Monatshefte für Mathematik (2020) 191:103–123
https://doi.org/10.1007/s00605-019-01350-1

Generalized greatest common divisors for orbits under rational functions

Keping Huang[1]

Received: 1 December 2017 / Accepted: 1 November 2019 / Published online: 18 November 2019

Abstract

Assume Vojta's Conjecture for blowups of $\mathbb{P}^1 \times \mathbb{P}^1$. Suppose $a, b, \alpha, \beta \in \mathbb{Z}$, and $f(x), g(x) \in \mathbb{Z}[x]$ are polynomials of degree $d \geq 2$. Assume that the sequence $(f^{\circ n}(a), g^{\circ n}(b))_n$ is generic and α, β are not exceptional for f, g respectively. We prove that for each given $\varepsilon > 0$, there exists a constant $C = C(\varepsilon, a, b, \alpha, \beta, f, g) > 0$, such that for all $n \geq 1$, we have

$$\gcd(f^{\circ n}(a) - \alpha, g^{\circ n}(b) - \beta) \leq C \cdot \exp(\varepsilon \cdot d^n).$$

We prove an estimate for rational functions and for a more general gcd and then obtain the above inequality as a consequence.

Keywords Greatest common divisor · Vojta's conjecture

Mathematics Subject Classification Primary 11G35; Secondary 11D75 · 11J25 · 14D10 · 14G25

1 Introduction

In [6], Bugeaud, Corvaja, and Zannier proved the following theorem.

Theorem 1.1 *Let a, b be multiplicatively independent integers ≥ 2, and let $\varepsilon > 0$. Then, provided n is sufficiently large, we have*

$$\gcd(a^n - 1, b^n - 1) < \exp(\varepsilon n).$$

Communicated by Adrian Constantin.

✉ Keping Huang
keping.huang@rochester.edu

[1] Department of Mathematics, University of Rochester, Rochester, NY 14627, USA

The authors of that paper obtained the result by contradiction. They began by constructing a family of vectors in terms of n, a, and b. Then they showed that if the bound is not satisfied, then the vectors must lie in a lower-dimensional linear subspace by the Schmidt Subspace Theorem. Using this result they are able to derive algebraic relations on powers of a and b, which guarantee that a, b are multiplicatively dependent. Silverman interpreted in [28] this result as a special case of Vojta's Conjecture. Theorem 1.1 has been further generalized in [19] where Levin interpreted it as another special case of Vojta's Conjecture.

One may ask whether a similar inequality holds for iterations of polynomials, as iterations are dynamical analogues of power maps. It seems that current tools are not powerful enough to tackle this problem unconditionally. In [25] Silverman observed that one can interpret the greatest common divisor as a height function on some blowup of the projective plane. Furthermore, assuming Vojta's Conjecture (cf. [31]), Silverman gave in [28] an upper bound for the greatest common divisor of the values of some polynomial functions, in terms of the absolute values of the initial points. See also [24] for an application of Silverman's method to gcd bounds of analytic functions. Many other authors have worked out various generalization and variations of this problem, both over number fields and function fields (see [1,8–10,14,17,21,27] for example). See also [13,23] for related unlikely intersection results, interpreted in the context of Ailon–Rudnick type result [1].

In this paper, we apply Silverman's method in the situation of iterations. In fact, we will prove a Silverman-type estimate for a fixed smaller iteration, and derive some results on gcd's. However, there are some technical difficulties. First, in order to have the required operands of the greatest common divisor, one needs to blow up a Zariski closed subset in general (as opposed to subvarieties in [28]), depending on the prescribed constant ε. Second, in the case of the rational functions the numerators of iterates might not be iterates of any polynomial, so we need a more detailed analysis. We also need to control the degree of ramification, for this we also need the very mild assumption that α, β are not exceptional.

Definition 1.2 Let X be an algebraic variety defined over $\overline{\mathbb{Q}}$. We say that a sequence $(x_n)_n \subseteq X(\overline{\mathbb{Q}})$ is *generic* in X if for any proper Zariksi closed subset $Y \subsetneq X$, there exists an $N \in \mathbb{N}$ such that for all $n \geq N$, $x_n \notin Y$. A point $x_0 \in \overline{\mathbb{Q}}$ is said to be *exceptional* for a rational function $\phi \in \overline{\mathbb{Q}}(x)$ if the backward orbit $\cup_{n=0}^{\infty}(\phi^{\circ n})^{-1}(\{x_0\})$ is finite.

A main result of this paper is the following theorem. It is based on Vojta's Conjecture, which is described in Conjecture 2.7.

Theorem A *Assume Vojta's Conjecture for blowups of* $\mathbb{P}^1 \times \mathbb{P}^1$. *Suppose* $a, b, \alpha, \beta \in \mathbb{Z}$, *and that* $f(x), g(x) \in \mathbb{Z}[x]$ *are polynomials of degree* $d \geq 2$. *Assume that* α, β *are not exceptional for* f, g *respectively. Assume that the sequence* $(f^{\circ n}(a), g^{\circ n}(b))_n$ *is generic in* $\overline{\mathbb{Q}}^2$. *Then for each given* $\varepsilon > 0$, *there exists a constant* $C = C(\varepsilon, a, b, \alpha, \beta, f, g) > 0$, *such that for all* $n \geq 1$, *we have*

$$\gcd(f^{\circ n}(a) - \alpha, g^{\circ n}(b) - \beta) \leq C \cdot \exp(\varepsilon \cdot d^n).$$

Remark Let $d_1 = \deg(f), d_2 = \deg(g)$. The result is trivial when $d_1 \neq d_2$ and $d = \max(d_1, d_2)$, and is proved in [8] for the case $d_1 = d_2 = 1$. We use the convention that $\gcd(0, 0) = 0$. But this involves only finitely many n, since the sequence $(f^{\circ n}(a), g^{\circ n}(b))_n$ is generic, and hence so is $(f^{\circ n}(a) - \alpha, g^{\circ n}(b) - \beta)_n$.

In [32] Xie proved the Dynamical Mordell–Lang Conjecture for polynomial endomorphisms of the affine plane. Therefore the genericity of the sequence $(f^{\circ n}(a), g^{\circ n}(b))_n$ is equivalent to the Zariski density of $(f^{\circ n}(a), g^{\circ n}(b))_n$. On the other hand, Medvedev and Scanlon gave in [20] characterizations of periodic curves under split polynomial endomorphisms of $\mathbb{P}^1 \times \mathbb{P}^1$. The equation of the curve should meet certain commutativity conditions, which are unlikely to hold in general. Therefore the genericity condition of the sequence $(f^{\circ n}(a), g^{\circ n}(b))_n$ is a mild condition.

Actually we will prove Theorem 2.11 and obtain Theorem A as a consequence. In [28] Silverman defined a more general gcd height which is the log of gcd in the case of rational integers. In the same paper he proved most results in this more general framework. See Sect. 2 for the precise definitions and statements. The idea of the proof of Theorem 2.11 is as follows. Following the idea of Silverman, we prove in Theorem 3.5 an upper bound for the greatest common divisor $\gcd(F_1(a'), G_1(b'))$ for general square-free polynomials F_1, G_1 and we will apply it (essentially) to $\gcd(f^{\circ D}(a'), g^{\circ D}(b'))$ for some large D depending on ε and d with $a' = f^{\circ(n-D)}(a)$ and $b' = g^{\circ(n-D)}(b)$.

The plan of this paper is as follows. Section 2 contains a table of notation, basics of height functions and algebraic geometry, a statement of Vojta's Conjecture, some results concerning the gcd height, and statements of other main theorems of this paper. We prove our main theorem concerning the gcd height in Sect. 3. In Sect. 4, we first cite a genericity criterion for the case when $f = g$ are non-special polynomials, replacing the genericity condition. We also cite a theorem of Corvaja and Zannier for the case of power maps. At the end of Sect. 4 we give several examples to explain why the genericity condition in Theorem A is necessary; our policy is to include only results which are easy to state and hopefully clarify things greatly. In Sect. 5, we give a conditional result for characterizing large gcd's.

2 Preliminaries

We use the following notation throughout this paper.

K	a number field.
$M(K)$	the set of places of K.
n_v	the local degree $[K_v : \mathbb{Q}_w]$ where w is the contraction of v on $\mathbb{Q}$; the product formula has power n_v for the place v.
f, g	rational functions defined over K.
d	the degree of f and g.
$h_{\mathbb{P}^n}$	the Weil height on $\mathbb{P}^n(K)$.
$\hat{h}_f$	the canonical height with respect to f.
$f^{\circ n}$	the n-th iterate of f.
$\lvert\cdot\rvert_v$	the v-adic absolute value.

$v^+(\cdot)$ $\max(0, -\log|\cdot|_v)$.

For $P = [x_0, \ldots, x_n] \in \mathbb{P}^n(\overline{K})$, choose a number field L over which P is defined and define the *Weil height*

$$h_{\mathbb{P}^n}(P) = \frac{1}{[L:\mathbb{Q}]} \sum_{v \in M(L)} n_v \max\left(\log|x_0|_v, \ldots, \log|x_n|_v\right). \qquad (2.1)$$

This definition is independent of the choice of L.

Suppose $f : \mathbb{P}^1 \to \mathbb{P}^1$ is an endomorphism of degree $d \geq 2$. Then following a construction of Tate, Call and Silverman defined in [7] the canonical height h_f associated with f as

$$\hat{h}_f(P) = \lim_{n\to\infty} \frac{h_{\mathbb{P}^1}\left(f^{\circ n}(P)\right)}{d^n}$$

for all $P \in \mathbb{P}^1(\overline{K})$.

Theorem 2.1 ([7]) *The canonical height satisfies*

1. $\hat{h}_f(P) = h_{\mathbb{P}^1}(P) + O(1)$,
2. $\hat{h}_f(f(P)) = d \cdot \hat{h}_f(P)$.

See also Section 3.3 of [29] for more details. Here the implied constant in $O(1)$ is effective and depends only on n and the morphism f, but not on the point $P \in \mathbb{P}^n(\overline{K})$.

Now we introduce some notions in algebraic geometry. For more information one may refer to [15].

Definition 2.2 Let $R = \overline{K}[X_0, \ldots, X_n]$ and let $T \subseteq R$ be a set of homogeneous polynomials in $X_0, \ldots, X_n$. Every set

$$\text{zero}(T) := \{P \in \mathbb{P}^n(\overline{K}) \mid f(P) = 0 \text{ for all } f \in T\}$$

is called a *Zariski closed* subset of $\mathbb{P}^n(\overline{K})$. A Zariski closed subset $V \subseteq \mathbb{P}^n(\overline{K})$ is called a *projective variety* if it cannot be written as a union of two Zariski closed proper subsets.

To give more general definition of height functions, we need the notion of divisors on nonsingular varieties. See Sections 1.5 and 2.6 of [15] for more details.

Definition 2.3 Let X be a nonsingular projective variety. The group of *Weil divisors* on X is the free abelian group generated by the closed subvarieties of codimension one on X. It is denoted by $\text{Div}(X)$. Denote by $K(X)^*$ the multiplicative group of nonzero rational functions on X. Each rational function $f \in K(X)^*$ gives a *principal divisor*

$$\text{div}(f) = \sum_{Y \subsetneq X \text{ codimension } 1} \text{ord}_Y(f) \cdot Y.$$

The group $\text{Div}(X)$ divided by the subgroup of principal divisors is called the *divisor class group* of X.

Remark In the case when X is nonsingular, the class group is canonically isomorphic to the group $\mathrm{Pic}(X)$. For the definition of the latter, see Section 2.6 of [15].

Definition 2.4 Suppose $D \in \mathrm{Div}(X)$. The *complete linear system* of D is the set

$$L(D) = \{f \in K(X)^* \mid D + \mathrm{div}(f) \geq 0\} \cup \{0\}.$$

If $L(D) \neq 0$, then $L(D)$ induces a rational morphism $\phi_D : X \dashrightarrow \mathbb{P}^n$. For more details refer to Section A.3 of [16].

Definition 2.5 A divisor $D \in \mathrm{Div}(X)$ is said to be *very ample* if the above map ϕ_D is an embedding. A divisor D is said to be *ample* if an positive integral multiple nD of D is very ample.

Fix a nonsingular variety X defined over K. For each divisor $D \in \mathrm{Div}(X)$ defined over K we can define height functions $h_{X,D} : X(\overline{K}) \to \mathbb{R}$ as below. For more details, including that these height functions are well-defined, refer to [16], Theorem B.3.2.

- If D is very ample, choose an embedding $\phi_D : X \to \mathbb{P}^n$. Then define $h_{X,D}(x) = h_{\mathbb{P}^n}(\phi_D(x))$.
- If D is ample, then suppose nD is very ample, define $h_{X,D} = 1/n \cdot h_{X,nD}$.
- In general, we can write $D = D_1 - D_2$ with D_1, D_2 ample, and define $h_{X,D} = h_{X,D_1} - h_{X,D_2}$.

The following theorem is one of the most important results in Diophantine geometry. See also Sections 2.3 and 2.4 of [5] and Chapter 4 of [18].

Theorem 2.6 (The Weil Height Machine, Part of [16], Theorem B.3.2) *In the context of the above paragraphs, the height functions constructed in this way, are determined, up to $O(1)$. They satisfy the following properties.*

- *Let $D, E \in \mathrm{Div}(X)$. Then $h_{X,D+E} = h_{X,D} + h_{X,E} + O(1)$.*
- *(Northcott's Theorem) Let $D \in \mathrm{Div}(X)$ be ample. Then for every finite extension K'/K and every constant B, the set*

  $$\{P \in X(K') \mid h_{X,D}(P) \leq B\}$$

  is finite.
- *Let $D, E \in \mathrm{Div}(X)$ with $D = E + \mathrm{div}(f)$. Then*

  $$h_{X,D}(P) = h_{X,E}(P) + O(1)$$

  for all $P \in X(\overline{K})$.

Remark Formula (2.1) can be thought of as $h_{\mathbb{P}^n,H}$ in the context of Theorem 2.6 where H is a hyperplane in $\mathbb{P}^n$.

Remark The "$O(1)''$ constants that appear in Theorem 2.6 depend on the varieties, divisors, and morphisms, but they are independent of the points on the varieties. In the sense of Theorem 2.6, height functions globally differed by $O(1)$ can be thought of as the same height function. Therefore in terms of Item 1 of Theorem 2.1, the canonical height $\hat{h}_f$ can be thought of as $h_{\mathbb{P}^1,H}$ where H is a point in $\mathbb{P}^1$.

Intuitively, ampleness is a positivity notion on algebraic varieties and it is closely related with height functions. The more "ample" a divisor D is, the more "positive" the height function $h_{X,D}$ is. We will use the following version of Vojta's Conjecture. It is Conjecture 3.4.3 of the monograph [31]. For the definition of normal crossing divisor, see Chapter 5, Remark 3.8.1 of [15].

Conjecture 2.7 (Vojta) *Let K be a number field, and let X be a nonsingular projective variety defined over K. Suppose A is an ample normal crossing divisor on X and K_X is the canonical divisor of X, both defined over K. Let h_A and h_{K_X} be the corresponding height functions respectively. For each fixed $\varepsilon > 0$, there is a Zariski closed proper subset V of X and a constant C such that*

$$h_{K_X}(x) \leq \varepsilon \cdot h_A(x) + C$$

for all $x \in X(K) \backslash V(K)$.

In fact, for algebraic variety X, Silverman defined in [25] height functions $h_{X,Y}$ with respect to any closed subschemes Y. For our purpose it is enough to recall the following part.

Theorem 2.8 ([25]) *Let X be a projective variety and let $Z(X)$ denote the set of closed subschemes of X. For each $V \in Z(X)$ there is a map $h_{X,D} : X(\overline{K}) \to \mathbb{R}_{\geq 0}$ such that these $h_{X,D}$ satisfy the following conditions:*

1. *If $D \in Z(X)$ is a positive divisor, then $h_{X,D}$ is the usual height function associated to D given by Theorem 2.6;*
2. *Let $\phi : X \to X'$ be a morphism of varieties, and let $Y' \in Z(X')$. Then*

$$h_{X,\phi^* Y'} = h_{X',Y'} + O(1). \tag{2.2}$$

Concerning the relationship between the greatest common divisor and heights, we briefly recall Silverman's idea in [28]. For all $v \in M(\mathbb{Q})$ and $a \in \mathbb{Z}$, recall that $v^+(a) = \max(-\log |a|_v, 0) \in [0, +\infty]$. Silverman began his discussion in [25] by writing the greatest common divisor as

$$\log \gcd(a, b) = \sum_{v \in M(\mathbb{Q})} \min(v^+(a), v^+(b)) \tag{2.3}$$

for $a, b \in \mathbb{Z}$. Then he extends this function for $a, b \in \mathbb{Q}$ by the same formula. By the last paragraph on page 337 of [28], Eq. (2.3) can be interpreted as the height function on $\mathbb{P}^1 \times \mathbb{P}^1$ with respect to the subschemes $(0, 0)$, and furthermore as a height function associated with a divisor on the blowup of $\mathbb{P}^1 \times \mathbb{P}^1$ along $(0, 0)$. See page 163 of [15] for the definition of blowup and strict transform. See pages 28–29 of [15] for a concrete example of blowing up a point.

Proposition 2.9 ([15], Chapter 5, Proposition 3.1) *Let $\pi : \tilde{W} \to W$ be the blowup of a nonsingular surface W at a point P. Then*

1. *π induces an isomorphism of $\tilde{W} - \pi^{-1}(P)$ and $W - P$,*
2. *The set $E := \phi^{-1}(P)$ is isomorphic to $\mathbb{P}^1$. It is called the* exceptional divisor *of the blowup π,*
3. *$\tilde{W}$ is nonsingular.*

The following definition is a slight generalization of that given by Silverman in [28].

Definition 2.10 Let K be a number field and let X/K be a smooth variety. Let $Y/K \subsetneq X/K$ be a subscheme of codimension $r \geq 2$. Let $\pi : \tilde{X} \to X$ be the blowup of X along Y, and let $\tilde{Y} = \pi^{-1}(Y)$ be the exceptional divisor of the blowup. For $x \in (X - Y)(K)$, we let $\tilde{x} = \pi^{-1}(x) \in \tilde{X}$. The generalized (logarithmic) greatest common divisor of the point $x \in (X - Y)(k)$ with respect to Y is the quantity

$$h_{\text{gcd}}(x; Y) := h_{X,Y}(x) = h_{\tilde{X},\tilde{Y}}(\tilde{x})$$

where the last inequality follows from (2.2).

For a number fields K and for $a, b \in K$ we also define the generalized gcd as

$$h_{\text{gcd}}(a, b) = \frac{1}{[K : \mathbb{Q}]} \sum_{v \in M(K)} n_v \min(v^+(a), v^+(b)). \tag{2.4}$$

As a consequence of the Weil height machine, the relationship between h_{gcd} as in Definition 2.10 and in Eq. (2.4) is shown at the end of this paragraph. See [25,28] for some interesting cases over $\mathbb{Z}$ where the contribution from the places at infinity is zero or bounded. Suppose K is a number field. Let $X = \mathbb{P}^1 \times \mathbb{P}^1$ and let $f(X_1) \in K[X_1]$, $g(X_2) \in K[X_2]$ be square-free polynomials. Then over $\overline{\mathbb{Q}}$ the vanishing set $Z(f)$ and $Z(g)$ define two divisors D_1 and D_2 on X. Set $Y = D_1 \cap D_2$. Then for all points $x = (x_1, x_2) \in (\mathbb{P}^1 \times \mathbb{P}^1)(K)$ such that $f(x_1) \neq 0$ and $g(x_2) \neq 0$, we have

$$\begin{aligned} h_{\text{gcd}}\,(f(x_1), g(x_2)) &= h_{\mathbb{P}^1 \times \mathbb{P}^1, (0,0)}(f(x_1), g(x_2)) \\ &= h_{\mathbb{P}^1 \times \mathbb{P}^1, (f,g)^*(0,0)}(x_1, x_2) + O(1) \\ &= h_{X,Y}(x) + O(1) \\ &= h_{\text{gcd}}(x; Y) + O(1), \end{aligned}$$

where the second equality follows from (2.2).

Our goal is to prove the following theorem.

Theorem 2.11 *Let K be a number field. Assume Vojta's Conjecture for blowups of $\mathbb{P}^1 \times \mathbb{P}^1$ and K. Suppose $a, b, \alpha, \beta \in K$. Let $f, g \in K(X)$ with degree $d \geq 2$. Assume that the sequence $(f^{\circ n}(a) - \alpha, g^{\circ n}(b) - \beta)_n \subseteq \mathbb{P}^1(\overline{\mathbb{Q}}) \times \mathbb{P}^1(\overline{\mathbb{Q}})$ is generic, and α and β are not exceptional for f and g respectively. Then for each given $\varepsilon > 0$, there exists a constant $C = C(\varepsilon, a, b, \alpha, \beta, f, g)$ such that*

for all $n \geq 1$, we have

$$h_{\text{gcd}}(f^{\circ n}(a) - \alpha, g^{\circ n}(b) - \beta) \leq \varepsilon \cdot d^n + C.$$

We can also conclude the periodicity of an irreducible component of the Zariski closure $\overline{(f^{\circ n}(a), g^{\circ n}(b))_n}$ under (f, g) in the cases when the Dynamical Mordell–Lang Conjecture is proved. See Sect. 4 for more details. Thanks to the powerful theorems proved in [2,20,22], we can give some concrete conditions for $(f^{\circ n}(a), g^{\circ n}(b))_n$ being generic in the case when $f = g$ are so-called non-special polynomials (see Sect. 4).

Theorem 2.12 *Let K be a number field and $f \in K[x]$ be a polynomial of degree $d \geq 2$. Assume Vojta's Conjecture for blowups of $\mathbb{P}^1 \times \mathbb{P}^1$ and for K. Assume that f is not conjugate (by a rational automorphism defined over $\overline{K}$) to a power map or a Chebyshev map. Suppose $a, b, \alpha, \beta \in K$ and α, β are not exceptional for f. Assume that there is no polynomial $h \in \overline{K}[x]$ such that $h \circ f^{\circ k} = f^{\circ k} \circ h$ for some $k \in \mathbb{N}_{>0}$ and $h(a) = b,\ h(\alpha) = \beta$ or $h(b) = a,\ h(\beta) = \alpha$, then for any $\varepsilon > 0$, there exists a $C = C(\varepsilon, a, b, \alpha, \beta, f, g) > 0$ such that for all $n \geq 1$, we have*

$$h_{\mathrm{gcd}}(f^{\circ n}(a) - \alpha, f^{\circ n}(b) - \beta) \leq \varepsilon \cdot d^n + C.$$

3 The Proof of Theorem 2.11

Throughout this section we denote by X the surface $\mathbb{P}^1 \times \mathbb{P}^1$.

3.1 Algebraic geometry of $\mathbb{P}^1 \times \mathbb{P}^1$ and its blowups

By Chapter 2, Example 6.6.1 of [15] we have

$$\mathrm{Pic}(X) \cong \mathbb{Z} \oplus \mathbb{Z}.$$

where the image of the divisor class of an irreducible curve C is the degrees of its projection into the two coordinates $(\deg(\mathrm{pr}_1 : C \to \mathbb{P}^1), \deg(\mathrm{pr}_2 : C \to \mathbb{P}^1))$. More generally, if the image of a divisor $D \in \mathrm{Pic}(X)$ is (a, b), then we say that D is *of type* (a, b). Fix $D_1 \in \mathrm{Pic}(X)$ to be a divisor of type $(1, 0)$ and Fix $D_2 \in \mathrm{Pic}(X)$ to be a divisor of type $(0, 1)$. The intersection product on X is given by the rule

$$((a, b).(a', b')) = ab' + a'b \tag{3.1}$$

and extend by $\mathbb{Q}$-linearity to $\mathrm{Pic}(X) \otimes \mathbb{Q}$. In other words, the intersection product on X is determined by the matrix

$$\begin{array}{cc} & \begin{array}{cc} D_1 & D_2 \end{array} \\ \begin{array}{c} D_1 \\ D_2 \end{array} & \begin{bmatrix} & 1 \\ 1 & \end{bmatrix} \end{array}. \tag{3.2}$$

Let K be a number field. Recall that a one-variable polynomial over a field K is called *square-free* if it does not have repeated roots in $\overline{K}$. Suppose $f \in K[X_1]$ and $g \in K[X_2]$ are square-free polynomials in one variable, Let Y be the scheme-theoretic intersection

$$Y = Z(f) \cap Z(g) \subseteq \mathbb{P}^1 \times \mathbb{P}^1,$$

which is the subscheme defined by the ideal $(f) + (g)$, is then a reduced cycle of codimension 2.

Suppose $Z(f) = \{\alpha_1, \ldots, \alpha_m\}$, $Z(g) = \{\beta_1, \ldots, \beta_n\}$. Then

$$Y = \cup_{1 \le i \le m, 1 \le j \le n} \{(\alpha_i, \beta_j)\},$$

each with multiplicity one. Also divisors $\{X_1 = \alpha_i\}$ and $\{X_2 = \beta_j\}$ meet transversally, hence Y is a reduced cycle of codimension 2. To simplify notation write $Y = \{Q_1, \ldots, Q_s\}$. Let $\pi : \tilde{X} \to X$ be the blowup of $X = \mathbb{P}^1 \times \mathbb{P}^1$ along Y, let $\tilde{Y}$ be the preimage of Y, and let $\tilde{P}$ be the preimage of P. Then $\tilde{X}$ is a nonsingular variety by Proposition 2.9.

The following properties are useful to find the canonical divisor and an ample divisor on $\tilde{X}$.

Proposition 3.1 ([15], Chapter 5, Propositions 3.2 and 3.3) *Suppose $\pi : \bar{X} \to X$ is the blowup of a surface X at a point P and let E be the exceptional divisor. The natural maps $\pi^* : \mathrm{Pic}(X) \to \mathrm{Pic}(\bar{X})$ and $\mathbb{Z} \to \mathrm{Pic}(\bar{X})$ defined by $1 \mapsto E$ give rise to an isomorphism $\mathrm{Pic}(\bar{X}) \to \mathrm{Pic}(X) \oplus \mathbb{Z}$. Let $\pi_* : \mathrm{Pic}(\bar{X}) \to \mathrm{Pic}(X)$ denote the projection on the first factor. The intersection theory on $\bar{X}$ is determined by the rules:*

1. *if $C, D \in \mathrm{Pic}(X)$, then $(\pi^* C.\pi^* D) = (C.D)$,*
2. *if $C \in \mathrm{Pic}(X)$, then $(\pi^* C.E) = 0$,*
3. *it holds that $E^2 = -1$,*
4. *(a special case of the projection formula) if $C \in \mathrm{Pic}(X)$ and $D \in \mathrm{Pic}(\bar{X})$, then $(\pi^* C.D) = (C.\pi_* D)$.*

Else, the canonical divisor of $\bar{X}$ is given by $K_{\bar{X}} = \pi^* K_X + E$ where E is the exceptional divisor.

Since the blowup of Y does not involve the blowup at a point on an exceptional curve, we have that $\tilde{X}$ can be obtained by blowing up s distinct points on X one by one. Therefore applying Proposition 3.1 s times yields

$$\mathrm{Pic}(\tilde{X}) \cong \mathrm{Pic}(X) \bigoplus \bigoplus_{i=1}^{s} \mathbb{Z} \cdot \tilde{Y}_i.$$

Define π^* and π_* similarly as in Proposition 3.1.

Since Y_i's are preimages of distinct Q_i's, so if $i = j$, then $(\tilde{Y}_i, \tilde{Y}_i) = -1$ by Item 3 of Proposition 3.1, and if $i \neq j$ then $\tilde{Y}_i$ and $\tilde{Y}_j$ do not intersect and we have $(\tilde{Y}_i, \tilde{Y}_j) = 0$. Therefore $(\tilde{Y}_i, \tilde{Y}_j) = -\delta_{ij}$. Combining this with Eq. (3.1) we know that the intersection product matrix on $\mathrm{Pic}(\tilde{X}) \otimes \mathbb{Q}$ is

$$\begin{array}{c|cccccc|} & \pi^*(D_1) & \pi^*(D_2) & \tilde{Y}_1 & \tilde{Y}_2 & \dots & \tilde{Y}_s \\ \hline \pi^*(D_1) & & 1 & & & & \\ \pi^*(D_2) & 1 & & & & & \\ \tilde{Y}_1 & & & -1 & & & \\ \tilde{Y}_2 & & & & -1 & & \\ \vdots & & & & & \ddots & \\ \tilde{Y}_s & & & & & & -1 \\ \hline \end{array} \tag{3.3}$$

with empty entries zero.

By Theorem 3.1

$$K_{\tilde{X}} = \pi^* K_X + \tilde{Y}_1 + \cdots + \tilde{Y}_s$$

where each $\tilde{Y}_i$ is the preimage of Q_i.

We can choose $-K_X$ to be the normal crossing divisor $\{X_1 = a\} + \{X_1 = b\} + \{X_2 = a'\} + \{X_2 = b'\}$ where a, b, a', b' are distinct nonzero algebraic numbers in K. By Definition 2 of [28], we still have $h_{\mathrm{gcd}}(P; Y) = h_{\tilde{X},\tilde{Y}}(\tilde{P})$.

To apply Vojta's Conjecture, let $A \in \mathrm{Pic}(X)$ be an ample divisor of type (1, 1) and consider the $\mathbb{Q}$-divisor

$$\tilde{A} := \pi^* A - \frac{1}{N}\left(\tilde{Y}_1 + \cdots + \tilde{Y}_s\right) \in \mathrm{Pic}(\tilde{X}) \otimes \mathbb{Q}.$$

Lemma 3.2 *$\tilde{A}$ is ample when $N > s$.*

Proof We need the following definition from Chapter 1, Exercise 5.3 of [15].

Definition 3.3 Let $Y \subseteq \mathbb{A}^2$ be a curve defined by the equation $f(X_1, X_2) = 0$. Let $P = (x_1, x_2)$ be a point of $\mathbb{A}^2$. Make a linear change of coordinates so that P becomes the point $(0, 0)$. Then write f as a sum $f = f_0 + f_1 + \ldots + f_d$, where f_i is a homogeneous polynomial of degree i in X_1 and X_2. Then we define the *multiplicity* of P on Y, denoted $\mu_P(Y)$, to be the least r such that $f_r \neq 0$.

We also need the following lemma, which we state without proof.

Lemma 3.4 ([15], Chapter 1, Exercise 7.5(a)) *An irreducible curve Y of degree $d > 1$ in $\mathbb{P}^2$ cannot have a point of multiplicity $\geq d$.*

Now let $C \subseteq \mathbb{P}^1 \times \mathbb{P}^1$ be an irreducible curve of type (a, b). Let $\tilde{C}$ be its strict transform. By Lemma 3.4 we know that C cannot have a point of multiplicity $\geq \deg(C)$. By Chapter 5, Proposition 3.6 of [15],

$$(\tilde{Y}_i.\tilde{C}) = (\tilde{Y}_i.\pi^* C - \mu_{Q_i}(C) \cdot \tilde{Y}_i) = \mu_{Q_i}(C). \tag{3.4}$$

Now let $\mathrm{pr}_i : C \to \mathbb{P}^1$ be the projection to the i-th coordinate. Then $\deg \mathrm{pr}_1 = a,\ \deg \mathrm{pr}_2 = b$. This is to say, if we restrict C to $\mathbb{A}^2$, then the defining equation has degree b on X_1 and degree a on X_2. It follows that $\deg(C) \leq a+b$. By the Item 4 of Proposition 3.1, we have

$$\left(\pi^* A.\tilde{C}\right) = \left(A.\pi_* \tilde{C}\right) = (A.C) = a+b.$$

Then by Eq. (3.4) and linearity

$$\begin{aligned}(\tilde{A}.\tilde{C}) &= \left(\pi^* A.\tilde{C}\right) - \frac{1}{N}\left((\tilde{Y}_1.\tilde{C}) + \cdots + (\tilde{Y}_s.\tilde{C})\right)\\ &= a+b-\frac{1}{N}\left(\mu_{Q_1}(C) + \cdots + \mu_{Q_s}(C)\right)\\ &\geq a+b-\frac{1}{N}\cdot s\cdot(a+b)\\ &> 0\end{aligned}$$

as $N > s$.

We also have

$$\begin{aligned}(\tilde{A}.\tilde{Y}_i) &= \left(\pi^* A.\tilde{Y}_i\right) - \frac{1}{N}\left((\tilde{Y}_1.\tilde{Y}_i) + \cdots + (\tilde{Y}_s.\tilde{Y}_i)\right)\\ &= 0 - \frac{1}{N}\left(-\delta_{1i} - \cdots - \delta_{si}\right)\\ &= \frac{1}{N}.\end{aligned}$$

Finally by the previous equality

$$\begin{aligned}(\tilde{A}.\tilde{A}) &= \left(\tilde{A}.\,\pi^* A\right) - \frac{1}{N}\left((\tilde{A}.\,\tilde{Y}_1) + \cdots + (\tilde{A}.\,\tilde{Y}_s)\right)\\ &> \left(\pi_* \tilde{A}.\,A\right) - \frac{1}{N}\cdot\frac{s}{N}\\ &= (A.A) - \frac{s}{N^2}\\ &\geq 1+1-\frac{s}{N^2}\\ &> 0\end{aligned}$$

as $N > s$.

But

$$\operatorname{Pic}(\tilde{X}) = \pi^* \operatorname{Pic}(X) \bigoplus \bigoplus_{i=1}^{s} \mathbb{Z}\cdot\tilde{Y}_i,$$

and every effective curve C in $\tilde{X}$ is linearly equivalent to a non-negative combination of $\tilde{Y}_i$'s and the strict transform of effective curves in X, so $\tilde{A}$ is ample by the Nakai-Moishezon criterion (see Chapter 5, Theorem 1.10 of [15]). □

3.2 The proof, continued

We first prove the following modification of Theorem 2 of [28].

Theorem 3.5 *With notation as in Sect. 3.1, let K be a number field. Suppose $f \in K[t_1]$ and $g \in K[t_2]$ are square-free polynomials in one variable, Let*

$$Y = Z(f) \cap Z(g) \subseteq X = \mathbb{P}^1 \times \mathbb{P}^1$$

as in the Sect. 3.1. Also recall from there that $\tilde{X}$ is the blowup of X along Y.

Assume that Vojta's conjecture is true for $\tilde{X}$ over K. Fix $\varepsilon > 0$. Then there is a algebraic subset $V \subsetneq \mathbb{P}^1 \times \mathbb{P}^1$, depending on f, g and ε, so that for each $P = (x_1, x_2) \in \mathbb{P}^1(K) \times \mathbb{P}^1(K)$, either

1. *$P \in V$, or*
2. *$h_{\mathrm{gcd}}(f(x_1), g(x_2)) \leq (3 + \varepsilon)(h(x_1) + h(x_2)) + O(1)$.*

Proof of Theorem 3.5 We follow the proof in [28]. By Lemma 3.2 and assuming Vojta's Conjecture we have

$$h_{\tilde{X}, K_{\tilde{X}}}(\tilde{P}) \leq \varepsilon \cdot h_{\tilde{X}, \tilde{A}}(\tilde{P}) + C_\varepsilon$$

for all $P \in X(K) \backslash V(K)$. Also $K_{\tilde{X}} = \pi^* K_X + \tilde{Y}$ and $\tilde{A} = \pi^* A - 1/N \cdot \tilde{Y}$, so

$$\begin{aligned} h_{\tilde{X}, \pi^* K_X}(\tilde{P}) + h_{\tilde{X}, \tilde{Y}}(\tilde{P}) &\leq \varepsilon \cdot h_{\tilde{X}, \pi^* A}(\tilde{P}) - \frac{1}{N} \cdot h_{\tilde{X}, \tilde{Y}}(\tilde{P}) + C_\varepsilon, \\ h_{X, K_X}(P) + \left(1 + \frac{1}{N}\right) h_{\tilde{X}, \tilde{Y}}(P) &\leq \varepsilon \cdot h_{X, A}(P) + C'_\varepsilon, \\ \left(1 + \frac{1}{N}\right) h_{\mathrm{gcd}}(P; Y) &\leq \varepsilon \cdot h_{X, A}(P) + h_{X, -K_X}(P) + C'_\varepsilon, \\ h_{\mathrm{gcd}}(P; Y) &\leq \varepsilon \cdot h_{X, A}(P) + h_{X, -K_X}(P) + C''_\varepsilon. \end{aligned}$$

But K_X is linearly equivalent to $-2A$, and let $P = (x_1, x_2)$. Then

$$\begin{aligned} h_{X, -K_X}(P) &= 2 \cdot (h(x_1) + h(x_2)) + O(1), \\ h_{X, A}(P) &= h(x_1) + h(x_2), \\ h_{\mathrm{gcd}}(P; Y) &= h_{\mathrm{gcd}}(f(x_1), g(x_2)). \end{aligned}$$

Now Theorem 3.5 is verified. □

For the proof of Theorem 2.11 we need with the following

Lemma 3.6 *Let $\sigma, \tau \in K(x)$ be Möbius transforms defined over K. Set $f_\sigma = \sigma f \sigma^{-1}$, $g_\tau = \tau g \tau^{-1}$. Then there exists a constant $C > 0$, depending on $\alpha, \beta, f, g, \sigma, \tau$, such that for all $a, b \in K$, for all finite set $S \subset M(K)$ containing all the archimedean places and for all $n \in \mathbb{N}$, we have*

$$\left| h_{\mathrm{gcd}, S}\left(f_\sigma^{\circ n}(\sigma a) - \sigma\alpha, g_\tau^{\circ n}(\tau b) - \tau\beta\right) - h_{\mathrm{gcd}, S}(f^{\circ n}(a) - \alpha, g^{\circ n}(b) - \beta) \right| \leq C.$$

Proof It suffices to show that for any fixed $\alpha \in K$, and for any fixed Möbius transform σ, there exists a finite set $S' \subset M(K)_{\text{fin}}$ and a constant $C' > 0$, such that for all $x \in K$ and $v \in S'$, we have $\left|v^+(\sigma x - \sigma\alpha) - v^+(x-\alpha)\right| \leq C'$, and for all $x \in K$ and $v \in M(K)_{\text{fin}} \backslash S'$, we have $v^+(\sigma x - \sigma\alpha) = v^+(x-\alpha)$.

Since each Möbius transform defined over K is a composition of translations, dilations and inverses defined over K, it suffices to prove the result for the case when σ is one of the above three types of maps. The result is trivial for translations and dilations.

If $\sigma(x) = 1/x$, write $x = x_1/x_2, \alpha = \alpha_1/\alpha_2$, $x_1, x_2, \alpha_1, \alpha_2 \in \mathcal{O}_K$. Since the class number of K is finite, there exists $\gamma \in \mathcal{O}_K$ such that for fixed $\alpha \in \mathcal{O}_K$ and for all $x \in \mathcal{O}_K$ we can always choose $x_1, x_2, \alpha_1, \alpha_2$ such that the ideals $\gcd(x_1, x_2) \mid \gamma$, $\gcd(\alpha_1, \alpha_2) \mid \gamma$. Now

$$|x-a|_v = \left|\frac{\alpha_2 x_1 - \alpha_1 x_2}{\alpha_2 x_2}\right|_v, \quad |\sigma x - \sigma\alpha|_v = \left|\frac{\alpha_2 x_1 - \alpha_1 x_2}{\alpha_1 x_1}\right|_v.$$

But the ideal

$$\begin{aligned}\gcd(\alpha_2 x_1 - \alpha_1 x_2, \alpha_2 x_2) &\mid \gcd(\alpha_2^2 x_1 - \alpha_1\alpha_2 x_2, \alpha_1\alpha_2 x_2) = \gcd(\alpha_2^2 x_1, \alpha_1\alpha_2 x_2) \\ &\mid \gcd(\alpha_1\alpha_2^2 x_1, \alpha_1\alpha_2^2 x_2) \mid \alpha_1\alpha_2^2\gamma,\end{aligned}$$

so

$$v^+(\alpha_2 x_1 - \alpha_1 x_2) - v(\alpha_1\alpha_2^2\gamma) \leq v^+(x-\alpha) \leq v^+(\alpha_2 x_1 - \alpha_1 x_2).$$

Similarly

$$v^+(\alpha_2 x_1 - \alpha_1 x_2) - v(\alpha_1^2\alpha_2\gamma) \leq v^+(\sigma x - \sigma\alpha) \leq v^+(\alpha_2 x_1 - \alpha_1 x_2).$$

Therefore

$$\left|v^+(\sigma x - \sigma\alpha) - v^+(x-\alpha)\right| \leq \max\left(v(\alpha_1\alpha_2^2), v(\alpha_1^2\alpha_2\gamma)\right) \leq v(\alpha_1^2\alpha_2^2\gamma).$$

Hence we may choose $S' = \{v \in M(K)_{\text{fin}} \mid v(\alpha_1) \neq 0,\ v(\alpha_2) \neq 0 \text{ or } v(\gamma) \neq 0\}$. □

Lemma 3.7 (Lemma 3.52 of [29]) *Let $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ be a rational map of degree at least 2 and let $Q \in \mathbb{P}^1$ be a point such that Q is not a totally ramified fixed point of $\mathbb{P}^1$. Let $e_Q(\phi)$ be the multiplicity of ϕ at Q. Then*

$$\lim_{m\to\infty} \frac{e_Q(\phi^m)}{(\deg\phi)^m} = 0.$$

Proof of Theorem 2.11 By Lemma 3.6 for $h_{\gcd,S}$ we may assume that $\alpha = \beta = 0$. For any fixed integer D, write in the lowest terms $f^{\circ D} = F_1/F_2$ and $g^{\circ D} = G_1/G_2$ where F_1, F_2, G_1, G_2 are polynomials with coefficients in $\mathcal{O}_K$.

Write

$$\begin{aligned}F_1(x) &= a_0 + \cdots + a_N x^N,\\ F_2(x) &= b_0 + \cdots + b_M x^M,\\ G_1(x) &= a_0' + \cdots + a_{N'}' x^{N'},\\ G_2(x) &= b_0' + \cdots + b_{M'}' x^{M'}\end{aligned}$$

with all coefficients in $\mathcal{O}_K$. By Lemma 3.6 we may assume that all preimages of 0 under f and g are not ∞. This implies that $N \geq M$. Let

$$S := \{v \in M(K) \mid v(a_N) \neq 0,\ v(b_M) \neq 0,\ v(a_{N'}') \neq 0,\ \text{or } v(b_{M'}') \neq 0\} \cup M(K)_\infty.$$

Then S is finite. For each place $v \notin S$ and for any $x_0 \in K$, if $v(x_0) \geq 0$, then $v(F_2(x)) \geq 0$ and hence $v^+(f^{\circ D}(x_0)) \leq v^+\left(F_1(x_0)\right)$. If $v(x_0) < 0$, then

$$v^+(f^{\circ D}(x_0)) = v^+\left(\frac{a_N x_0^N}{b_M x_0^M}\right) = v^+\left(x_0^{N-M}\right) = 0 \leq v^+\left(F_1(x_0)\right).$$

In either case we have

$$v^+(f^{\circ D}(x_0)) \leq v^+\left(F_1(x_0)\right).$$

Similarly for any $v \notin S$ and for any $y_0 \in K$,

$$v^+(g^{\circ D}(y_0)) \leq v^+\left(G_1(y_0)\right).$$

Therefore the sum of the part of h_{gcd} outside S satisfies

$$\begin{aligned}h_{\text{gcd},S}\big(f^{\circ D}(a'), g^{\circ D}(b')\big) &:= \frac{1}{[K:\mathbb{Q}]}\sum_{v\in M(K)_{\text{fin}}\setminus S} n_v \min\left(v^+(f^{\circ D}(a')), v^+(g^{\circ D}(b'))\right)\\ &\leq \frac{1}{[K:\mathbb{Q}]}\sum_{v\in M(K)_{\text{fin}}\setminus S} n_v \min\left(v^+(F_1(a')), v^+(G_1(b'))\right)\\ &\leq h_{\text{gcd},S}\big(F_1(a'), G_1(b')\big). \qquad (3.5)\end{aligned}$$

Let $F_1^{\text{rad}}(x) = \text{rad}(F_1)(x)$, and let $G_1^{\text{rad}}(y) = \text{rad}(G_1)(y)$, where for a one-variable polynomial P, $\text{rad}(P)$ is the product of all monic irreducible polynomials dividing P. As the sequence $\big(f^{\circ(n-D)}(a), g^{\circ(n-D)}(b)\big)_n$ is generic in $\mathbb{P}^1(\overline{\mathbb{Q}}) \times \mathbb{P}^1(\overline{\mathbb{Q}})$, there exists $N'' = N''(\varepsilon, f, g, a, b$, such that for all $n \geq N''$ we have

$$\left(f^{\circ(n-D)}(a), g^{\circ(n-D)}(b)\right) \notin V(K) \qquad (3.6)$$

where V is as in Theorem 3.5. Apply Theorem 3.5 to the point $\big(f^{\circ(n-D)}(a), g^{\circ(n-D)}(b)\big)$ and the functions F_1^{rad} and G_1^{rad}, with $\varepsilon = 1$. Let $u = f^{\circ(n-D)}(a)$, $v = g^{\circ(n-D)}(b)$. Then

$$h_{\mathrm{gcd},S}\left(F_1^{\mathrm{rad}}(u), G_1^{\mathrm{rad}}(v)\right) \leq h_{\mathrm{gcd}}\left(F_1^{\mathrm{rad}}(u), G_1^{\mathrm{rad}}(v)\right) \leq 4\left(h\left(u\right)+h(v)\right)+O(1). \tag{3.7}$$

Let $M' = \sup E$ where

$$E = \cup_{(x,y)\in(f^{\circ D},\ g^{\circ D})^{-1}(0,0)}\left\{e_x(f^{\circ D}-0), e_y(g^{\circ D}-0)\right\}$$

where $e_Q(\phi)$ is the multiplicity of ϕ at Q. In the following inequalities, the implied constants only depend on $f, g, a, b, \alpha, \beta, D$. Compared with Theorem 2.11, we have an extra dependence with D. However, this dependence will be removed when ε is involved later. We have

$$\begin{aligned}
&h_{\mathrm{gcd},S}\left(f^{\circ n}(a), g^{\circ n}(b)\right)\\
&\quad= h_{\mathrm{gcd},S}\left(f^{\circ D}(f^{\circ(n-D)}(a)), g^{\circ D}(g^{\circ(n-D)}(b))\right)\\
&\quad\leq h_{\mathrm{gcd},S}\left(F_1(f^{\circ(n-D)}(a)), G_1(g^{\circ(n-D)}(b)))\right) \text{ (by (3.5))}\\
&\quad\leq h_{\mathrm{gcd},S}\left(\left(F_1^{\mathrm{rad}}\circ f^{\circ(n-D)}(a)\right)^{M'}, \left(G_1^{\mathrm{rad}}\circ g^{\circ(n-D)}(b)\right)^{M'}\right)+O(1)\\
&\quad\leq M'\cdot\left(4\cdot h\left(f^{\circ(n-D)}(a)\right)+4\cdot h\left(g^{\circ(n-D)}(b)\right)+O(1)\right)+O(1) \text{ (by (3.7))}\\
&\quad\leq M'\cdot\left(4d^{n-D}\cdot\hat{h}_f\left(a\right)+4d^{n-D}\cdot\hat{h}_g\left(b\right)+O(1)\right)+O(1) \text{ (by 2 of Theorem 2.1)}\\
&\quad\leq d^n\cdot\frac{M'}{d^D}\cdot\left(4\hat{h}_f(a)+4\hat{h}_g(b)+C\right)+O(1) \text{ (by 1 of Theorem 2.1).}
\end{aligned}$$

Since 0 is not exceptional for f or g, we know that they are not totally ramified fixed point of $f^{\circ 2}, g^{\circ 2}$ respectively. Indeed, if 0 were totally ramified fixed point of $f^{\circ 2}$, then

$$\cup_{i=1}^{\infty}(f^{\circ i})^{-1}(0) = \{0\}\cup f^{-1}(0)$$

is a finite set, and hence 0 is exceptional for f. Similar argument holds for g. Therefore by Lemma 3.7, we can choose $D = D(\varepsilon, f, g, a, b) \in \mathbb{N}$ sufficiently large so that

$$\frac{M'}{d^D}\cdot\left(4\hat{h}_f(a)+4\hat{h}_g(b)+C\right) < \frac{\varepsilon}{2}.$$

Thus, we have

$$h_{\mathrm{gcd},S}\left(f^{\circ n}(a), g^{\circ n}(b)\right) \leq \frac{\varepsilon}{2}\cdot d^n. \tag{3.8}$$

Now look at all places $v \in S$ and all infinite v. By assumption we know that 0 is not exceptional with respect to f and g and a and b are not preperiodic with respect to f and g. By Lemma 4.1 of [30] (cited below as Lemma 3.8, see also Theorem E of [26] for an archimedean version), we know for all sufficiently large $n \in \mathbb{N}$,

$$\begin{aligned} n_v v^+\left(f^{\circ n}(a)\right) &\leq \frac{\varepsilon}{2\cdot([K:\mathbb{Q}]+|S|)}\cdot d^n, \\ n_v v^+\left(g^{\circ n}(b)\right) &\leq \frac{\varepsilon}{2\cdot([K:\mathbb{Q}]+|S|)}\cdot d^n. \end{aligned} \tag{3.9}$$

Combining equations (2.4), (3.8) and (3.9), we obtain the requested estimate and hence finish up the proof of Theorem 2.11. □

Lemma 3.8 ([30]) *Let K be a number field and let ϕ be a rational function of degree $d \geq 2$ defined over K. Suppose 0 is exceptional with respect to ϕ and let a be a point in $\mathbb{P}^1(\overline{K})$ for which there is a strictly increasing sequence integers $(e_i)_{i=1}^{\infty}$ such that $\phi^{\circ e_i}(a) \neq 0$. Then*

$$\lim_{i\to\infty} \frac{v^+\left(\phi^{\circ e_i}(a)\right)}{d^{e_i}} = 0.$$

4 On the genericity condition

The Dynamical Mordell–Lang Conjecture predicts that given an endomorphism $\phi : X \to X$ of a complex quasi-projective variety X, for any point $P \in X$ and any subvariety $Y \subsetneq X$, the set $\{n \in \mathbb{N} \mid \phi^{\circ n}(P) \in Y\}$ is a finite union of arithmetic progressions (sets of the form $\{a, a+d, a+2d, \dots\}$ with $a, d \in \mathbb{N}_{\geq 0}$). The Dynamical Mordell–Lang Conjecture was proposed in [12]. See also [3,11] for earlier works. In the case of étale maps we know that the Dynamical Mordell–Lang Conjecture is true. See the recent monograph [4]. Xie proved in [32] the Dynamical Mordell–Lang Conjecture for polynomial endomorphisms of the affine plane.

Proof of Theorem 2.12 The result is clearly true in the case when (a, b) is preperiodic under (f, f). When (a, b) is not preperiodic under (f, f), by Theorem A it suffices to show that the sequence $(f^{\circ n}(a), f^{\circ n}(b))_n$ is generic. If there were infinitely many iterates $(f^{\circ n}(a), f^{\circ n}(b))$ lying on a curve C, then by Theorem 0.1 of [32], the Dynamical Mordell–Lang Conjecture for polynomial endomorphisms of the affine plane, we know C itself is periodic under (f, f). Replacing f by an iterate $f^{\circ m}$ we may assume that C is fixed under (f, f). Now we can apply the results of [20,22] classification for invariant curves. In fact, using these results Baker and DeMarco demonstrated in page 32 of [2] that the irreducible invariant curve in the above theorem must be a graph of the form $y = h(x)$ or $x = h(y)$, for a polynomial h which commutes with some $f^{\circ k}$ with initial conditions as in Theorem 2.12. This contradicts the assumption of Theorem 2.12. □

We give two examples to show that if the assumption of Theorem 2.12 is not verified, then we might not have the upper bound.

Example 4.1 Under the hypothesis of the above proof and use the same notation. Assume that the curve is given by $y = h(x)$ and $h \circ f^{\circ k} = f^{\circ k} \circ h$ for some $k \in \mathbb{N}_{>0}$. Suppose $n = mk$ with $k \in \mathbb{N}$. If $h(\alpha) = \alpha$, then

$$\begin{aligned} \gcd(f^{\circ n}(a) - \alpha, f^{\circ n}(b) - \alpha) &= \gcd(f^{\circ mk}(a) - \alpha, f^{\circ mk}(h(a)) - \alpha) \\ &= \gcd(f^{\circ mk}(a) - \alpha, h(f^{\circ mk}(a)) - h(\alpha)) \\ &= |f^{\circ mk}(a) - \alpha| = |f^{\circ n}(a) - \alpha|. \end{aligned}$$

Example 4.2 Let $f(x) = g(x) = x^3 + x$. Assume $a = -b$ and $\alpha = -\beta$. Then for $h(x) = -x$, we have $h \circ f = f \circ h$, $h(a) = b$ and $h(\alpha) = \beta$. Now

$$f^{\circ n}(a) - \alpha = f^{\circ n}(-b) + \beta = -f^{\circ n}(b) + \beta = -(g^{\circ n}(b) - \beta),$$

so

$$\gcd(f^{\circ n}(a) - \alpha, g^{\circ n}(b) - \beta) = |f^{\circ n}(a) - \alpha| \gg |a|^{\delta^n}$$

for any $\delta < 3$.

In the case of power maps, if $(f^{\circ n}(a), g^{\circ n}(b))_n$ is generic, the following unconditional result is proved by Corvaja and Zannier ([8]).

Example 4.3 Suppose K is a number field and suppose $a, b, \alpha, \beta \in K$. Also suppose that f and g are power maps, and a, b are multiplicatively independent. Let $d = \max(\deg f, \deg g)$, then for each fixed $\varepsilon > 0$, there exists some $C = C(f, g, a, b)$ such that

$$\gcd(f^{\circ n}(a) - \alpha, g^{\circ n}(b) - \beta) \leq C \cdot \max\left(h(a), h(b)\right)^{\varepsilon d^n}. \tag{4.1}$$

In fact, the genericity of the sequence $(f^{\circ n}(a), g^{\circ n}(b))_n$ is equivalent to the multiplicative independence of a and b. The assumption that α and β are not exceptional implies that $\alpha \neq 0$ and $\beta \neq 0$. Then Inequality (4.1) is a consequence of Inequality (1.2) of Corvaja and Zannier [8].

Now we provide an example to explain that the genericity of $(f^{\circ n}(a), f^{\circ n}(b))_n$ is necessary for power maps.

Example 4.4 Let $a = 125, b = 25, \alpha = \beta = 1, f(x) = x^2, g(y) = y^2$. Then $\gcd(f^{\circ n}(a) - \alpha, g^{\circ n}(b) - \beta)$ is divisible by $5^{2^n} - 1 = O\left((f^{\circ n}(a))^{1/3}\right)$.

5 When is the gcd large?

As we have seen, when the sequence $(f^{\circ n}(a), g^{\circ n}(b))_n$ is not generic, $\gcd(f^{\circ n}(a) - \alpha, g^{\circ n}(b) - \beta)$ might be big in general. Our goal in this section is to show the following result.

Theorem 5.1 *Assume Vojta's Conjecture. Suppose $f, g \in \mathbb{Z}[X]$ and $a, b, \alpha, \beta \in \mathbb{Z}$. Then for all $\eta > 0$,*

- *either the set*

$$\{n \in \mathbb{N} \mid \log \gcd(f^{\circ n}(a) - \alpha, g^{\circ n}(b) - \beta) \geq \eta \cdot d^n\}$$

  is a finite union of arithmetic progressions, or
- *there is a finite union of arithmetic progressions J such that*

$$\lim_{n \to \infty, n \in J} \frac{1}{\eta d^n} \cdot \log \gcd(f^{\circ n}(a) - \alpha, g^{\circ n}(b) - \beta) = 1.$$

Proof We choose D as in the proof of Theorem 2.11. That is, we choose $D = D(\varepsilon, f, g, a, b) \in \mathbb{N}$ sufficiently large so that

$$\frac{M'}{d^D} \cdot \left(4\hat{h}_f(a) + 4\hat{h}_g(b) + C\right) < \frac{\eta}{2}$$

where

$$M' = \max_{f^{\circ D}(x) = \alpha,\ g^{\circ D}(y) = \beta} \left(e_x(f^{\circ D} - \alpha), e_y(g^{\circ D} - \beta)\right).$$

Then the proof of Theorem 2.11 shows that assuming Vojta's Conjecture, there is a proper algebraic subset $V \subseteq \mathbb{P}^1 \times \mathbb{P}^1$ such that as long as $(f^{\circ(n-D)}(a), g^{\circ(n-D)}(b)) \notin V$ and n is sufficiently large, we have

$$\log \gcd(f^{\circ n}(a) - \alpha, g^{\circ n}(b) - \beta) < \frac{\eta}{2} \cdot d^n.$$

Let $I = \{n \in \mathbb{N} \mid (f^{\circ(n-D)}(a), g^{\circ(n-D)}(b)) \in V\}$. Then the set

$$\{n \in \mathbb{N} \backslash I \mid \log \gcd(f^{\circ n}(a) - \alpha, g^{\circ n}(b) - \beta) \geq \eta \cdot d^n\}$$

is finite. By the Dynamical Mordell–Lang Theorem for polynomial maps on the affine plane (cf. [32]), I is a finite union of arithmetic progressions. Hence it suffices to show that the set

$$\{n \in I \mid \log \gcd(f^{\circ n}(a) - \alpha, g^{\circ n}(b) - \beta) \geq \eta \cdot d^n\}$$

is a finite union of arithmetic progressions. Looking at each irreducible component of V, it is enough to consider the case when V is a curve. In that case the set

$$\{(f^{\circ n}(a) - \alpha, g^{\circ n}(b) - \beta) \mid n \in I\}$$

is contained in the curve $V' := f^{\circ(D)}(V) + (-\alpha, -\beta)$ where $+$ means translation on $\mathbb{A}^2$. By abuse of notation, we also donote by V' its Zariski closure in $\mathbb{P}^1 \times \mathbb{P}^1$. Suppose $\iota : V' \hookrightarrow \mathbb{P}^1 \times \mathbb{P}^1$ is the inclusion map.

Suppose $(x_1, x_2) \in V'$ and fix $D' \in \mathrm{Div}(V')$ of degree 1, then

$$\begin{aligned} h_{\mathrm{gcd}}(x_1, x_2) &= h_{\mathbb{P}^1 \times \mathbb{P}^1, (0,0)}(x_1, x_2) \\ &= h_{V',\, \iota^*(0,0)}(x_1, x_2) + O(1) \\ &= \deg(\iota^*(0,0)) \cdot h_{V', D'}(x_1, x_2) + O(1) \end{aligned}$$

where the last equality follows from Proposition B.3.5 of [16], due originally to Siegel.

Clearly it's enough to consider the case when a is not preperiodic under f and b is not preperiodic under g. In this case the projection $\pi_1 : V' \to \mathbb{P}^1,\ (x_1, x_2) \mapsto x_1$ is dominant. Fix $D \in \mathrm{Div}(\mathbb{P}^1)$ of degree 1. Then

$$h_{V', D'}(x_1, x_2) = \frac{1}{\deg(\pi_1)} \cdot h_{\mathbb{P}^1, D}(x_1) + O(1)$$

by Theorem 2.6. Now

$$\begin{aligned} h_{\mathrm{gcd}}(f^{\circ n}(a) - \alpha, g^{\circ n}(b) - \beta) &= \frac{\deg(\iota^*(0,0))}{\deg(\pi_1)} \cdot h_{\mathbb{P}^1, D}(f^{\circ n}(a) - \alpha) + O(1) \\ &= \frac{\deg(\iota^*(0,0))}{\deg(\pi_1)} \cdot \left(\hat{h}_f(a) \cdot d^n + O(1)\right) + O(1). \end{aligned}$$

Therefore, in the case when V' is a curve, if $\eta = \hat{h}_f(a) \cdot \dfrac{\deg(\iota^*(0,0))}{\deg(\pi_1)}$, then

$$\lim_{n \to \infty, n \in J} \frac{1}{\eta \cdot d^n} \cdot \log \gcd(f^{\circ n}(a) - \alpha, g^{\circ n}(b) - \beta) = 1$$

for a finite union of arithmetic progression J; otherwise the set

$$\{n \in I \mid \log \gcd(f^{\circ n}(a) - \alpha, g^{\circ n}(b) - \beta) \geq \eta \cdot d^n\}$$

is always a finite set or complement of a finite set. Hence for general V', for all but finitely many η, the set in the statement is a finite union of arithmetic progressions. □

Acknowledgements I want to express my gratitude to my advisor Thomas Tucker for suggesting this project and for many valuable discussions. I also would like to thank Joseph Silverman for useful comments on an earlier draft of this paper. I would like to thank the referee for many useful comments and suggestions. In addition, I want to thank Shouman Das, Wayne Peng, and Uğur Yiğit for proofreading this paper.

References

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

2. Baker, M., DeMarco, L.: Special curves and postcritically finite polynomials. Forum Math. **1**, e3, 35 (2013)
3. Bell, J.P.: A generalised Skolem–Mahler–Lech theorem for affine varieties. J. Lond. Math. Soc. (2) **73**(2), 367–379 (2006)
4. Bell, J.P., Ghioca, D., Tucker, T.J.: The Dynamical Mordell–Lang Conjecture, vol. 210. American Mathematical Society, Providence (2016)
5. Bombieri, E., Gubler, W.: Heights in Diophantine Geometry, volume 4 of New Mathematical Monographs. Cambridge University Press, Cambridge (2006)
6. Bugeaud, Y., Corvaja, P., Zannier, U.: An upper bound for the G.C.D. of $a^n - 1$ and $b^n - 1$. Math. Z. **243**(1), 79–84 (2003)
7. Call, G.S., Silverman, J.H.: Canonical heights on varieties with morphisms. Compos. Math. **89**(2), 163–205 (1993)
8. Corvaja, P., Zannier, U.: A lower bound for the height of a rational function at S-unit points. Monatsh. Math. **144**(3), 203–224 (2005)
9. Corvaja, P., Zannier, U.: Some cases of Vojta's conjecture on integral points over function fields. J. Algebraic Geom. **17**(2), 295–333 (2008)
10. Corvaja, P., Zannier, U.: 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), 1927–1942 (2013)
11. Denis, L.: Géométrie diophantienne sur les modules de Drinfel'd. In: The Arithmetic of Function Fields (Columbus, OH, 1991), volume 2 of Ohio State University, Mathematical Research Institute Publications, pp. 285–302. de Gruyter, Berlin (1992)
12. Ghioca, D., Tucker, T.J.: Periodic points, linearizing maps, and the dynamical Mordell–Lang problem. J. Number Theory **129**(6), 1392–1403 (2009)
13. Ghioca, D., Hsia, L.-C., Tucker, T.: A variant of a theorem by Ailon–Rudnick for elliptic curves. Pac. J. Math. **295**(1), 1–15 (2018)
14. Ghioca, D., Hsia, L.-C., Tucker, T.J.: On a variant of the Ailon–Rudnick theorem in finite characteristic. N.Y. J. Math. **23**, 213–225 (2017)
15. Hartshorne, R.: Algebraic Geometry, Graduate Texts in Mathematics, No. 52. Springer, New York (1977)
16. Hindry, M., Silverman, J.H.: Diophantine Geometry. Graduate Texts in Mathematics, vol. 201. Springer, New York (2000). An introduction
17. Hsia, L.-C., Tucker, T.: Greatest common divisors of iterates of polynomials. Algebra Number Theory **11**(6), 1437–1459 (2017)
18. Lang, S.: Fundamentals of Diophantine Geometry. Springer, New York (1983)
19. Levin, A.: Greatest common divisors and Vojta's conjecture for blowups of algebraic tori. Invent. Math. **215**(2), 493–533 (2019)
20. Medvedev, A., Scanlon, T.: Invariant varieties for polynomial dynamical systems. Ann. Math. (2) **179**(1), 81–177 (2014)
21. Ostafe, A.: On some extensions of the Ailon–Rudnick theorem. Monatsh. Math. **181**(2), 451–471 (2016)
22. Pakovich, F.: Polynomial semiconjugacies, decompositions of iterations, and invariant curves. Ann. Sc. Norm. Super. Pisa Cl. Sci. (5) **17**(4), 1417–1446 (2017)
23. Pakovich, F., Shparlinski, I.E.: Level curves of rational functions and unimodular points on rational curves (2018). arXiv:1805.02913v2
24. Pasten, H., Wang, J.T.-Y.: GCD bounds for analytic functions. Int. Math. Res. Notices **2017**(1), 47–95 (2017). https://doi.org/10.1093/imrn/rnw028
25. Silverman, J.H.: Arithmetic distance functions and height functions in Diophantine geometry. Math. Ann. **279**(2), 193–216 (1987)
26. Silverman, J.H.: Integer points, Diophantine approximation, and iteration of rational maps. Duke Math. J. **71**(3), 793–829 (1993)
27. Silverman, J.H.: Common divisors of $a^n - 1$ and $b^n - 1$ over function fields. N. Y. J. Math. **10**, 37–43 (2004). (electronic)
28. Silverman, J.H.: Generalized greatest common divisors, divisibility sequences, and Vojta's conjecture for blowups. Monatsh. Math. **145**(4), 333–350 (2005)
29. Silverman, J.H.: The Arithmetic of Dynamical Systems, volume 241 of Graduate Texts in Mathematics. Springer, New York (2007)

30. Szpiro, L., Tucker, T.J.: Equidistribution and generalized mahler measures. In: Number Theory, Analysis and Geometry, pp. 609–638. Springer, New York (2012)
31. Vojta, P.: Diophantine Approximations and Value Distribution Theory, volume 1239 of Lecture Notes in Mathematics, vol. 1239. Springer, Berlin (1987)
32. Xie, J: The dynamical Mordell–Lang conjecture for polynomial endomorphisms of the affine plane. Astérisque, **394**, vi+110 (2017)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.