\mathfrak{q}}(\varphi^m(\alpha)), v_{\mathfrak{q}}(\varphi^{n-i}(\alpha) - \gamma_j)) > 0$ for some positive integer $m < n$ and some prime $\mathfrak{q}$ of L with $\mathfrak{q} \mid \mathfrak{p}$.

So it suffices to show that for any δ, we have

$$\sum_{\ell=1}^{n-B-i} h(\varphi^\ell(\alpha)) < \delta(h(\varphi^n(\alpha))), \tag{5.4}$$

for all sufficiently large n. We will use the canonical height of Call and Silverman [7] here. Recall that by (2.4), we have $h_\varphi(\varphi(z)) = dh_\varphi(z)$ for all $z \in K$ and that by (2.5), there is a constant C_φ such that $|h(z) - h_\varphi(z)| < C_\varphi$ for all $z \in K$.

Choose B_δ such that $1/d^{B_\delta+i} < \delta/4$ and $d^n(h_\varphi(\alpha)) > (n+1)C_\varphi/\delta/2$ for all $n > B_\delta$. Then for all $n > B_\delta$, we have

$$\begin{aligned}
\sum_{\ell=1}^{n-B_\delta-i} h(\varphi^\ell(\alpha)) &\leqslant \sum_{\ell=1}^{n-B_\delta-i} h_\varphi(\varphi^\ell(\alpha)) + nC_\varphi \\
&= \frac{1}{d^{B_\delta+i}} \sum_{r=0}^{n-B_\delta-i-1} \frac{h_\varphi(\varphi^n(\alpha))}{d^r} + nC_\varphi \quad \text{(by (2.4))} \\
&\leqslant \left(\frac{1}{d^{B_\delta+i}} \sum_{r=0}^{\infty} \frac{1}{d^r} \right) h_\varphi(\varphi^n(\alpha)) + nC_\varphi \\
&\leqslant \frac{\delta}{2} h_\varphi(\varphi^n(\alpha)) + nC_\varphi \\
&\leqslant \frac{\delta}{2} h(\varphi^n(\alpha)) + (n+1)C_\varphi \quad \text{(by (2.5))} \\
&\leqslant \delta h(\varphi^n(\alpha)).
\end{aligned} \tag{5.5}$$

Thus, (5.4) holds, and our proof is complete. □

LEMMA 5.2. *Let K be an abc-field. If $\gamma \in \bar{K}$ is not exceptional, then $\varphi^{-3}(\gamma)$ contains at least two distinct points in $\mathbb{P}^1(\bar{K})$.*

Proof. If φ^{-3} contains only one point, τ, then φ is totally ramified at τ, $\varphi(\tau)$, and $\varphi^2(\tau)$. By Riemann–Hurwitz, φ can have at most two totally ramified points, so this means that τ, $\varphi(\tau)$, and $\varphi^2(\tau)$ are not distinct, so we must have $\varphi^2(\tau) = \tau$, so τ is exceptional. But then γ must be exceptional too. □

Now, we prove a very simple lemma that allows us to reduce the proofs of Theorems 1.1 and 1.2 to the case where $\beta = 0$. In the statement below ρ^{-1} denotes the compositional inverse of a linear polynomial ρ.

LEMMA 5.3. *Let K be an abc-field. Let $\beta \in K$, let ρ be the linear polynomial $\rho(x) = x + \beta$, let $\varphi \in K(x)$, and let $\varphi^\rho = \rho^{-1} \circ \varphi \circ \rho$. Then we have the following*:

(i) $(\varphi^\rho)^n(\rho^{-1}(\alpha)) = \varphi^n(\alpha) - \beta$ *for any $\alpha \in K$ and any positive integer n and*
(ii) *the map φ^ρ is dynamically unramified over 0 if and only if φ is dynamically unramified over β.*

Proof. We have $(\varphi^\rho)^n = (\rho^{-1} \circ \varphi \circ \rho)^n = \rho^{-1} \circ \varphi^n \circ \rho$ for any positive integer n. Since $\rho^{-1}(x) = x - \beta$, statement (i) above is immediate. To verify (ii), note that for any $\tau \in \bar{K}$ such that $\varphi^n(\tau) = \beta$, we therefore have $(\varphi^\rho)^n(\rho(\tau)) = 0$ and $e_{\varphi^n}(\tau/\beta) = e_{(\varphi^\rho)^n}(\rho(\tau)/0)$. □

With the tools that we have assembled, the remainder of the proof of Theorem 1.1 is a short computation.

Proof of Theorem 1.1. Lemma 5.3 allows us to immediately reduce to the case that $\beta = 0$.

There is an i such that P_i has a factor $F \in K[x]$ of degree 4 or more such that every root γ_j of F is non-periodic and satisfies $\varphi^\ell(\gamma_j) \neq 0$ for $\ell = 0, \ldots, i-1$ (see Remark 5.4). To see this, note that since Lemma 5.2 tells us that $\varphi^{-3}(0)$ contains two points, we see that at least one of these points is not periodic. Taking the third inverse image of this point yields at least four non-periodic points; if one of these is the point at infinity, then three further inverse images yields eight points, at none of which is the point at infinity. Let i be the smallest integer such that $\varphi^i(z) = 0$ for these points z (this i is the same for all of them since they are all inverse images of the same non-periodic point), and let $F \in K[x]$ be a factor of P_i that vanishes at all of these z. Then $\deg F \geqslant 4$ by construction.

By Propositions 3.4 and 4.2, with $\epsilon = 1$, there is a non-zero constant C_1 such that

$$\sum_{v_\mathfrak{p}(F(\varphi^{n-i}(\alpha)))>0} N_\mathfrak{p} > (\deg F - 3)h(\varphi^{n-i}(\alpha)) \geqslant h(\varphi^{n-i}(\alpha)) + C_1.$$

Applying Proposition 5.1 with $\delta = 1/(2d^i)$ and using the fact that $h(\varphi^i(z)) \leqslant d^i h(z) + O(1)$ for all $z \in K$, we see that there is a constant C_2 such that

$$\sum_{\mathfrak{p} \in Z} N_\mathfrak{p} \leqslant \frac{1}{2} h_\varphi(\varphi^{n-i}(\alpha)) + C_2,$$

where Z is the set of primes $\mathfrak{p}$ such that $\min(v_\mathfrak{p}(F(\varphi^{n-i}(\alpha))), v_\mathfrak{p}(\varphi^m(\alpha))) > 0$ for some positive integer $m < n$. Thus, when $h(\varphi^{n-i}(\alpha)) > 2(C_2 - C_1)$, we have

$$\sum_{v_\mathfrak{p}(F(\varphi^{n-i}(\alpha)))>0} N_\mathfrak{p} > \sum_{\mathfrak{p} \in Z} N_\mathfrak{p}\,,$$

so there is a prime $\mathfrak{p}$ such that $v_\mathfrak{p}(P_i(\varphi^{n-i}(\alpha))) > 0$ but $v_\mathfrak{p}(\varphi^m(\alpha)) \leqslant 0$ for all $m < n$. Now, writing $\varphi^i(x) = F(x)R(x)/T(x)$, where FR and T are coprime, we see that for all but finitely many $\mathfrak{p}$, we have $v_\mathfrak{p}(\varphi^i(z)) > 0$ whenever $v_\mathfrak{p}(F(z)) > 0$. Since $\lim_{n\to\infty} h(\varphi^{n-i}(\alpha)) = \infty$ (by

(2.6)), we see then that for all but finitely many n, there is a prime $\mathfrak{p}$ such that $v_{\mathfrak{p}}(\varphi^n(\alpha)) > 0$ and $v_{\mathfrak{p}}(\varphi^m(\alpha)) \leqslant 0$ for all $1 \leqslant m < n$. □

Theorem 1.2 is proved in the same manner as Theorem 1.1. The only significant difference is that we use a square-free factor F of P_i, which is possible because φ is dynamically unramified over β.

Proof. As in the proof of Theorem 1.1, we may assume that $\beta = 0$, using Lemma 5.3. By Remark 5.4, there is an i such that P_i has a factor F of degree 8 or more such that every root γ_j of F is non-periodic, satisfies $\varphi^\ell(\gamma_j) \neq 0$ for $\ell = 0, \ldots, i-1$, and has multiplicity 1 as a root of P_i. To see this, note that since φ is dynamically unramified over 0, there are *infinitely* many points τ such that $\varphi^n(\tau) = 0$ and $e_{\varphi^n}(\tau/0) = 1$ for some n. Thus, we may choose such a τ that is not periodic and which is not in the forward orbit of any ramification points or the point at infinity. Then $\varphi^{-3}(\tau)$ contains at least eight points (since $d \geqslant 2$) in $\varphi^{-(n+3)}(0)$ none of which are ramification points of φ^{n+3}. None of these points can be periodic since τ is not periodic. Let i be the smallest i such that $\varphi^i(z) = 0$ for these points z (this i is the same for all of them since they are all inverse images of the same non-periodic point), and let $F \in K[x]$ be a factor of P_i that vanishes at all of these z. Then $\deg F \geqslant 8$ by construction.

Applying Roth-*abc* to F with $\epsilon = 1$, we obtain

$$\sum_{v_{\mathfrak{p}}(F(\varphi^{n-i}(\alpha)))>0} N_{\mathfrak{p}} > (\deg F - 3)h(\varphi^{n-i}(\alpha)) + C_3,$$

for some constant C_3, depending only on F. Since

$$\sum_{v_{\mathfrak{p}}(F(\varphi^{n-i}(\alpha)))>0} v_{\mathfrak{p}}(F(\varphi^{n-i}(\alpha)))\, N_{\mathfrak{p}} \leqslant (\deg F)h(\varphi^{n-i}(\alpha)) + O(1),$$

we see that there is a constant C_4 such that

$$\sum_{v_{\mathfrak{p}}(F(\varphi^{n-i}(\alpha)))\geqslant 2} N_{\mathfrak{p}} > \frac{\deg F}{2} h(\varphi^{n-i}(\alpha)) + C_4.$$

Since $\deg F \geqslant 8$, we have $(\deg F)/2 - 3 \geqslant 1$, so there is a constant C_5 such that

$$\sum_{v_{\mathfrak{p}}(F(\varphi^{n-i}(\alpha)))=1} N_{\mathfrak{p}} > h(\varphi^{n-i}(\alpha)) + C_5.$$

Applying Theorem 5.1 with $\delta = 1/(2d^i)$ and using the fact that $h(\varphi^i(z)) \leqslant d^i h(z) + O(1)$ for all $z \in K$, we see that there is a constant C_6 such that

$$\sum_{\mathfrak{p}\in Z} N_{\mathfrak{p}} \leqslant \frac{1}{2} h_\varphi(\varphi^n(\alpha)) + C_6,$$

where Z is the set of primes $\mathfrak{p}$ such that $\min(v_{\mathfrak{p}}(F(\varphi^{n-i}(\alpha)), v_{\mathfrak{p}}(\varphi^m(\alpha)))) > 0$ for $1 \leqslant m < n$. Thus, when $h(\varphi^{n-i}(\alpha)) > 2(C_6 - C_4)$, there is prime $\mathfrak{p}$ such that $v_{\mathfrak{p}}(F(\varphi^{n-i}(\alpha))) = 1$ but $v_{\mathfrak{p}}(\varphi^m(\alpha)) \leqslant 0$ for all $m < n$. Now, writing $\varphi^i(x) = F(x)R(x)/T(x)$, where F, R, and T are pairwise coprime, we see that for all but finitely many $\mathfrak{p}$, we have $v_{\mathfrak{p}}(\varphi^i(z)) = v_{\mathfrak{p}}(F)$ whenever $v_{\mathfrak{p}}(F(z)) > 0$. Since $\lim_{n\to\infty} h(\varphi^{n-i}(\alpha)) = \infty$ (by (2.6)), we see then that for all but finitely many n, there is a prime $\mathfrak{p}$ such that $v_{\mathfrak{p}}(\varphi^n(\alpha)) = 1$ and $v_{\mathfrak{p}}(\varphi^m(\alpha)) \leqslant 0$ for all $1 \leqslant m < n$. □

REMARK 5.4. In the proofs of Theorems 1.1 and 1.2, the degree of the polynomial F could be taken as large as one likes. Degrees 4 and 8, respectively, are simply convenient for the estimates. We wish to avoid the point at infinity so that we can take a polynomial $F(x)$ that vanishes at all of the points (without introducing homogenous coordinates). The reason we do not take $\deg F$ to be exactly 4 or 8 is that doing so might require passing to a finite extension of K, and we do not wish to assume the *abc*-conjecture for extensions of K when K is a number field.

REMARK 5.5. When φ is not dynamically unramified over β, there are at most finitely many $\mathfrak{p}$ that appear as square-free factors of any $\varphi^n(\alpha) - \beta$. To see this, note that by Lemma 5.3, it suffices to check what happens when $\beta = 0$ and φ is not dynamically unramified over 0. In this case, there are at most finitely many polynomials that appear as factors of any P_n, where P_n is the numerator of φ. Thus, for any α, there are only finitely many $\mathfrak{p}$ such that $v_{\mathfrak{p}}(\varphi^n(\alpha)) = 1$ for some n. Thus, the conclusion of Theorem 1.2 will never hold for a rational function that is not dynamically unramified over β.

6. *An application to iterated Galois groups*

Our original motivation for the problem of square-free primitive divisors comes from the study of Galois groups of iterates of polynomials, that is, Galois groups of splitting fields of $f^m(x)$ for f a polynomial. Odoni [**23**, **24**] calculated these groups for 'generic polynomials' and for the specific polynomial x^2+1. Stoll [**32**] later calculated them for polynomials of the form x^2+a, where a is a positive integer congruent to 1 or 2 modulo 4. In particular, Stoll defines $\Omega_{n,a}$ to be the splitting field of $f_a^n(x)$ for $f_a(x) = x^2 + a$ and shows that if a is a positive integer congruent to 1 or 2 modulo 4, then $[\Omega_{n+1,a} : \Omega_{n,a}] = 2^{2^n}$ for all $n \geqslant 0$. This allows for a completely explicit description of $\mathrm{Gal}(\Omega_{m,a}/\mathbb{Q})$ for any m in terms of an inductive wreath product structure. Stoll notes that this will not be true for $f_a(x) = x^2 + a$ when a is an integer of the form $-b^2 - 1$ for b a positive integer, since in this case one has $[\Omega_{2,a} : \Omega_{1,a}] = 2$.

PROPOSITION 6.1. *Suppose that the abc-conjecture for $\mathbb{Q}$ holds. Let $a \neq -2$ be an integer such that $-a$ is not a perfect square in $\mathbb{Z}$. Then, with notation above, we have*

$$[\Omega_{n+1,a} : \Omega_{n,a}] = 2^{2^n}, \tag{6.1}$$

for all but finitely many natural numbers n.

Proof. By Stoll [**32**, Lemma 1.6], we have (6.1) whenever $f_a^{n+1}(0)$ is not a square in $\Omega_{n,a}$. A simple calculation with discriminants (see [**23**, Lemma 3.1] or [**17**, Lemma 4.10], for example) shows that $\mathrm{Disk}\, f^m(x) = 2^{2^m} \cdot \mathrm{Disk}(f^{m-1}(x)) \cdot f^m(0)$. Hence, by induction we see that $\Omega_{n,a}$ is unramified away from primes dividing $2\prod_{i=1}^n f^i(0)$. Since $f_a(x)$ is dynamically unramified over 0 and 0 is not preperiodic for f_a, we may apply Theorem 1.2 and conclude that for all but finitely many n, there is a prime $\mathfrak{p} \neq 2$ such that $v_{\mathfrak{p}}(f^{n+1}(0)) = 1$ and $v_{\mathfrak{p}}(f^m(0)) = 0$ for all $1 \leqslant m < n+1$ (note that a negative valuation for any $f^m(0)$ is not possible since a is an integer). Thus, for all but finitely many n, we see that $f_a^{n+1}(0)$ is not a square in $\Omega_{n,a}$, which completes our proof. □

REMARK 6.2. Using arguments from [**18**], one can show Proposition 6.1 holds for any $a \neq 0, -1, -2$; the proof, however, becomes more complicated. One can also use similar arguments to show that the *abc*-conjecture implies [**19**, Conjecture 1.1]. We plan to return to this problem in more generality in future work.

REMARK 6.3. Let T be the binary rooted tree whose vertices at level n are the roots of $f^n(x)$. Then Proposition 6.1 implies that the natural image of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ into $\mathrm{Aut}(T)$ has finite index in Aut(T). This can be interpreted as a dynamical analog of Serre's openness theorem for Galois representations on torsion points of elliptic curves [28] (see [6]).

Acknowledgements. The authors would like to thank Xander Faber, Dragos Ghioca, Andrew Granville, Patrick Ingram, Rafe Jones, Lukas Pottmeyer, Joseph Silverman, and Paul Vojta for many helpful conversations and comments on earlier drafts of this paper. This paper was written while the authors were visiting ICERM in Providence and it is our pleasure to thank ICERM for its hospitality. In addition, the authors would like to thank the BLMS referee for doing such a quick and thorough review of this paper. The referee's comments and suggestions were very helpful, and much appreciated!

References

1. M. Baker, 'A finiteness theorem for canonical heights attached to rational maps over function fields', *J. Reine Angew. Math.* 626 (2009) 205–233.
2. A. S. Bang, 'Taltheoretiske Undersogelse', *Tidsskrift Mat.* 4 (1886) 70–80, 130–137.
3. G. V. Belyĭ, 'Galois extensions of a maximal cyclotomic field', *Izv. Akad. Nauk SSSR Ser. Mat.* 43 (1979) 267–276, 479.
4. R. L. Benedetto, 'Heights and preperiodic points of polynomials over function fields', *Int. Math. Res. Not.* 2005 (2005) 3855–3866.
5. E. Bombieri and W. Gubler, *Heights in diophantine geometry*, New Mathematical Monographs 4 (Cambridge University Press, Cambridge, 2006).
6. N. Boston and R. Jones, 'The image of an arboreal Galois representation', *Pure Appl. Math. Q.* 5 (2009) 213–225.
7. G. S. Call and J. H. Silverman, 'Canonical heights on varieties with morphism', *Compos. Math.* 89 (1993) 163–205.
8. K. Doerksen and A. Haensch, 'Primitive prime divisors in zero orbits of polynomials', *Integers* 12 (2012) 7 pp.
9. N. D. Elkies, '*ABC* implies Mordell', *Int. Math. Res. Not.* 1991 (1991) 99–109.
10. G. Everest, G. Mclaren and T. Ward, 'Primitive divisors of elliptic divisibility sequences', *J. Number Theory* 118 (2006) 71–89.
11. X. Faber and A. Granville, 'Prime factors of dynamical sequences', *J. Reine Angew. Math.* 661 (2011) 189–214.
12. C. Gasbarri, 'The strong *abc* conjecture over function fields (after McQuillan and Yamanoi)', *Séminaire Bourbaki.* vol. 2007/2008, Astérisque (2009), no. 326, Exp. No. 989, viii, 219–256 (2010).
13. A. Granville, '*ABC* allows us to count squarefrees', *Int. Math. Res. Not.* 1998 (1998) 991–1009.
14. R. Hartshorne, *Algebraic geometry* (Springer, New York, 1977).
15. P. Ingram, 'Elliptic divisibility sequences over certain curves', *J. Number Theory* 123 (2007) 473–486.
16. P. Ingram and J. H. Silverman, 'Primitive divisors in arithmetic dynamics', *Math. Proc. Cambridge Philos. Soc.* 146 (2009) 289–302.
17. R. Jones, 'Iterated Galois towers, their associated martingales, and the p-adic Mandelbrot set', *Compos. Math.* 143 (2007) 1108–1126.
18. R. Jones, 'The density of prime divisors in the arithmetic dynamics of quadratic polynomials', *J. London Math. Soc.* (2) 78 (2008) 523–544.
19. R. Jones and M. Manes, 'Galois theory of quadratic rational functions', Preprint, 2011, arxiv.org/abs/1101.4339, 38 pp.
20. H. Krieger, 'Primitive prime divisors in the critical orbit of $z^d + c$', *IMRN*, to appear (doi:10.1093/imrn/rns213, published online 8 October 2012).
21. R. C. Mason, *Diophantine equations over function fields*, London Mathematical Society Lecture Note Series 96 (Cambridge University Press, Cambridge, 1984).
22. M. McQuillan, 'Old and new techniques in function field arithmetic', Preprint, 2009. http://www.mat.uniroma2.it/∼mcquilla/files/oldnew.pdf
23. R. W. K. Odoni, 'The Galois theory of iterates and composites of polynomials', *Proc. London Math. Soc.* (3) 51 (1985) 385–414.
24. R. W. K. Odoni, 'Realising wreath products of cyclic groups as Galois groups', *Mathematika* 35 (1988) 101–113.
25. B. Rice, 'Primitive prime divisors in polynomial arithmetic dynamics', *Integers* 12 (2007) 16 pp.
26. K. F. Roth, 'Rational approximations to algebraic numbers', *Mathematika* 2 (1955) 1–20, corrigendum, ibid. 2 (1955) 168.
27. A. Schinzel, 'Primitive divisors of the expression $a^n - b^n$ in algebraic number fields', *J. Reine Angew. Math.* 268/269 (1974) 27–33, Collection of articles dedicated to Helmut Hasse on his seventy-fifth birthday, II.

28. J.-P. Serre, 'Propriétés galoisiennes des points d'ordre fini des courbes elliptiques', *Invent. Math.* 15 (1972) 259–331.
29. J. H. Silverman, 'The S-unit equation over function fields', *Math. Proc. Cambridge Philos. Soc.* 95 (1984) 3–4.
30. J. H. Silverman, 'Wieferich's criterion and the *abc*-conjecture', *J. Number Theory* 30 (1988) 226–237.
31. J. H. Silverman, *The arithmetic of dynamical systems*, Graduate Texts in Mathematics (Springer, New York, 2007).
32. M. Stoll, 'Galois groups over $\mathbf{Q}$ of some iterated polynomials', *Arch. Math. (Basel)* 59 (1992) 239–244.
33. W. W. Stothers, 'Polynomial identities and Hauptmoduln', *Quart. J. Math. Oxford Ser.* (2) 32 (1981) 349–370.
34. P. Vojta, *Diophantine approximations and value distribution theory*, Lecture Notes in Mathematics 1239 (Springer, Berlin, 1987).
35. P. Vojta, 'A more general abc conjecture', *Int. Math. Res. Not.* 1998 (1998) 1103–1116.
36. P. Vojta, 'Diophantine approximation and Nevanlinna theory', *Arithmetic geometry*, Lecture Notes in Mathematics 2009 (Springer, Berlin, 2011) 111–224.
37. K. Yamanoi, 'The second main theorem for small functions and related problems', *Acta Math.* 192 (2004) 225–294.
38. K. Zsigmondy, 'Zur Theorie der Potenzreste', *Monatsh. Math. Phys.* 3 (1892) 265–284.

C. Gratton and T. J. Tucker
Department of Mathematics
University of Rochester
Hylan Building
Rochester, NY 14627
USA

grattonchad@gmail.com
thomas.tucker@rochester.edu

K. Nguyen
Department of Mathematics
University of California
Berkeley, CA 94720
USA

khoanguyen2511@gmail.com