Algebra & Number Theory

Volume 11

2017

No. 6

Greatest common divisors of iterates of polynomials

Liang-Chung Hsia and Thomas J. Tucker

msp

ALGEBRA AND NUMBER THEORY 11:6 (2017)
dx.doi.org/10.2140/ant.2017.11.1437

Greatest common divisors of iterates of polynomials

Liang-Chung Hsia and Thomas J. Tucker

Following work of Bugeaud, Corvaja, and Zannier for integers, Ailon and Rudnick prove that for any multiplicatively independent polynomials, $a, b \in \mathbb{C}[x]$, there is a polynomial h such that for all n, we have

$$\gcd(a^n - 1, b^n - 1) \mid h$$

We prove a compositional analog of this theorem, namely that if $f, g \in \mathbb{C}[x]$ are compositionally independent polynomials and $c(x) \in \mathbb{C}[x]$, then there are at most finitely many λ with the property that there is an n such that $(x - \lambda)$ divides $\gcd(f^{\circ n}(x) - c(x), g^{\circ n}(x) - c(x))$.

Bugeaud, Corvaja, and Zannier [2003] obtained an upper bound for the greatest common divisors among two families of integer sequences. More precisely, let a and b be two positive integers that are multiplicatively independent and let $\epsilon > 0$ be given. Then for all n, we have $\gcd(a^n - 1, b^n - 1) \ll_\epsilon \exp(\epsilon n)$ where the implied constant is independent of n.

Since Bugeaud, Corvaja, and Zannier's paper appeared, there have been many extensions and generalizations of their results (see, for example, [Ailon and Rudnick 2004; Silverman 2004a; 2004b; 2005; Corvaja and Zannier 2005; 2008; 2013; Luca 2005; Murty and Murty 2011; Zannier 2012; Ghioca et al. 2017a; 2017b; Huang 2017]). In particular, Ailon and Rudnick [2004] obtained a stronger upper bound in the setting of function fields of characteristic zero. They showed that for two multiplicatively independent nonconstant polynomials $a, b \in \mathbb{C}[x]$, there is a polynomial $h \in \mathbb{C}[x]$, depending on a and b such that $\gcd(a^n - 1, b^n - 1) \mid h$ for all positive integer n. We note here that the result of Ailon and Rudnick also holds when one takes the greatest common divisors of $a^m - 1$ and $b^n - 1$ across all pairs of positive integers m and n (not merely those where $m = n$).

Instead of taking multiplicative powers of polynomials, one can consider iterated compositions of polynomials and look for an upper bound on the degrees of the

---

The first author was partially supported by MOST Grant 105-2628-M-002-003. The second author was partially supported by NSF Grant DMS-0101636.

MSC2010: primary 37P05; secondary 14G25.

Keywords: gcd, composition, heights, equidstribution.

greatest common divisors among two such sequences of polynomials as asked by A. Ostafe [2016, Problem 4.2]. In this paper, we prove a compositional analog of theorem of Ailon and Rudnick described above.

In the following, for a polynomial q, we let $q^{\circ n}$ denote the composition of q with itself n times. To state our theorem precisely, we need a definition of compositional independence.

Definition. We say two polynomials f and g are *compositionally independent* if the semigroup generated by f and g under composition is isomorphic to the free semigroup with two generators. This is equivalent to the property that whenever $i_1, \dots, i_s, j_1, \dots, j_s, \ell_1, \dots, \ell_t, m_1, \dots m_t$ are positive integers such that

$$f^{\circ i_1} \circ g^{\circ j_1} \circ \cdots \circ f^{\circ i_s} \circ g^{\circ j_s} = f^{\circ \ell_1} \circ g^{\circ m_1} \circ \cdots \circ f^{\circ \ell_t} \circ g^{\circ m_t},$$

we must have $s = t$, and $i_k = \ell_k$, $j_k = m_k$ for $k = 1, \dots, s$.

Under the compositional independence condition, our first result is the finiteness of the irreducible factors of $\gcd(f^{\circ m}(x) - c(x), g^{\circ n}(x) - c(x))$ where f, g and c are polynomials with complex coefficients. More precisely, we have the following theorem which answers Ostafe's question.

Theorem 1. *Let $f(x)$ and $g(x)$ be two compositionally independent polynomials in $\mathbb{C}[x]$, at least one of which has degree greater than one. Suppose that $c(x)$ is not a compositional power of f or g. Then there are at most finitely many $\lambda \in \mathbb{C}$ such that*

$$(x - \lambda) \mid \gcd(f^{\circ m}(x) - c(x), g^{\circ n}(x) - c(x))$$

for some positive integers m, n.

The restriction on the degrees of the two polynomials f and g in Theorem 1 is necessary. As the examples at the beginning of Section 3 demonstrate that Theorem 1 must be modified when f and g are both linear. If we restrict to the case $m = n$ in Theorem 1, then we still obtain a finiteness result when the two polynomials f and g are both linear.

Theorem 2. *Let f and g be two compositionally independent linear polynomials and let c be any polynomial. Then there is a polynomial $h \in \mathbb{C}[x]$ such that*

$$\gcd(f^{\circ n}(x) - c(x), g^{\circ n}(x) - c(x)) \mid h$$

for all positive integers n.

Putting Theorem 2 together with Theorem 1 under the condition that the composition power $m = n$, then for *any* polynomials $c(x)$ we have the same conclusion.

Theorem 3. *Let f and g be two compositionally independent polynomials. Then there are at most finitely many $\lambda \in \mathbb{C}$ such that*

$$(x-\lambda) \mid \gcd(f^{\circ n}(x)-c(x), g^{\circ n}(x)-c(x))$$

for some positive integer n.

We note that Theorem 2 is a compositional analog of Ailon and Rudnick's result for linear polynomials. To obtain a theorem that is parallel to their result for nonlinear polynomials, we need a bound for the multiplicity of each irreducible factor that divides the greatest common divisors. In general, one cannot expect such a bound exists. For instance, take $f(x) = x^3 + x^2$, $g(x) = x^3 + 5x^2$ and $c = 0$. Then, for any positive integer n, we have

$$x^{2^n} \mid \gcd(f^{\circ n}(x), g^{\circ n}(x))$$

Hence, in this case there does not exist a polynomial h divisible by all the greatest common divisors of the sequences in question. To get control on the bound of the multiplicities of irreducible factors dividing the greatest common multiples, we need one extra condition.

Definition. We say that $\xi \in \mathbb{C}$ is in a ramified cycle of a polynomial q if there is a positive integer i such that $q^{\circ i}(\xi) = \xi$ and $(q^{\circ i})'(\xi) = 0$.

Once we exclude this sort of possibility, we are able to show that there exists a polynomial that is divisible by all the greatest common divisors of the compositional sequences formed by f and g.

Theorem 4. *Let $f(x)$ and $g(x)$ be two compositionally independent polynomials of degree greater than one in $\mathbb{C}[x]$. Suppose that $c(x)$ is not a compositional power of f or g. Suppose furthermore that $c(x)$ is not equal to a constant c that is in a ramified cycle of both f and g. Then there is a polynomial $h \in \mathbb{C}[x]$ such that*

$$\gcd(f^{\circ m}(x)-c(x), g^{\circ n}(x)-c(x)) \mid h$$

for all positive integers m and n.

Remark. (1) One might naturally ask if the theorems of this paper still hold when one replaces $\gcd(f^{\circ m}(x)-c(x), g^{\circ n}(x)-c(x))$ with

$$\gcd(f^{\circ m}(x)-c_1(x), g^{\circ n}(x)-c_2(x))$$

for any $c_1(x), c_2(x) \in \mathbb{C}[X]$ (with $c_1(x)$ and $c_2(x)$ not necessarily equal). The proof of Theorem 1 goes through without change to treat this generalization as long as $f(x), g(x), c_1(x), c_2(x) \in \overline{\mathbb{Q}}[x]$; we believe that the case of complex coefficients can probably also be treated with some additional work. We do not, however, have an idea of how to generalize Theorem 2 to treat the case where $c_1(x) \neq c_2(x)$.

(2) In the situation considered by Ailon and Rudnick, the number 1 is not in a ramified cycle of any powering map. In fact, any nonzero polynomial $c(x)$ is not in a ramified cycle of any powering map.

We give a brief description of the organization of our paper and explain the ideas of the proofs. In Section 1, we set up notations and provide some background about canonical height functions associated to rational maps on the projective line over a global field. After the preliminaries in Section 1, we begin to prove our results.

We prove Theorem 1 in Section 2. The proof is split into two parts. We first treat the case where neither f nor g is linear. This is done in Proposition 8. An additional ingredient is required for the case where one of f and g is linear; we treat this case separately in Proposition 9. Then Theorem 1 is just the combination of these two propositions. We sketch the proof of Proposition 8 here. Assume that the set of λ that are roots of

$$\gcd\bigl(f^{\circ m}(x) - c(x),\, g^{\circ n}(x) - c(x)\bigr)$$

is infinite as m and n run through all positive integers. Then these numbers have the property that the canonical heights $\hat{h}_f(\lambda)$ and $\hat{h}_g(\lambda)$ both converge to zero (see Lemma 6). Applying equidistribution theorems in arithmetic dynamics, following the pattern of [Ghioca and Tucker 2010; Baker and DeMarco 2011; Ghioca et al. 2015], we conclude that both polynomials f and g have the same Julia set in the complex plane. Then the work of Baker and Erëmenko [1987] and Schmidt and Steinmetz [1995] shows that a compositional relation between f and g exists. Thus we get a contradiction to the assumption that f and g are compositionally independent and finish the proof.

Section 3 is devoted to the proof of Theorem 2 and Theorem 3. The proof of Theorem 2 is quite different, as the tools used to prove Theorem 1 are no longer applicable to the case where both polynomials f and g are linear. The proof for this case relies heavily on diophantine methods, in particular an application of results from [Corvaja and Zannier 2005], Roth's theorem, and a lemma of Siegel. These results are used to prove the case where everything is defined over $\overline{\mathbb{Q}}$, in Proposition 15. The general case of Theorem 2 then follows via specialization. Theorem 3 follows easily by combining Theorem 1 and Theorem 2.

We prove Theorem 4 in Section 4. It is sufficient to bound the multiplicities of the roots of $\gcd(f^{\circ m}(x) - c(x), g^{\circ n}(x) - c(x))$ in Theorem 1 provided that $c(x)$ is not a constant in a ramified cycle of both f and g. The analysis on the bound of the multiplicity used here is similar to those used in [Morton and Silverman 1995, Lemma 3.4]. We provide such a bound in Lemma 16. Then, Theorem 4 follows from Theorem 1 coupled with Lemma 16. Finally, we end this paper by raising several questions for further study in Section 5.

1. Preliminaries

In this section, we set up some notations and recall facts from the theory of height functions that will be used in this paper.

Let K be a field of characteristic 0 equipped with a set of inequivalent absolute values (places) Ω_K, normalized so that the product formula holds. More precisely, for each $v \in \Omega_K$ there exists a positive integer N_v such that for all $\alpha \in K^*$ we have $\prod_{v\in\Omega} |\alpha|_v^{N_v} = 1$ where for $v \in \Omega_K$, the corresponding absolute value is denoted by $|\cdot|_v$. Examples of product formula fields (or *global fields*) are number fields and function fields of projective varieties which are regular in codimension 1 over another field k (see [Lang 1983, §2.3] or [Bombieri and Gubler 2006, §1.4.6]).

We let $\mathbb{C}_v$ be the completion of an algebraic closure of K_v, a completion of K with respect to $|\cdot|_v$. When v is an archimedean valuation, then $\mathbb{C}_v = \mathbb{C}$. We fix an extension of $|\cdot|_v$ to an absolute value of $\mathbb{C}_v$ which by abuse of notation, we still denote by $|\cdot|_v$.

If K is a number field, we let Ω_K be the set of all absolute values of K which extend the (usual) absolute values of $\mathbb{Q}$. For each $v \in \Omega_K$, we let v_0 denote the (unique) absolute value of $\mathbb{Q}$ such that $v|_{\mathbb{Q}} = v_0$ and we let $N_v := [K_v : \mathbb{Q}_{v_0}]$. If K is a function field of a projective normal variety $\mathcal{V}$ defined over a field k, then Ω_K is the set of all absolute values on K associated to the irreducible divisors of $\mathcal{V}$. Then there exist positive integers N_v (for each $v \in \Omega_K$) such that $\prod_{v\in\Omega_K} |x|_v^{N_v} = 1$ for each nonzero $x \in K$. (See [Lang 1983; Serre 1997] for more details).

Let L be a finite extension of K, and let Ω_L be the set of all absolute values of K which extend the absolute values in Ω_K. For each $w \in \Omega_L$ extending some $v \in \Omega_K$ we let $N_w := N_v \cdot [L_w : K_v]$. The (naive) Weil height of any point $x \in L$ is defined as

$$h(x) = \frac{1}{[L:K]} \sum_{w\in\Omega_L} N_w \cdot \log\max\{1, |x|_w\}.$$

To ease the notation, we set $\|x\|_v := |x|_v^{N_v}$ for $x \in K$.

Let $f \in K(x)$ be any rational map of degree $d \geq 2$. Then the *global canonical height* $\hat{h}_f(x)$ of $x \in \overline{K}$ associated to f is given by the limit

$$\hat{h}_f(x) = \lim_{n\to\infty} \frac{h(f^n(x))}{d^n}$$

(see [Call and Silverman 1993] for details). In addition, Call and Silverman proved that the global canonical height decomposes as a sum of the local canonical heights, i.e.,

$$\hat{h}_f(x) = \frac{1}{[K(x):K]} \sum_{\sigma:K(x)\to\overline{K}} \sum_{v\in\Omega_K} N_v \hat{h}_{f,v}(x^\sigma), \tag{4.1}$$

where σ runs through all embeddings of $K(x)$ into $\overline{K}$ and for each $v \in \Omega_K$ the function $\hat{h}_{f,v}$ is the local canonical height associated to f. For the existence and functorial property of the local canonical height see [Call and Silverman 1993, Theorem 2.1].

The following facts about height functions are well known.

Proposition 5. *Let $f \in K(x)$ be a rational function of degree $d \geq 2$ defined over K. There are constants c_1, c_2, c_3, and c_4, depending only on d, such that the following estimates hold for all $x \in \overline{K}$:*

(a) $\left|h(f(x)) - dh(x)\right| \leq c_1 h(f) + c_2$.

(b) $\left|\hat{h}_f(x) - h(x)\right| \leq c_3 h(f) + c_4$.

(c) $\hat{h}_f(f(x)) = d\hat{h}_f(x)$.

(d) *If K is a number field then $x \in \mathrm{PrePer}(f)$ if and only if $\hat{h}_f(x) = 0$.*

Here, $h(f)$ is the height of the polynomial f, see for example [Bombieri and Gubler 2006, §1.6] for the definition of $h(f)$.

Proof. See, for example, [Hindry and Silverman 2000, §B.2, §B.4] or [Silverman 2007, §3.4]. □

We use the following lemma (see also [Call and Silverman 1993; Ingram 2013] for more general techniques along these lines).

Lemma 6. *Let K be a global field. Let $(\lambda_n)_{n=1}^{\infty}$ be a sequence in $\overline{K}$ satisfying $f^{\circ n}(\lambda_n) = c(\lambda_n)$ for all n, where $f, c \in K[x]$ and $\deg f > 1$. Then*

$$\lim_{n\to\infty} \hat{h}_f(\lambda_n) = 0.$$

Proof. By Proposition 5 (b), the canonical height $\hat{h}_f(\cdot)$ associated to f is a height function on the projective line $\mathbb{P}^1$. It follows that

$$\hat{h}_f(c(\lambda)) = (\deg c)\hat{h}_f(\lambda) + O(1), \quad \text{for all } \lambda \in \overline{K}. \tag{6.1}$$

Since by assumption the sequence $(\lambda_n)_{n=1}^{\infty}$ satisfies $f^{\circ n}(\lambda_n) = c(\lambda_n)$ for all n, we have that $(\deg f)^n \hat{h}_f(\lambda_n) = \hat{h}_f(f^{\circ n}(\lambda_n)) = \hat{h}_f(c(\lambda_n))$ and thus

$$(\deg f)^n \hat{h}_f(\lambda_n) = (\deg c)\hat{h}_f(\lambda_n) + O(1), \quad \text{for all } n \in \mathbb{N}, \tag{6.2}$$

where the implied constant is independent of n.

Therefore, $((\deg f)^n - \deg c)\hat{h}_f(\lambda_n)$ is bounded by a constant independent of n. Since by assumption $\deg f > 1$, it's clear that $\hat{h}_f(\lambda_n)$ must go to zero as n goes to infinity. □

We now state a result about equalities of canonical heights.

Proposition 7. *Let K be a global field of characteristic zero and let $f, g \in K[x]$ be polynomials of degree greater than one. If there is an infinite nonrepeating sequence $(\lambda_i)_{i=1}^{\infty}$, where $\lambda_i \in \overline{K}$, such that*

$$\lim_{i\to\infty} \hat{h}_f(\lambda_i) = \lim_{i\to\infty} \hat{h}_g(\lambda_i) = 0,$$

then $\hat{h}_f = \hat{h}_g$.

Proof. In the case where K is a number field, this is proved in [Petsche et al. 2012, Theorem 3] and [Mimar 2013, Theorem 1.8]. The proof given in [Petsche et al. 2012] goes through for function fields without any changes. Proofs of similar equalities over function fields appear in [Baker and DeMarco 2011; 2013; Ghioca et al. 2011; 2015; Yuan and Zhang 2017], Thus, we only give a sketch here. The idea is to apply equidistribution results such as those in [Favre and Rivera-Letelier 2004; Baker and Rumely 2006; Chambert-Loir 2006], all of which hold over both number fields and function fields of characteristic 0. For each place v of K, the λ_i equidistribute with respect to the measures of maximal entropy $\mu_{f,v}$ and $\mu_{g,v}$ for f and g respectively at v. This implies that the local canonical heights $\hat{h}_{f,v}$ and $\hat{h}_{g,v}$ for f and g are equal to each other. By (4.1), the global canonical heights $\hat{h}_f$ and $\hat{h}_g$ are the sum of the corresponding local canonical heights. Therefore, $\hat{h}_f = \hat{h}_g$, as desired. □

2. Proof of Theorem 1

In this section we prove Theorem 1 by first treating the case where f and g both have degree greater than one.

Proposition 8. *Let $f(x)$ and $g(x)$ be two compositionally independent polynomials with complex coefficients of degree greater than one. Then there are at most finitely many $\lambda \in \mathbb{C}$ such that there are positive integers m and n with the following properties*:

(i) $f^{\circ m}(x) \neq c(x)$.

(ii) $g^{\circ n}(x) \neq c(x)$.

(iii) $(x-\lambda) \mid \gcd(f^{\circ m}(x) - c(x), g^{\circ n}(x) - c(x))$.

Proof. Let K be the field generated by all the coefficients of f, g, and c over $\mathbb{Q}$. Then either K is a number field or a function field of finite transcendence degree over $\overline{\mathbb{Q}}$. In the latter case, we let $k = K \cap \overline{\mathbb{Q}}$ be its field of constants.

We prove the proposition by contradiction. Suppose that there is an infinite nonrepeating sequence $(\lambda_i)_{i=1}^{\infty}$ such for every i, there is an m_i and n_i such that $f^{\circ m_i} \neq c$ and $g^{\circ n_i} \neq c$, and $(x-\lambda_i)$ divides both $f^{\circ m_i}(x) - c(x)$ and $g^{\circ n_i}(x) - c(x)$. We will show that the two polynomials f and g must be compositionally dependent.

Observe that for such m_i and n_i, the polynomials $f^{\circ m_i}(x)-c(x)$ and $g^{\circ n_i}(x)-c(x)$ have only finitely many roots, so m_i and n_i must both go to infinity as i goes to infinity. Then, by Lemma 6, we have

$$\lim_{i\to\infty} \hat{h}_f(\lambda_i) = \lim_{i\to\infty} \hat{h}_g(\lambda_i) = 0.$$

It follows from Proposition 7 that $\hat{h}_f = \hat{h}_g$.

Let $\Lambda_0 := \{\lambda \in \overline{K} \mid \hat{h}_f(\lambda) = 0\} = \{\lambda \in \overline{K} \mid \hat{h}_g(\lambda) = 0\}$. If K is a number field, then by Proposition 5 (d), we immediately conclude that f and g share the same set of preperiodic point. Likewise, if K is a function field and neither f nor g is isotrivial over k, then by [Benedetto 2005; Baker 2009], Proposition 5 (d) also holds and hence f and g also share the same set of preperiodic points.

Now assume that at least one of f and g is isotrivial. Without loss of generality, we assume that f is isotrivial. Since $\hat{h}_f = \hat{h}_g$, it follows from the weak Northcott property of [Baker 2009] that g is also isotrivial. Here, we provide an elementary proof of this fact as follows. Since f is isotrivial, there exists a linear polynomial $\sigma \in \overline{K}[x]$ such that $f^\sigma = \sigma \circ f \circ \sigma^{-1} \in \bar{k}[x]$. Then, the canonical height $\hat{h}_{f^\sigma}(x)$ associated to f^σ is equal to the Weil height $h(x)$ of $x \in \overline{K}$. On the other hand,

$$\begin{aligned}\hat{h}_{f^\sigma}(\sigma(x)) &= \lim_{n\to\infty} \frac{h((f^\sigma)^{\circ n}(\sigma x))}{d^n} = \lim_{n\to\infty} \frac{h(\sigma \circ f^{\circ n}(x))}{d^n}\\ &= \lim_{n\to\infty} \frac{h(f^{\circ n}(x))}{d^n} = \hat{h}_f(x).\end{aligned}$$

Thus, $\hat{h}_f(x) = 0$ if and only if $h(\sigma x) = \hat{h}_{f^\sigma}(\sigma x) = 0$. In other words, we have $\sigma(\Lambda_0) = \bar{k} = \overline{\mathbb{Q}}$. Note that $g^\sigma : \sigma(\Lambda_0) \to \sigma(\Lambda_0)$ (since $g : \Lambda_0 \to \Lambda_0$). We see that $g^\sigma(\alpha) \in \overline{\mathbb{Q}}$ for $\alpha \in \overline{\mathbb{Q}}$. It follows that $g^\sigma \in \overline{\mathbb{Q}}[x]$ as well. Then after conjugating by σ, we assume that both f and g are defined over $\overline{\mathbb{Q}}$. Note that since each λ_i is a solution to $f^{m_i}(\lambda_i) = g^{n_i}(\lambda_i)$, each λ_i must be in $\overline{\mathbb{Q}}$. Since $c(\lambda_i)$ is thus in $\overline{\mathbb{Q}}$ for each λ_i, and there are infinitely many λ_i, it follows that $c \in \overline{\mathbb{Q}}[x]$ as well.

We have reduced to the case where K is a number field, and we conclude that the set of preperiodic points of f and g are the same. This means that the Julia set $\mathcal{J}_f$ and $\mathcal{J}_g$ are equal. By [Baker and Erëmenko 1987; Schmidt and Steinmetz 1995], it follows that unless f and g are both conjugate to a multiple of a Chebychev polynomial or a multiple of powering map, then there is a polynomial q and a finite (compositional) order linear map τ such that any word in f and g is equal to $\tau^{\circ i} q^{\circ j}$ for some i, j. This means that f and g must be compositionally dependent.

Now, we are left with the case where f and g are both conjugate to either a multiple of a Chebychev polynomial or a multiple of a powering map. If f and g are conjugate to $\pm T_{d_1}$ and $\pm T_{d_2}$, respectively, where T_{d_i} is the monic Chebychev polynomial of degree d_i, then f and g are compositionally dependent (easy to check). If f and g are both conjugate to powering maps, then after conjugation we may write $f(x) = x^{d_1}$ and $g(x) = \gamma x^{d_2}$ for some $\gamma \in \overline{\mathbb{Q}}$. Note that both f and g have the same set of preperiodic points which are all the roots of unity in this case. In particular, $\gamma = g(1)$ is a root of unity. Therefore f and g must be compositionally dependent as well. □

Next, we treat the case where exactly one of f and g is linear.

Proposition 9. *Let $f(x)$ and $g(x)$ be two polynomials of $\mathbb{C}[x]$ such that* $\deg f > 1$ *and* $\deg g = 1$. *Then there are at most finitely many $\lambda \in \mathbb{C}$ such that there are positive integers m and n with the following properties*:

(i) $f^{\circ m} \neq c(x)$.

(ii) $g^{\circ n} \neq c(x)$.

(iii) $(x - \lambda) \mid \gcd(f^{\circ m}(x) - c(x), g^{\circ n}(x) - c(x))$.

Proof. Let K be the field generated by the coefficients of f, g, and c. Since $g^{\circ n}(x) - c(x)$ is a polynomial of degree at most $\deg c + 1$, we see that every λ such that $g^{\circ n}(\lambda) - c(\lambda) = 0$ has degree at most $\deg c + 1$ over K. Note that for any nonrepeating infinite sequences $(\lambda_i)_{i=1}^{\infty}$ and $(n_i)_{i=1}^{\infty}$ such that $f^{\circ n_i}(\lambda_i) = c(\lambda_i)$ for all i, we have $\lim_{i\to\infty} \hat{h}_f(\lambda_i) = 0$ by Lemma 6. If K is a number field, then by the Northcott property we conclude that there are at most finitely many λ that satisfy properties (i) to (iii) given above. Hence, the proposition holds in this case.

Now, let's assume that K is a function field and that there is a nonrepeating infinite sequences $(\lambda_i)_{i=1}^{\infty}$ and $(n_i)_{i=1}^{\infty}$ such that $f^{\circ n_i}(\lambda_i) = c(\lambda_i)$ for all $i \in \mathbb{N}$. We note that as in the proof of Proposition 8, both m_i and n_i must go to infinity since $c(x)$ is not a compositional power of f or g.

By [Baker 2009], if there is an infinite sequence of $(\lambda_i)_{i=1}^{\infty}$ of bounded degree with $\hat{h}_f(\lambda_i) = 0$ then f must be isotrivial. Thus, after changing variables, we may assume that $f \in k[x]$ for some number field k. As a consequence, $\hat{h}_f(x) = h(x)$ the Weil height of x for all $x \in \overline{K}$. On the other hand, it follows from the definition of the Weil height that for $x \in \overline{K}$ with $h(x) > 0$ we must have $h(x) \geq 1/(\deg x)$. Now the sequence $(\lambda_i)_{i=1}^{\infty}$ has the property that all λ_i have degree bounded above by $\deg c + 1$ over K and that $\lim_{i\to\infty} h(\lambda_i) = 0$. Therefore we must have $h(\lambda_i) = 0$ for all but finitely many i. Also note that for $x \in \overline{K}$ we have $h(x) = 0$ if and only if $x \in \bar{k} = \overline{\mathbb{Q}}$. So, all but finitely many λ_i in the sequence $(\lambda_i)_{i=1}^{\infty}$ must be in $\overline{\mathbb{Q}}$.

We are left to treat the case where there are infinitely many λ in $\overline{\mathbb{Q}}$ such that $f^{\circ m}(\lambda) = c(\lambda) = g^{\circ n}(\lambda)$. We see in this case that c must have coefficients in $\overline{\mathbb{Q}}$ since there are infinitely many $\lambda \in \overline{\mathbb{Q}}$ such that $c(\lambda) \in \overline{\mathbb{Q}}$. Let k be the field generated by the coefficients of f and c over $\mathbb{Q}$, and let $g(x) = \alpha x + \beta$. Then all λ such that $f^{\circ m}(\lambda) = c(\lambda) = g^{\circ n}(\lambda)$ lie in extensions of $\overline{\mathbb{Q}} \cap k(\alpha, \beta)$ having degree at most $\deg c + 1$. Since $\overline{\mathbb{Q}} \cap k(\alpha, \beta)$ is a finitely generated extension of k, all such λ have bounded degree over $\mathbb{Q}$. Since the λ also have bounded height, again we have a contradiction by Northcott's theorem. $\square$

Proof of Theorem 1. If $\deg f, \deg g > 1$, then Theorem 1 follows immediately from Proposition 8. If $\max(\deg f, \deg g) > 1$ and $\min(\deg f, \deg g) = 1$, then we may assume without loss of generality that $\deg f > 1$ and $\deg g = 1$. Theorem 1 then follows from Proposition 9. $\square$

3. Proof of Theorem 2

When f and g are both linear, there may be infinitely many λ such that $(x-\lambda)$ divides $\gcd(f^{\circ m}(x)-c(x), g^{\circ n}(x)-c(x))$ for some m and n. Take for example, $c(x)=x^2$, with $f(x)=2x$ and $g(x)=x+1$. Then

$$f^{\circ n}(x)-c(x)=2^n x - x^2 = -x(x-2^n)$$

while if $m=2^n(2^n-1)$, then

$$g^{\circ m}(x)-c(x)=x+2^n(2^n-1)-x^2=-(x+2^n-1)(x-2^n),$$

so clearly there are infinitely many λ such that

$$(x-\lambda) \mid \gcd(f^{\circ m}(x)-c(x), g^{\circ n}(x)-c(x)),$$

for some positive integers m and n. On the other hand, if we restrict to the case where $m=n$, then we may obtain a suitable finiteness result.

The techniques in this section are mostly from diophantine geometry. We use these to prove Proposition 15 which treats the case where the coefficients of f, g, and c are algebraic. We then derive Theorem 2 using some simple specialization arguments. Theorem 3 then follows from Theorem 2 and Propositions 8 and 9.

3.1. ***Results from diophantine geometry.*** We will use the following version of Roth's Theorem (see [Lang 1983, Chapter 7, Theorem 1.1 and Remark (v)]).

Theorem 10. *Let k be a number field, let $\alpha_1, \dots, \alpha_n$ be distinct points in k, and let S be a finite set of places of k. Then for any $\epsilon > 0$, there are at most finitely many $\beta \in k$ such that*

$$\frac{1}{[k:\mathbb{Q}]}\left(\sum_{v\in S}\sum_{i=1}^{n} -\min(\log\|\alpha_i-\beta\|_v, 0)+\sum_{v\in S}\max(\log\|\beta\|_v, 0)\right) \geq (2+\epsilon)h(\beta) \quad (10.1)$$

The following is Siegel's well-known theorem on the set of integral points of curves of genus zero, which can be derived from Theorem 10 without difficulty. We refer the reader to [Lang 1983, Chapter 8, Theorem 5.1] for a proof.

Theorem 11. *Let k be a number field. Let C be a complete nonsingular curve of genus* 0, *defined over k, let S be a finite set of places of k containing all the archimedean places, and let ϕ be a nonconstant function in $k(C)$ with at least three distinct poles. Then there are at most finitely many $Q \in C(k)$ such that $\phi(Q)$ is an S-integer.*

As a corollary to Theorem 11, we have the following, which we will use to treat the case where the coefficients of the linear terms of f and g are multiplicatively dependent.

Proposition 12. *Let W be a one-dimensional subtorus in $\mathbb{G}_m^2$ defined over a number field k and let S be a finite set of places of k containing all the archimedean places. Let $\Phi(X, Y) = P(X, Y)/Q(X, Y)$ where $P, Q \in k[X, Y]$ are two relatively prime polynomials neither of which is divisible by X or Y. Assume that Φ restricts to a nonconstant rational function ϕ on W with at least a pole in $W(\bar{k})$. Let Γ be a finitely generated subgroup of $W(k)$. Then, there are at most finitely many points $Q \in \Gamma$ such that $\phi(Q)$ is an S-integer.*

Proof. Here, as usual, we consider $\mathbb{G}_m^2$ to be the open subset of $\mathbb{P}^2$ with coordinates $[x : y : z]$ defined by $x \neq 0$, $y \neq 0$, $z \neq 0$. The functions X and Y are equal to x/z and y/z with respect to these coordinates. By making a finite extension of k, we assume that the poles of ϕ are all k-rational points of W. Moreover, because Γ is finitely generated, we may assume, possibly after extending S to a larger finite set of places, that the coordinates of all of the elements of Γ and all of poles of ϕ are S-units. Let Γ^* be the union of Γ and the set of poles of ϕ.

Now, we fix a positive integer $m > 3$ and let $\mu_m : \mathbb{G}_m^2 \to \mathbb{G}_m^2$ be the m-th powering map. Namely, $\mu_m(X, Y) = (X^m, Y^m)$ for all $(X, Y) \in \mathbb{G}_m^2$. By Kummer theory, there exists a finite extension L over k such that the inverse image $\mu_m^{-1}(\Gamma^*)$ of Γ^* is contained in $W(L)$. Let S' denote the set of places of L that extend the places in S.

As $\mu_m : W \to W$ is an unramified map of degree m we see that the function $\phi_m := \phi \circ \mu_m$ is a rational function with at least m distinct poles on W. The subtorus W is viewed as an affine curve in the projective plane $\mathbb{P}_k^2$ and we denote its Zariski closure in $\mathbb{P}^2$ by $\overline{W}$. Note that ϕ_m extends to a rational function on $\overline{W}$ which we still denote by ϕ_m. Let $\pi : \widetilde{W} \to \overline{W}$ denote the normalization of $\overline{W}$. Then, $\widetilde{W}$ is a projective smooth curve of genus 0. Furthermore, the function $\psi_m := \phi_m \circ \pi$ is a rational function on $\widetilde{W}$ with at least m distinct poles. On the other hand, the set of L-rational points $W(L)$ lift to the set $\widetilde{W}(L)$.

Observe that for any point $Q \in \Gamma$ such that $\phi(Q)$ is an S-integer, then $\psi_m(Q')$ is an S'-integer where $Q' \in \widetilde{W}(L)$ is any point such that $(\mu_m \circ \pi)(Q') = Q$. On the other hand, since $m \geq 3$, there are at most finitely many $Q' \in \widetilde{W}(L)$ such that $\psi_m(Q')$ is an S'-integer by Theorem 11. Thus, there are at most finitely many Q such that $\phi(Q)$ is an S-integer. $\square$

We will use the following lemma, due originally to Siegel [2014]. We provide a proof in modern language for the sake of completeness.

Lemma 13. *Let w be an element of a number field k, let y be a nonzero element of k, and let S be a finite set of places of k including all the archimedean places. Let $\epsilon > 0$. Then*

$$\frac{1}{[k:\mathbb{Q}]}\sum_{v\notin S} -\min(\log\|w^n - y\|_v, 0) \geq (1-\epsilon)nh(w), \tag{13.1}$$

for all sufficiently large n.

Proof. We may assume that S contains all the places v of k such that $\|w\|_v \neq 1$. Then applying Theorem 10, to the points 0 and y, we see that for any $\epsilon > 0$, we have

$$\frac{1}{[k:\mathbb{Q}]}\sum_{v\in S}(-\min(\log\|w^n - y\|_v, 0) - \min(\log\|w^n\|_v, 0) + \max(\log\|w^n\|_v, 0)) \leq (2+\epsilon)nh(w) + O(1).$$

Since S contains all places such that $\|w\| \neq 1$, we have

$$\frac{1}{[k:\mathbb{Q}]}\sum_{v\in S}(-\min(\log\|w^n\|_v, 0) + \max(\log\|w^n\|_v, 0)) = 2nh(w).$$

Thus,

$$\frac{1}{[k:\mathbb{Q}]}\sum_{v\in S} -\min(\log\|w^n - y\|_v, 0) \leq \epsilon nh(w) + O(1). \tag{13.2}$$

Since

$$nh(w) \leq \frac{1}{[k:\mathbb{Q}]}\sum_{v\in \Omega_k} -\min(\log\|w^n - y\|_v, 0) + O(1),$$

we see that (13.1) must hold. □

The following lemma will be used to treat the case where the coefficients of the linear terms of f and g are multiplicatively independent.

Lemma 14. *Let w_1 and w_2 be two multiplicatively independent elements of a number field k, neither of which is a root of unity, and let y be a nonzero element of k. Let S be a finite set of places of k including all the archimedean places. Then for all sufficiently large n, there is a $v \notin S$ such that $|w_1^n - y|_v < |w_2^n - y|_v \leq 1$.*

Proof. We begin by showing that if w_1 and w_2 are multiplicatively independent, then w_1^n/y and w_2^n/y are multiplicatively independent for all but at most finitely many n. Note that if y is not in the multiplicative group generated by w_1 and w_2, then w_1^n/y and w_2^n/y are multiplicatively independent for all n. Otherwise, we have $y^{\ell_1} = w_1^{\ell_2} w_2^{\ell_3}$ for some integer $\ell_1 > 0$ and some integers ℓ_2 and ℓ_3. Since it suffices to prove our lemma for ℓ_1-th roots of w_1 and w_2 we may assume that we have $y = w_1^i w_2^j$ for some integers i and j. Now, if $w_1^n/(w_1^i w_2^j)$ and $w_2^n/(w_1^i w_2^j)$ are multiplicatively dependent, then we must have $(n-i)(n-j) = (-i)(-j)$, since w_1 and w_2 are multiplicatively independent. For all sufficiently large n, we clearly have $(n-i)(n-j) > (-i)(-j)$, so we are done.

By Theorem 1 and equation (1.2) of [Corvaja and Zannier 2005], we see that for any $\epsilon > 0$, there is a constant C_ϵ such that

$$\frac{1}{[k:\mathbb{Q}]} \sum_{v \in \Omega_k} -\log^- \max(\|w_1^n - y\|_v, \|w_2^n - y\|_v) < \epsilon n h(w_1) + C_\epsilon, \qquad (14.1)$$

where $\log^-(\cdot) = \min(0, \log(\cdot))$. We may enlarge S to include the place v where $|w_1|_v > 1$ or $|y|_v > 1$. Suppose that for a positive integer n, inequalities $|w_1^n - y|_v \geq |w_2^n - y|_v$ hold for all $v \notin S$. Then, from (14.1) we have that

$$\begin{aligned} \epsilon n h(w_1) + C_\epsilon &\geq \frac{1}{[k:\mathbb{Q}]} \sum_{v \in \Omega_k} (-\min(0, \max\{\log\|w_1^n - y\|_v, \log\|w_2^n - y\|_v\}) \\ &\geq \frac{1}{[k:\mathbb{Q}]} \sum_{v \notin S} -\min(0, \log\|w_1^n - y\|_v) \\ &\geq (1-\epsilon) n h(w_1), \end{aligned}$$

where the last inequality follows from (13.1). Taking $\epsilon = \frac{1}{3}$, we see that there are only finitely many positive integers n such that the above inequality holds. Hence, for all sufficiently large n there is a $v \notin S$ such that $|w_1^n - y|_v < |w_2^n - y|_v \leq 1$, as desired. □

3.2. *Proofs of Theorems 2 and 3.* We are now ready to treat the case where f and g are linear polynomials, and f, g, and c all have algebraic coefficients. The proof breaks into several cases. The first case is when c is constant; this case is already treated in [Ghioca et al. 2008]. The idea in all of the other cases is the same: to force certain quantities coming from any solutions to $f^{\circ n}(x) = c(x) = g^{\circ n}(x)$ to have poles outside a finite set and then derive contradictions from the existence of these poles to show that there are no solutions to $f^{\circ n}(x) = c(x) = g^{\circ n}(x)$ when n is sufficiently large.

Proposition 15. *Let $f(x) = \alpha x$ and $g(x) = \beta x + \gamma$ where α, β, and γ are nonzero algebraic numbers such that α is not a root of unity, $\alpha\beta$ is not a root of unity, β is not a root of unity other than* 1, *and $\gamma \neq 0$. Let $c(x)$ be any polynomial with coefficients in $\overline{\mathbb{Q}}$. Then for all but at most finitely many n, we have*

$$\gcd(f^{\circ n}(x) - c(x), g^{\circ n}(x) - c(x)) = 1. \qquad (15.1)$$

Proof. Suppose that there are infinitely many n such that (15.1) does not hold. Let n be an integer such that $\gcd(f^{\circ n}(x) - c(x), g^{\circ n}(x) - c(x)) \neq 1$. Then there exists a $\lambda_n \in \overline{\mathbb{Q}}$ such that

$$(x - \lambda_n) \mid \gcd(f^{\circ n}(x) - c(x), g^{\circ n}(x) - c(x))$$

and thus, $f^{\circ n}(\lambda_n) = c(\lambda_n) = g^{\circ n}(\lambda_n)$.

In the following, we break the proof into four cases and show a contradiction in each case.

Case I. Suppose that c is a constant. Let θ be the compositional inverse of f and let τ be the compositional inverse of g. We observe that if $f^{\circ n}(\lambda) = g^{\circ n}(\lambda) = c$ then $\theta^{\circ n}(c) = \tau^{\circ n}(c)$. By [Ghioca et al. 2008, Proposition 5.4], this implies that either θ and τ have a common iterate or that c is periodic under both θ and τ. Since $\theta = \alpha^{-1}x$, we see that zero is the only periodic point of θ. Since $\tau = x/\beta - \gamma/\beta$, we see that the constant term of $\tau^{\circ n}$ is always nonzero, so 0 cannot be a periodic point of τ. Thus, there is an n such that $\theta^{\circ n} = \tau^{\circ n}$, which means that f and g have a common iterate. Since the constant term of $g^{\circ n}$ is nonzero for all n, we see that f and g cannot have a common iterate, which gives a contradiction.

In the following, we assume that $\deg c \geq 1$.

Case II. Assume that $\beta = 1$. Then

$$\lambda_n = \frac{n\gamma}{\alpha^n - 1}.$$

Let S be the set of places v that are archimedean or where α, γ, or a coefficient of c has v-adic absolute value not equal to 1. Assume that λ_n is an S-integer. Then,

$$\begin{aligned}
h(\lambda_n) &= \frac{1}{[K:\mathbb{Q}]} \sum_{v\in S} \max\left(0, \log \left\| \frac{n\gamma}{\alpha^n - 1} \right\|_v\right) \\
&\leq \frac{1}{[K:\mathbb{Q}]} \sum_{v\in S} \left\{ \max\left(0, \log \left\| \frac{1}{\alpha^n - 1} \right\|_v\right) + \max(0, \log\|n\gamma\|_v) \right\} \\
&= \frac{1}{[K:\mathbb{Q}]} \sum_{v\in S} \max\left(0, \log \left\| \frac{1}{\alpha^n - 1} \right\|_v\right) + h(n\gamma) \\
&\leq \frac{1}{[K:\mathbb{Q}]} \sum_{v\in S} \max\left(0, \log \left\| \frac{1}{\alpha^n - 1} \right\|_v\right) + \log n + O(1). \qquad (15.2)
\end{aligned}$$

Let $\epsilon > 0$ be given. By (13.2), there exists a constant C_ϵ such that

$$\frac{1}{[K:\mathbb{Q}]} \sum_{v\in S} \max\left(0, \log \left\| \frac{1}{\alpha^n - 1} \right\|_v\right) \leq \epsilon n h(\alpha) + C_\epsilon. \qquad (15.3)$$

On the other hand, there is a constant $D = D(\gamma)$ such that

$$h(\lambda_n) = h\left(\frac{n\gamma}{\alpha^n - 1}\right) \geq nh(\alpha) - h(n) - D = nh(\alpha) - \log n - D.$$

Fixing a positive $\epsilon < 1$ and combing (15.2) with (15.3), we see that λ_n cannot be an S-integer if n is large enough. Therefore, for n large there exists a place

v outside of S such that $|\lambda_n|_v > 1$. If $\deg c > 1$, then $|c(\lambda)|_v = |\lambda_v|^{\deg c}$ but $|f^{\circ n}(\lambda_n)| = |\alpha^n \lambda_n|_v = |\lambda_n|_v$. This gives a contradiction.

If $\deg c = 1$, then we write $c(x) = tx + u$ and note that since $f^{\circ n}(\lambda_n) = g^{\circ n}(\lambda_n) = c(\lambda_n)$, we must have

$$\lambda_n = \frac{u - n\gamma}{1 - t} = \frac{u}{\alpha^n - t}.$$

If $u \neq 0$ and n is large, then by enlarging S to contain the places v where $|1-t|_v \neq 1$, then $(u - n\gamma)/(1 - t)$ is an S-integer for all n. On the other hand, by taking $\Phi(X, Y) = u/(X - t)$ in Proposition 12, we see that $u/(\alpha^n - t)$ cannot be an S-integer for n sufficiently large. This gives a contradiction. If $u = 0$, then we have $\lambda_n = \alpha^n \lambda_n = t\lambda_n = g^{\circ n}(\lambda_n)$, which has no solutions when $\alpha^n \neq t$, and thus has a solution for at most one n, since α is not a root of unity. Thus the proof of this case is complete.

We assume in the following that $\beta \neq 1$. Note that when $\alpha^n = \beta^n$, there is no solution to $f^{\circ n}(x) = g^{\circ n}(x)$ and that when $\alpha^n \neq \beta^n$, the unique solution to $f^{\circ n}(x) = c(x) = g^{\circ n}(x)$ is given by

$$\lambda_n = \frac{(\beta^n - 1)\gamma}{(\beta - 1)(\alpha^n - \beta^n)}. \tag{15.4}$$

Case III. Suppose that α and β are multiplicatively dependent. Then, the point $P = (\alpha, \beta)$ is in a one-dimensional subtorus W of $\mathbb{G}_m^2$. Let S be the set of places v that are archimedean or where α, γ, $\beta - 1$, or a coefficient of c has v-adic absolute value not equal to 1. Then, by taking $\Phi(X, Y) = (Y - 1)/(X - Y)$ and Γ to be the group generated by P in Proposition 12, we see that for all sufficient large n there exists a place v outside of S such that

$$\left| \frac{\beta^n - 1}{\alpha^n - \beta^n} \right|_v > 1.$$

It follows that for such v we have $|\lambda_n|_v > 1$. Observe that on the one hand, $|f^{\circ n}(\lambda_n)|_v = |\alpha^n \lambda_n|_v = |\lambda_n|_v$ while on the other hand, we have $|f^{\circ n}(\lambda_n)|_v = |c(\lambda_n)|_v = |\lambda_n|_v^{\deg c}$. This gives a contradiction if $\deg c > 1$.

If $\deg c = 1$, we write $c(x) = tx + u$, $t \neq 0$. If $f^{\circ n}(\lambda_n) = c(\lambda_n) = g^{\circ n}(\lambda_n)$ then we have

$$\lambda_n = \frac{u - \gamma \frac{\beta^n - 1}{\beta - 1}}{\beta^n - t} = \frac{u}{\alpha^n - t}. \tag{15.5}$$

From this we deduce that

$$u\left(\frac{\beta^n - t}{\alpha^n - t}\right) = u - \left(\frac{\gamma}{\beta - 1}\right)(\beta^n - 1). \tag{15.6}$$

Note that the right-hand side of (15.6) is an S-integer. However, by taking $\Phi(X, Y) = (Y - t)/(X - t)$ in Proposition 12 we conclude that for n large enough the left-hand side of (15.6) is not an S-integer. This leads to a contradiction and completes the proof in this case.

Case IV. Suppose that α and β are multiplicatively independent. Let S be the set of places v that are archimedean or where α, γ, or a coefficient of c has v-adic absolute value not equal to 1.

Suppose that $\deg c > 1$. Then, applying Lemma 14 to $\beta^n - 1$ and $(\alpha/\beta)^n - 1$, we see that there is a place v outside of S such that $|\lambda_n|_v > 1$. Again, if $\deg c > 1$, this gives a contradiction since $|c(\lambda)|_v = |\lambda_v|^{\deg c}$ but $|f^{\circ n}(\lambda_n)| = |\alpha^n \lambda_n|_v = |\lambda_n|_v$.

Now suppose that $\deg c = 1$. Again, we write $c(x) = tx + u$. Then we also have

$$\lambda_n = \frac{u - \gamma \frac{\beta^n - 1}{\beta - 1}}{\beta^n - t} = \frac{u}{\alpha^n - t}. \tag{15.7}$$

This is equivalent to

$$1 - \frac{\gamma(\beta^n - 1)}{u(\beta - 1)} = \frac{\beta^n - t}{\alpha^n - t}. \tag{15.8}$$

We enlarge S to include all the places such that u or $\beta - 1$ are S-unit. Then applying Lemma 14, we see that for all sufficiently large n, there is a place $v \notin S$ such that $|\alpha^n - t|_v < |\beta^n - t|_v \leq 1$. For this v, we see that the left-hand side of (15.8) is a v-adic integer while the right-hand side is not. Therefore, (15.7) cannot hold for n sufficiently large. $\square$

Remark. To see that Proposition 15 does not hold in general if $\alpha\beta$ is a root of unity, consider the case where $f(x) = x/2$, $g(x) = 2x + 1$ and $c(x) = -(x + 1)$. Then for any n, the common root of $f^{\circ n}$ and $g^{\circ n}$ is

$$\frac{2^n - 1}{2^{-n} - 2^n} = -2^n \frac{2^n - 1}{2^{2n} - 1} = \frac{-2^n}{2^n + 1}.$$

while the common root of $f^{\circ n}$ and $c(x)$ is

$$\frac{-1}{\left(\frac{1}{2}\right)^n + 1} = \frac{-2^n}{2^n + 1}.$$

Thus, for every positive integer n, there is a λ_n such that

$$f^{\circ n}(\lambda_n) - c(\lambda_n) = g^{\circ n}(\lambda_n) - c(\lambda_n) = 0.$$

We can now prove Theorem 2 by specializing from $\mathbb{C}$ to a number field.

Proof of Theorem 2. First we note that any nonconstant affine map $x \mapsto ax + b$ has a fixed point unless $a = 1$. Any two monic linear polynomial must commute with each other. Thus, we may assume that at least one of f and g has a fixed point. Without loss of generality, we may assume that f has a fixed point. After a possible change of coordinates, we may then write $f(x) = \alpha x$ and $g(x) = \beta x + \gamma$.

If α is a root of unity, then f and g are not compositionally independent since f itself has finite order, so α must not be a root of unity. Similarly, if β is a root of unity other than one, then g has finite order so that f and g are not compositionally independent either. We may therefore assume that β is not a root of unity other than one. Finally, we see that if there are integers i and j such that $\alpha^i\beta^j = 1$, then the linear terms in $f^{\circ i}g^{\circ j}$ and $g^{\circ j}f^{\circ i}$ are both 1, which means that $f^{\circ i}g^{\circ j}$ and $g^{\circ j}f^{\circ i}$ commute. This would imply f and g are not compositionally dependent, so we may assume that there are no positive integer i and j such that $\alpha^i\beta^j = 1$.

As in the proof of Proposition 15, we assume that there are infinitely many n such that (15.1) does not hold. Let K be the field generated by α, β, and γ over $\mathbb{Q}$, and let R be the ring generated over $\mathbb{Z}$ by α, β, γ, and the coefficients of c. Observe that any solution λ_n to $f^{\circ n}(\lambda_n) = g^{\circ n}(\lambda_n) = c(\lambda_n)$ must lie in K. By our assumption, there are infinitely many such n, so c takes infinitely many values in K to other values in K so $c \in K[x]$. Hence, we may assume that $c \in K[x]$.

If α, β, and γ are in $\overline{\mathbb{Q}}$, then we are done by Proposition 15. If K has positive transcendence degree over $\overline{\mathbb{Q}}$, then there exists a specialization map t from R to $\overline{\mathbb{Q}}$ such that $\gamma_t \neq 0$ and α_t, β_t, $\alpha_t\beta_t$, and α_t/β_t are not roots of unity. We may prove this, for example, by induction on the transcendence degree of $\mathbb{Q}(\alpha, \beta, \gamma)$. If the transcendence degree is 0, there is nothing to prove. If it is n, take a subfield L of transcendence degree of $n-1$ in K. Then, by [Call and Silverman 1993, Theorem 4.1], for all specializations s from R to $\bar{L}$ of sufficiently large height, we have that $\gamma_s \neq 0$ and that α_s, β_s, $\alpha_s\beta_s$, and α_s/β_s are not roots of unity. We then apply the inductive hypothesis on the transcendence degree to $\mathbb{Q}(\alpha_s, \beta_s, \gamma_s)$.

Let $f_t = \alpha_t x$, $g_t = \beta_t x + \gamma_t$, and c_t be the polynomial obtained by specializing all the coefficient of c at t. Now, if $\gcd(f^{\circ n}(x) - c(x), g^{\circ n}(x) - c(x)) \neq 1$, then $\gcd(f_t^{\circ n}(x) - c_t(x), g_t^{\circ n}(x) - c_t(x)) \neq 1$. But there are at most finitely many n such that $\gcd(f_t^{\circ n}(x) - c_t(x), g_t^{\circ n}(x) - c_t(x)) \neq 1$, by Proposition 15, which gives a contradiction, and finishes our proof. □

Remark. We note that by Proposition 15, the condition needed for Theorem 2 is weaker than compositional dependency, since Proposition 15 holds unless the linear term of $f \circ g$ is a root of unity. Mike Zieve has shown us that something similar is true for polynomials of higher degree, namely that the sorts of compositional dependencies that may arise all take a specific form.

We now prove Theorem 3.

Proof of Theorem 3. The case where f and g are both linear is covered by Theorem 2, so we may assume that either both f and g are nonlinear or that g is linear and f is not.

By Propositions 8 and 9, there are at most finitely many λ such that $(x-\lambda)$ divides $\gcd(f^{\circ n}(x) - c(x), g^{\circ n}(x) - c(x))$ for some n such that $f^{\circ n} \neq c$ and $g^{\circ n} \neq c$. Let

$\mathcal{S}$ denote the set of such λ. Since f and g are compositionally independent, there is at most one N such that $f^{\circ N} = c$ or $g^{\circ N} = c$ exclusively. If such an N exists, let $\mathcal{T}$ denote the set of λ such that $(x-\lambda)$ divides $\gcd(f^{\circ N}(x) - c(x), g^{\circ N}(x) - c(x))$. We observe that $\mathcal{T}$ must be finite since otherwise we would have $f^{\circ N} - c = 0 = g^{\circ N} - c$. However, this cannot happen because f and g are compositionally independent. Any λ such that $(x-\lambda)$ divides $\gcd(f^{\circ n}(x) - c(x), g^{\circ n}(x) - c(x))$ is in $\mathcal{S} \cup \mathcal{T}$, so our proof is complete $\square$

4. Proof of Theorem 4

Theorem 4 is now an easy consequence of the following lemma. To state the lemma, we introduce a small bit of new notation: for any nonzero polynomial $q(x)$ we let $v_\lambda(q)$ denote the largest positive integer e such that $(x-\lambda)^e$ divides q when $(x-\lambda) \mid q$ and let $v_\lambda(q) = 0$ if $(x-\lambda)$ does not divide q.

Lemma 16. *Let q be a polynomial in $\mathbb{C}[x]$ of degree greater than one and let $c(x) \in \mathbb{C}[x]$ be a polynomial that is not equal to a constant that is in a ramified cycle of f. Let $\lambda \in \mathbb{C}$. Then there is a constant $M_{\lambda,q}$ such that $v_\lambda(q^{\circ n}(x) - c(x)) \le M_{\lambda,q}$ for all n such that $q^{\circ n}(x) \ne c(x)$.*

Proof. We write $c(x) = \sum_{i=0}^{d_c} c_i (x-\lambda)^i$ as a polynomial in $(x-\lambda)$. If there are finitely many n such that $v_\lambda(q^{\circ n}(x) - c(x)) > 0$, then the proof is immediate. Thus, we assume that there are infinitely many n such that $v_\lambda(q^{\circ n}(x) - c(x)) > 0$. It follows that $q^{\circ n}(\lambda) = c_0$ for infinitely many n, so c_0 must be periodic under q. Let ℓ be the smallest positive integer such that $q^{\circ \ell}(\lambda) = c_0$ and let r be the smallest positive integer such that $q^{\circ r}(c_0) = c_0$. Then we see that $v_\lambda(q^{\circ n}(x) - c(x)) > 0$ if and only if n can be written as $\ell + kr$ for some k. We write $q^{\circ r}(x) = \sum_{i=0}^{d_r} a_i (x-c_0)^i$ and $q^{\circ \ell}(x) = \sum_{j=0}^{d_\ell} b_j (x-\lambda)^j$. Let e be the smallest positive integer such that $b_e \ne 0$.

Suppose now that $c(x) = c_0$ is a constant. By assumption, c_0 is not in a ramified cycle of q, thus $a_1 \ne 0$ in this case. Then by induction we find that

$$q^{\circ(\ell+rk)}(x) = c_0 + a_1^k b_e (x-\lambda)^e + \text{higher order terms in } (x-\lambda),$$

so $v_\lambda(q^{\circ(\ell+rk)}(x) - c) = e$ for all k.

Suppose now that $c(x)$ is not a constant. We may suppose that there are infinitely many n such that $v_\lambda(q^{\circ n}(x) - c(x)) > e$ since otherwise the lemma clearly holds. Note that it's possible that c_0 is in a ramified cycle of q. In any case, let u be the smallest integer such that $a_u \ne 0$.

We first assume that $u = 1$. Equivalently, c_0 is not in a ramified cycle of q. Then, we must have $a_1^k b_e = c_e$ for infinitely many k. Since $a_1 b_e \ne 0$, this means that a_1 must be a root of unity. Suppose that $a_1^s = 1$. Then we may write

$$q^{\circ rs}(x) = c_0 + (x-c_0) + \alpha_d (x-c_0)^d + O((x-c_0)^{d+1}),$$

for some $d > 0$ with $\alpha_d \neq 0$. It follows that for any k, we have

$$q^{\circ rsk}(x) = c_0 + (x - c_0) + k\alpha_d(x - c_0)^d + O((x - c_0)^{d+1}).$$

Now, let $g(x) = \sum_{i=0}^{\infty} \beta_i (x - \lambda)^i$ be any nonconstant polynomial in $(x - \lambda)$ such that $\beta_0 = c_0$. Let t be the smallest positive integer such that $\beta_t \neq 0$. Then, for any k, the coefficient of $(x - \lambda)^{td}$ in $q^{\circ rsk} \circ g$ is $k\alpha_d \beta_t^d + \beta_{td}$. Since $\alpha_d \neq 0$, there are in particular at most finitely many k such that the coefficient of $(x - \lambda)^{td}$ in $q^{\circ rsk} \circ g$ is equal to c_{td}. Thus, there are at most finitely many k such that $v_\lambda(q^{\circ rsk} \circ g(x) - c(x)) > td$, and hence $v_\lambda(q^{\circ rsk} \circ g(x) - c(x))$ is bounded for all k. Applying this to $g = q^{\circ y}$ for $y = \ell, \ell + r, \dots, \ell + (s - 1)r$ completes our proof, since any number of the form $\ell + kr$ can be written as $y + krs$ for some such y.

Assume now that $u > 1$. Then, by induction

$$q^{\circ \ell + rk}(x) = c_0 + a_u^{(u^k - 1)/(u-1)} b_e^{u^k} (x - \lambda)^{eu^k} + O((x - \lambda)^{eu^k + 1}).$$

So, $v_\lambda(q^{\circ n}(x) - c(x)) \leq \deg c$ for all sufficiently large k. Hence, $v_\lambda(q^{\circ n}(x) - c(x))$ is bounded above by a constant depending on λ and q only. □

Remark. We note that in Lemma 16, if $v_\lambda(q^{\circ n}(x) - c(x)) > 0$ then the integer n is in a congruence class $\ell + r\,\mathbb{N}$ for some positive integer r. In fact, r is the least period of $c_0 = c(\lambda)$ under the action of q.

Proof of Theorem 4. We may assume without loss of generality that c is not in a ramified cycle of f. By Theorem 1, there are at most finitely many λ such that $(x - \lambda)$ divides $\gcd(f^{\circ m}(x) - c(x), g^{\circ n}(x) - c(x))$ for some m and n. Let $\mathcal{S}$ be the set of all such λ. By Lemma 16, there is an M_λ such that $v_\lambda(q^{\circ n}(x) - c(x)) \leq M_{\lambda,q}$ for all n, since c is not a compositional power of f. Then, if

$$h(x) = \prod_{\lambda \in \mathcal{S}} (x - \lambda)^{M_\lambda},$$

we see that

$$\gcd(f^{\circ m}(x) - c(x), g^{\circ n}(x) - c(x)) \mid h(x),$$

for all m and n, as desired. □

5. Further directions

Many of these techniques may work more generally. We close with several questions.

Silverman [2004a] showed that the characteristic p function field analog of the theorem of Bugeaud, Corvaja, and Zannier theorem is not true; in particular, one can find multiplicatively independent polynomials $a, b \in \mathbb{F}_q[x]$ (where $\mathbb{F}_q$ is as usual the finite field with q elements) and an $\epsilon > 0$ such that $\deg(\gcd(a^n - 1, b^n - 1)) > \epsilon n$ for infinitely many n. Similarly, we suspect that one can find compositionally independent polynomials $f, g \in \mathbb{F}_q[x]$, an $\epsilon > 0$, and a $c(x) \in \mathbb{F}_q[x]$ that is not a compositional power of f or g such that $\deg(\gcd(f^{\circ n}(x)-c(x), g^{\circ n}(x)-c(x))) > \epsilon n$ for infinitely many n. On the other hand, one might ask the following question in characteristic p. See also [Ghioca et al. 2017a, Corollary 17] for an answer to a slightly different question.

Question 17. *Let $F = \mathbb{F}_q[T]$ be the polynomial ring in one variable over the finite field with q elements. Let f and g be two compositionally independent nonisotrivial polynomials in $F[x]$, and let $c \in F[x]$. Is it true that there are at most finitely many $\lambda \in \overline{F}$ such that there is an n for which $(x-\lambda)$ divides $\gcd(f^{\circ n}(x)-c(x), g^{\circ n}(x)-c(x))$? Given an $\epsilon > 0$ and assuming that $c(x)$ is not in a ramified cycle of f and g, is it even true that*

$$\deg(\gcd(f^{\circ n}(x)-c(x), g^{\circ n}(x)-c(x))) < \epsilon n$$

for all but finitely many n?

We might also ask for characteristic 0 results in more general settings.

Question 18. *Let $\phi_1, \phi_2 : \mathbb{P}^1_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$ be two nonconstant, compositionally independent morphisms. Let $c : \mathbb{P}^1_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$ be any morphism. It is true that there must be at most finitely many $\lambda \in \mathbb{C}$ such that $\phi_1^{\circ n}(\lambda) = \phi_2^{\circ n}(\lambda) = c(\lambda)$?*

We should note that the counterexamples to the dynamical Manin–Mumford conjecture given in [Ghioca et al. 2011] do not yield counterexamples here in an obvious way, since the Lattés maps given there commute with each other and hence they are not compositionally independent.

For more general varieties, we ask the following.

Question 19. *Let V be a variety defined over $\mathbb{C}$ and let $\phi_1, \phi_2 : V \to V$ be two dominant compositionally independent morphisms. Let $c : V \to V$ be any morphism. Is it true that the set of $\lambda \in V(\mathbb{C})$ such that $\phi_1^{\circ n}(\lambda) = \phi_2^{\circ n}(\lambda) = c(\lambda)$ must be contained in a proper Zariski closed subset of V?*

In the case where V is projective and some iterates of ϕ_1 and ϕ_2 extend to maps on projective space of degree greater than one (the case where ϕ_1 and ϕ_2 are "polarizable" in the language of Zhang [2006]), it may be possible, using higher dimensional results such as those of [Yuan 2008; Gubler 2008; Yuan and Zhang 2017], to show that $h_{\phi_1} = h_{\phi_2}$ whenever the λ such that $\phi_1^n(\lambda) = \phi_2^n(\lambda) = c(\lambda)$ are Zariski dense. On the other hand, that may not imply a compositional dependence between ϕ_1 and ϕ_2. One natural place to look for counterexamples might be abelian varieties with quaternion endomorphism rings.

Finally, it is natural to ask for a result along the lines of [Bugeaud et al. 2003] where one considers iterates of integers under polynomial maps rather than simply powers of integers. More precisely, one might hope that for $a, b \in \mathbb{Z}$, two polynomials $f, g \in \mathbb{Z}[x]$ of degree $d > 1$, and an $\epsilon > 0$, the inequality

$$\gcd(f^{\circ n}(a), g^{\circ n}(b)) < \epsilon d^n$$

should hold for all but at most finitely many n, given reasonable conditions on f, g, a, and b. Huang [2017] has shown that such an inequality must indeed hold for all sufficiently large n whenever the sequence $(f^{\circ n}(a), g^{\circ n}(b))_n$ is Zariski dense in $\mathbb{A}^2$ if one assumes Vojta's conjecture for heights with respect to canonical divisors on surfaces (see [Vojta 1987, Conjecture 3.4.3]). The proof uses an idea of Silverman [2005], which relates the original results of [Bugeaud et al. 2003] to Vojta's conjecture.

Acknowledgements

We would like to thank Dragos Ghioca, Keping Huang, Alina Ostafe, Juan Rivera-Letelier, Umberto Zannier, Shou-Wu Zhang, and Mike Zieve for helpful conversations. We'd also like to thank the anonymous referee for many helpful comments and corrections. The first named author would like to thank his coauthor for his hospitality during the visit to the math department of University of Rochester in the summer of 2014 when this project was initiated.

References

[Ailon and Rudnick 2004] N. Ailon and Z. Rudnick, "Torsion points on curves and common divisors of $a^k - 1$ and $b^k - 1$", *Acta Arith.* **113**:1 (2004), 31–38. MR Zbl

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

[Baker and De Marco 2013] M. Baker and L. De Marco, "Special curves and postcritically finite polynomials", *Forum Math. Pi* **1** (2013), e3, 35. MR Zbl

[Baker and DeMarco 2011] M. Baker and L. DeMarco, "Preperiodic points and unlikely intersections", *Duke Math. J.* **159**:1 (2011), 1–29. MR Zbl

[Baker and Erëmenko 1987] I. N. Baker and A. Erëmenko, "A problem on Julia sets", *Ann. Acad. Sci. Fenn. Ser. A I Math.* **12**:2 (1987), 229–236. MR Zbl

[Baker and Rumely 2006] M. H. Baker and R. Rumely, "Equidistribution of small points, rational dynamics, and potential theory", *Ann. Inst. Fourier* (*Grenoble*) **56**:3 (2006), 625–688. MR Zbl

[Benedetto 2005] R. L. Benedetto, "Heights and preperiodic points of polynomials over function fields", *Int. Math. Res. Not.* **2005**:62 (2005), 3855–3866. MR Zbl

[Bombieri and Gubler 2006] E. Bombieri and W. Gubler, *Heights in Diophantine geometry*, New Mathematical Monographs **4**, Cambridge University Press, 2006. MR Zbl

[Bugeaud et al. 2003] Y. Bugeaud, P. Corvaja, and U. Zannier, "An upper bound for the G.C.D. of $a^n - 1$ and $b^n - 1$", *Math. Z.* **243**:1 (2003), 79–84. MR Zbl

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

[Chambert-Loir 2006] A. Chambert-Loir, "Mesures et équidistribution sur les espaces de Berkovich", *J. Reine Angew. Math.* **595** (2006), 215–235. MR Zbl

[Corvaja and Zannier 2005] P. Corvaja and U. Zannier, "A lower bound for the height of a rational function at S-unit points", *Monatsh. Math.* **144**:3 (2005), 203–224. MR Zbl

[Corvaja and Zannier 2008] P. Corvaja and U. Zannier, "Some cases of Vojta's conjecture on integral points over function fields", *J. Algebraic Geom.* **17**:2 (2008), 295–333. MR Zbl

[Corvaja and Zannier 2013] P. Corvaja and U. Zannier, "Greatest common divisors of $u-1,\ v-1$ in positive characteristic and rational points on curves over finite fields", *J. Eur. Math. Soc. (JEMS)* **15**:5 (2013), 1927–1942. MR Zbl

[Favre and Rivera-Letelier 2004] C. Favre and J. Rivera-Letelier, "Théorème d'équidistribution de Brolin en dynamique p-adique", *C. R. Math. Acad. Sci. Paris* **339**:4 (2004), 271–276. MR Zbl

[Ghioca and Tucker 2010] D. Ghioca and T. J. Tucker, "Proof of a dynamical Bogomolov conjecture for lines under polynomial actions", *Proc. Amer. Math. Soc.* **138**:3 (2010), 937–942. MR Zbl

[Ghioca et al. 2008] D. Ghioca, T. J. Tucker, and M. E. Zieve, "Intersections of polynomials orbits, and a dynamical Mordell–Lang conjecture", *Invent. Math.* **171**:2 (2008), 463–483. MR Zbl

[Ghioca et al. 2011] D. Ghioca, T. J. Tucker, and S. Zhang, "Towards a dynamical Manin–Mumford conjecture", *Int. Math. Res. Not.* **2011**:22 (2011), 5109–5122. MR Zbl

[Ghioca et al. 2015] D. Ghioca, L.-C. Hsia, and T. J. Tucker, "Preperiodic points for families of rational maps", *Proc. Lond. Math. Soc.* (3) **110**:2 (2015), 395–427. MR Zbl

[Ghioca et al. 2017a] D. Ghioca, L.-C. Hsia, and T. J. Tucker, "On a variant of the Ailon–Rudnick theorem in finite characteristic", *New York J. Math.* **23** (2017), 213–225. MR Zbl

[Ghioca et al. 2017b] D. Ghioca, L.-C. Hsia, and T. J. Tucker, "A variant of a theorem by Ailon–Rudnick for elliptic curves", preprint, 2017. arXiv

[Gubler 2008] W. Gubler, "Equidistribution over function fields", *Manuscripta Math.* **127**:4 (2008), 485–510. MR Zbl

[Hindry and Silverman 2000] M. Hindry and J. H. Silverman, *Diophantine geometry*, Graduate Texts in Mathematics **201**, Springer, 2000. MR Zbl

[Huang 2017] K. Huang, "Generalized Greatest Common Divisors for the Orbits under Rational Functions", preprint, 2017. arXiv

[Ingram 2013] P. Ingram, "Variation of the canonical height for a family of polynomials", *J. Reine Angew. Math.* **685** (2013), 73–97. MR Zbl

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

[Luca 2005] F. Luca, "On the greatest common divisor of $u-1$ and $v-1$ with u and v near S-units", *Monatsh. Math.* **146**:3 (2005), 239–256. MR Zbl

[Mimar 2013] A. Mimar, "On the preperiodic points of an endomorphism of $\mathbb{P}^1 \times \mathbb{P}^1$ which lie on a curve", *Trans. Amer. Math. Soc.* **365**:1 (2013), 161–193. MR Zbl

[Morton and Silverman 1995] P. Morton and J. H. Silverman, "Periodic points, multiplicities, and dynamical units", *J. Reine Angew. Math.* **461** (1995), 81–122. MR Zbl

[Murty and Murty 2011] M. R. Murty and V. K. Murty, "On a problem of Ruderman", *Amer. Math. Monthly* **118**:7 (2011), 644–650. MR Zbl

[Ostafe 2016] A. Ostafe, "On some extensions of the Ailon–Rudnick theorem", *Monatsh. Math.* **181**:2 (2016), 451–471. MR Zbl

[Petsche et al. 2012] C. Petsche, L. Szpiro, and T. J. Tucker, "A dynamical pairing between two rational maps", *Trans. Amer. Math. Soc.* **364**:4 (2012), 1687–1710. MR Zbl

[Schmidt and Steinmetz 1995] W. Schmidt and N. Steinmetz, "The polynomials associated with a Julia set", *Bull. London Math. Soc.* **27**:3 (1995), 239–241. MR Zbl

[Serre 1997] J.-P. Serre, *Lectures on the Mordell–Weil theorem*, 3rd ed., Aspects of Mathematics, Friedr. Vieweg & Sohn, Braunschweig, 1997. MR Zbl

[Siegel 2014] C. L. Siegel, "Über einige Anwendungen diophantischer Approximationen [reprint of Abhandlungen der Preußischen Akademie der Wissenschaften. Physikalisch-mathematische Klasse 1929, Nr. 1]", pp. 81–138 in *On some applications of Diophantine approximations*, edited by U. Zannier, Quad./Monogr. **2**, Ed. Norm., Pisa, 2014. MR Zbl

[Silverman 2004a] J. H. Silverman, "Common divisors of $a^n - 1$ and $b^n - 1$ over function fields", *New York J. Math.* **10** (2004), 37–43. MR Zbl

[Silverman 2004b] J. H. Silverman, "Common divisors of elliptic divisibility sequences over function fields", *Manuscripta Math.* **114**:4 (2004), 431–446. MR Zbl

[Silverman 2005] J. H. Silverman, "Generalized greatest common divisors, divisibility sequences, and Vojta's conjecture for blowups", *Monatsh. Math.* **145**:4 (2005), 333–350. MR Zbl

[Silverman 2007] J. H. Silverman, *The arithmetic of dynamical systems*, Graduate Texts in Mathematics **241**, Springer, 2007. MR Zbl

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

[Yuan 2008] X. Yuan, "Big line bundles over arithmetic varieties", *Invent. Math.* **173**:3 (2008), 603–649. MR Zbl

[Yuan and Zhang 2017] X. Yuan and S.-W. Zhang, "The arithmetic Hodge index theorem for adelic line bundles", *Math. Ann.* **367**:3-4 (2017), 1123–1171. MR Zbl

[Zannier 2012] U. Zannier, *Some problems of unlikely intersections in arithmetic and geometry*, Annals of Mathematics Studies **181**, Princeton University Press, 2012. MR Zbl

[Zhang 2006] S.-W. Zhang, "Distributions in algebraic dynamics", pp. 381–430 in *Surveys in differential geometry. Vol. X*, edited by S. T. Yau, Surv. Differ. Geom. **10**, International Press, Somerville, MA, 2006. MR Zbl

Communicated by Shou-Wu Zhang
Received 2016-12-07 Revised 2017-04-11 Accepted 2017-05-13

hsia@math.ntnu.edu.tw *Department of Mathematics, National Taiwan Normal University, Taipei, Taiwan*

ttucker@math.rochester.edu *Department of Mathematics, University of Rochester, Rochester, NY 14627, United States*

Algebra & Number Theory

msp.org/ant

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

The subscription price for 2017 is US $325/year for the electronic version, and $520/year (+$55, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

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

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

Algebra & Number Theory

Volume 11 No. 6 2017

The motivic Donaldson–Thomas invariants of (-2)-curves 1243
BEN DAVISON and SVEN MEINHARDT

Classifying tilting complexes over preprojective algebras of Dynkin type 1287
TAKUMA AIHARA and YUYA MIZUNO

Distinguished-root formulas for generalized Calabi–Yau hypersurfaces 1317
ALAN ADOLPHSON and STEVEN SPERBER

On defects of characters and decomposition numbers 1357
GUNTER MALLE, GABRIEL NAVARRO and BENJAMIN SAMBALE

Slicing the stars: counting algebraic numbers, integers, and units by degree and height 1385
ROBERT GRIZZARD and JOSEPH GUNTHER

Greatest common divisors of iterates of polynomials 1437
LIANG-CHUNG HSIA and THOMAS J. TUCKER

The role of defect and splitting in finite generation of extensions of associated graded rings along a valuation 1461
STEVEN DALE CUTKOSKY

1937-0652(2017)11:6;1-F