Monatsh Math (2016) 181:451–471
DOI 10.1007/s00605-016-0911-3

On some extensions of the Ailon–Rudnick theorem

Alina Ostafe[1]

Received: 31 May 2015 / Accepted: 18 April 2016 / Published online: 30 April 2016

Abstract In this paper we present some extensions of the Ailon–Rudnick theorem, which says that if $f, g \in \mathbb{C}[T]$, then $\gcd(f^n - 1, g^m - 1)$ is bounded for all $n, m \geq 1$. More precisely, using a uniform bound for the number of torsion points on curves and results on the intersection of curves with algebraic subgroups of codimension at least 2, we present two such extensions in the univariate case. We also give two multivariate analogues of the Ailon–Rudnick theorem based on Hilbert's irreducibility theorem and a result of Granville and Rudnick about torsion points on hypersurfaces.

Keywords Greatest common divisor · Polynomials

Mathematics Subject Classification 11R58 · 11D61

1 Introduction

1.1 Motivation

Let a, b be multiplicatively independent positive integers and $\varepsilon > 0$. Bugeaud et al. [9] have proved that

$$\gcd\left(a^n - 1, b^n - 1\right) \leq \exp(\varepsilon n)$$

Communicated by A. Constantin.

✉ Alina Ostafe
alina.ostafe@unsw.edu.au

[1] School of Mathematics and Statistics, University of New South Wales, Sydney, NSW 2052, Australia

as n tends to infinity. Corvaja and Zannier [10] have generalised this result and replaced a^n, b^n with multiplicatively independent S-units $u, v \in \mathbb{Z}$.

In the function field case, Ailon and Rudnick [1, Theorem 1] proved that if $f, g \in \mathbb{C}[T]$ are multiplicatively independent polynomials, then there exists $h \in \mathbb{C}[T]$ such that

$$\gcd(f^n - 1, g^n - 1) \mid h \tag{1.1}$$

for all $n \geq 1$. Examining their argument one can easily see that the same statement holds in a larger generality; namely there exists $\widetilde{h} \in \mathbb{C}[T]$ such that

$$\gcd(f^n - 1, g^m - 1) \mid \widetilde{h} \tag{1.2}$$

for all $n, m \geq 1$.

In the case of finite fields $\mathbb{F}_q$ of characteristic p, Silverman [36] proves that even more restrictions on the polynomials $f, g \in \mathbb{F}_q[T]$ do not allow a similar conclusion as the result of [1]. In particular, Silverman proves that the analogue of (1.1) is false in a very strong sense: there exists a constant $c(f, g; q)$, depending only on f, g and q, such that

$$\deg \gcd(f^n - 1, g^n - 1) \geq c(f, g; q)n$$

for infinitely many n.

More results in positive characteristic are obtained in [13,15], as well as variants for elliptic divisibility sequences [37,38].

In this paper we present some extensions of the Ailon–Rudnick Theorem [1, Theorem 1] over $\mathbb{C}$, both in the univariate and multivariate cases. Although the method of proof in the univariate case is similar to, or reduces to using [1], we find these extensions exciting and we hope they will be of independent interest. Moreover, as we explain below, in certain situation we reduce our problem to applying [1, Theorem 1], however for this we need a uniform bound for (1.1) that depends only on the degree of the polynomials f and g.

Besides the generality of results, the new ingredients of the paper are employing results [5–7,27] on the number of points on intersections of curves in the n-dimensional multiplicative torus $\mathbb{G}_m^n$ with algebraic subgroups. We also present two multivariate generalisations that are based on the use of Hilbert's irreducibility theorem [31] and a transformation using the Kronecker substitution to reduce the problem to the univariate case, as well as a result of Granville and Rudnick [20] about torsion points on hypersurfaces.

1.2 Conventions and notation

We denote by $\mathbb{C}[X_1, \ldots, X_\ell]$ the polynomial ring in ℓ variables and $\mathbb{C}(X_1, \ldots, X_\ell)$ the field of rational functions F/G, $F, G \in \mathbb{C}[X_1, \ldots, X_\ell]$. When working with univariate polynomials we reserve the variable T. All polynomials in $\mathbb{C}[T]$ are denoted with small letters $f, g, \ldots$, and for polynomials in $\mathbb{C}[X_1, \ldots, X_\ell]$ we use capital letters $F, G, \ldots$.

Throughout the paper, for a univariate polynomial $f \in \mathbb{C}[T]$, the notation d_f is used for the degree of f.

For a family of polynomials $F_1, \ldots, F_s \in \mathbb{C}[X_1, \ldots, X_\ell]$, we denote by $Z(F_1, \ldots, F_s)$ their set of common zeros in $\mathbb{C}^\ell$.

Throughout the paper we assume that the greatest common divisor of two (or more) polynomials is monic, so it is well-defined.

We also define here the main concept of this paper.

Definition 1.1 The polynomials $F_1, \ldots, F_s \in \mathbb{C}[X_1, \ldots, X_\ell]$ are called *multiplicatively independent* if there does not exist a nonzero vector $(\nu_1, \ldots, \nu_s) \in \mathbb{Z}^s$ such that

$$F_1^{\nu_1} \ldots F_s^{\nu_s} = 1.$$

Similarly, we say that the polynomials $F_1, \ldots, F_s \in \mathbb{C}[X_1, \ldots, X_\ell]$ are *multiplicatively independent in the group* $\mathbb{C}(X_1, \ldots, X_\ell)^*/\mathbb{C}^*$ if there do not exist a nonzero vector $(\nu_1, \ldots, \nu_s) \in \mathbb{Z}^s$ and $a \in \mathbb{C}^*$ such that

Finally, we define $\mathbb{G}_m^k$ as the set of k-tuples of non-zero complex numbers equipped with the group law defined by component-wise multiplication. We refer to [31, Appendix by Umberto Zannier] for necessary definitions on algebraic subgroups.

$$F_1^{\nu_1} \ldots F_s^{\nu_s} = a.$$

We present now in more details the main results of this paper.

1.3 Our results: univariate case

Section 2 is dedicated to outlining the tools and results needed along the paper. In particular, in Sect. 2.1 we recall the result of [1, Theorem 1] and, using a uniform bound for the number of points on a curve with coordinates roots of unity due to Beukers and Smyth [5], we derive in Lemma 2.2 a version of (1.2) that gives an upper bound on $\deg \gcd(f^n - 1, g^m - 1)$ that depends only the degrees of f and g (rather than on the polynomials themselves).

Such a uniform bound is crucial for some of our main results presented below and proved in Sect. 3. In particular, our first extension of [1, Theorem 1], which is proved in Sect. 3.1, is based on this uniform bound.

Theorem 1.2 *Let $f, g, h_1, h_2 \in \mathbb{C}[T]$. If f and g are multiplicatively independent in $\mathbb{C}(T)^*/\mathbb{C}^*$, then for all $n, m \geq 1$ we have*

$$\deg \gcd\left(h_1\left(f^n\right), h_2\left(g^m\right)\right) \leq d_{h_1} d_{h_2} \left(11 d_* (d_f + d_g)^2\right)^{d_*},$$

where $d_* = \min\{d_f, d_g\}$.

For the second extension of [1, Theorem 1], which is proved in Sect. 3.2, we apply the finiteness result of [7,27], see also [6], for the number of points on the intersection

of curves in $\mathbb{G}_m^n$ with algebraic subgroups, see Lemma 2.3. No uniform bounds are known so far for such finiteness results.

We recall that for a polynomial $f \in \mathbb{C}[T]$, we denote by $Z(f)$ the set of zeros of f in $\mathbb{C}$.

Theorem 1.3 *Let $f_1, \ldots, f_\ell, \varphi_1, \ldots, \varphi_k, g_1, \ldots, g_r, \psi_1, \ldots, \psi_s \in \mathbb{C}[T]$, $\ell, k, r, s \geq 1$, be multiplicatively independent polynomials such that*

$$Z(f_1 \ldots f_\ell) \cap Z(\varphi_1 \ldots \varphi_k) = \emptyset, \quad Z(g_1 \ldots g_r) \cap Z(\psi_1 \ldots \psi_s) = \emptyset. \tag{1.3}$$

Then we have:

1. *For all $n_1, \ldots, n_\ell, \nu_1, \ldots, \nu_k, m_1, \ldots, m_r, \mu_1, \ldots, \mu_s \geq 0$, there exists a polynomial $h \in \mathbb{C}[T]$ such that*

$$\gcd\left(\prod_{i=1}^{\ell} f_i^{n_i} - \prod_{i=1}^{k} \varphi_i^{\nu_i}, \prod_{i=1}^{r} g_i^{m_i} - \prod_{i=1}^{s} \psi_i^{\mu_i}\right) \mid h.$$

2. *If in addition*

$$\gcd(f_1 \ldots f_\ell - 1, g_1 \ldots g_r - 1) = 1,$$

then there exists a finite set S and monoids $\mathcal{L}_t \subseteq \mathbb{N}^{\ell+k+r+s}$, $t \in S$, such that the remaining set

$$\mathcal{N} = \mathbb{N}^{\ell+k+r+s} \setminus \cup_{t \in S} \mathcal{L}_t$$

is of positive asymptotic density and for any vector

$$(n_1, \ldots, n_\ell, \nu_1, \ldots, \nu_k, m_1, \ldots, m_r, \mu_1, \ldots, \mu_s) \in \mathcal{N}$$

we have

$$\gcd\left(\prod_{i=1}^{\ell} f_i^{n_i} - \prod_{i=1}^{k} \varphi_i^{\nu_i}, \prod_{i=1}^{r} g_i^{m_i} - \prod_{i=1}^{s} \psi_i^{\mu_i}\right) = 1.$$

Although we prefer to keep the language of polynomials, one can easily see that Theorem 1.3 can be reformulated in terms of S-units in $\mathbb{C}[T]$ and implies that for any set of S-units, there exists a polynomial $h \in \mathbb{C}[T]$ such that for any multiplicatively independent S-units U, V we have

$$\gcd(U - 1, V - 1) \mid h.$$

In particular, this extension of [1] is fully analogous to the aforementioned extension of [10] over [9].

We also compare Theorem 1.3, which for multiplicatively independent S-units U, V, gives a uniform bound for $\deg \gcd(U-1, V-1)$, while the result of Corvaja and Zannier [12, Corollary 2.3] gives

$$\deg \gcd(U-1, V-1) \ll \max\{\deg U, \deg V\}^{2/3}.$$

However, [12, Corollary 2.3] applies to more general situations.

It is interesting to unify Theorems 1.2 and 1.3 and obtain a similar result for

$$\gcd\left(h_1\left(f_1^{n_1}\dots f_\ell^{n_\ell}\right), h_2\left(g_1^{m_1}\dots g_r^{m_r}\right)\right),$$

where $h_1, h_2 \in \mathbb{C}[T]$. Similar ideas may work for this case however they require a uniform bound for the number of points on intersections of curves in $\mathbb{G}_m^{\ell+r}$ with algebraic subgroups of dimension $k \le \ell + r - 2$ in Lemma 2.3. We note that for $\ell = r = 1$ this was possible due to the uniform bounds of [5]. However, no such bounds are available in the more general case that we need.

1.4 Our results: multivariate case

For our first result in the multivariate case, we reduce the problem to the univariate case using Hilbert's irreducibility theorem (see Sect. 2.4), and to control the degree for such specialisation we also couple this approach with a transformation involving the Kronecker substitution. We obtain:

Theorem 1.4 *Let $h_1, h_2 \in \mathbb{C}[T]$ and $F, G \in \mathbb{C}[X_1, \dots, X_\ell]$. We define $D = \max_{i=1\dots,\ell}\left\{\deg_{X_i} F, \deg_{X_i} G\right\}$. If F, G are multiplicatively independent in $\mathbb{C}(X_1, \dots, X_\ell)^*/\mathbb{C}^*$, then for all $n, m \ge 1$ we have*

$$\deg \gcd\left(h_1\left(F^n\right), h_2\left(G^m\right)\right) \le d_{h_1} d_{h_2}\left(44(D+1)^{2\ell}\right)^{(D+1)^\ell}.$$

We note that if $h_1 = h_2 = T - 1$ as in [1, Theorem 1], then in Theorem 1.4 we need F, G to be just multiplicatively independent.

Theorem 1.4 is proved in Sect. 3.3.

Another natural extension of [1, Theorem 1] to the multivariate case is related to the fact that the greatest common divisor of two univariate polynomials is given by their common zeros. Thus [1, Theorem 1] says that the number of common zeros of $f^n - 1$ and $g^m - 1$, for two polynomials $f, g \in \mathbb{C}[T]$, is bounded by a constant depending only on f and g for all $n, m \ge 1$, and Lemma 2.2 gives a uniform bound.

For positive integers $\ell, D \ge 1$, we denote

$$\gamma_\ell(D) = \binom{\ell + 1 + D^\ell}{\ell + 1}. \tag{1.4}$$

We now obtain the following result proved in Sect. 3.4. This multivariate generalisation is based on a result of Granville and Rudnick [20, Corollary 3.1], which describes the structure of torsion points on hypersurfaces, see Lemma 2.5.

Theorem 1.5 *Let $F_1, \ldots, F_{\ell+1} \in \mathbb{C}[X_1, \ldots, X_\ell]$ be multiplicatively independent polynomials of degree at most D. Then*

$$\bigcup_{n_1,\ldots,n_{\ell+1}\in\mathbb{N}} Z\left(F_1^{n_1} - 1, \ldots, F_{\ell+1}^{n_{\ell+1}} - 1\right)$$

is contained in at most

$$N \le (0.792\gamma_\ell(D)/\log(\gamma_\ell(D) + 1))^{\gamma_\ell(D)}$$

algebraic varieties, each defined by at most $\ell + 1$ polynomials of degree at most $(\ell + 1)D^\ell \prod_{p\le\gamma_\ell(D)} p$, where the product runs over all primes $p \le \gamma_\ell(D)$.

We recall that by the prime number theorem, for an integer $k \ge 1$,

$$\prod_{p\le k} p = \exp(k + o(k)).$$

We note that a bound on the number of algebraic subgroups that contain the points on $\mathcal{H}$ with coordinates roots of unity can also be derived from [2, Theorem 1.1], which says that, for a hypersurface defined by $H \in \mathbb{C}[X_1, \ldots, X_s]$, $s \ge 2$, of degree D, the number of maximal torsion cosets contained in $\mathcal{H}$ is at most

$$c_1(s)D^{c_2(s)}$$

with

$$c_1(s) = s^{\frac{3}{2}(2+s)5^s} \quad \text{and} \quad c_2(s) = \frac{1}{16}\left(49 \cdot 5^{s-2} - 4s - 9\right).$$

We also note that any argument that is based on the Bezout theorem ultimately leads to bounds that depend on the exponents $n_1, \ldots, n_{\ell+1}$, while the bounds of Theorem 1.5 depend only on the initial data.

We conclude the paper with comments on future work.

2 Preliminaries

2.1 The Ailon–Rudnick theorem

The Ailon–Rudnick theorem is based on a well-known conjecture of Lang, proved by Ihara, Serre and Tate [23], which says that a plane curve, which does not contain a translate of an algebraic subgroup of $\mathbb{G}_m^2$, contains only finitely many torsion points. In this case, Beukers and Smyth [5, Section 4.1] give a uniform bound for the number of such points (see Lemma 2.1 below), and Corvaja and Zannier [11] give an upper bound (actually for curves in $\mathbb{G}_m^n$) for the maximal order of torsion points on the curve.

We now present the result of Ailon and Rudnick [1, Theorem 1], coupled with the result of Beukers and Smyth [5, Section 4.1], which we first mention separately.

Lemma 2.1 *An algebraic curve $H(X, Y) = 0$ has at most $11(\deg H)^2$ points which are roots of unity, unless H has a factor of the form $X^i - \rho Y^j$ or $X^i Y^j - \rho$ for some nonnegative integers i, j not both zero and some root of unity ρ.*

Using Lemma 2.1, we obtain the following more precise form of [1, Theorem 1].

Lemma 2.2 *Let $f, g \in \mathbb{C}[T]$ be non constant polynomials. If f and g are multiplicatively independent, then there exists a polynomial $h \in \mathbb{C}[T]$ with*

$$\deg h \leq \left(11 d_*(d_f + d_g)^2\right)^{d_*},$$

where $d_* = \min\{d_f, d_g\}$, such that

$$\gcd(f^n - 1, g^m - 1) \mid h$$

for all $n, m \geq 1$.

Proof The proof, except for the explicit bound for the degree, is given in [1, Theorem 1]. In particular, from the proof of [1, Theorem 1], the polynomial $h \in \mathbb{C}[T]$ is defined by

$$h(T) = \prod_{t \in S} (T - t)^{d_*}, \tag{2.1}$$

where S is the finite set of $t \in \mathbb{C}$ such that both $f(t)$ and $g(t)$ are roots of unity.

To see the degree bound, we just apply Lemma 2.1. Our curve is given in parametric form $\{(f(t), g(t)) \ : \ t \in \mathbb{C}\}$ and we need to find the degree of the implicit form H such that $H(f(t), g(t)) = 0, t \in \mathbb{C}$. This is obtained using resultants, that is,

$$H = \mathrm{Res}_T \left(f(T) - X_1, g(T) - X_2\right),$$

which is a polynomial of degree d_g in X_1 and d_f in X_2. Thus, the total degree of H is at most $d_f + d_g$.

Let $\widetilde{H}$ be an absolutely irreducible factor of H and assume that $\widetilde{H}(f(t), g(t)) = 0$ for infinitely many $t \in \mathbb{C}$. As $\widetilde{H}(f(T), g(T))$ is a univariate polynomial , we must have the identity $\widetilde{H}(f(T), g(T)) = 0$. Then, by Lemma 2.1 applied with the curve defined by the polynomial $\widetilde{H}$, we obtain that $\widetilde{H}$ is of the form $X_1^{n_1} X_2^{n_2} = \omega$, for some root of unity ω and integers n_1, n_2 not both zero. This implies that f, g are multiplicatively dependent, which contradicts the hypothesis. Thus, there is no such absolutely irreducible divisor of H.

Therefore, the number of torsion points of the form $(f(t), g(t)), t \in \mathbb{C}$, is at most $11(d_f + d_g)^2$. Taking into account that the largest possible number of preimages for each pair $(f(t), g(t))$ is at most d_*, we get the bound

$$\#S \leq 11 d_*(d_f + d_g)^2.$$

The degree bound of the polynomial h now follows from (2.1). □

2.2 Intersection of curves with algebraic groups

One of the main tools in our paper is a result on the finiteness of the number of points on the intersection of a curve in $\mathbb{G}_m^k$ with algebraic subgroups of codimension at least 2, initially obtained in [6] for curves over $\overline{\mathbb{Q}}$, and later on extended over $\mathbb{C}$, see [7,27] and references therein. We present it in the following form.

Lemma 2.3 *Let $C \subset \mathbb{G}_m^k$, $k \geq 2$, be an irreducible curve over $\mathbb{C}$. Assume that for every nonzero vector $(r_1, \ldots, r_k) \in \mathbb{Z}^k$ the monomial $X_1^{r_1} \ldots X_k^{r_k}$ is not identically 1 on C. Then there are finitely many points $(x_1, \ldots, x_k) \in C(\mathbb{C})$ for which there exist linearly independent vectors $(a_1, \ldots, a_k)$, $(b_1, \ldots, b_k)$ in $\mathbb{Z}^k$ such that*

$$x_1^{a_1} \ldots x_k^{a_k} = x_1^{b_1} \ldots x_k^{b_k} = 1.$$

Remark 2.4 As explained in [6], the condition of Lemma 2.3 that the monomial $X_1^{r_1} \ldots X_k^{r_k}$ is not identically 1 on C is equivalent with the curve not being contained in a proper subtorus of $\mathbb{G}_m^k$.

2.3 Torsion points on hypersurfaces

Results regarding uniform bounds on the number of torsion points in subvarieties of $\mathbb{G}_m^k$ go back to work of Bombieri and Zannier [8], Schlickewei [32] and Evertse [14]. For example, Evertse [14], improving bounds of Schlickewei [32], shows that the number of non-degenerate solutions in roots of unity to the equation $a_1x_1 + \cdots + a_kx_k = 1$, $a_1, \ldots, a_k \in \mathbb{C}$, is at most $(k+1)^{3(k+1)^2}$.

For our results we use the following result of Granville and Rudnick, see [20, Corollary 3.1], which describes the structure of the algebraic subgroups that contain the roots of unity on a hypersurface. Although the statement of their result does not contain the bound for the degree or the number of the polynomials defining the algebraic subgroups, this follows directly from or is explicitly stated in their proof. Moreover, we recall this result only for the case of hypersurfaces, however their result holds for any algebraic variety.

Lemma 2.5 *Let $\mathcal{H} = Z(H)$ be a hypersurface in $\mathbb{C}^k$ defined by a polynomial $H \in \mathbb{C}[X_1, \ldots, X_k]$ of degree D and with $s(H)$ terms. There exists a finite list $\mathcal{B}$ of at most*

$$N(H) \leq (0.792s(H)/\log(s(H)+1))^{s(H)}$$

integer $k \times k$ matrices $B = (b_{j,i})$, $i, j = 1, \ldots, k$, and

$$|b_{j,i}| \leq D \prod_{p \leq s(H)} p,$$

where the product runs over all primes $p \le s(H)$, such that if $\xi \in \mathcal{H}$ is a torsion point, then $\xi \in \cup_{B\in\mathcal{B}} W_B$, where

$$W_B = \bigcap_{j=1}^{k} Z\left(X_1^{b_{j,1}} X_2^{b_{j,2}} \dots X_k^{b_{j,k}} - 1\right).$$

Proof The proof is essentially given in [20, Corollary 3.1]. Indeed, each matrix B corresponds to a partition of the set $\{1, 2, \dots, s(H)\}$, and thus, the number of matrices B in the set $\mathcal{B}$ is given by the number of such partitions, which, by [4, Theorem 2.1], is at most $N(H)$.

The number of rows n_B of a matrix $B \in \mathcal{B}$ is not specified in [20, Corollary 3.1]. However, we can choose the largest linear independent set of these vectors $\mathbf{b}_j$, which is of cardinality at most k, and all other varieties of the form $Z\left(X_1^{b_{i,1}} X_2^{b_{i,2}} \dots X_k^{b_{i,k}} - 1\right)$ are defined by combinations of these vectors. Thus, we can consider $n_B \le k$. Repeating some rows if necessary we can take $n_B = k$ which concludes the proof. □

2.4 Hilbertian fields and multiplicative independence

For the first multivariate generalisation of [1, Theorem 1] we need a result which says that given $F_1, \dots, F_s \in \mathbb{C}[X_1, \dots, X_\ell]$ that are multiplicatively independent in $\mathbb{C}(X_1, \dots, X_\ell)^*/\mathbb{C}^*$, there exists a specialisation $(\alpha_2, \dots, \alpha_\ell) \in \mathbb{C}^{\ell-1}$ such that $F_i(X_1, \alpha_2, \dots, \alpha_\ell), i = 1, \dots, s$, are multiplicatively independent in $\mathbb{C}(X_1)^*/\mathbb{C}^*$ (see Lemma 2.8 below). Such a result follows directly from [6, Theorem 1] which says that the points lying in the intersection of a curve $\mathcal{C}$, not contained in any translate of a proper subtorus of $\mathbb{G}_m^\ell$, with the union of all proper algebraic subgroups is of bounded height (see also [6, Theorem 1]).

Furthermore, this also follows from previous work of Néron [28] (see also [33, Chapter 11]), Silverman [34, Theorem C] and Masser [25] (see also [40, Notes to Chapter 1] where Masser's method is explained) on specialisations of finitely generated subgroups of abelian varieties. In particular, Masser's result [25] gives explicit bounds for the least degree of a hypersurface containing the set of exceptional points, that is, points that lead to multiplicative dependence, of bounded degree and height.

Although the above results are sufficient for our purpose, for the sake of completeness we now give a simple self-contained proof that follows directly from Hilbert's irreducibility theorem, see [31, Theorem 46]. Moreover, this proof does not appeal to the notion of height and applies to arbitrary Hilbertian fields (see Definition 2.6 below), rather than to just finite extensions of $\mathbb{Q}$.

Definition 2.6 We say that a field $\mathbb{K}$ is Hilbertian if for any irreducible polynomials $P_1, \dots, P_r \in \mathbb{K}[X_1, \dots, X_\ell]$ over $\mathbb{K}$ there exists a specialisation $(\alpha_2, \dots, \alpha_\ell) \in \mathbb{K}^{\ell-1}$ such that $P_i(X_1, \alpha_2, \dots, \alpha_\ell), i = 1, \dots, r$, are all irreducible over $\mathbb{K}$.

In particular, by the famous Hilbert's irreducibility theorem, any finite extension of $\mathbb{Q}$ is a Hilbertian field. Furthermore, by [31, Theorem 49] every finitely generated

infinite field and every finitely generated transcendental extension of an arbitrary field are Hilbertian.

We prove first the following simple fact.

Lemma 2.7 *Let $\mathbb{K}$ be a field and $F, G \in \mathbb{K}[X_1, \ldots, X_\ell]\backslash\mathbb{K}[X_\ell]$ non-constant polynomials such that $F/G \notin \mathbb{K}(X_\ell)$. Then, there are only finitely many $\alpha \in \mathbb{K}$ such that the polynomials $F(X_1, \ldots, X_{\ell-1}, \alpha)$ and $G(X_1, \ldots, X_{\ell-1}, \alpha)$ are proportional.*

Proof We write

$$\begin{aligned} F(X_1, \ldots, X_{\ell-1}, \alpha) &= \sum_{i_1,\ldots,i_{\ell-1}} f_{i_1,\ldots,i_{\ell-1}}(\alpha) X_1^{i_1} \ldots X_{\ell-1}^{i_{\ell-1}}, \\ G(X_1, \ldots, X_{\ell-1}, \alpha) &= \sum_{j_1,\ldots,j_{\ell-1}} g_{j_1,\ldots,j_{\ell-1}}(\alpha) X_1^{j_1} \ldots X_{\ell-1}^{j_{\ell-1}}, \end{aligned} \tag{2.2}$$

for some polynomials $f_{i_1,\ldots,i_{\ell-1}}, g_{j_1,\ldots,j_{\ell-1}} \in \mathbb{K}[X_\ell]$.

We exclude finitely many $\alpha \in \mathbb{K}$ for which the coefficients $f_{i_1,\ldots,i_{\ell-1}}(\alpha)$ and $g_{j_1,\ldots,j_{\ell-1}}(\alpha)$ are zero. For the rest of $\alpha \in \mathbb{K}$, the polynomials $F(X_1, \ldots, X_{\ell-1}, \alpha)$ and $G(X_1, \ldots, X_{\ell-1}, \alpha)$ are proportional if there exists a constant $a \in \mathbb{K}^*$ such that

$$F(X_1, \ldots, X_{\ell-1}, \alpha) = aG(X_1, \ldots, X_{\ell-1}, \alpha). \tag{2.3}$$

If both F and G are monomials, then (2.3) is possible for either $\alpha = 0$, or the case when $F/G \in \mathbb{K}(X_\ell)$, which contradicts our assumption.

If at least one of F and G is not a monomial, by comparing the coefficients of the monomials in (2.3), we obtain at least one nontrivial equation of the type

$$f_{i_1,\ldots,i_{\ell-1}}(\alpha) g_{j_1,\ldots,j_{\ell-1}}(\alpha) = f_{j_1,\ldots,j_{\ell-1}}(\alpha) g_{i_1,\ldots,i_{\ell-1}}(\alpha),$$

for some vectors of indices $(i_1, \ldots, i_{\ell-1})$, $(j_1, \ldots, j_{\ell-1})$ which define the monomials of the polynomials in (2.2). As the number of solutions α to such univariate equations is at most their degree, we conclude the proof. □

We now have the following result which is essential for the proof of Theorem 1.4.

Lemma 2.8 *Let $\mathbb{K}$ be a Hilbertian field and $F_1, \ldots, F_s \in \mathbb{K}[X_1, \ldots, X_\ell]$ multiplicatively independent polynomials in $\mathbb{K}(X_1, \ldots, X_\ell)^*/\mathbb{K}^*$ such that all their irreducible factors belong to $\mathbb{K}[X_1, \ldots, X_\ell]\backslash\mathbb{K}[X_2, \ldots, X_\ell]$. Then, there exists a specialisation $(\alpha_2, \ldots, \alpha_\ell) \in \mathbb{K}^{\ell-1}$ such that the polynomials $F_i(X_1, \alpha_2, \ldots, \alpha_\ell)$, $i = 1, \ldots, s$, are multiplicatively independent in $\mathbb{K}(X_1)^*/\mathbb{K}^*$.*

Proof We order all monomials lexicographically (with X_1 being the leading variable) which in a natural way leads to the notion of the leading coefficient. Thus we say that $F \in \mathbb{K}[X_1, \ldots, X_\ell]$ is *monic* if the leading coefficient is 1. Let $P_1, \ldots, P_r \in \mathbb{K}[X_1, \ldots, X_\ell]\backslash\mathbb{K}[X_2, \ldots, X_\ell]$ be the distinct monic irreducible factors of $F_1, \ldots, F_s$, that is, we have the factorisation

$$F_i = a_i P_1^{e_{i,1}} \ldots P_r^{e_{i,r}}, \quad \text{with } a_i \in K^*, \quad i = 1, \ldots, s.$$

We note that the polynomials $F_1, \dots, F_s$ are multiplicatively independent in $\mathbb{K}(X_1, \dots, X_\ell)^*/\mathbb{K}^*$ if and only if the matrix $(e_{i,j})_{\substack{1\le i\le s\\ 1\le j\le r}}$ has full rank.

Since $\mathbb{K}$ is Hilbertian, there exists a specialisation $(\alpha_2, \dots, \alpha_\ell) \in \mathbb{K}^{\ell-1}$ such that $P_j(X_1, \alpha_2, \dots, \alpha_\ell)$, $j = 1, \dots, r$, are all distinct (up to a constant factor) and irreducible over $\mathbb{K}$. Indeed, this follows recursively from Hilbert's irreducibility theorem coupled with Lemma 2.7. First we specialise only the last variable X_ℓ, and by Hilbert's irreducibility theorem there are infinitely many α_ℓ such that $P_j(X_1, \dots, X_{\ell-1}, \alpha_\ell)$, $j = 1, \dots, r$, are all irreducible. However, by Lemma 2.7 there are only finitely many such α_ℓ leading to proportional polynomials, which concludes this case. We fix now $\alpha_\ell \in \mathbb{K}$ such that $P_j(X_1, \dots, X_{\ell-1}, \alpha_\ell)$, $j = 1, \dots, r$, are all distinct (up to a constant factor) and irreducible over $\mathbb{K}$ and choose $\alpha_{\ell-1}$ in the same way. We continue till we find $(\alpha_2, \dots, \alpha_\ell) \in \mathbb{K}^{\ell-1}$ such that $P_j(X_1, \alpha_2, \dots, \alpha_\ell)$, $j = 1, \dots, r$, are all distinct (up to a constant factor) and irreducible over $\mathbb{K}$.

Thus, for $i = 1, \dots, s$, we have the factorisation

$$F_i(X_1, \alpha_2, \dots, \alpha_\ell) = a_i P_1(X_1, \alpha_2, \dots, \alpha_\ell)^{e_{i,1}} \dots P_r(X_1, \alpha_2, \dots, \alpha_\ell)^{e_{i,r}}.$$

If the polynomials $F_i(X_1, \alpha_2, \dots, \alpha_\ell)$, $i = 1, \dots, s$, are multiplicatively dependent in $\mathbb{K}(X_1)^*/\mathbb{K}^*$, then there exist integers $\ell_1, \dots, \ell_s$, not all zero, such that

$$F_1(X_1, \alpha_2, \dots, \alpha_\ell)^{\ell_1} \dots F_s(X_1, \alpha_2, \dots, \alpha_\ell)^{\ell_s} = c$$

for some $c \in \mathbb{K}^*$. This is equivalent to the fact that the matrix $(e_{i,j})_{\substack{1\le i\le r\\ 1\le j\le s}}$ does not have full rank, which contradicts the fact that the initial polynomials $F_1, \dots, F_s \in \mathbb{K}[X_1, \dots, X_\ell]$ are multiplicatively independent in $\mathbb{K}(X_1, \dots, X_\ell)^*/\mathbb{K}^*$. □

2.5 Multiplicities of zeroes

To prove Theorem 1.3 we need a uniform bound for the multiplicities of zeros of polynomials of the form $f_1^{n_1} \dots f_\ell^{n_\ell} - g_1^{m_1} \dots g_r^{m_r}$. We present such a result below, as well as deduce as a consequence a similar uniform bound for rational functions, which we hope to be of independent interest.

For a rational function $h \in \mathbb{C}(T)$, we denote by $M(h)$ the largest multiplicity of the zeros of h and by $Z(h)$ the set of zeros of h in $\mathbb{C}$, respectively. We also recall that for a polynomial $f \in \mathbb{C}[T]$, we use the notation d_f for the degree of f.

Lemma 2.9 *Let $f_1, \dots, f_\ell, g_1, \dots, g_r \in \mathbb{C}[T]$ be polynomials satisfying*

$$Z(f_1 \dots f_\ell) \cap Z(g_1 \dots g_\ell) = \emptyset. \tag{2.4}$$

Then, for all $n_1, \dots, n_\ell, m_1, \dots, m_r \ge 0$, we have

$$M\left(f_1^{n_1} \dots f_\ell^{n_\ell} - g_1^{m_1} \dots g_r^{m_r}\right) \le \sum_{i=1}^{\ell} d_{f_i} + \sum_{j=1}^{r} d_{g_j}.$$

Proof We denote $\mathbf{n} = (n_1, \ldots, n_\ell) \in \mathbb{N}^\ell$ and $\mathbf{m} = (m_1, \ldots, m_r) \in \mathbb{N}^r$.

Writing the factorisation into linear factors, we have

$$f_1^{n_1} \ldots f_\ell^{n_\ell} - g_1^{m_1} \ldots g_r^{m_r} = a_{\mathbf{n},\mathbf{m}} \prod_{t \in Z\left(f_1^{n_1} \ldots f_\ell^{n_\ell} - g_1^{m_1} \ldots g_r^{m_r}\right)} (T-t)^{e_t},$$

where $a_{\mathbf{n},\mathbf{m}} \in \mathbb{C}$ is the leading coefficient of $f_1^{n_1} \ldots f_\ell^{n_\ell} - g_1^{m_1} \ldots g_r^{m_r}$.

For simplicity we write

$$S_{\mathbf{n},\mathbf{m}} = Z\left(f_1^{n_1} \ldots f_\ell^{n_\ell} - g_1^{m_1} \ldots g_r^{m_r}\right).$$

Let $M = \max_{t \in S_{\mathbf{n},\mathbf{m}}} e_t$ be the largest multiplicity of the zeros of $f_1^{n_1} \ldots f_\ell^{n_\ell} - g_1^{m_1} \ldots g_r^{m_r}$.

The bound for M follows immediately from the polynomial ABC theorem (proved first by Stothers [39], and then independently by Mason [24] and Silverman [35]). Indeed, we apply the polynomial ABC theorem with $A = a_{\mathbf{n},\mathbf{m}} \prod_{t \in S_{\mathbf{n},\mathbf{m}}} (T-t)^{e_t}$, $B = f_1^{n_1} \ldots f_\ell^{n_\ell}$ and $C = g_1^{m_1} \ldots g_r^{m_r}$, which by (2.4) are pairwise coprime. We obtain

$$\sum_{t \in S_{\mathbf{n},\mathbf{m}}} e_t \le \sum_{i=1}^{\ell} d_{f_i} + \sum_{j=1}^{r} d_{g_j} + \#S_{\mathbf{n},\mathbf{m}} - 1. \tag{2.5}$$

Taking into account that

$$\sum_{t \in S_{\mathbf{n},\mathbf{m}}} e_t \ge M + \#S_{\mathbf{n},\mathbf{m}} - 1,$$

from (2.5) we obtain

$$M \le \sum_{i=1}^{\ell} d_{f_i} + \sum_{j=1}^{r} d_{g_j},$$

which concludes the proof. □

We present now a similar result for rational functions.

Corollary 2.10 *Let $h_1, \ldots, h_\ell \in \mathbb{C}(T)$, $h_i = f_i/g_i$, $f_i, g_i \in \mathbb{C}[T]$, $i = 1, \ldots, \ell$, with $Z(f_1 \ldots f_\ell) \cap Z(g_1 \ldots g_\ell) = \emptyset$. Then, for all $n_1, \ldots, n_\ell \ge 0$, we have*

$$M\left(h_1^{n_1} \ldots h_\ell^{n_\ell} - 1\right) \le \sum_{i=1}^{\ell} (\deg f_i + \deg g_i).$$

Proof We note that $Z\left(h_1^{n_1} \ldots h_\ell^{n_\ell} - 1\right) = Z\left(f_1^{n_1} \ldots f_\ell^{n_\ell} - g_1^{n_1} \ldots g_\ell^{n_\ell}\right)$. The result now follows directly from Lemma 2.9 applied with $r = \ell$ and $m_i = n_i$, $i = 1, \ldots, \ell$. □

2.6 Algebraic dependence

We need the following result [29, Theorem 1.1] which gives a degree bound for the annihilating polynomial of algebraically dependent polynomials, which is always the case when the number of polynomials exceeds the number of variables. The result holds over any field, but we present it only over $\mathbb{C}$.

Lemma 2.11 *Let $F_1, \dots, F_{\ell+1} \in \mathbb{C}[X_1, \dots, X_\ell]$ be of degree at most D. Then there exists a nonzero polynomial $R \in \mathbb{C}[Z_1, \dots, Z_{\ell+1}]$ of degree at most D^ℓ such that $R(F_1, \dots, F_{\ell+1}) = 0$.*

3 Proofs of main results

3.1 Proof of Theorem 1.2

We use the same idea as in the proof of [1, Theorem 1] and Lemma 2.2. Indeed, we write the factorisation in linear factors,

$$h_1 = \prod_{i=1}^{d_{h_1}} (T - \omega_{1,i}), \quad h_2 = \prod_{i=1}^{d_{h_2}} (T - \omega_{2,i}),$$

where $\omega_{1,i}, \omega_{2,j} \in \mathbb{C}$, $i = 1, \dots, d_{h_1}$, $j = 1, \dots, d_{h_2}$.

Thus, we reduce the problem to estimating the degree of each

$$\gcd\left(f^n - \omega_{1,i}, g^m - \omega_{2,j}\right).$$

For simplicity we use the notation ω_1 and ω_2 for any two roots of h_1 and h_2, respectively, and we denote

$$\mathcal{D}_{n,m}(\omega_1, \omega_2) = \gcd\left(f^n - \omega_1, g^m - \omega_2\right).$$

For every $n, m \geq 1$, we fix an element $t_{n,m} \in \mathbb{C}$ such that

$$f(t_{n,m})^n = \omega_1, \quad g(t_{n,m})^m = \omega_2 \tag{3.1}$$

(if no such $t_{n,m}$ exists then we immediately have $\deg \mathcal{D}_{n,m}(\omega_1, \omega_2) = 0$). We define new polynomials

$$\widetilde{f}_{n,m}(T) = \frac{1}{f(t_{n,m})} f(T) \quad \text{and} \quad \widetilde{g}_{n,m}(T) = \frac{1}{g(t_{n,m})} g(T).$$

As f and g are multiplicatively independent in $\mathbb{C}(T)^*/\mathbb{C}^*$, we obtain that $\widetilde{f}_{n,m}$ and $\widetilde{g}_{n,m}$ are multiplicatively independent for every n, m.

Thus, we can apply Lemma 2.2 and conclude that

$$\deg \gcd\left(\widetilde{f}_{n,m}^{n}-1, \widetilde{g}_{n,m}^{m}-1\right) \le \left(11d_*(d_f+d_g)^2\right)^{d_*}.$$

From (3.1) and the definition of $\widetilde{f}_{n,m}$ and $\widetilde{g}_{n,m}$, we have

$$\deg \mathcal{D}_{n,m}(\omega_1,\omega_2) = \deg \gcd\left(\widetilde{f}_{n,m}^{n}-1, \widetilde{g}_{n,m}^{m}-1\right),$$

and thus, for every $n, m \ge 1$, we obtain

$$\deg \mathcal{D}_{n,m}(\omega_1,\omega_2) \le \left(11d_*(d_f+d_g)^2\right)^{d_*}.$$

As this holds for any roots ω_1, ω_2 of h_1 and h_2, respectively, we obtain

$$\deg \gcd\left(h_1\left(f^n\right), h_2\left(g^m\right)\right) \le d_{h_1}d_{h_2}\left(11d_*(d_f+d_g)^2\right)^{d_*},$$

which concludes the proof. □

3.2 Proof of Theorem 1.3

We use the same idea as in the proof of [1, Theorem 1] combined with Lemma 2.3.

First, we note that for any zero $t \in \mathbb{C}$ of

$$\gcd\left(\prod_{i=1}^{\ell} f_i^{n_i} - \prod_{i=1}^{k} \varphi_i^{\nu_i}, \prod_{i=1}^{r} g_i^{m_i} - \prod_{i=1}^{s} \psi_i^{\mu_i}\right)$$

the condition (1.3) ensures that $\varphi_i(t), \psi_j(t) \ne 0$, $i = 1, \dots, l$, $j = 1, \dots, k$. Therefore each such zero t satisfies

$$\prod_{i=1}^{\ell} f_i(t)^{n_i} \cdot \prod_{i=1}^{k} \varphi_i(t)^{-\nu_i} = \prod_{i=1}^{r} g_i(t)^{m_i} \cdot \prod_{i=1}^{s} \psi_i(t)^{-\mu_i} = 1. \tag{3.2}$$

We apply Lemma 2.3 with k replaced by $L = \ell + k + r + s$ and with the curve

$$C = \big\{(f_1(t), \dots, f_\ell(t), \varphi_1(t), \dots, \varphi_k(t), g_1(t), \dots, g_r(t), \\ \psi_1(t), \dots, \psi_s(t)) \ : \ t \in \mathbb{C}\big\} \subseteq \mathbb{G}_m^L.$$

Indeed, we write

$$\mathbf{a} = (n_1, \dots, n_\ell, -\nu_1, \dots, -\nu_k), \ \mathbf{b} = (m_1, \dots, m_r, -\mu_1, \dots, -\mu_s).$$

As the vectors

$$(\mathbf{a}, \mathbf{0}), \ (\mathbf{0}, \mathbf{b}) \in \mathbb{Z}^L$$

are linearly independent, by Lemma 2.3 we obtain that there are only finitely many $t \in \mathbb{C}$ such that (3.2) holds for some vectors $\mathbf{a}, \mathbf{b}$ as above.

We denote by S the set of such $t \in \mathbb{C}$. For vectors $\mathbf{v} \in \mathbb{N}^{\ell+k}$ and $\mathbf{w} \in \mathbb{N}^{r+s}$ given by

$$\mathbf{v} = (n_1, \dots, n_\ell, \nu_1, \dots, \nu_k), \ \mathbf{w} = (m_1, \dots, m_r, \mu_1, \dots, \mu_s),$$

we denote

$$\mathcal{D}_{\mathbf{v},\mathbf{w}} = \gcd\left(\prod_{i=1}^{\ell} f_i^{n_i} - \prod_{i=1}^{k} \varphi_i^{\nu_i}, \prod_{i=1}^{r} g_i^{m_i} - \prod_{i=1}^{s} \psi_i^{\mu_i}\right).$$

We see from the above that set of zeros $Z(\mathcal{D}_{\mathbf{v},\mathbf{w}})$ belongs to some fixed set that depends only on the above curve C and thus only on the polynomials in the initial data. To construct the required polynomial $h \in \mathbb{C}[T]$ as in the statement of Theorem 1.3 we only need to prove that the multiplicity of the roots $t \in S$ of $\mathcal{D}_{\mathbf{v},\mathbf{w}}$ can be bounded uniformly for all vectors $\mathbf{v}, \mathbf{w}$ as above. This is given by Lemma 2.9 applied with the polynomials $\prod_{i=1}^{\ell} f_i^{n_i} - \prod_{i=1}^{k} \varphi_i^{\nu_i}$ and $\prod_{i=1}^{r} g_i^{m_i} - \prod_{i=1}^{s} \psi_i^{\mu_i}$.

Indeed, if we denote by M_1 and M_2 the largest multiplicity of roots in S of the first and second polynomials, respectively, we get

$$M_1 \le \sum_{i=1}^{\ell} d_{f_i} + \sum_{i=1}^{k} d_{\varphi_i}, \quad M_2 \le \sum_{i=1}^{r} d_{g_i} + \sum_{i=1}^{s} d_{\psi_i}.$$

Thus, there exists a polynomial $h \in \mathbb{C}[T]$ defined by

$$h = \prod_{t \in S} (T - t)^d, \quad d = \min\left\{\sum_{i=1}^{\ell} d_{f_i} + \sum_{i=1}^{k} d_{\varphi_i}, \sum_{i=1}^{r} d_{g_i} + \sum_{i=1}^{s} d_{\psi_i}\right\},$$

such that $\mathcal{D}_{\mathbf{v},\mathbf{w}} \mid h$ for every vectors $\mathbf{v}, \mathbf{w}$ as above. This concludes the proof of Part **i**.

For Part **ii**, for each $t \in S$, let

$$\mathcal{L}_t = \{(\mathbf{v}, \mathbf{w}) \in \mathbb{N}^L \ : \ (T - t) \mid \mathcal{D}_{\mathbf{v},\mathbf{w}}\}.$$

We note that $\mathcal{L}_t$ is actually a monoid as the sum of any two elements in $\mathcal{L}_t$ is also an element of $\mathcal{L}_t$. As the set S is finite, there are finitely many such monoids $\mathcal{L}_t$, $t \in S$, such that $\deg \mathcal{D}_{\mathbf{v},\mathbf{w}} \ge 1$ for any $(\mathbf{v}, \mathbf{w}) \in \mathcal{L}_t$.

We are left to show that $\cup_{t \in S} \mathcal{L}_t$ is not the entire space $\mathbb{N}^L$. Indeed, this follows directly from [1, Theorem 1] as for the diagonal case, that is $\mathbf{v} = n(\underbrace{1, \dots, 1}_{\ell}, 0, \dots, 0) \in \mathbb{N}^{\ell+k}$ and $\mathbf{w} = n(\underbrace{1, \dots, 1}_{r}, 0, \dots, 0) \in \mathbb{N}^{r+s}$, we have

$$\gcd\left((f_1 \dots f_\ell)^n - 1, (g_1 \dots g_r)^n - 1\right) = 1$$

infinitely often.

Thus, for any $(\mathbf{v}, \mathbf{w})$ outside $\cup_{t \in S} \mathcal{L}_t$, we have $\mathcal{D}_{\mathbf{v},\mathbf{w}} = 1$, and we conclude the proof. □

3.3 Proof of Theorem 1.4

The idea of the proof lies in applying Hilbert's irreducibility theorem, and in particular Lemma 2.8, to reduce via specialisations to the univariate case and thus use Theorem 1.2.

We denote $d = D + 1$, that is $d > \deg_{X_j} F, \deg_{X_j} G$ for any $j = 1, \ldots, \ell$. We define the polynomials

$$\widetilde{F}(X_1, \ldots, X_\ell) = F\left(X_1, X_2 + X_1^d, \ldots, X_\ell + X_1^{d^{\ell-1}}\right),$$
$$\widetilde{G}(X_1, \ldots, X_\ell) = G\left(X_1, X_2 + X_1^d, \ldots, X_\ell + X_1^{d^{\ell-1}}\right).$$

The polynomials $\widetilde{F}, \widetilde{G}$ have the property that

$$\deg \widetilde{F}, \deg \widetilde{G} \le D\frac{d^\ell - 1}{d-1} < (D+1)^\ell$$

and

$$\deg \widetilde{F}(X_1, \alpha_2, \ldots, \alpha_\ell) = \deg \widetilde{F}, \ \deg \widetilde{G}(X_1, \alpha_2, \ldots, \alpha_\ell) = \deg \widetilde{G}$$

for any specialisation $(\alpha_2, \ldots, \alpha_\ell) \in \mathbb{C}^{\ell-1}$.

Moreover, we note that the polynomials $\widetilde{F}, \widetilde{G}$ are also multiplicatively independent in $\mathbb{C}(X_1, \ldots, X_\ell)^*/\mathbb{C}^*$. Indeed, if this would not be the case, then there would exist i_1, i_2 not both zero and $a \in \mathbb{C}^*$ such that

$$\widetilde{F}^{i_1}\widetilde{G}^{i_2} = a.$$

Composing this polynomial identity with the polynomial automorphism

$$(X_1, \ldots, X_\ell) \to \left(X_1, X_2 - X_1^d, \ldots, X_\ell - X_1^{d^{\ell-1}}\right) \tag{3.3}$$

we obtain that the polynomials F, G are multiplicatively dependent in $\mathbb{C}(X_1, \ldots, X_\ell)^*/\mathbb{C}^*$ and thus we get a contradiction.

Let $\mathbb{K}$ be the field extension of $\mathbb{Q}$ generated by the coefficients of the polynomials F, G. By the Hilbert's irreducibility theorem, see [31, Theorem 46], $\mathbb{K}$ is a Hilbertian field. We apply now Lemma 2.8 with the polynomials $\widetilde{F}, \widetilde{G}$, and thus infer that there exists a specialisation $(\alpha_2, \ldots, \alpha_\ell) \in \mathbb{K}^{\ell-1}$ such that $\widetilde{F}(X_1, \alpha_2, \ldots, \alpha_\ell)$ and $\widetilde{G}(X_1, \alpha_2, \ldots, \alpha_\ell)$ are multiplicatively independent in $\mathbb{C}(X_1)^*/\mathbb{C}^*$. For simplicity, we put

$$f = \widetilde{F}(X_1, \alpha_2, \ldots, \alpha_\ell) \ \text{ and } \ g = \widetilde{G}(X_1, \alpha_2, \ldots, \alpha_\ell).$$

We denote $\mathcal{D}_{n,m} = \gcd\left(h_1\left(F^n\right), h_2\left(G^m\right)\right)$. Moreover, we note that

$$\mathcal{D}_{n,m}\left(X_1, X_2 + X_1^d, \ldots, X_\ell + X_1^{d^{\ell-1}}\right) = \gcd\left(h_1\left(\widetilde{F}^n\right), h_2\left(\widetilde{G}^m\right)\right).$$

We denote $E_{n,m} = \gcd\left(h_1\left(\widetilde{F}^n\right), h_2\left(\widetilde{G}^m\right)\right)$, and for the specialisation $(\alpha_2, \ldots, \alpha_\ell)$ one has

$$E_{n,m}(X_1, \alpha_2, \ldots, \alpha_\ell) \mid \gcd\left(h_1\left(f^n\right), h_2\left(g^m\right)\right).$$

In particular, we have

$$\deg \mathcal{D}_{n,m} \leq \deg E_{n,m} \leq \deg \gcd\left(h_1\left(f^n\right), h_2\left(g^m\right)\right).$$

We make here the remark that using the automorphism (3.3) was essential to have these degree inequalities, as if one just uses Hilbert's irreducibility theorem applied directly with the polynomials F and G, we cannot guarantee that when we make specialisations we get that $\deg \mathcal{D}_{n,m} \leq \deg \gcd\left(h_1\left(f^n\right), h_2\left(g^m\right)\right)$.

We apply now Theorem 1.2 and using the fact that $\deg f, \deg g < (D+1)^\ell$ we conclude that

$$\deg \gcd\left(h_1\left(f^n\right), h_2\left(g^m\right)\right) \leq d_{h_1} d_{h_2} (44(D+1)^{2\ell})^{(D+1)^\ell},$$

which finishes the proof. □

3.4 Proof of Theorem 1.5

We define

$$\mathcal{H} = \{(F_1(\boldsymbol{\alpha}), \ldots, F_{\ell+1}(\boldsymbol{\alpha})) \mid \boldsymbol{\alpha} \in \mathbb{C}^\ell\}.$$

By Lemma 2.11 there exists a polynomial $R \in \mathbb{C}[Z_1, \ldots, Z_{\ell+1}]$ of degree at most D^ℓ such that $R(F_1, \ldots, F_{\ell+1}) = 0$. In other words, any point of $\mathcal{H}$ is a point on the hypersurface defined by the zero set of R in $\mathbb{C}^{\ell+1}$. In particular, any point $\boldsymbol{\alpha} \in \mathbb{C}^\ell$ such that $F_i(\boldsymbol{\alpha})^{n_i} = 1, i = 1, \ldots, \ell+1$, gives a point on the hypersurface defined by the zero set of R with coordinates roots of unity.

From Lemma 2.5 we get that there are at most

$$N \leq N(R) \leq (0.792 s(R)/\log(s(R)+1))^{s(R)}$$

algebraic subgroups, each defined by the zero set of at most $\ell+1$ Laurent polynomials of the form

$$Z_1^{b_{j,1}} Z_2^{b_{j,2}} \ldots Z_{\ell+1}^{b_{j,\ell+1}} - 1 \in \mathbb{C}(Z_1, \ldots Z_{\ell+1})$$

with

$$\sum_{i=1}^{\ell+1} |b_{j,i}| \leq (\ell+1) D^\ell \prod_{p \leq s(R)} p, \qquad j = 1, \ldots, \ell+1,$$

where the product runs over all primes $p \le s(R)$, that contain all the points in $Z(R)$ with coordinates roots of unity. In particular, all points $(F_1(\boldsymbol{\alpha}), \ldots, F_{\ell+1}(\boldsymbol{\alpha}))$ such that $F_i(\boldsymbol{\alpha})^{n_i} = 1$, $i = 1, \ldots, \ell+1$, lie in these algebraic subgroups. It remains to estimate $s(R)$.

As R is a polynomial in $\ell+1$ variables and $\deg R \le D^\ell$, we have that $s(R) \le \gamma_\ell(D)$, where $\gamma_\ell(D)$ is defined by (1.4).

Thus, the points $\boldsymbol{\alpha}$ such that $F_i(\boldsymbol{\alpha})^{n_i} = 1$, $i = 1, \ldots, \ell+1$, lie in at most N algebraic varieties, each defined by at most $\ell+1$ Laurent polynomials of the form $F_1^{b_{j,1}} F_2^{b_{j,2}} \ldots F_{\ell+1}^{b_{j,\ell+1}} - 1$ (note that these polynomials are non constant since $F_1, \ldots, F_{\ell+1}$ are multiplicatively independent) of degree at most

$$\sum_{i=1}^{\ell+1} |b_{j,i}| \deg F_i \le (\ell+1) D^{\ell+1} \prod_{p \le \gamma_\ell(D)} p, \qquad j = 1, \ldots, \ell+1,$$

where the product runs over all primes $p \le \gamma_\ell(D)$. □

4 Final comments and questions

4.1 Extensions over $\mathbb{C}$

Lemma 2.3 gives only the finiteness of the intersection of curves in $\mathbb{G}_m^\ell$ with algebraic subgroups. As already mentioned after Theorem 1.3, it is of high interest to have available uniform bounds for the size of this intersection. This implies uniform bounds on the degree of h in Theorem 1.3.

More generally, one can use bounds for the number of solutions to $f(x, y) = 0$, with $x^n, y^m \in S$ for some nonzero integers n and m, where S is the group of S-units of some fixed number field, to obtain further generalisations. In fact such bounds are known, for example see [30, Theorem 1.2] for a more general result.

It is certainly interesting to obtain a similar result as Theorem 1.4 for

$$\gcd\left(H_1\left(F_1^{n_1}, \ldots, F_s^{n_s}\right), H_2\left(G_1^{m_1}, \ldots, G_r^{m_r}\right)\right),$$

with polynomials $H_1 \in \mathbb{C}[Y_1, \ldots, Y_s]$, $H_2 \in \mathbb{C}[Z_1, \ldots, Z_r]$ and also $F_1, \ldots, F_s, G_1, \ldots, G_r \in \mathbb{C}[X_1, \ldots, X_\ell]$.

If one chooses

$$H_1 = Y_1 \ldots Y_s - 1, \quad H_2 = Z_1 \ldots Z_r - 1,$$

then following the same proof as for Theorem 1.4, we reduce (via specialisations) the problem to Theorem 1.3, and thus get that

$$\deg \gcd\left(H_1\left(F_1^{n_1}, \ldots, F_s^{n_s}\right), H_2\left(G_1^{m_1}, \ldots, G_r^{m_r}\right)\right) \tag{4.1}$$

is bounded by a constant depending only on $F_1, \ldots, F_s, G_1, \ldots, G_r$.

However, the approach of Theorem 1.4 does not seem to work for more general multivariate polynomials H_1, H_2.

4.2 Dynamical analogues

Another interesting direction of research is obtaining dynamical analogues of the results of Ailon–Rudnick [1] and Silverman [36]. That is, investigating the greatest common divisors of polynomials iterates.

More precisely, let $\mathbb{K}$ be a field and $f, g \in \mathbb{K}[T]$. We define

$$f^{(0)} = T, \quad f^{(n)} = f(f^{(n-1)}), \quad n \geq 1,$$

and similarly for g.

Problem 4.1 *Give, under some natural conditions, an upper bound for*

$$\deg \gcd \left(f^{(n)}, g^{(m)} \right).$$

Problem 4.2 *Show, under some natural conditions, that the iterates of f and g are coprime for infinitely many n, m.*

We note that some conditions on f, g are certainly needed in Problem 4.2 as, for example, if f and g have 0 as fixed point, that is, $f(0) = g(0) = 0$, then $f^{(n)}$ and $g^{(m)}$ are never coprime.

We note that there are many results regarding the arithmetic structure of polynomial iterates. For example in [18,19,21,22] and references therein, results regarding the irreducibility of iterates are given. Irreducible polynomials $f \in \mathbb{K}[T]$ such that all the iterates $f^{(n)}$, $n \geq 1$, remain irreducible are called *stable polynomials*. For quadratic polynomials the stability is given by the presence of squares in the orbit of the critical point of the polynomial. Thus, if $f, g \in \mathbb{K}[T]$ are stable, then $f^{(n)}$ and $g^{(m)}$ are coprime for every $n, m \geq 1$.

For $h_1, h_2 \in \mathbb{K}[T]$, one can also consider the more general case

$$G_{n,m} = \gcd \left(h_1 \left(f^{(n)} \right), h_2 \left(g^{(m)} \right) \right).$$

We note that, following the ideas of [1, Theorem 1] and of this paper, bounding the zeros of $G_{n,m}$ reduces to proving the finiteness (or even finding uniform bounds) of the number of $t \in \mathbb{C}$ such that $(f^{(n)}(t), g^{(m)}(t)) \in V$, where V is the set of zeros of $\{h_1(X_1), h_2(X_2)\}$.

This naturally leads to the question of counting the occurrences

$$\left(f^{(n)}(t), g^{(m)}(t) \right) \in V, \qquad (n, m, t) \in [1, N] \times [1, N] \times \mathbb{C},$$

for an arbitrary variety $V \subseteq \mathbb{C}^2$ and a sufficiently large integer $N \geq 1$.

For a fixed t and the diagonal case $n = m$, this is of the same flavour as the uniform *dynamical Mordell–Lang conjecture*, which, for a fixed $(t_1, t_2) \in \mathbb{C}^2$ asserts that the integers $n, \geq 1$ such that $\left(f^{(n)}(t_1), g^{(n)}(t_2)\right) \in V$, see [3,16,17] and references therein, lie in finitely many arithmetic progressions (which number does not depend on t_1, t_2).

Acknowledgments The author is very grateful to Joseph Silverman for drawing the attention on the Ailon–Rudnick theorem and related results. The author would also like to thank Igor Shparlinski, Joseph Silverman, Thomas Tucker and Umberto Zannier for their valuable suggestions and stimulating discussions, and also for their comments on an early version of the paper. The author is also grateful to the anonymous referee for spotting an error in the previous version of Lemma 2.8, and for other comments which improved the presentation of the paper.The research of A. O. was supported by the UNSW Vice Chancellor's Fellowship.

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. Aliev, I., Smyth, C.: Solving algebraic equations in roots of unity. Forum Math. **24**, 641–665 (2012)
3. Benedetto, R., Ghioca, D., Kurlberg, P., Tucker, T.: A case of the dynamical Mordell–Lang conjecture. Math. Ann. **352**, 1–26 (2012)
4. Berend, D., Tassa, T.: Improved bounds on Bell numbers and on moments of sums of random variables. Prob. Math. Stat. **30**, 185–205 (2010)
5. Beukers, F., Smyth, C.J.: Cyclotomic Points on Curves. Number Theory for the Millenium (Urbana, Illinois, 2000), I. A K Peters, Natick (2002)
6. Bombieri, E., Masser, D., Zannier, U.: Intersecting a curve with algebraic subgroups of multiplicative groups. Int. Math. Res. Notices **20**, 1119–1140 (1999)
7. Bombieri, E., Masser, D., Zannier, U.: On unlikely intersections of complex varieties with tori. Acta Arith. **133**, 309–323 (2008)
8. Bombieri, E., Zannier, U.: Algebraic points on subvarieties of $\mathbb{G}_m^n$. Int. Math. Res. Notices **7**, 333–347 (1995)
9. 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**, 79–84 (2003)
10. Corvaja, P., Zannier, U.: A lower bound for the height of a rational function at S-unit points. Monatsh. Math. **144**, 203–224 (2005)
11. Corvaja, P., Zannier, U.: On the maximal order of a torsion point on a curve in $\mathbb{G}_m^n$. Rend. Lincei Mat. Appl. **19**, 73–78 (2008)
12. Corvaja, P., Zannier, U.: Some cases of Vojta's conjecture on integral points over function fields. J. Algebraic Geom. **17**, 295–333 (2008)
13. 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**, 1927–1942 (2013)
14. Evertse, J.-H.: The number of solutions of linear equations in roots of unity. Acta Arith. **89**, 45–51 (1999)
15. Denis, L.: Facteurs communs et torsion en caractéristique non nulle. J. Thor. Nombres Bordeaux **23**, 347–352 (2011)
16. Ghioca, D., Tucker, T.J.: Periodic points, linearizing maps, and the dynamical Mordell–Lang problem. J. Number Theory **129**, 1392–1403 (2009)
17. Ghioca, D., Tucker, T., Zieve, M.: Intersections of polynomial orbits, and a dynamical Mordell–Lang conjecture. Invent. Math. **171**, 463–483 (2008)
18. Gomez-Perez, D., Nicolás, A.P., Ostafe, A., Sadornil, D.: On the length of critical orbits of stable arbitrary polynomials over finite fields. Rev. Matem. Iberoamer. **30**, 523–535 (2014)
19. Gomez-Perez, D., Ostafe, A., Shparlinski, I.: On irreducible divisors of iterated polynomials. Rev. Matem. Iberoamer. **30**, 1123–1134 (2014)
20. Granville, A., Rudnick, Z.: Torsion points on curves. NATO Sci. Ser. II Math. Phys. Chem. **237**, 85–92 (2007)
21. Jones, R.: The density of prime divisors in the arithmetic dynamics of quadratic polynomials. J. Lond. Math. Soc. **78**, 523–544 (2008)

22. Jones, R., Boston, N.: Settled polynomials over finite fields. Proc. Am. Math. Soc. **140**, 1849–1863 (2012)
23. Lang, S.: Fundamentals of Diophantine Geometry. Springer, New York (1983)
24. Mason, R.C.: Diophantine equations over function fields. London Mathematical Society Lecture Note Series, vol. 96. Cambridge University Press, Cambridge (1984)
25. Masser, D.: Specializations of finitely generated subgroups of abelian varieties. Trans. Am. Math. Soc. **311**, 413–424 (1989)
26. Masser, D.: Unlikely intersections for curves in multiplicative groups over positive characteristic. Q. J. Math. **65**, 505–515 (2014)
27. Maurin, G.: Courbes algébriques et équations multiplicatives. Math. Ann. **341**, 789–824 (2008)
28. Néron, A.: Problèmes arithmétiques et géométriques rattachés à la notion de rang d'une courbe algébrique dans un corps. Bull. Soc. Math. France **80**, 101–166 (1952)
29. Płoski, A.: Algebraic Dependence of Polynomials after O. Perron and Some Applications: Computational Commutative and Non-Commutative Algebraic Geometry. IOS Press, Amsterdam, pp. 167–173 (2005)
30. Rémond, G.: Sur les sous-variétés des tores. Compositio Math. **134**, 337–366 (2002)
31. Schinzel, A.: Polynomials with Special Regard to Reducibility. Appendix by Umberto Zannier, Encyclopedia of Mathematics and its Applications, vol. 77. Cambridge University Press, Cambridge (2000)
32. Schlickewei, H.P.: Equations in roots of unity. Acta Arith. **76**, 99–108 (1996)
33. Serre, J.-P.: Lectures on the Mordell–Weil theorem, 2nd edn. Vieweg (1990)
34. Silverman, J.H.: Heights and the specialization map for families of Abelian varieties. J. Reine Angew. Math. **342**, 197–211 (1983)
35. Silverman, J.H.: The S-unit equation over function fields. Proc. Camb. Philos. Soc. **95**, 3–4 (1984)
36. Silverman, J.H.: Common divisors of $a^n - 1$ and $b^n - 1$ over function fields. N. Y. J. Math. (electronic) **10**, 37–43 (2004)
37. Silverman, J.: Common divisors of elliptic divisibility sequences over function fields. Manuscripta Math. **114**, 432–446 (2004)
38. Silverman, J.H.: Generalized greatest common divisors, divisibility sequences, and Vojta's conjecture for blowups. Monatsh. Math. **145**, 333–350 (2005)
39. Stothers, W.W.: Polynomial identities and Hauptmoduln. Q. J. Math. Oxf. **32**, 349–370 (1981)
40. Zannier, U.: Some Problems of Unlikely Intersections in Arithmetic and Geometry. Annals of Mathematics Studies, vol. 181. Princeton University Press, Princeton (2012)