Journal of Number Theory ••• (••••) •••–•••

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

ABC implies a Zsigmondy principle for ramification

Andrew Bridy *, Thomas J. Tucker

Department of Mathematics, University of Rochester, Rochester, NY, 14620, USA

ARTICLE INFO

Article history:
Received 3 August 2016
Received in revised form 19 June 2017
Accepted 20 June 2017
Available online xxxx
Communicated by A. Pal

MSC:
37P05
11G50
14G25

Keywords:
Arithmetic dynamics
Ramification
abc conjecture

ABSTRACT

Let K be a number field or a function field of characteristic 0. If K is a number field, assume the *abc*-conjecture for K. We prove a variant of Zsigmondy's theorem for ramified primes in preimage fields of rational functions in $K(x)$ that are not postcritically finite. For example, suppose K is a number field and $f \in K[x]$ is not postcritically finite, and let K_n be the field generated by the nth iterated preimages under f of $\beta \in K$. We show that for all large n, there is a prime of K that ramifies in K_n and does not ramify in K_m for any $m < n$.

1. Introduction

Let K be either a number field or a function field of characteristic 0 of transcendence degree 1 over its field of constants. Let $\phi \in K(x)$ be a rational function. Recall that the morphism $\phi : \mathbb{P}^1(K) \to \mathbb{P}^1(K)$ is *postcritically finite* if the forward orbit of the ramification locus of ϕ is a finite set. Let ϕ be a non-postcritically finite rational function

* Corresponding author.
E-mail addresses: abridy@ur.rochester.edu (A. Bridy), thomas.tucker@rochester.edu (T.J. Tucker).

http://dx.doi.org/10.1016/j.jnt.2017.06.015
0022-314X/

of degree $d \geq 2$ and let $\beta \in \mathbb{P}^1(K)$. As is usual in dynamics, we use ϕ^n to denote the map ϕ composed with itself n times. For each $n \geq 1$, let

$$K_n = K(\phi^{-n}(\beta)) = K(\gamma \in \overline{K} : \phi^n(\gamma) = \beta).$$

It is a theorem of the first author and coauthors [BIJ+15] that for any $\beta \in \mathbb{P}^1(K)$, there are infinitely many primes in K that ramify in $\bigcup_{n=1}^{\infty} K_n$. The main idea of the theorem is to produce prime divisors of $\phi^n(\alpha) - \beta$ for α a critical point of ϕ with canonical height $h_\phi(\alpha) > 0$. The fact that there are infinitely many such primes follows from [Sil93]. Various authors (see [Zsi92,Elk91,Ric07,Kri13,IS09,FG11,GNT13] for example) have sought to show that not only are there infinitely many primes that divide $\phi^n(\alpha) - \beta$ for some n, but the stronger statement that there exists an N such that for all $n > N$, there is a prime that divides $\phi^n(\alpha) - \beta$ that does not divide $\phi^m(\alpha) - \beta$ for any $m < n$. If this is true, one might say that there are infinitely many primes dividing $\phi^n(\alpha) - \beta$ for some n because after a certain point each "new iterate" $\phi^n(\alpha) - \beta$ gives a "new prime" dividing $\phi^n(\alpha) - \beta$. This is sometimes referred as the "Zsigmondy principle", after Zsigmondy [Zsi92] who studied these questions in the context of primitive divisors of $a^n - b^n$.

In this paper, we prove a Zsigmondy principle for ramification for certain types of rational functions, including polynomials. Our results are conditional on the *abc* conjecture when K is a number field. For polynomials, our result is the following. Recall that if K is a function field with field of constants k, f is said to be *isotrivial* if there is an element $\sigma \in \overline{K}(x)$ of degree one such that $\sigma \circ \phi \circ \sigma^{-1} \in \bar{k}(x)$.

Theorem 1.1. *Let K be a number field or a function field of characteristic 0. Let $f \in K[x]$ be a polynomial with* $\deg f \geq 2$ *that is not postcritically finite, and let $\beta \in K$. If K is a number field, assume the abc conjecture for K. If K is a function field, assume that f is not isotrivial. Then, for all sufficiently large n, there exists a prime of K that ramifies in $K(f^{-n}(\beta))$ and does not ramify in $K(f^{-m}(\beta))$ for $m < n$.*

Our most general theorem is most easily stated in terms of grand orbits. The *orbit* or *forward orbit* of $\beta \in \mathbb{P}^1(K)$ is

$$\mathcal{O}_\phi(\beta) = \{\phi^n(\beta) : n \geq 0\} = \{\beta, \phi(\beta), \phi^2(\beta), \dots\}.$$

The *backward orbit* of β is

$$\mathcal{O}_\phi^-(\beta) = \{\alpha \in \mathbb{P}^1(\overline{K}) : \phi^n(\alpha) = \beta \text{ for some } n \geq 0\} = \bigcup_{n=0}^{\infty} \phi^{-n}(\beta).$$

The *grand orbit* of β is the backward orbit of the forward orbit, that is,

$$\mathcal{GO}_\phi(\beta) = \{\alpha \in \mathbb{P}^1(\overline{K}) : \phi^m(\alpha) = \phi^n(\beta) \text{ for some } m, n \in \mathbb{Z}_{\geq 0}\}.$$

Please cite this article in press as: A. Bridy, T.J. Tucker, *ABC* implies a Zsigmondy principle for ramification, J. Number Theory (2017), http://dx.doi.org/10.1016/j.jnt.2017.06.015

Grand orbits under ϕ partition $\mathbb{P}^1(\overline{K})$ into equivalence classes. A point β is said to be *exceptional* for ϕ if its grand orbit is a finite set. It is well known that if β is exceptional for ϕ, then (up to conjugacy by a fractional linear transformation) either ϕ is a polynomial and $\beta = \infty$, or $\phi(x) = x^d$ for some $d \in \mathbb{Z}$ and $\beta \in \{0, \infty\}$.

A point $\beta \in \mathbb{P}^1(K)$ is *periodic* if $\phi^n(\beta) = \beta$ for some $n > 0$ and *preperiodic* if $\phi^n(\beta) = \phi^m(\beta)$ for some $n > m \geq 0$. A point that is not preperiodic is *wandering*. We define a grand orbit to be preperiodic if one (equivalently any) of its points is preperiodic, and wandering otherwise.

We now state the main theorem. If K is a number field, we will assume that the *abc* conjecture holds for K. If K is a function field of characteristic 0, the *abc* conjecture is a theorem of Mason–Stothers [Mas84,Sto81] (see also Silverman [Sil84]). As we now consider rational maps from $\mathbb{P}^1(K)$ to itself, it is possible for ∞ to arise as a preimage of K, in which case we simply declare that $K(\infty) = K$.

Theorem 1.2. *Let $\phi \in K(x)$ with $\deg \phi \geq 2$. Suppose that ϕ is not postcritically finite and that $\beta \in \mathbb{P}^1(K)$ is not exceptional for ϕ. If K is a number field, assume the abc conjecture for K. If K is a function field, assume that ϕ is not isotrivial. Suppose that the ramification locus R_ϕ intersects at most $d-1$ distinct wandering grand orbits. For all sufficiently large n, there exists a prime of K that ramifies in $K(\phi^{-n}(\beta))$ and does not ramify in $K(\phi^{-m}(\beta))$ for $m < n$.*

Remark 1.3. Note that in Theorem 1.1, we do not need to assume that β is non-exceptional. This is because if $\beta \in K$ (i.e. $\beta \neq \infty$) and f is a polynomial of degree at least 2, the only possible way for β to be exceptional is if f is a powering map and $\beta = 0$ (up to conjugation by a fractional linear transformation). But then f is postcritically finite, which is ruled out by assumption.

The restriction that ϕ be non-isotrivial is not a serious one. Indeed, we can treat the case of isotrivial rational functions by a fairly elementary argument, provided that β is not in the field of constants of K. See Theorem 5.1.

Theorem 1.2 immediately produces Theorem 1.1 as a special case, since a polynomial of degree d has at most $d-1$ critical points other than the point at infinity (which is of course a fixed point). For rational functions in general we have the following theorem, which shows that a new prime ramifies at every two levels in the tower of fields K_n.

Theorem 1.4. *Let $\phi \in K(x)$ with $\deg \phi \geq 2$. Suppose that ϕ is not postcritically finite and that $\beta \in \mathbb{P}^1(K)$ is not exceptional for ϕ. If K is a number field, assume the abc conjecture for K. If K is a function field, assume that ϕ is not isotrivial. For all sufficiently large n, there exists a prime of K that ramifies in $K(\phi^{-n}(\beta))$ and does not ramify in $K(\phi^{-m}(\beta))$ for $m \leq n-2$.*

One of our motivations for proving Theorem 1.2 was an application to the growth rate of Galois groups of iterates of polynomials. The group $\mathrm{Gal}(K_n/K)$ injects into $\mathrm{Aut}(T_n)$,

Please cite this article in press as: A. Bridy, T.J. Tucker, *ABC* implies a Zsigmondy principle for ramification, J. Number Theory (2017), http://dx.doi.org/10.1016/j.jnt.2017.06.015

the automorphism group of the complete d-ary rooted tree of height n where $d = \deg \phi$. The group $\mathrm{Aut}(T_n)$ is isomorphic to an iterated wreath product of the symmetric group S_d, so $|\mathrm{Aut}(T_n)|$ grows doubly exponentially in n. It is expected that in many cases the index $|\mathrm{Aut}(T_n) : \mathrm{Gal}(K_n/K)|$ remains bounded as $n \to \infty$, which implies that the degree of the splitting field of $\phi^n(x) - \beta$ over K grows doubly exponentially for large n. Odoni proved that generic polynomials have this property, as well as the particular polynomial $x^2 - x + 1$ [Odo85,Odo88]; Juul [Juu15] proved that generic rational functions have this property. Stoll proved that an infinite family of quadratic polynomials [Sto92] have this property. Boston and Jones [BJ09] have proposed a dynamical analog of the Serre open image theorem (see [Ser72]), and we hope to use the techniques of this paper to treat some special cases of this problem, in particular the case of cubic polynomials.

It follows from our main theorem that the growth rate for many non-postcritically finite rational maps is at least simply exponential (conditional on the *abc* conjecture when K is a number field). For example, this includes all polynomial maps.

Corollary 1.5. *Suppose that K, $\phi \in K(x)$, and $\beta \in \mathbb{P}^1(K)$ satisfy the assumptions of Theorem 1.2. Then there exists C such that for all sufficiently large n, $[K(\phi^{-n}(\beta)) : K] \geq C2^n$.*

The strategy of our proof combines the approaches of both [GNT13] and [BIJ+15]. We begin with Lemma 3.1, which gives a necessary condition for K_n to ramify over $\mathfrak{p}$; this is adapted from [BGH+13]. We then prove Lemma 3.2, which gives a sufficient condition for a prime $\mathfrak{p}$ to ramify in K_n. Note that the condition in both Lemmas has to do with whether or not a suitable iterate of a critical point of ϕ meets β at $\mathfrak{p}$. We then use a so-called "Roth-abc" result (see Proposition 2.2) to show that for each critical point α of ϕ, the quantities $\phi^n(\alpha) - \beta_j$ have very few repeated factors for large n and suitable preimages β_j of β. This is done in Lemma 4.2. We are also able to bound the contribution to the logarithmic height $h(\phi^n(\alpha) - \beta_j)$ coming from primes that divide $\phi^m(\alpha') - \beta_j$ for some $m < n$ and some critical point α' of ϕ. This is done in Lemmas 4.1 and 4.3 (note that in the application of Lemma 4.3, it is crucial that the number of wandering grand orbits of ϕ containing a critical point is small). Putting these together along with some other simple estimates gives a prime $\mathfrak{p}$ such that $v_{\mathfrak{p}}(\phi^n(\alpha) - \beta_j) = 1$ for some suitable preimage β_j of β with the property that $\mathfrak{p}$ does not ramify in K_m for any $m < n$. Applying Lemma 3.2 then gives our main result, Theorem 1.2.

2. Preliminaries

Let K be either a number field or a function field of characteristic 0 with transcendence degree 1 over its field of constants k. Let $\phi \in K(x)$ be a rational function of degree $d \geq 2$. If K is a number field, let $\mathfrak{o}_K$ be the ring of integers of K. If K is a function field, choose a prime $\mathfrak{q}$ and let $\mathfrak{o}_K = \{z \in K : v_{\mathfrak{p}}(z) \geq 0 \text{ for all primes } \mathfrak{p} \neq \mathfrak{q} \text{ of } K\}$. For any prime $\mathfrak{p}$, let $k_{\mathfrak{p}}$ be the residue field $\mathfrak{o}_K/\mathfrak{p}$.

Please cite this article in press as: A. Bridy, T.J. Tucker, *ABC* implies a Zsigmondy principle for ramification, J. Number Theory (2017), http://dx.doi.org/10.1016/j.jnt.2017.06.015

We use the notion of good reduction of rational functions as introduced by Morton and Silverman [MS94]. Let $\phi : \mathbb{P}^1(K) \to \mathbb{P}^1(K)$ be a morphism, written in homogeneous coordinates as $\phi([X : Y]) = [P(X,Y) : Q(X,Y)]$, where $P, Q \in \mathfrak{o}_K[X,Y]$ are homogeneous polynomials of the same degree without any common factor in $\overline{K}[X,Y]$. Letting $P_0(X,Y) = P(X,Y)$ and $Q_0(X,Y) = Q(X,Y)$, we recursively define $P_{m+1} = P(P_m(X,Y), Q_m(X,Y))$ and $Q_{m+1} = Q(P_m(X,Y), Q_m(X,Y))$. We let $p_m(X) = P_m(X,1)$ and let $q_m(X) = Q_m(X,1)$.

Let $\phi_\mathfrak{p} = [P_\mathfrak{p} : Q_\mathfrak{p}]$, where $P_\mathfrak{p}, Q_\mathfrak{p} \in k_\mathfrak{p}[X,Y]$ are the reductions of P and Q modulo $\mathfrak{p}$. We say that ϕ has *good reduction* at $\mathfrak{p}$ if there is some way of writing ϕ in homogeneous coordinates as $\phi = [P,Q]$ such that $\max(\deg P_\mathfrak{p}, \deg Q_\mathfrak{p})$ equals $\max(\deg P, \deg Q)$ and $P_\mathfrak{p}$, $Q_\mathfrak{p}$ have no common factor in $\bar{k}_\mathfrak{p}[X,Y]$. When ϕ has good reduction at $\mathfrak{p}$, $\phi_\mathfrak{p}$ induces a nonconstant morphism from $\mathbb{P}^1_{k_\mathfrak{p}}$ to itself. When this morphism is separable, we say that ϕ has *good separable* reduction at $\mathfrak{p}$.

2.1. Heights

For a rational prime $\mathfrak{p}$ of K, define

$$N_\mathfrak{p} = \frac{1}{[K:\mathbb{Q}]} \log \# k_\mathfrak{p}$$

if K is a number field and

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

if K is a function field. As in [GNT13], normalizing by the degree of the number field will make it easier to state proofs in the same way for both number fields and function fields.

If K is a number field, the height of $z \in K$ is defined as

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

where the second sum is taken over all maps $\sigma : K \to \mathbb{C}$ (in particular, complex conjugate embeddings are not identified). We extend h to $\mathbb{P}^1(K)$ by setting $h(\infty) = 0$. If K is a function field, instead the height of $z \in K$ is

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

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

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

Please cite this article in press as: A. Bridy, T.J. Tucker, *ABC* implies a Zsigmondy principle for ramification, J. Number Theory (2017), http://dx.doi.org/10.1016/j.jnt.2017.06.015

We will use the Call–Silverman canonical height h_ϕ, which is defined by

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

This limit exists by the same telescoping series argument that shows the existence of the Nerón–Tate height on an elliptic curve. See [CS93] for details. The canonical height satisfies the following important properties for some absolute constant C_ϕ and for every $x \in K$:

$$h_\phi(\phi(x)) = dh_\phi(x), \text{ and}$$
$$|h(x) - h_\phi(x)| \leq C_\phi.$$

It follows immediately from these properties that $h_\phi(x) \neq 0$ if and only if $h(\phi^n(x)) \to \infty$ as $n \to \infty$.

If K is a number field, then for $n \geq 2$ we define the height of the nonzero n-tuple $(z_1, z_2, \ldots, z_n) \in K^n$ by

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

2.2. The abc-conjecture

For $z_1, \ldots, z_n \in K^\times$, we define

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

and

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

With this notation, we assume the *abc*-conjecture as follows.

Conjecture 2.1. *Let K be a number field. For any $\epsilon > 0$, there exists a constant $C_{K,\epsilon}$ such that for all $a, b, c \in K^\times$ with $a + b = c$, we have*

$$h(a, b, c) < (1 + \epsilon) \operatorname{rad}(a, b, c) + C_{K,\epsilon}.$$

We will make use of the following estimate, sometimes called "Roth-*abc*" as in [GNT13], which holds for number fields conditionally on the *abc*-conjecture and is true unconditionally for function fields of characteristic 0. The following combines Propositions 3.4 and 4.2 from [GNT13].

Please cite this article in press as: A. Bridy, T.J. Tucker, *ABC* implies a Zsigmondy principle for ramification, J. Number Theory (2017), http://dx.doi.org/10.1016/j.jnt.2017.06.015

Proposition 2.2. *Let K be a number field or function field of characteristic 0. If K is a number field, suppose that the abc-conjecture holds for K. Let $F \in K[x]$ be a polynomial of degree at least 3 with no repeated factors and let $\epsilon > 0$. Then there exists $C_{F,\epsilon}$ such that for all $x \in K$,*

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

Note that in the case where K is a function field, the Roth-*abc* estimate does not follow from the *abc* conjecture but instead requires Yamanoi's proof [Yam04] of the Vojta conjecture for algebraic points on curves over function fields of characteristic 0.

2.3. Base extension

Certain arguments are made more easily after passing from our number field or function field K to a finite extension L of K. We will quickly show that our results are true over K exactly when they are true over a finite extension.

Lemma 2.3. *Let K be a number field or function field of characteristic 0, let L be a finite extension of K, let $\mathfrak{p}$ be a finite prime of K that does not ramify in L, and let $\mathfrak{q}$ be a finite prime of L such that $\mathfrak{q}|\mathfrak{p}$. Then, for any finite Galois extension M of K, the prime $\mathfrak{p}$ ramifies in M if and only if $\mathfrak{q}$ ramifies in the compositum $M \cdot L$.*

Proof. Suppose that $\mathfrak{p}$ does not ramify in M. Then $\mathfrak{p}$ does not ramify in $M \cdot L$ since $\mathfrak{p}$ does not ramify in L. Thus, any prime $\mathfrak{q}$ of L such that $\mathfrak{q}|\mathfrak{p}$ cannot ramify in $M \cdot L$.

Suppose that $\mathfrak{p}$ ramifies in M. Since M is Galois over K, this means that $e(\mathfrak{m}/\mathfrak{p}) > 1$ for any $\mathfrak{m}|\mathfrak{p}$ in M. Thus, for any $\mathfrak{r}|\mathfrak{p}$ in $L \cdot M$, we have $e(\mathfrak{r}/\mathfrak{p}) > 1$. Since $e(\mathfrak{q}/\mathfrak{p}) = 1$, we must have $e(\mathfrak{r}/\mathfrak{p}) = e(\mathfrak{r}/\mathfrak{q})$; hence, $e(\mathfrak{r}/\mathfrak{q}) > 1$ so $\mathfrak{q}$ ramifies in $M \cdot L$. □

Lemma 2.4. *Let K be a number field or function field of characteristic 0, let $\beta \in K$, and let ϕ be a rational function with coefficients in K. Let L be a finite extension of K. Then the following statements are equivalent:*

(a) For all sufficiently large n, there is a finite prime $\mathfrak{p}$ of K such that $\mathfrak{p}$ ramifies in $K(\phi^{-n}(\beta))$ and $\mathfrak{p}$ does not ramify in $K(\phi^{-m}(\beta))$ for $m < n$.
(b) For all sufficiently large n, there is a finite prime $\mathfrak{q}$ of L such that $\mathfrak{q}$ ramifies in $L(\phi^{-n}(\beta))$ and $\mathfrak{q}$ does not ramify in $L(\phi^{-m}(\beta))$ for $m < n$.

Proof. Let S be the set of finite primes of K that ramify in L and let T be the set of primes of L that lie over primes in S.

Suppose that (a) holds. Then, since S is finite, for all sufficiently large n, there is a finite prime $\mathfrak{p} \notin S$ of K such that $\mathfrak{p}$ ramifies in $K(\phi^{-n}(\beta))$ and $\mathfrak{p}$ does not ramify in

Please cite this article in press as: A. Bridy, T.J. Tucker, *ABC* implies a Zsigmondy principle for ramification, J. Number Theory (2017), http://dx.doi.org/10.1016/j.jnt.2017.06.015

$K(\phi^{-m}(\beta))$ for $m < n$. If $\mathfrak{q}$ is a prime of L such that $\mathfrak{q}|\mathfrak{p}$, then $\mathfrak{q}$ ramifies in $L(\phi^{-n}(\beta))$ and $\mathfrak{q}$ does not ramify in $L(\phi^{-m}(\beta))$ for $m < n$, by Lemma 2.3.

Likewise, if (b) holds, then, since T is finite, for all sufficiently large n, there is a finite prime $\mathfrak{q} \notin T$ of L such that $\mathfrak{q}$ ramifies in $L(\phi^{-n}(\beta))$ and $\mathfrak{q}$ does not ramify in $L(\phi^{-m}(\beta))$ for $m < n$. If $\mathfrak{p}$ is a prime of K such that $\mathfrak{q}|\mathfrak{p}$, then $\mathfrak{p}$ ramifies in $K(\phi^{-n}(\beta))$ and $\mathfrak{p}$ does not ramify in $K(\phi^{-m}(\beta))$ for $m < n$, again by Lemma 2.3. □

By Lemma 2.4, it suffices to prove Theorem 1.2 over a finite extension L of K. We argue here that it also suffices to prove the Theorem after replacing ϕ with $\phi^\sigma = \sigma \circ \phi \circ \sigma^{-1}$ for any Möbius transformation $\sigma \in L(x)$, and replacing β with $\sigma(\beta)$. Note that for any $\phi \in K(x)$ and $\beta \in \mathbb{P}^1(K)$, the hypotheses of Theorem 1.2 (ϕ is postcritically finite, β is non-exceptional, and the condition on wandering grand orbits intersecting R_ϕ) are invariant under this change of variables. This is because α is a critical point of ϕ if and only if $\sigma(\alpha)$ is a critical point of ϕ^σ, and because the map σ induces a bijection from the grand orbits of ϕ to the grand orbits of ϕ^σ that preserves their structure as grand orbits. Thus, we may assume that ϕ has a fixed point defined over K, and, after changing variables, we may assume that $\beta = 0$ and $\phi(\infty) = \infty$. Note that this means that $\deg P_m > \deg Q_m$ for all m and that when ϕ has good reduction at $\mathfrak{p}$, the leading coefficient of P_m is not divisible by $\mathfrak{p}$ for all m.

3. Criteria for ramification

To prove Theorem 1.1, we will need some conditions for ramification in preimage fields. The necessary condition is an adaptation of a standard result about ramification in $\mathfrak{p}$-adic fields, for example [BGH+13, Lemma 1]. Recall that K is either a number field or a function field of characteristic 0. From this point forward, for $\phi \in K(x)$ and $\beta \in \mathbb{P}^1(K)$, we use the notation $K_n = K(\phi^{-n}(\beta))$ as defined in the introduction.

Proposition 3.1. *Let $\phi \in K(x)$ and $\beta \in K$. Let $\mathfrak{p}$ be a prime of K such that ϕ has good separable reduction and $v_\mathfrak{p}(\beta) \geq 0$. If $\mathfrak{p}$ ramifies in K_n, there exists $\alpha \in R_\phi$ such that $v_\mathfrak{p}(\phi^m(\alpha) - \beta) > 0$ for some m with $1 \leq m \leq n$.*

Proof. Let $(p_n)_\mathfrak{p}$ and $(q_n)_\mathfrak{p}$ denote the reductions of p_n and q_n at $\mathfrak{p}$, and let $\beta_\mathfrak{p}$ denote the reduction of β at $\mathfrak{p}$. Since K_n is the splitting field of $p_n(X) - \beta q_n(X)$, it follows that if K_n ramifies at $\mathfrak{p}$ then $F(X) = (p_n)_\mathfrak{p}(X) - \beta_\mathfrak{p}(q_n)_\mathfrak{p}(X)$ has a multiple root. Thus, there is a root of $F(X)$ that is also a root of the derivative of $F(X)$.

Note that if γ is a root of both $F(X)$ and $F'(X)$, then γ is also a root of $(p_n)'_\mathfrak{p}(X)(q_n)_\mathfrak{p}(X) - (p_n)_\mathfrak{p}(X)(q_n)'_\mathfrak{p}(X)$. Since $(\phi_\mathfrak{p})^n$ is separable at $\mathfrak{p}$, we see that $(p_n)'_\mathfrak{p}(X)(q_n)_\mathfrak{p}(X) - (p_n)_\mathfrak{p}(X)(q_n)'_\mathfrak{p}(X)$ is not identically zero. Hence, all of its roots are the reduction modulo $\mathfrak{p}$ of a root of $p'_n(X)q_n(X) - p_n(X)q'_n(X)$. Therefore, there is a critical point α of ϕ^n that reduces to a root of $(p_n)_\mathfrak{p}(X) - \beta(q_n)_\mathfrak{p}(X)$ at $\mathfrak{p}$. This means that $v_\mathfrak{p}(\phi^m(\alpha) - \beta) > 0$. □

Please cite this article in press as: A. Bridy, T.J. Tucker, *ABC* implies a Zsigmondy principle for ramification, J. Number Theory (2017), http://dx.doi.org/10.1016/j.jnt.2017.06.015

Proposition 3.2. *Let $\phi \in K(x)$ and $\beta \in K$. For all primes $\mathfrak{p}$ of K such that ϕ has good separable reduction at $\mathfrak{p}$ and $v_{\mathfrak{p}}(\beta) \geq 0$, if there exists a critical point α of ϕ such that $\phi^n(\alpha) \neq \infty$ and $v_{\mathfrak{p}}(\phi^n(\alpha) - \beta) = 1$, then $\mathfrak{p}$ ramifies in K_n.*

Proof. This is the criterion that forms the main argument of [BIJ+15, Theorem 5]. We provide a brief proof here. First note that by Lemma 2.3, we may assume without loss of generality that $\alpha \in K$, as otherwise we can replace K by $K(\alpha)$.

Since K_n is the splitting field of $p_n(X) - q_n(X)\beta$ and $\alpha \in K$, it follows that K_n is also the splitting field of the polynomial $p_n(X + \alpha) - q_n(X + \alpha)\beta$. We write

$$p_n(X + \alpha) - q_n(X + \alpha)\beta = a_k X^k + \cdots + a_0.$$

Note that $v_{\mathfrak{p}}(a_0) = v_{\mathfrak{p}}((\phi^n(\alpha) - \beta)q_n(\alpha)) = 1$, because $v_{\mathfrak{p}}(q_n(\alpha)) = 0$ since $v_{\mathfrak{p}}(\beta) \geq 0$ and ϕ^n has good reduction at $\mathfrak{p}$. Also note that $v_{\mathfrak{p}}(a_k) = 0$, again using the fact that ϕ^n has good reduction at $\mathfrak{p}$.

Now, $p_n(X + \alpha) - q_n(X + \alpha)\beta$ is congruent to $p_n(X + \alpha) - q_n(X + \alpha)\phi^n(\alpha)$ mod $\mathfrak{p}$, because $v_{\mathfrak{p}}(\phi^n(\alpha) - \beta) > 0$. We have that X^e divides $p_n(X + \alpha) - q_n(X + \alpha)\phi^n(\alpha)$, where $e > 1$ is the ramification index of α, so there is an $\ell > 1$ such that $v_{\mathfrak{p}}(a_j) > 0$ for $k = 0, \ldots, \ell - 1$ and $v_{\mathfrak{p}}(a_\ell) = 0$. Thus, the first segment of the $\mathfrak{p}$-adic Newton polygon of $p_n(X+\alpha)-q_n(X+\alpha)\beta$ is the line from $(0, 1)$ to $(\ell, 0)$. Therefore, $p_n(X+\alpha)-q_n(X+\alpha)$ has a root γ such that $v_{\mathfrak{p}}(\gamma) = 1/\ell$, which means that K_n ramifies over K at $\mathfrak{p}$. (See [Kob77, IV.3] for summary of the theory of Newton polygons.) □

In the next section, we will use Propositions 3.1 and 3.2 in tandem to show the existence of primes that ramify in the nth preimage field but do not ramify earlier.

4. Proofs of main theorems

To prove Theorem 1.2, we want to reduce to the case where the base point β is non-periodic and non-postcritical. This ensures that the preimage sets $\phi^{-n}(\beta)$ are of size d^n, and in particular, that the numerator of $\phi^n(x) - \beta$ is a squarefree polynomial. This will allow us to easily use the Roth-*abc* estimate of Proposition 2.2. Of course, in general β may be periodic or postcritical. Let t be the smallest positive integer such that no element of $\phi^{-t}(\beta) \setminus \phi^{-(t-1)}(\beta)$ is periodic or postcritical. Let $\{\beta_1, \ldots, \beta_N\}$ denote $\phi^{-t}(\beta) \setminus \phi^{-(t-1)}(\beta)$. Note that if $x \in \phi^{-n}(\beta)$ for some $n > t$, and x is not periodic, not critical, and not postcritical, then $x \in \bigcup_{j=1}^{N} \mathcal{O}_\phi^-(\beta_j)$. By the discussion at the end of Section 2, we may adjoin the critical points of ϕ and the points $\beta_1, \ldots, \beta_N$ to K, and also make a change of variables such that $\beta = 0$ and $\phi(\infty) = \infty$.

Lemma 4.1. *Let $\alpha \in \mathbb{P}^1(K)$ with $h_\phi(\alpha) > 0$ and let $\beta_1, \ldots, \beta_N$ be as above. If K is a number field, assume the abc conjecture for K. Let $\delta > 0$. For $n > 0$, let $\mathcal{Z}(n)$ denote the set of primes $\mathfrak{p}$ of K such that*

Please cite this article in press as: A. Bridy, T.J. Tucker, *ABC* implies a Zsigmondy principle for ramification, J. Number Theory (2017), http://dx.doi.org/10.1016/j.jnt.2017.06.015

$$\min(v_{\mathfrak{p}}(\phi^n(\alpha)-\beta_i), v_{\mathfrak{p}}(\phi^m(\alpha)-\beta_j)) > 0$$

for some $0 < m < n$ and some i, j between 1 and N. Then there exists a constant C_δ such that

$$\sum_{\mathfrak{p}\in\mathcal{Z}(n)} N_{\mathfrak{p}} \leq \delta d^n h_\phi(\alpha) + C_\delta$$

for all sufficiently large n.

Proof. Let $F(X) = \prod_{i=1}^N (X-\beta_i)$. Then F divides the numerator of ϕ^t (because $\phi^t(\beta_i) = 0$ for all i), none of the β_i are periodic, and $\phi^\ell(\beta_i) \neq 0$ for all i and any $\ell = 0, \dots t-1$. Then Proposition 5.1 of [GNT13] asserts that if $\mathcal{Z}'(n)$ is the set of primes $\mathfrak{p}$ such that $\min(v_{\mathfrak{p}}(\phi^{m+t}(\alpha)), v_{\mathfrak{p}}(F(\phi^n(\alpha)))) > 0$, then for any $\delta > 0$, there is a constant C_δ such that

$$\sum_{\mathfrak{p}\in\mathcal{Z}'(n)} N_{\mathfrak{p}} \leq \delta h(\phi^n(\alpha)) + C_\delta$$

for all n. If ϕ has good reduction at $\mathfrak{p}$ and

$$\min(v_{\mathfrak{p}}(\phi^n(\alpha)-\beta_i), v_{\mathfrak{p}}(\phi^m(\alpha)-\beta_j)) > 0,$$

then $\phi^m(\alpha) \equiv \beta_j \pmod{\mathfrak{p}}$, so $\phi^{m+t}(\alpha) \equiv \phi^t(\beta_j) \equiv 0 \pmod{\mathfrak{p}}$, and so we have $v_{\mathfrak{p}}(\phi^{m+t}(\alpha)) > 0$. Likewise, $v_{\mathfrak{p}}(F(\phi^n(\alpha))) > 0$ since β_i is a root of F which is congruent to $\phi^n(\alpha)$ mod $\mathfrak{p}$. Thus, we see that if $\mathfrak{p} \in \mathcal{Z}(n)$ and ϕ has good reduction at $\mathfrak{p}$, then $\mathfrak{p}$ is in $\mathcal{Z}'(n)$. The contribution to the sum of $N_{\mathfrak{p}}$ for the finitely many primes $\mathfrak{p}$ where ϕ has bad reduction can be absorbed into the constant C_δ. Using the properties of h_ϕ established in Section 2, namely that $h_\phi(\phi(x)) = dh_\phi(x)$ and that $|h(x) - h_\phi(x)|$ is bounded independently of x, our proof is complete. □

Lemma 4.2. *Let β_j be as above. If K is a number field, suppose that the abc-conjecture holds for K. For every $\epsilon > 0$, there is a constant C_ϵ such that*

$$\sum_{v_{\mathfrak{p}}(\phi^n(\alpha)-\beta_j)=1} N_{\mathfrak{p}} \geq (d-\epsilon)d^{n-1}h_\phi(\alpha) + C_\epsilon.$$

Proof. Choose $m > 0$ such that $3/d^m < \epsilon/d$. Since β_j is not in the post-critical set, for any m, the set of solutions to $\phi^m(x) = \beta_j$ consists of exactly d^m distinct points. Thus, $p_m(X) - \beta_j q_m(X)$ has no repeated roots. Thus, using Proposition 2.2, and the fact that $|h - h_\phi|$ is bounded, there is a constant C_1 such that

$$\sum_{v_{\mathfrak{p}}(p_m(x)-\beta_j q_m(x))=1} N_{\mathfrak{p}} \geq (d^m - 3)h_\phi(x) + C_1$$

Please cite this article in press as: A. Bridy, T.J. Tucker, *ABC* implies a Zsigmondy principle for ramification, J. Number Theory (2017), http://dx.doi.org/10.1016/j.jnt.2017.06.015

for all $x \in K$. Letting $x = \phi^{n-m}(\alpha)$, we see there is a constant C_2 such that

$$\sum_{v_{\mathfrak{p}}(\phi^m(\phi^{n-m}(\alpha)))=1} N_{\mathfrak{p}} \geq (1-\epsilon/d)d^m d^{n-m} h_\phi(\alpha) + C_1 \geq (d-\epsilon)d^{n-1}h_\phi(\alpha) + C_2.$$

For all but at most finitely many $\mathfrak{p}$ we have $v_{\mathfrak{p}}(\phi^n(\alpha)) = v_{\mathfrak{p}}(F(\phi^n(\alpha)))$, so the Lemma follows immediately. □

Lemma 4.3. *Let G be a set of critical points of ϕ that all have the same grand orbit. Let $\mathcal{Y}(i,j)$ be the set of primes $\mathfrak{p}$ such that*

$$v_{\mathfrak{p}}(\phi^i(\gamma) - \beta_j) > 0$$

for some $\gamma \in G$. Let $M_G = \max_{\gamma \in G} h_\phi(\gamma)$. Then, for all n, we have

$$\sum_{i=1}^{n-1}\sum_{j=1}^{N}\sum_{\mathfrak{p}\in\mathcal{Y}(i,j)} N_{\mathfrak{p}} \leq N\left(\frac{1}{d-1}\right)d^n M_G + O(n).$$

Proof. Let $\alpha \in G$ be the critical point of largest canonical height $h_\phi(\alpha)$. For every $\gamma \in G$, we have $\phi^n(\alpha) = \phi^m(\gamma)$ for some $n, m \geq 0$, so $d^n h_\phi(\alpha) = d^m h_\phi(\gamma)$ and $m \geq n$. In other words, α is the "farthest forward" critical point in the grand orbit. So except for $1 \leq i \leq m-n$, the primes that divide $\phi^i(\gamma) - \beta_j$ also divide $\phi^k(\alpha) - \beta_j$ for some k. The indicated initial values of i have a finite contribution to the sum that can be absorbed into the $O(n)$ term.

By the product formula and properties of heights we have

$$\sum_{v_{\mathfrak{p}}(\phi^i(\alpha)-\beta_j)>0} N_{\mathfrak{p}} \leq h(\phi^i(\alpha) - \beta_j) \leq d^i h(\alpha) + h(\beta_j) + C_\phi.$$

So we can use the estimation

$$\sum_{i=1}^{n-1}\sum_{j=1}^{N}\sum_{\mathfrak{p}\in\mathcal{Y}(i,j)} N_{\mathfrak{p}} \leq N M_G \frac{d^n-1}{d-1} + nC_{\phi,\beta_1,\ldots,\beta_N} + O(n)$$

and the lemma follows. □

Now, we are ready to prove Theorem 1.2.

Proof of Theorem 1.2. Assume that $\phi \in K(x)$ is not postcritically finite and that $\beta \in \mathbb{P}^1(K)$ is not exceptional for ϕ. Let $\beta_1, \ldots, \beta_N$ be as above. If necessary, replace K with $K(\alpha, \beta_1, \ldots, \beta_N)$ (by Lemma 2.4 this loses no generality). Let g be the number of wandering grand orbits that R_ϕ intersects (we have $g \leq d-1$) and let $\alpha \in R_\phi$ be a critical point of maximum canonical height $h_\phi(\alpha)$. Observe that $h_\phi(\alpha) > 0$, because if every critical point has canonical height 0, then ϕ is postcritically finite. This follows

Please cite this article in press as: A. Bridy, T.J. Tucker, *ABC* implies a Zsigmondy principle for ramification, J. Number Theory (2017), http://dx.doi.org/10.1016/j.jnt.2017.06.015

from the fact that if K is a number field, then any nonpreperiodic point must have positive canonical height by Northcott's theorem, while if K is a function field, Baker [Bak09] and Benedetto [Ben05] have proved that any nonpreperiodic point has positive canonical height whenever ϕ is not isotrivial. Hence, we may apply Lemma 4.1 to the orbit of α.

As in the proof of Lemma 4.3, α is the farthest forward critical point in its grand orbit. So for each other critical point γ in the same grand orbit as α, we have $\phi^u(\gamma) = \phi^s(\alpha)$ for some positive integers s, u with $s \leq u$. Choose u to be maximal such that there is a critical point γ in the same grand orbit as α such that $\phi^u(\gamma) = \phi^s(\alpha)$ for some s (this occurs when γ is of minimal canonical height among all critical points in the same grand orbit).

Now, let $\mathcal{X}(n)$ be the set of primes $\mathfrak{p}$ of K such that

- ϕ has good separable reduction at $\mathfrak{p}$,
- $v_\mathfrak{p}(\phi^m(\gamma) - \beta_j) \leq 0$ for all critical points γ in the same grand orbit as α, all $1 \leq m \leq u-1$, and all $1 \leq j \leq N$.
- $v_\mathfrak{p}(\phi^n(\alpha) - \beta_j) = 1$ for some $1 \leq j \leq N$,
- $v_\mathfrak{p}(\phi^m(\alpha) - \beta_j) \leq 0$ for all $1 \leq m \leq n-1$ and $1 \leq j \leq N$, and
- $v_\mathfrak{p}(\phi^m(\gamma) - \beta_j) \leq 0$ for every critical point γ not in the same grand orbit as α, and all $1 \leq m \leq n-1$ and $1 \leq j \leq N$.

Suppose that $\mathfrak{p} \in \mathcal{X}(n)$. We claim that $\mathfrak{p}$ ramifies in K_n and does not ramify in K_m for $m < n$. By Propositions 3.1 and 3.2, we need only show that there is no critical point γ in the same grand orbit as α so that $v_\mathfrak{p}(\phi^m(\gamma) - \beta_j) > 0$ for some j and some $m < n$. Aiming for a contradiction, suppose there is some such γ. We have $\phi^u(\gamma) = \phi^s(\alpha)$ for u as above and some positive s. Since $v_\mathfrak{p}(\phi^m(\gamma) - \beta_j) > 0$, we must have $m \geq u$ by the second bullet point defining $\mathcal{X}(n)$. So $\phi^m(\gamma) = \phi^{m-u+s}(\alpha) \equiv \beta_j \pmod{\mathfrak{p}}$. But $m - u + s \leq n-1$, which is a contradiction by the fourth bullet point.

It remains to show that $\mathcal{X}(n)$ is nonempty for all large n. There are only finitely many primes $\mathfrak{p}$ for which ϕ fails to have good separable reduction at $\mathfrak{p}$ or $v_\mathfrak{p}(\phi^m(\gamma) - \beta_j) > 0$ for a critical point γ in the same grand orbit as α, some β_j, and some $1 \leq m \leq u-1$. Therefore we focus on the other conditions that define $\mathcal{X}(n)$, as this finite set of primes will only contribute a constant to our height estimates.

By Lemma 4.2, for a given j and any $\epsilon > 0$ we have

$$\sum_{v_\mathfrak{p}(\phi^n(\alpha) - \beta_j) = 1} N_\mathfrak{p} \geq (d - \epsilon) d^{n-1} h_\phi(\alpha) + C_\epsilon.$$

It follows that

$$\sum_{v_\mathfrak{p}(\phi^n(\alpha) - \beta_j) = 1 \text{ for some } j} N_\mathfrak{p} \geq N(d - \epsilon) d^{n-1} h_\phi(\alpha) + C_\epsilon$$

Please cite this article in press as: A. Bridy, T.J. Tucker, *ABC* implies a Zsigmondy principle for ramification, J. Number Theory (2017), http://dx.doi.org/10.1016/j.jnt.2017.06.015

because the primes $\mathfrak{p}$ such that $v_{\mathfrak{p}}(\phi^n(\alpha) - \beta_j) > 0$ for $j = j_1$ and $j = j_2$ are divisors of $\beta_{j_1} - \beta_{j_2}$. The set of primes dividing $\beta_{j_1} - \beta_{j_2}$ for $j_1 \neq j_2$ is finite, so the contribution to the sum from these primes can be absorbed into the constant C_ϵ. At this point, we can also absorb into C_ϵ any contribution to the sum of $N_{\mathfrak{p}}$ from the finite set of primes mentioned in the previous paragraph.

Now we apply Lemma 4.1 to α and each β_j, and we apply Lemma 4.3 to the grand orbits not containing α that intersect R_ϕ. There are at most $d-2$ such wandering grand orbits; any preperiodic grand orbits contribute at most an $O(n)$ term to the sum because the term M_G coming from Lemma 4.3 is zero. Now we subtract the conclusion of Lemma 4.1 (N times) and Lemma 4.3 ($g-1$ times) from the conclusion of Lemma 4.2. This gives the following: for every $\epsilon > 0$ and $\delta > 0$, there are constants C_ϵ, C_δ, and C such that, for all sufficiently large n, we have

$$\begin{aligned}\sum_{\mathfrak{p}\in\mathcal{X}(n)} N_{\mathfrak{p}} \geq & N(d-\epsilon)d^{n-1}h_\phi(\alpha) + C_\epsilon - N\delta d^n h_\phi(\alpha) - C_\delta \\ & - (g-1)N\frac{1}{d-1}d^n h_\phi(\alpha) + Cn \\ \geq & d^n h_\phi(\alpha) N\left(1 - \epsilon d^{-1} - \delta - \frac{d-2}{d-1}\right) + Cn.\end{aligned}$$

Choosing ϵ and δ small enough, this quantity is positive for all large n, and we are done. □

Proof of Theorem 1.4. By the chain rule, the critical points of ϕ^2 are either critical points of ϕ or preimages of these points under ϕ, so the critical points of ϕ^2 lie in at most $\#R_\phi \leq 2d-2$ distinct grand orbits. We have $2d-2 < d^2-1$ because $d > 1$. Applying Theorem 1.2 to the map ϕ^2 and the point β, and also to a distinct point in $\phi^{-1}(\beta)$ (which exists because β is not exceptional) yields the result. □

Proof of Corollary 1.5. By Theorem 1.1, for all sufficiently large n there is a prime of K that ramifies in K_{n+1} but not in K_n. Therefore the kernel of the natural surjection $\mathrm{Gal}(K_{n+1}/K) \to \mathrm{Gal}(K_n/K)$ is nontrivial, so it must be at least order 2. The result follows. □

5. The isotrivial case

In this section we treat the case of isotrivial rational functions. The techniques here are much more elementary than in the rest of the paper.

Theorem 5.1. *Let K be a function field of characteristic 0 with field of constants k, and let $\phi \in K(x)$ be a rational function of degree greater than one. Suppose that there is a finite extension K' of K and $\sigma \in K'(x)$ such that $\sigma\phi\sigma^{-1} \in k'(x)$, where k' is the algebraic closure of k in K'. Then we have the following:*

Please cite this article in press as: A. Bridy, T.J. Tucker, *ABC* implies a Zsigmondy principle for ramification, J. Number Theory (2017), http://dx.doi.org/10.1016/j.jnt.2017.06.015

(a) If $\sigma(\beta) \in k'$, then there are at most finitely many primes of K that ramify in $\bigcup_{n=1}^{\infty} K_n$.

(b) If $\sigma(\beta) \notin k'$ and ϕ is not postcritically finite, then for all sufficiently large n, there exists a prime of K that ramifies in K_n and does not ramify in K_m for $m < n$.

Proof. Suppose that $\sigma(\beta) \in k'$. Then, if $\phi^n(\alpha) = \beta$, we have

$$\sigma\phi\sigma^{-1}(\sigma(\alpha)) = \sigma(\beta) \in k'.$$

Since $\sigma\phi\sigma^{-1} \in k'(x)$, where k' is algebraic over k, it follows that $\sigma(\alpha) \in \bar{k}$. Thus, α is in the compositum $\bar{k} \cdot K'$. Since K' ramifies over at most finitely many primes of K and $\bar{k} \cdot K'$ is unramified everywhere over K', we see that $\bar{k} \cdot K'$ ramifies over at most finitely many primes of K. Thus, there are only finitely many primes of K that ramify in $\bigcup_{n=1}^{\infty} K_n$.

Now suppose that $\sigma(\beta) \notin k'$. After passing to a finite extension, we may assume that all the critical points of ϕ are defined over K'. Let ϕ^σ denote $\sigma\phi\sigma^{-1}$. Since every critical point of ϕ^σ is simply $\sigma(z)$ for a critical point z of σ and every critical point of ϕ^σ is algebraic over k, we see then that every critical point of ϕ^σ is in k'.

Now, note that $\sigma(\beta)$ is not algebraic over k', and that K' is therefore a finite extension of $k'(\sigma(\beta))$. For any critical point α' of ϕ^σ and any m, we see that $(\phi^\sigma)^m(\alpha') - \sigma(\beta)$ generates a prime in $k'(\sigma(\beta))$. Since ϕ^σ is not postcritically finite, there is a critical point α of ϕ^σ such that $(\phi^\sigma)^m(\alpha) \neq (\phi^\sigma)^n(\alpha')$ for any $n < m$ and any critical point $\alpha \neq \alpha'$. Thus, for every $n > 0$, there is a prime $\mathfrak{m}$ of $k'(\sigma(\beta))$ such that $v_{\mathfrak{m}}((\phi^\sigma)^n(\alpha) - \sigma(\beta)) = 1$ and $v_{\mathfrak{m}}((\phi^\sigma)^m(\alpha)' - \sigma(\beta)) = 0$ for all $m < n$. Then, by Proposition 3.2 and 3.1, this prime $\mathfrak{m}$ ramifies in $k'(\sigma(\beta))((\phi^\sigma)^{-n}(\sigma(\beta)))$ and does not ramify in $k'(\sigma(\beta))((\phi^\sigma)^{-m}(\sigma(\beta)))$ for any $m < n$. Note that since σ is defined over K' and $(\phi^\sigma)^n = \sigma\phi^n\sigma^{-1}$, we see that for any z we have $(\phi^\sigma)^n(z) = \sigma(\beta)$ if and only if $\phi^n(\sigma(z)) = \beta$. Thus, by Lemma 2.4 it follows that for all but finitely many n, there is a prime $\mathfrak{q}$ of K' such that $\mathfrak{q}$ ramifies in $K(\phi^{-n}(\beta))$ but $\mathfrak{q}$ does not ramify in $K(\phi^{-m}(\beta))$ for any $m < n$. Applying Lemma 2.4 again, we see that for all but finitely many n, there is a prime $\mathfrak{p}$ of K such that $\mathfrak{p}$ ramifies in $K(\phi^{-n}(\beta))$ but $\mathfrak{p}$ does not ramify in $K(\phi^{-m}(\beta))$ for any $m < n$, as desired. □

Acknowledgments

We would like to thank the referee for many useful suggestions and corrections. The second author was partially supported by NSF Grant DMS-1501515.

References

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

[Ben05] R.L. Benedetto, Heights and preperiodic points of polynomials over function fields, Int. Math. Res. Not. IMRN (62) (2005) 3855–3866.

Please cite this article in press as: A. Bridy, T.J. Tucker, *ABC* implies a Zsigmondy principle for ramification, J. Number Theory (2017), http://dx.doi.org/10.1016/j.jnt.2017.06.015

[BGH+13] R.L. Benedetto, D. Ghioca, B. Hutz, P. Kurlberg, T. Scanlon, T.J. Tucker, Periods of rational maps modulo primes, Math. Ann. 355 (2) (2013) 637–660.

[BJ09] N. Boston, R. Jones, The image of an arboreal Galois representation, Pure Appl. Math. Q. 5 (1) (2009) 213–225.

[BIJ+15] A. Bridy, P. Ingram, R. Jones, J. Juul, A. Levy, M. Manes, S. Rubinstein-Salzedo, J.H. Silverman, Finite ramification for preimage fields of postcritically finite morphisms, available at arXiv:1511.00194, 2015.

[CS93] G.S. Call, J.H. Silverman, Canonical heights on varieties with morphisms, Compos. Math. 89 (2) (1993) 163–205.

[Elk91] N.D. Elkies, *ABC* implies Mordell, Int. Math. Res. Not. IMRN (7) (1991) 99–109.

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

[GNT13] C. Gratton, K. Nguyen, T.J. Tucker, *ABC* implies primitive prime divisors in arithmetic dynamics, Bull. Lond. Math. Soc. 45 (6) (2013) 1194–1208.

[IS09] P. Ingram, J.H. Silverman, Primitive divisors in arithmetic dynamics, Math. Proc. Cambridge Philos. Soc. 146 (2) (2009) 289–302.

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

[Kob77] N. Koblitz, p-Adic Numbers, p-Adic Analysis, and Zeta-Functions, Graduate Texts in Mathematics, vol. 58, Springer-Verlag, New York–Heidelberg, 1977.

[Kri13] H. Krieger, Primitive prime divisors in the critical orbit of $z^d + c$, Int. Math. Res. Not. IMRN (23) (2013) 5498–5525.

[Mas84] R.C. Mason, Diophantine Equations over Function Fields, London Mathematical Society Lecture Note Series, vol. 96, Cambridge University Press, Cambridge, 1984.

[MS94] P. Morton, J.H. Silverman, Rational periodic points of rational functions, Int. Math. Res. Not. IMRN (2) (1994) 97–110.

[Odo85] R.W.K. Odoni, The Galois theory of iterates and composites of polynomials, Proc. Lond. Math. Soc. (3) 51 (3) (1985) 385–414.

[Odo88] R.W.K. Odoni, Realising wreath products of cyclic groups as Galois groups, Mathematika 35 (1) (1988) 101–113.

[Ric07] B. Rice, Primitive prime divisors in polynomial arithmetic dynamics, Integers 7 (A26) (2007) 16.

[Ser72] J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Invent. Math. 15 (4) (1972) 259–331.

[Sil84] J.H. Silverman, The S-unit equation over function fields, Math. Proc. Cambridge Philos. Soc. 95 (1) (1984) 3–4.

[Sil93] J.H. Silverman, Integer points, Diophantine approximation, and iteration of rational maps, Duke Math. J. 71 (3) (1993) 793–829.

[Sto92] M. Stoll, Galois groups over $\mathbf{Q}$ of some iterated polynomials, Arch. Math. (Basel) 59 (3) (1992) 239–244.

[Sto81] W.W. Stothers, Polynomial identities and Hauptmoduln, Quart. J. Math. Oxford Ser. (2) 32 (127) (1981) 349–370.

[Yam04] K. Yamanoi, The second main theorem for small functions and related problems, Acta Math. 192 (2) (2004) 225–294.

[Zsi92] K. Zsigmondy, Zur Theorie der Potenzreste, Monatsh. Math. Phys. 3 (1) (1892) 265–284.

Please cite this article in press as: A. Bridy, T.J. Tucker, *ABC* implies a Zsigmondy principle for ramification, J. Number Theory (2017), http://dx.doi.org/10.1016/j.jnt.2017.06.015