# ANNALES MATHÉMATIQUES



CLEMENS FUCHS & CHRISTINA KAROLUS

# Composite values of polynomial power sums

Volume 26, nº 1 (2019), p. 1-24.

<http://ambp.centre-mersenne.org/item?id=AMBP\_2019\_26\_1\_1\_0>

© Université Clermont Auvergne, Laboratoire de mathématiques Blaise Pascal, 2019, Certains droits réservés.

Cet article est mis à disposition selon les termes de la licence CREATIVE COMMONS ATTRIBUTION – PAS DE MODIFICATION 4.0 FRANCE. http://creativecommons.org/licenses/by-nd/4.0/fr/

L'accès aux articles de la revue « Annales mathématiques Blaise Pascal » (http://ambp.centre-mersenne.org/), implique l'accord avec les conditions générales d'utilisation (http://ambp.centre-mersenne.org/legal/).

Publication éditée par le laboratoire de mathématiques Blaise Pascal de l'université Clermont Auvergne, UMR 6620 du CNRS Clermont-Ferrand — France



Article mis en ligne dans le cadre du Centre de diffusion des revues académiques de mathématiques http://www.centre-mersenne.org/

# Composite values of polynomial power sums

# Clemens Fuchs Christina Karolus

#### Abstract

Let  $(G_n(x))_{n=0}^{\infty}$  be a *d*-th order linear recurrence sequence having polynomial characteristic roots, one of which has degree strictly greater than the others. Moreover, let  $m \ge 2$  be a given integer. We ask for  $n \in \mathbb{N}$  such that the equation  $G_n(x) = g \circ h$  is satisfied for a polynomial  $g \in \mathbb{C}[x]$  with deg g = m and some polynomial  $h \in \mathbb{C}[x]$  with deg h > 1. We prove that for all but finitely many *n* these decompositions can be described in "finite terms" coming from a generic decomposition parameterized by an algebraic variety. All data in this description will be shown to be effectively computable.

## 1. Introduction and results

Let  $\mathbb{C}[x]$  be the polynomial ring in the indeterminate x (we remark right away that  $\mathbb{C}$  might be replaced by an algebraically closed field of characteristic 0; however, all polynomials below are assumed to have coefficients in  $\mathbb{C}$ ). Composition of polynomials is a well-defined operation on  $\mathbb{C}[x]$ . It is associative and has with f(x) = x an identity element, but it is neither commutative nor distributive. There are many reasons to be interested in polynomial composition, e.g. the knowledge of a composition of  $f \in \mathbb{C}[x]$  can be of use if one wishes to factor a given polynomial. We illustrate this with a simple example. The polynomial  $f(x) = x^8 - 14x^4 + 7$  is irreducible over the rationals. However, since f(x) = g(h(x)), where  $g(x) = x^2 - 14x + 7$  and  $h(x) = x^4$ , we can easily determine all solutions of f(x) = 0 in radicals by first calculating the roots y of  $y^2 - 14y + 7$  and then determining the corresponding x from  $y = x^4$ . Even though in the present paper we restrict ourselves to polynomials over  $\mathbb{C}$ , we also mention that, if for given  $f \in k[x]$  over an arbitrary field k there is a  $g \in k[x]$  with  $f \circ g$  irreducible over k, then f is an irreducible polynomial in k[x] as well. Another example is that the decompositions of f exhibit arithmetical properties associated with f, which is used to solve equations of separated variable type (cf. [2, 3]). The invertible elements in  $\mathbb{C}[x]$  with respect to decomposition are the linear polynomials. We call  $f(x) = g \circ h$  a non-trivial decomposition if neither g nor h is linear. Let  $m \ge 2$  be an integer; we call  $f(x) = g \circ h$  an *m*-decomposition if deg g = m and we say that f is m-decomposable if an m-decomposition of f exists. We call f indecomposable if f admits only trivial decompositions. A pair  $(g, h) \in \mathbb{C}[x]^2$  is called equivalent to (g', h')

Supported by Austrian Science Fund (FWF) Grant No. P24574.

*Keywords*: Decomposable polynomials, linear recurrence sequences, Brownawell–Masser inequality.

<sup>2010</sup> Mathematics Subject Classification: 11B37, 12Y05, 11R58.

if there are  $a, b \in \mathbb{C}, a \neq 0$  such that g(x) = g'(ax + b), h(x) = (h'(x) - b)/a. It is easy to see that every polynomial  $f \in \mathbb{C}[x]$  can be decomposed as  $f(x) = f_1 \circ f_2 \circ \cdots \circ f_k$ with  $f_i$  indecomposable. Moreover, this decomposition is unique in the following sense: if  $f(x) = f'_1 \circ \cdots \circ f'_l$  with  $f'_j$  indecomposable is another decomposition, then k = land  $f_1, \ldots, f_k$  are obtained applying certain transformations a finite number of times, where in each step a neighboring pair of  $f'_1, \ldots, f'_l$  is replaced by another one having the same composition. (This is known as Ritt's first theorem; cf. [19].) There is a nice algebraic description of decompositions of a polynomial  $f \in \mathbb{C}[x]$  since they are (up to equivalence) in one-to-one correspondence to intermediate fields between  $\mathbb{C}(x)$  and  $\mathbb{C}(f(x))$  (cf. again [19]).

We start with a few general remarks. First, it might happen that for a given  $f \in \mathbb{C}[x]$ and a given  $g \in \mathbb{C}[x]$  we have different  $h_1, h_2 \in \mathbb{C}[x]$  such that  $f(x) = g \circ h_1 = g \circ h_2$ . However, in this case g(X) = g(Y) has a solution  $X = h_1(x), Y = h_2(x)$ . This situation was completely solved in [1]. It follows that  $g = g' \circ x^k$  for some  $g' \in \mathbb{C}[x], k > 1$  and  $h_1$  and  $h_2$  just differ by a constant (to be more precise, by a k-th root of unity). Second, by linear equivalence we can control the leading coefficient and the constant term of h. E.g. we may assume that  $h \in \mathbb{C}[x]$  is monic and satisfies h(0) = 0 (every other value in  $\mathbb{C}$  is fine as well). Moreover, assume that f is given and that we have  $f(x) = g \circ h$  with  $f, g, h \in \mathbb{C}[x]$ . Let  $a \in \mathbb{C} \setminus \{0\}$  be the leading coefficient of f. Then we may also assume that g is monic by writing  $f(x) = a(g \circ h)$ . Third, assume that  $f, h \in \mathbb{C}[x]$  are given. Then there are at most finitely many  $g \in \mathbb{C}[x]$  with  $f(x) = g \circ h$ . This can be seen as follows: We may assume that f, g, h are all monic. Write  $g(x) = (x - b_1) \dots (x - b_m)$ , where  $b_1, \ldots, b_m \in \mathbb{C}$  are not necessarily distinct. Assume that  $f(x) = (x - a_1) \ldots (x - a_n)$  with  $a_1, \ldots, a_n \in \mathbb{C}$ . Then  $g(h(x)) = (h(x) - b_1) \ldots (h(x) - b_m) = (x - a_1) \ldots (x - a_n) = f(x)$ . It follows that there is a partition of the multi-set  $\{a_1, \ldots, a_n\}$  with equally large blocks (of size deg h) that describe g uniquely. If we assume that h(0) = 0, then the  $b_i$  are just the product of all elements in the *i*-th block. The unique g can be found, without calculating the roots of *f*, by comparing coefficients in  $f(x) = g \circ h$  (cf. [17]).

In this paper we are interested in non-trivial decompositions (with two factors, an "inner" and an "outer" factor) of polynomials with coefficients in  $\mathbb{C}$ . This problem is hard in general since the decompositions of polynomials can be anything *a priori* (since conversely, every pair (g, h) gives a polynomial  $g \circ h$ ). Therefore, it is natural to restrict to a subset of  $\mathbb{C}[x]$  which is described by a finite amount of data and then to ask whether or not all decompositions in this subset can be described *in finite terms* depending on the data describing the subset. We give a few (important and non-trivial) examples to illustrate this approach.

Let  $n \ge 2$  be a given integer. We consider the set of all polynomials  $f \in \mathbb{C}[x]$  of degree *n*. Then there is an integer *J* and for every  $1 \le j \le J$  an algebraic variety

 $V_j \subset \mathbb{A}^{n+t_j}$  for some  $2 \le t_j \le n$  defined over  $\mathbb{Q}$  for which equations can be written down effectively and there are polynomials  $f_j, h_j, g_j$  with coefficients in the coordinate ring of the variety and depending on integers  $k_1, \ldots, k_{t_j}$  and  $(l_1, \ldots, l_n) \in \{0, 1, \ldots, n-1\}^n$ such that the following holds: a)  $g_j \circ h_j = f_j$  is a polynomial of degree *n* with coefficients in the coordinate ring; b) for every point  $P \in \mathcal{V}_j(\mathbb{C})$  and integers  $k_1, \ldots, k_{t_j}, l_1, \ldots, l_n$ one gets a decomposition  $f_j(P, x) = g_j(P, h_j(P, x))$ ; c) conversely, for every polynomial  $f \in \mathbb{C}[x]$  of degree *n* and every non-trivial decomposition  $f(x) = g \circ h$  with g(x) not of the shape  $(ax + b)^m, m \in \mathbb{N}, a, b \in \mathbb{C}$  there are  $P \in \mathcal{V}_j(\mathbb{C}), k_1, \ldots, k_{t_j}, l_1, \ldots, l_n$  such that  $f(x) = f_j(P, x), g(x) = g_j(P, x), h(x) = h_j(P, x)$ . This result (formulated in different forms) can be found in [4, 12, 17].

Let  $\ell$  be a given integer. We consider the set of *lacunary* polynomials (with respect to  $\ell$ ), that is the set of all polynomials  $f \in \mathbb{C}[x]$  with  $\ell$  non-constant terms. Then there are integers p, J depending on  $\ell$  and for every  $1 \leq j \leq J$  an algebraic variety  $\mathcal{V}_j$ defined over  $\mathbb{Q}$  and a lattice  $\Lambda_j$  for which equations can be written down explicitly and (Laurent-)polynomials  $f_j, h_j \in \mathbb{Q}[\mathcal{V}_j][z_1^{\pm 1}, \ldots, z_p^{\pm 1}], g_j \in \mathbb{Q}[\mathcal{V}_j][z]$  with coefficients in the coordinate ring of the variety such that the following holds: a)  $g_j \circ h_j = f_j$  is a (Laurent-)polynomial with  $\ell$  non-constant terms with coefficients in the coordinate ring; b) for every point  $P \in \mathcal{V}_j(\mathbb{C})$  and  $(u_1, \ldots, u_p) \in \Lambda_j$  one gets a decomposition  $f_j(P, x^{u_1}, \ldots, x^{u_p}) =$  $g_j(P, h_j(P, x^{u_1}, \ldots, x^{u_p}))$ ; c) conversely, for every polynomial  $f \in \mathbb{C}[x]$  with  $\ell$  nonconstant terms and every non-trivial decomposition  $f(x) = g \circ h$  with h(x) not of the shape  $ax^m + b, m \in \mathbb{N}, a, b \in \mathbb{C}$  there is a j, a point  $P \in \mathcal{V}_j(\mathbb{C})$  and  $(u_1, \ldots, u_p) \in \Lambda_j$ such that  $f(x) = f_j(P, x^{u_1}, \ldots, x^{u_p}), g(x) = g_j(P, x), h(x) = h_j(P, x^{u_1}, \ldots, x^{u_p})$ . This result can be found in [25]; cf. also [24, 26]. (A similar result holds for lacunary rational functions  $f \in \mathbb{C}(x)$  by a combination of [10] and [16].)

In the present paper we are interested in another subset of  $\mathbb{C}[x]$  namely the subset  $\{G_n(x); n \in \mathbb{N}\}\$  that consists of elements of a linear recurrence sequence  $(G_n(x))_{n=0}^{\infty}$  of polynomials in  $\mathbb{C}[x]$ . The sequence is fixed by the recurrence relation and by the initial values. Equivalently, every element of the sequence can be written by a Binet-type formula  $G_n(x) = a_1 \alpha_1^n + \cdots + a_t \alpha_t^n$ , where  $\alpha_1, \ldots, \alpha_t$  are the distinct roots of the characteristic polynomial associated to the recurring relation and the  $a_i$  are polynomials in n with coefficients in the splitting field  $\mathbb{C}(x, \alpha_1, \ldots, \alpha_t)$  of degree less than the corresponding multiplicity of  $\alpha_i$  as a root of the characteristic equation. In this way all elements are given by a finite amount of data. Our goal is to describe all decomposable  $G_n$ 's in this set and all their decompositions in finite terms, depending only on the given data. To fix terms we shall consider the *d*-th order linear recurrence sequence  $(G_n(x))_{n=0}^{\infty}$ , given by the relation

$$G_{n+d}(x) = A_{d-1}(x)G_{n+d-1}(x) + \dots + A_0(x)G_n(x),$$
(1.1)

with  $A_0, \ldots, A_{d-1} \in \mathbb{C}[x]$  and initial terms  $G_0, \ldots, G_{d-1} \in \mathbb{C}[x]$ . Denote by  $\alpha_1, \ldots, \alpha_t$  the distinct characteristic roots of the sequence, that is the characteristic polynomial  $\mathcal{G} \in \mathbb{C}(x)[T]$  splits as

$$\mathcal{G}(T) = T^d - A_{d-1}T^{d-1} - \dots - A_0 = (T - \alpha_1)^{k_1}(T - \alpha_2)^{k_2} \dots (T - \alpha_t)^{k_t}$$

where  $k_1, \ldots, k_t \in \mathbb{N}$ . We assume that all roots are simple, i.e. t = d, and that they are polynomials, i.e.  $\alpha_i \in \mathbb{C}[x]$  for  $i = 1, \ldots, d$ . Then  $G_n(x)$  admits a representation of the form

$$G_n(x) = a_1 \alpha_1^n + a_2 \alpha_2^n + \dots + a_d \alpha_d^n.$$
 (1.2)

By assumption we consider the special situation that  $a_1, \ldots, a_d \in \mathbb{C}$  and  $\alpha_1, \ldots, \alpha_t \in \mathbb{C}[x]$ . Finally, we assume that  $\deg(\alpha_1) > \deg(\alpha_i)$  for i > 1.

We mention that for binary recurrences the authors together with Kreso proved in [9] that if  $G_n(x) = g \circ h$ , then either deg g is bounded independently of n and only in terms of the initial data, unless h is special (meaning that (g, h) is equivalent to  $(g', x^m)$  or  $(g'', T_m(x))$  where  $(T_n(x))_{n=0}^{\infty}$  denotes the sequence of Chebyshev polynomials and  $g', g'' \in \mathbb{C}[x]$ ) or a technical condition is not verified (see the paper for details). This describes the "outer" decomposition factor in such a decomposition. In view of this result, which we expect (without the technical condition) to hold in general, we restrict ourselves to *m*-decompositions for an integer  $m \ge 2$  which we view as fixed from now on.

We further mention that for a given sequence  $(G_n(x))_{n=0}^{\infty}$  the decompositions of the form  $G_n(x) = G_m \circ h$  for a fixed polynomial  $h \in \mathbb{C}[x]$ , deg  $h \ge 2$  were considered in [8, 13, 14]. It was Zannier who proved in general that this equation has only finitely many solutions  $(n, m), n \ne m$ , unless we are in the cyclic or Chebyshev case as above (cf. [23]). This result was made effective in [11]. A further result in this direction can be found in [15].

There are a few trivial situations that we have to take into account below. If  $G_n(x) = f(\beta^n)$  with  $f, \beta \in \mathbb{C}[x]$ , then every decomposition  $f(x) = g \circ h$  with deg g = m leads to a sought decomposition  $G_n(x) = g(h(\beta^n))$  for every  $n \in \mathbb{N}$ . Observe that this situation might also lead to slightly different decompositions. Assume e.g. that  $G_n(x) = a_1\alpha_1^n + a_2, a_1, a_2 \in \mathbb{C}, \alpha_1 \in \mathbb{C}[x]$ ; if *n* is a multiple of *m*, i.e.  $n = m\ell$ , then  $G_n(x) = g \circ h$  with  $g(x) = a_1x^m + a_2, h(x) = \alpha_1^\ell$ . More generally, when  $G_n(x) = g(H_n(x))$  with  $g \in \mathbb{C}[x]$ , deg g = m and  $(H_n(x))_{n=0}^{\infty}$  is another linear recurrence sequence in  $\mathbb{C}[x]$ , then obviously we again have a sought decomposition for every  $n \in \mathbb{N}$ . Unfortunately it seems that these cases are not exhaustive. There might be many "sporadic" solutions that arise by polynomial-exponential equations that are complicated to control in general.

We start with the following theorem, which clarifies the structure of the "inner" decomposition factor that may appear in an *m*-decomposition of elements in the sequence  $(G_n(x))_{n=0}^{\infty}$ .

**Theorem 1.1.** Let  $(G_n(x))_{n=0}^{\infty}$  be a non-degenerate simple linear recurrence sequence of order  $d \ge 2$  with power sum representation  $G_n(x) = a_1 \alpha_1^n + \dots + a_d \alpha_d^n$  with  $a_1, \dots, a_d \in \mathbb{C}$ ,  $\alpha_1, \dots, \alpha_d \in \mathbb{C}[x]$  satisfying deg  $\alpha_1 > \max\{\deg \alpha_2, \dots, \deg \alpha_d\}$ . Moreover, let  $m \ge 2$  be an integer. Write  $m_0$  for the least integer such that  $\alpha_1^{m_0/m} \in \mathbb{C}[x]$ . Then there is an effectively computable positive constant C such that the following holds: Assume that for some  $n \in \mathbb{N}$  with n > C we have  $G_n(x) = g \circ h$  with deg g = m, deg h > 1. Then there are  $c_1, \dots, c_l \in \mathbb{C}$  such that

$$h(x) = c_1 \gamma_1^{\ell} + \dots + c_l \gamma_l^{\ell},$$

where  $m_0 \ell = n$  and  $l \in \mathbb{N}$  is bounded explicitly in terms of m, d and  $\deg(\alpha_1) + \cdots + \deg(\alpha_d)$ and  $\gamma_1, \ldots, \gamma_l \in \mathbb{C}(x)$  can be given explicitly in terms of  $\alpha_1, \ldots, \alpha_d$ , both independently of n.

This result should be compared with Proposition 2 in [25].

We illustrate the result with an example. Let  $(G_n(x))_{n=0}^{\infty}$  be given by  $G_n(x) = x^{3n} + 3(2x^2)^n + 3(4x)^n + 2^{3n}$  for all  $n \ge 0$  and let m = 3. We have  $\alpha_1 = x^3, \alpha_2 = 2x^2, \alpha_3 = 4x, \alpha_4 = 8$  and  $m_0 = 1$ . The proof of the theorem shows that we must have  $n \le 30$  or  $h(x) = c_1x^n + c_2$  with  $c_1, c_2 \in \mathbb{C}$ . Let  $g(x) = x^3$ . Then  $g(h(x)) = (c_1x^n + c_2)^3 = c_1^3x^{3n} + 3c_1^2c_2x^{2n} + 3c_1c_2^2x^n + c_3^3$ . Comparing g(h(x)) with  $G_n(x)$  shows that  $c_1^3 = 1, c_1^2c_2 = 2^n, c_1c_2^2 = 4^n, c_3^2 = 8^n$ . This defines a subvariety  $\mathcal{V}$  of  $\mathbb{A}^2 \times \mathbb{G}_m$ . Up to (possibly) finitely many exceptions for small n we have  $G_n(x) = g(h(x)) = (c_1x^n + c_2)^3$ , where  $(c_1, c_2, n) \in \mathcal{V}(\mathbb{C})$ .

Observe that  $m_0$  in the theorem can also be described as follows: Write  $\alpha_1(x) = v(x - v_1)^{k_1} \dots (x - v_t)^{k_t}$  and define  $\psi$  by  $\psi^m = \alpha_1$ . Put  $d = \text{gcd}(k_1, \dots, k_t, m)$ . Then  $m_0 = m/d$ . Obviously,  $\psi^{m/d} \in \mathbb{C}[x]$ . Conversely, observe that  $m_0$  is a divisor of m since by definition of  $m_0$  the polynomial  $T^{m_0} - \psi^{m_0}$  is the minimal polynomial of  $\psi$  over  $\mathbb{C}(x)$  (cf. Proposition 2.2) and thus divides  $T^m - \psi^m$  over  $\mathbb{C}(x, \psi)$ . Since  $\psi^{m_0} \in \mathbb{C}(x)$ , it follows  $m_0k_i/m \in \mathbb{N}$  and thus  $m/m_0$  divides  $k_i$  (thus  $\text{gcd}(k_1, \dots, k_t, m) = d$ ) for  $i = 1, \dots, t$ . The smallest such integer is obtained in the case of equality giving  $m = m_0 d$  as claimed.

The structure of all *m*-decompositions for a given  $m \ge 2$  can now be described as follows.

**Theorem 1.2.** Let  $(G_n(x))_{n=0}^{\infty}$  be a non-degenerate simple linear recurrence sequence of order  $d \ge 2$  with power sum representation  $G_n(x) = a_1 \alpha_1^n + \dots + a_d \alpha_d^n$  with  $a_1, \dots, a_d \in \mathbb{C}$ ,  $\alpha_1, \dots, \alpha_d \in \mathbb{C}[x]$  satisfying deg  $\alpha_1 > \max\{\deg \alpha_2, \dots, \deg \alpha_d\}$ . Moreover, let  $m \ge 2$  be an integer. Write  $m_0$  for the least integer such that  $\alpha_1^{m_0/m} \in \mathbb{C}[x]$ . Then there is an

explicitly computable positive constant C, and a subvariety  $\mathcal{V}$  of  $\mathbb{A}^{l+m+1} \times \mathbb{G}_{m}^{t}$  with t, l bounded explicitly in terms of m, d and  $\deg(\alpha_{1}) + \cdots + \deg(\alpha_{d})$  for which a system of polynomial-exponential equations in the polynomial variables  $c_{1}, \ldots, c_{l}, g_{0}, \ldots, g_{m}$  and the exponential variable  $\ell$  (with coefficients in  $\mathbb{Q}$ ) can be written down explicitly such that the following holds:

- (1) Defining  $G(x) = g_0 x^m + g_1 x^{m-1} + \dots + g_m \in \mathbb{C}[\mathcal{V}][x]$  and  $H_\ell = c_1 \gamma_1^\ell + c_2 \gamma_2^\ell + \dots + c_l \gamma_l^\ell \in \mathbb{C}[\mathcal{V}][x]$ , where  $\gamma_1, \dots, \gamma_l \in \mathbb{C}(x)$  can be given explicitly in terms of  $\alpha_1, \dots, \alpha_d$ , then  $G_{m_0\ell} = G \circ H_\ell$  holds as an equation in x with coefficients in the coordinate ring of  $\mathcal{V}$ . In particular, for any point  $P = (c_1, \dots, c_l, g_0, \dots, g_m, \ell) \in \mathcal{V}(\mathbb{C})$  we get a decomposition  $G_n(x) = g \circ h$ ,  $g(x) = G(P, x) \in \mathbb{C}[x]$  and  $h(x) = H_l(P, x) \in \mathbb{C}[x]$  (with  $n = m_0\ell$ ).
- (2) Conversely, let  $G_n(x) = g \circ h$  be a decomposition of  $G_n(x)$  for some  $n \in \mathbb{N}$  with  $g, h \in \mathbb{C}[x]$ , deg g = m, deg h > 1. Then either  $n \leq C$  or there exists a point  $P = (g_0, \ldots, g_m, c_1, \ldots, c_l, \ell) \in \mathcal{V}(\mathbb{C})$  with g(x) = G(P, x) and  $h(x) = H_\ell(P, x)$  and  $n = m_0 \ell$ .

Remarks and special cases.

- (a) Binary case: Let  $(G_n(x))_{n=0}^{\infty}$  be a non-degenerate binary simple linear recurrence which does not satisfy a recurrence relation of order less than 2; thus, we have  $G_n(x) = a_1 \alpha_1^n + a_2 \alpha_2^n$  with  $a_1, a_2 \in \mathbb{C}$ . We assume that  $\alpha_1, \alpha_2 \in \mathbb{C}[x]$  and deg  $\alpha_1 >$ deg  $\alpha_2$ . Moreover, we assume that one of the conditions of [9, Theorem 2] is satisfied. Then there is an effectively computable constant *C* and there are finitely many subvarieties  $\mathcal{V}_i$  of  $\mathbb{A}^{m_i+1+l_i} \times \mathbb{G}_m^{t_i}$  and equations  $G_{m_{0,i}\ell}(x) = G^{(i)} \circ H_\ell^{(i)}$ , where deg  $G^{(i)} = m_i \ge 2$ , in the coordinate ring of  $\mathcal{V}_i$  such that the following holds: If  $G_n(x) = g \circ h$  for some  $n \in \mathbb{N}$  and  $g, h \in \mathbb{C}[x]$ , deg g, deg h > 1 with h(x) indecomposable and not of the shape  $ax^m + b, m \in \mathbb{N}, a, b \in \mathbb{C}$ , then either  $n \le C$  or there is an i and a  $P = (g_{i0}, \dots, g_{im_i}, c_{i1}, \dots, c_{il_i}, \ell) \in \mathcal{V}_i(\mathbb{C})$  such that  $n = m_{0,i}\ell, g(x) = G^{(i)}(P, x), h(x) = H_\ell^{(i)}(P, x).$
- (b) When all  $\alpha_i$  are monic, then the varieties can be chosen without the  $\mathbb{G}_m$ -part.
- (c) Assume that  $\alpha_1 \in \mathbb{C}[x]$  satisfies  $1 \le k := \deg \alpha_1 \le m$ . Then  $G_n(x) = g \circ h$  with n > C implies that *h* is of the form  $c_1 + c_2 \alpha_1^{\deg G_n/(mk)}$  with  $c_1, c_2 \in \mathbb{C}$ .
- (d) Assume that  $\alpha_1 = \beta^{m_1}, \alpha_2 = \beta^{m_2}, \dots, \alpha_d = \beta^{m_d}$  with  $m_1 > m_2 \ge \dots \ge m_d \ge 0$ . Then  $G_n(x) = f(\beta^n)$ , where  $f(x) = f_1 x^{m_1} + f_2 x^{m_2} + \dots + f_d x^{m_d}$ . In this case it follows that either  $n \le C$  or  $h(x) = c_1 \beta^{k_1 \ell} + \dots + c_l \beta^{k_l \ell} = h'(\beta^\ell)$  for some

 $h' \in \mathbb{C}[x]$ . Thus if  $G_n(x) = g \circ h = (g \circ h')(\beta^{\ell}) = f(\beta^{m_0 \ell})$ . Therefore, the problem reduces to find all *m*-decompositions of the polynomial  $f \circ x^{m_0}$ .

- (e) The proof shows that if  $(G_n(x))_{n=0}^{\infty}$  is defined over a number field, i.e. the coefficients of the Binet-type equation (1.2) as well as the characteristic roots are polynomials with coefficients in some number field *K*, then all decomposition factors *g*, *h* are defined over *K* as well. In this case we are interested in decompositions over *K*, which can be described by the above conclusion of the statements.
- (f) We also remark that the above results include a description in finite terms of all *m*-th powers in a linear recurring sequence of polynomials satisfying the conditions of the theorem (i.e. the sequence is non-degenerate and simple and the characteristic roots are polynomials where one has degree larger than all others). This follows by fixing  $g(x) = x^m$  and then going through the proof of the above theorem.
- (g) Finally, we mention that if we know that the  $c_i$  can be parametrized by power sums as well (in particular if they are constant) and that we have a decomposition for any  $\ell$  (or for all members along an arithmetic progression), then these families are easy to calculate. This follows since we may identify varying powers by indeterminates (see e.g. [6, Lemma 2.1]) and then use the algorithm in [4] for polynomials in several variables (actually, we view such a polynomial as a polynomial in one of the variables; the other variables can be embedded into  $\mathbb{C}$ so that we may view the polynomial again as an element in  $\mathbb{C}[x]$ ) to determine the decompositions.

The proof of the theorems follows essentially the ideas of [25]. Assume that  $G_n(x) = g \circ h$ . This equality is viewed as an equation for the unknown h = h(x); it is a root of  $g(T) - G_n(x) = 0$  over the (rational) function field  $\mathbb{C}(G_n(x))$ . Thus we can expand h as a Puiseux series in terms of quantities  $G_n(x)^{s/m}$ ,  $s = 1, 0, -1, \ldots$ , where  $m = \deg g$ . Then one uses the multinomial series to expand  $G_n(x)^{s/m}$  for any s; in order to justify this multiple expansion, the "dominant root condition" on the degrees of the characteristic roots is needed. Afterwards we use, as in [25], a function field variant of the Schmidt subspace theorem (Proposition 2.4) proved in [25], to find that either n is bounded or h can be expressed as given in Theorem 1.1. Using this information, one views the  $c_1, \ldots, c_l$  as well as the coefficients  $g_0, \ldots, g_m$  of g, while the degree of g is fixed, as indeterminants and then compares  $g \circ h$  with  $G_n(x)$  for the given  $n \in \mathbb{N}$ . Using unit equations over function fields, this either implies that n is bounded or we have two linear recurrences

that are related (see [20] for this notation). In the latter case, up to a permutation, the characteristic roots have to match up and then, since they are monic polynomials at that point, the coefficients coincide. This gives polynomial-exponential equations that can be written down explicitly and which define a variety. From this the statement follows.

The rest of the paper is organized as follows. In the next section we collect some auxiliary results that will be needed for the proof of the theorems. In Section 3 we give the proofs of Theorem 1.1 and 1.2. In Section 4 we give some more details justifying the remarks and special cases.

#### 2. Auxiliary results

In this section, we recall some basic information and collect some statements, which we will make use of in our proofs later on.

Generally, an algebraic function field F/K is a finite algebraic extension of K(x), where x is some element transcendental over K. If F is itself of the shape F = K(x), then F is said to be rational. The rational function field has genus  $g_F = 0$ . Throughout this paper, we will work over the complex numbers  $K = \mathbb{C}$ , even though our proofs hold over any other algebraically closed field as well. Then

$$\mathbb{C}(x) = \left\{ \frac{f(x)}{g(x)}; \ f(x), g(x) \in \mathbb{C}[x], \ g(x) \neq 0 \right\},\$$

i.e.  $\mathbb{C}(x)$  is the field of fractions of  $\mathbb{C}[x]$ . On  $\mathbb{C}(x)$  we define valuations as follows. For each  $a \in \mathbb{C}$ , let  $v_a(f)$  be the unique integer such that  $f(x) = (x - a)^{v_a(f)}p(x)/q(x)$ , where  $p, q \in \mathbb{C}[x]$  are such that  $p(a)q(a) \neq 0$ . Moreover, with the symbol  $\infty$  we associate the valuation  $v_{\infty}(f) = \deg q - \deg p$ , where f(x) = p(x)/q(x). If  $v_a(f) > 0$  for an  $a \in \mathbb{C}$ , ais called a zero of f, and it is called a pole of f, if  $v_a(f) < 0$ . These functions are all (normalized, up to equivalence) valuations on  $\mathbb{C}(x)$  and for a finite extension L of  $\mathbb{C}(x)$ each one of them can be extended to at most  $[F : \mathbb{C}(x)]$  valuations on F, which again gives all discrete valuations on F. Both, in  $\mathbb{C}(x)$  and in F, for any  $f \in F/\mathbb{C}$  the so-called sum formula holds, that is

$$\sum_{\nu}\nu(f)=0,$$

where the sum is taken over all valuations on the respective function field. There is a one-to-one relation between valuations and places, namely for any valuation  $v_a$  on  $\mathbb{C}(x)$ ,  $a \in \mathbb{C} \cup \{\infty\}$ , there is a place  $P_a = \{f \in \mathbb{C}(x); v_a(f) > 0\}$  (it is the unique maximal ideal of the valuation ring  $O_{P_a} = \{f \in \mathbb{C}(x); v_a(f) \ge 0\}$ ). Therefore, valuations are sometimes introduced in terms of places (and often instead of  $P_a$  we simply write a). We write  $\mathbb{P}_F$  for the set of places of the field F. Now let F' be an algebraic extension of

the function field *F*. Then a place  $P' \in \mathbb{P}_{F'}$  is said to lie over  $P \in \mathbb{P}_F$ , if  $P \subset P'$ . We write P'|P in this case. Then there is an integer e = e(P'|P),  $1 \le e \le [F' : F]$ , called the ramification index of P' over P, such that  $v_{P'}(x) = e \cdot v_P(x)$  for all  $x \in F$ . We say that P'|P is ramified if e(P'|P) > 1 and unramified otherwise. If e(P'|P) = [F' : F], there is exactly one place  $P' \in F'$  lying above  $P \in F$  and P' is said to be totally ramified. The places  $P' \in \mathbb{P}_{F'}$  lying above  $P \in \mathbb{P}_F$  correspond to the extensions of the respective valuation  $v_P$  in *F*. Denote by  $F_P$  the residue class field  $O_P/P$ . We shall need the following two statements, which can be found in [21].

**Proposition 2.1.** Let  $F/\mathbb{C}$  be a function field in one variable and  $\varphi \in F[T]$ ,

$$\varphi(T) = a_n T^n + a_{n-1} T^{n-1} + \dots + a_1 T + a_0$$

If there is a place  $P \in \mathbb{P}_F$  such that  $v_P(a_n) = 0$ ,  $v_P(a_i) \ge 0$  for i = 1, ..., n-1,  $v_P(a_0) < 0$ and  $gcd(n, v_P(a_0)) = 1$ , then  $\varphi(T)$  is irreducible in F[T]. Furthermore, if F' = F(y), where y is a root of  $\varphi(T)$ , then P has a unique extension  $P' \in \mathbb{P}_{F'}$  and e(P'|P) = n.

**Proposition 2.2.** Let  $F/\mathbb{C}$  be a function field in one variable. Suppose that  $u \in F$  satisfies  $u \neq w^d$  for all  $w \in F$  and d|n, d > 1. Let F' = F(z) with  $z^n = u$ . Then F' is said to be a Kummer extension of F and we have:

- The polynomial φ(T) = T<sup>n</sup> − u is the minimal polynomial of z over F (in particular, it is irreducible over F). The extension F'/F is Galois of degree n; its Galois group is cyclic, and all automorphisms of F'/F are given by σ(z) = ζz, where ζ ∈ C is an n-th root of unity.
- (2) Let  $P \in \mathbb{P}_F$  and  $P' \in \mathbb{P}_{F'}$  be an extension of P. Let  $r_P := \operatorname{gcd}(n, v_P(u))$ . Then  $e(P'|P) = n/r_P$ .
- (3) Denote by g (resp. g') the genus of  $F/\mathbb{C}$  (resp.  $F'/\mathbb{C}$ ). Then

$$\mathfrak{g}' = 1 + n(\mathfrak{g} - 1) + \frac{1}{2} \sum_{P \in \mathbb{P}_F} (n - r_P) \deg P.$$

Our strategy also involves the use of height functions in function fields. Define the projective height  $\mathcal{H}$  of  $u_1, \ldots, u_n \in F/\mathbb{C}$ , where  $n \ge 2$  and not all  $u_i$  are zero, via

$$\mathcal{H}(u_1,\ldots,u_n)=-\sum_{\nu}\min(\nu(u_1),\ldots,\nu(u_n))$$

Also, for a single element  $f \in F^*$ , set

$$\mathcal{H}(f) = -\sum_{\nu} \min(0, \nu(f)).$$

In both cases the sum is taken over all discrete valuations v on F. Note that  $v(f) \neq 0$  only for a finite number of valuations v and that  $\mathcal{H}(f) = \sum_{v} \max(0, v(f))$  if  $f \in F^*$ , by the sum formula. For f = 0, we define  $\mathcal{H}(f) = \infty$ . We state some basic properties of the projective height, cf. [9].

**Lemma 2.3.** Denote as above by  $\mathcal{H}$  the projective height on  $F/\mathbb{C}$ . Then for  $f, g \in F^*$  the following properties hold:

- (1)  $\mathcal{H}(f) \ge 0$  and  $\mathcal{H}(f) = \mathcal{H}(1/f)$ ,
- (2)  $\mathcal{H}(f) \mathcal{H}(g) \le \mathcal{H}(f+g) \le \mathcal{H}(f) + \mathcal{H}(g),$
- (3)  $\mathcal{H}(f) \mathcal{H}(g) \leq \mathcal{H}(fg) \leq \mathcal{H}(f) + \mathcal{H}(g),$
- (4)  $\mathcal{H}(f^n) = |n| \cdot \mathcal{H}(f),$
- (5)  $\mathcal{H}(f) = 0 \Leftrightarrow f \in \mathbb{C}^*$ ,
- (6)  $\mathcal{H}(A(f)) = \deg A \cdot \mathcal{H}(f)$  for any  $A \in \mathbb{C}[T] \setminus \{0\}$ .

The following proposition is an important ingredient for the proof of our first theorem. It can be seen as a function field analogue of the Schmidt subspace theorem, modelled by Zannier, cf. [25].

**Proposition 2.4** (Zannier). Let  $F/\mathbb{C}$  be a function field in one variable, of genus g, let  $\varphi_1, \ldots, \varphi_n \in F$  be linearly independent over  $\mathbb{C}$  and let  $r \in \{0, 1, \ldots, n\}$ . Let S be a finite set of places of F containing all the poles of  $\varphi_1, \ldots, \varphi_n$  and all the zeros of  $\varphi_1, \ldots, \varphi_r$ . Put  $\sigma = \sum_{i=1}^n \varphi_i$ . Then

$$\sum_{\nu \in S} \left( \nu(\sigma) - \min_{i=1,\dots,n} \nu(\varphi_i) \right) \le \binom{n}{2} (|S| + 2\mathfrak{g} - 2) + \sum_{i=r+1}^n \deg(\varphi_i).$$

Recall that for a finite set *S* of places (or valuations, respectively) of *F*, an element  $f \in F$  is called an *S*-unit, if it has zeros and poles only at places in *S*, i.e. the set of *S*-units is given by

$$O_S^* = \{ f \in L; v(f) = 0 \text{ for all } v \notin S \}.$$

We will also use the following result due to Brownawell and Masser [5] taken from [16], giving an upper bound for the height of *S*-units, which arise as a solution of certain *S*-unit-equations.

**Proposition 2.5** (Brownawell–Masser). Let  $F/\mathbb{C}$  be a function field in one variable of genus g. Moreover, for a finite set S of discrete valuations, let  $u_1, \ldots, u_n$  be S-units, not all constant, and

$$1 + u_1 + u_2 + \dots + u_n = 0$$
,

where no proper subsum of the left side vanishes. Then it holds

$$\max_{i=1,\ldots,n} \mathcal{H}(u_i) \le \frac{1}{2}n(n-1)(|S|+2\mathfrak{g}-2).$$

In our proof we will use an expansion of the polynomial h in  $G_n = g \circ h$  as a Puiseux series. Therefore, we give a quick review on formal power series, Laurent series and Puiseux series (cf. [22] and [18]). Formally, a (complex) polynomial is a sequence  $(a_0, a_1, \ldots)$ , where  $a_i \in \mathbb{C}$  and where there exists an  $n \in \mathbb{N}$  such that  $a_j = 0$  for all  $j \ge n$ . Such an element is associated with the finite sum  $a_0 + a_1x + \cdots + a_nx^n$ , where x is an indeterminate identified with the element (0, 1, 0, 0, ...). Together with the usual addition and multiplication this gives the  $\mathbb{C}$ -algebra of (complex) polynomials  $\mathbb{C}[x]$ . If we also allow sequences with infinite support, we obtain the algebra of formal power series, denoted by  $\mathbb{C}[x]$ , that is the set

$$\mathbb{C}[\![x]\!] = \{(a_0, a_1, a_2, \dots); a_i \in \mathbb{C}\} = \{a_0 + a_1 x + a_2 x^2 + \dots; a_i \in \mathbb{C}\},\$$

where addition and multiplication are defined just in the same way as for polynomials. Note that the notation as an infinite sum is meant only formally, i.e. questions of convergence are disregarded.  $\mathbb{C}[x]$  is an integral domain and the units in  $\mathbb{C}[x]$  are precisely the elements with non-zero constant term. The field of fractions of  $\mathbb{C}[x]$  is the field of formal Laurent series, denoted by  $\mathbb{C}(x)$ . It is the localization of  $\mathbb{C}[x]$  with respect to the ideal (x) and its elements are given by the set

$$\mathbb{C}(\!(x)\!) = \{(a_m, a_{m+1}, a_{m+2}, \ldots); \ m \in \mathbb{Z}, \ a_i \in \mathbb{C}\} \\ = \{a_m x^m + a_{m+1} x^{m+1} + a_{m+2} x^{m+2} + \ldots; \ m \in \mathbb{Z}, \ a_i \in \mathbb{C}\},\$$

so a Laurent series is the sum of a formal power series plus possibly a finite number of terms with negative exponent. Defining  $\operatorname{ord}(f)$  to be the smallest *i* such that  $a_i \neq 0$  if  $f \neq 0$ , and  $\operatorname{ord}(0) = \infty$  gives a discrete valuation on  $\mathbb{C}(x)$ . The valuation ring is given by  $\mathbb{C}[x]$  and the residue field is  $\mathbb{C}$ . Moreover,  $\mathbb{C}(x)$  is a field (in general, K(x)) is a field if *K* is a field), which is the completion with respect to this valuation topology of the field  $\mathbb{C}(x)$  of rational functions.

As a generalization, the field of formal Puiseux series is obtained by allowing also fractional exponents, i.e. Laurent series in  $\mathbb{C}(x^{1/n})$  for some  $n \in \mathbb{N}$ . More precisely, the

field of formal Puiseux series is given by

$$\mathbb{C}(\!(x^{1/\infty})\!) = \bigcup_{n=0}^{\infty} \mathbb{C}(\!(x^{1/n})\!).$$

The valuation ord naturally extends to this field and it is complete with respect to the induced topology. The classical Newton–Puiseux theorem shows that  $\mathbb{C}((x^{1/\infty}))$  is an algebraic closure of the field of formal Laurent series  $\mathbb{C}((x))$ .

If  $F/\mathbb{C}$  is a function field in one variable of degree  $[F : \mathbb{C}(x)] = n$ , then there is a primitive element  $y \in F$  over  $\mathbb{C}(x)$  which satisfies an irreducible equation

$$f(x,Y) = Y^{n} + c_{1}(x)Y^{n-1} + \dots + c_{n}(x) = 0$$
(2.1)

with coefficients  $c_i(x)$  in  $\mathbb{C}(x)$ . Without loss of generality, we can also assume the  $c_i(x)$  to be polynomials. For the expansion of *h* as a Puiseux series, we rely on the following classical theorem, cf. [7].

**Proposition 2.6** (Puiseux's Theorem). Let  $F/\mathbb{C}$  be a function field in one variable of degree  $[F : \mathbb{C}(x)] = n$ . Then there are  $1 \le r \le n$  natural numbers  $e_i$  satisfying

$$e_1 + e_2 + \dots + e_r = n$$

which have the following meaning: the irreducible equation (2.1) satisfied by an arbitrary function y in F has for solutions the r series

$$y_i = \sum_{k=\nu_i}^{\infty} a_{ik} x^{-k/e_i}, \quad a_{i\nu_i} \neq 0, \quad i = 1, 2, \dots, r.$$
 (2.2)

With a primitive  $e_i$ -th root of unity  $\zeta$  form

$$y_{ij} = \sum_{k} a_{ik} \zeta^{jk} x^{-k/e_i}, \quad j = 0, \dots, e_i - 1;$$

then f(x, Y) is identical with

$$f(x,Y) = \prod_{i,j} (Y - y_{ij}).$$
 (2.3)

The coefficients  $a_{ik}$  are constant, i.e.  $a_{ik} \in \mathbb{C}$ , and their images under isomorphisms of  $\mathbb{C}$  give permutations of the  $y_{ij}$  in (2.3).

We remark that in the above theorem *r* is the number of places  $P_i|P_{\infty}$  for the unique infinite place  $P_{\infty} \in \mathbb{P}_{\mathbb{C}(x)}$ , where  $P_i \in \mathbb{P}_F$ . Moreover,  $v_i = v_{P_i}(y)$  is the valuation of *y* at  $P_i$  and  $e_i = e(P_i|P_{\infty})$  is the ramification index of  $P_i$  over  $P_{\infty}$ .

Finally, we state the following little lemma that will be useful in the proof.

**Lemma 2.7.** Let  $f \in \mathbb{C}[x]$ . Then  $f(1/y) \in \mathbb{C}(y)$  with a pole only at y = 0. Moreover, the order of vanishing at y = 0 of f(1/y) is equal to  $-\deg f$ .

*Proof.* Write  $f(x) = f_0(x - a_1)^{k_1} \dots (x - a_t)^{k_t}$  with  $k_1 + \dots + k_t = \deg f$ . Put y = 1/x. Then  $f(1/y) = f(x) = y^{-(k_1 + \dots + k_t)} f_0(1 - a_1 y)^{k_2} \dots (1 - a_t y)^{k_t}$ , which shows that the multiplicity of y = 0 as a pole of f(1/y) in  $\mathbb{C}(y)$  is equal to deg f. This is the claim.  $\Box$ 

#### 3. Proof of Theorem 1.1 and 1.2

#### 3.1. Proof of Theorem 1.1

Let  $g \in \mathbb{C}[x]$  be a polynomial of degree deg  $g = m \ge 2$  and  $(G_n(x))_{n=0}^{\infty}$  as given in the theorem.

Let  $b_1, \ldots, b_d \in \mathbb{C}$  be the leading coefficients of  $\alpha_1, \ldots, \alpha_d$  respectively. We write  $\alpha_i^n = b_i^n \beta_i^n$  for  $i = 1, \ldots, d$  and therefore have

$$G_n(x) = a_1 b_1^n \beta_1^n + \dots + a_d b_d^n \beta_d^n$$

where  $a_1, \ldots, a_d, b_1, \ldots, b_d \in \mathbb{C}$  and  $\beta_1, \ldots, \beta_d \in \mathbb{C}[x]$  have leading coefficients equal to 1 and satisfy deg  $\beta_1 > \max{\deg \beta_2, \ldots, \deg \beta_d}$ .

Let *K* be the rational function field  $K = \mathbb{C}(x)$  and let *z* be a root of  $\varphi(T) = g(T) - x = g_0 T^m + \cdots + g_m \in K[T]$ . At the infinite place  $P = P_\infty$  we have  $v_\infty(g_0) = v_\infty(g_i) = 0$  for  $i = 1, \ldots, m - 1$  and  $v_\infty(g_m) = v_\infty(g(0) - x) = -1$ . Also,  $gcd(deg \varphi, v_\infty(g_m)) = gcd(m, -1) = 1$ . Therefore, by Proposition 2.1,  $\varphi(T)$  is irreducible over  $\mathbb{C}(x)$  and  $P_\infty$  has a unique extension  $P'_{\infty'} \in \mathbb{P}_L$ , where  $L = \mathbb{C}(x)(z) = \mathbb{C}(x, z)$ . By Puiseux's Theorem (Theorem 2.6), it follows that there is an expansion of *z* of the form

$$z = \sum_{k=\nu_{\infty'}}^{\infty} u_k (\sqrt[m]{1/x})^k$$
  
=  $u_{-1} (\sqrt[m]{1/x})^{-1} + u_0 (\sqrt[m]{1/x})^0 + u_1 (\sqrt[m]{1/x})^1 + u_2 (\sqrt[m]{1/x})^2 + \dots$   
=  $u_{-1} x^{1/m} + u_0 + u_1 x^{-1/m} + u_2 x^{-2/m} + \dots,$  (3.1)

where the  $u_j \in \mathbb{C}$  depend only on g. Note that we have used that  $e_i(\infty') = m$  in Theorem 2.6, by Proposition 2.1 and that  $v_{\infty'}(z) = -1$ . This can be seen as follows. Since z is a root of  $\varphi(T)$ , we have that g(z) = x, hence  $v_{\infty'}(g_0 z^m + \cdots + g_{m-1}z + g(0)) = v_{\infty'}(x) = m \cdot v_{\infty}(x) = -m$ . By integrality we have  $v_{\infty'}(z) < 0$ , so using the strict triangle inequality we get

$$m \cdot v_{\infty'}(z) = \min_{i=1,\dots,m} (i \cdot v_{\infty'}(z)) = \min_{i=1,\dots,m} (v_{\infty'}(g_{m-i}z^i)) = -m.$$

This expansion is understood as an equality in the algebraic closure of the field of formal Laurent series  $\mathbb{C}(x)$ , which itself is the usual metric completion of *K* (which has the property that an infinite sum converges if and only if each fixed power of *x* appears in

only finitely many terms). Hence, if  $G_n(x) = g \circ h$ , substituting  $G_n(x)$  for x and h(x) for z, this yields an expansion for h(x) of the form

$$h(x) = u_{-1}G_n(x)^{1/m} + u_0 + u_1G_n(x)^{-1/m} + u_2G_n(x)^{-2/m} + \dots,$$
(3.2)

for a suitable choice of the *m*-th root of  $G_n(x)$ , where the coefficients  $u_i \in \mathbb{C}$  depend only on *g*. As in [25], we expand the different roots  $G_n(x)^{s/m}$  for  $s \in \{1, 0, -1, ...\}$  using the multinomial theorem and equation (1.2) to get

$$G_{n}(x)^{s/m} = (a_{1}\alpha_{1}^{n} + a_{2}\alpha_{2}^{n} + \dots + a_{d}\alpha_{d}^{n})^{s/m}$$
  
$$= a_{1}^{s/m}\alpha_{1}^{ns/m} \left(1 + \frac{a_{2}}{a_{1}} \left(\frac{\alpha_{2}}{\alpha_{1}}\right)^{n} + \dots + \frac{a_{d}}{a_{1}} \left(\frac{\alpha_{d}}{\alpha_{1}}\right)^{n}\right)^{s/m}$$
  
$$= a_{1}^{s/m}\alpha_{1}^{ns/m} \sum_{\bar{h}} b_{\bar{h}}a_{2}^{h_{2}} \dots a_{d}^{h_{d}}a_{1}^{-(h_{2}+\dots+h_{d})} \left(\alpha_{2}^{h_{2}} \dots \alpha_{d}^{h_{d}}\alpha_{1}^{-(h_{2}+\dots+h_{d})}\right)^{n},$$

where  $\bar{h} = (h_2, ..., h_d)$  runs through  $\mathbb{N}^{d-1}$ . Now, we put y = 1/x. Then we see that h(x) = h(1/y) can be written as an infinite sum

$$h(1/y) = u_{-1}G_n(1/y)^{1/m} + u_0 + u_1G_n(1/y)^{-1/m} + u_2G_n(1/y)^{-2/m} + \dots$$

of terms  $t(x) = t_{h_2,...,h_d,s}(1/y)$  of the shape

$$c \cdot \alpha_1 (1/y)^{ns/m - n(h_2 + \dots + h_d)} \cdot \alpha_2 (1/y)^{nh_2} \dots \alpha_d (1/y)^{nh_d}, \quad c \in \mathbb{C}.$$
 (3.3)

Observe that as an element of  $\mathbb{C}(y)$  the rational function h(1/y) equals  $y^{-\deg h} + \dots$ , since by Lemma 2.7 it can be written as  $y^{-\deg h}$  times a polynomial in y starting with a non-zero constant term (which is a unit in the ring  $\mathbb{C}[\![y]\!]$ ). (Here we assume, as we may, that h is monic; otherwise the series would start with  $y^{-\deg h}$  times the leading coefficient of h.) A similar consideration shows that each of the terms on the right hand side, written down explicitly in (3.3), up to a non-zero constant equals  $v^{(-\deg \alpha_1(s/m-(h_2+\dots+h_d)-h_2\deg \alpha_2-\dots-h_d\deg \alpha_d)n}$  times a power series that is a unit in the ring  $\mathbb{C}[y]$ . The "smallest" such term (i.e. the term with smallest order as a Laurent series) appears precisely with s = 1 and  $h_2 = \cdots = h_d = 0$  (since by assumption deg  $\alpha_1 > \deg \alpha_i$ for  $i \ge 2$ ), from which we see that the right hand side starts with  $y^{-n \deg \alpha_1/m}$  up to a constant in C. In view of deg  $G_n = n \deg \alpha_1 = m \deg h = \deg g \deg h = \deg(g \circ h)$ this perfectly makes sense. We also remark that only terms with s = 0, 1 contribute to  $h(1/y) = y^{-\deg h} + \cdots + h_0$ , where  $h_0 = 0 = h(0)$ , since terms with s < 0, up to a constant, start with  $y^{|s| \deg \alpha_1 n/m}$ . We still have to show that the infinite sum converges as an element of  $\mathbb{C}(y)$ . This is clear since for  $s \to -\infty$  the power of y goes to  $\infty$ . We give an alternative proof: We show that for an arbitrary  $J \in \mathbb{N}$ , there is an upper bound on the number L of quantities  $t_1(1/y), \ldots, t_L(1/y)$  in the expansion of h(1/y) that satisfy  $v_0(t_i(1/y)) < nJ$ , where  $v_0$  denotes the order on  $\mathbb{C}(y)$  (observe that *n* is considered at this point to be fixed such that  $G_n(x) = g \circ h$ ). For a term of the shape (3.3), its order is given by

$$v_{0}(t(1/y)) = n \cdot \left[ \left( \frac{s}{m} - (h_{2} + \dots + h_{t}) \right) \cdot v_{0}(\alpha_{1}(1/y)) + h_{2}v_{0}(\alpha_{2}(1/y)) + \dots + h_{d}v_{0}(\alpha_{d}(1/y)) \right]$$
  
=  $n \cdot \left[ \frac{s}{m} \cdot v_{0}(\alpha_{1}(1/y)) + h_{2}(v_{0}(\alpha_{2}(1/y) - v_{0}(\alpha_{1}(1/y))) + \dots + h_{d}(v_{0}(\alpha_{d}(1/y)) - v_{0}(\alpha_{1}(1/y))) \right].$  (3.4)

Note again that by Lemma 2.7 we have  $v_0(\alpha_i(1/y)) = v_0(\alpha_i(x)) = -\deg \alpha_i$ . Since by assumption  $\deg \alpha_1 > \deg \alpha_i$  for  $i \ge 2$ , it follows that  $\deg \alpha_1 \ge \deg A_0/d$ . In the case  $s \le 0$  we therefore find

$$\nu_0(t(1/y)) = n \left[ \frac{-s}{m} \deg \alpha_1 + h_2(\deg \alpha_1 - \deg \alpha_2) + \dots + h_d(\deg \alpha_1 - \deg \alpha_d) \right]$$
  
$$\geq n \left[ \frac{-s}{m} \cdot \frac{\deg A_0}{d} + h_2 + \dots + h_d \right].$$

We observe that if  $v_0(t_i(1/y)) < nJ$ , we must have that  $s \in \{0, -1, ..., -Jmd/\deg A_0+1\}$ , since otherwise we would get

$$\nu_0(t(1/y)) \ge n \left[ \frac{-s}{m} \cdot \frac{\deg A_0}{d} + h_2 + \dots + h_d \right] \ge n \left[ \frac{Jmd}{\deg A_0} \cdot \frac{\deg A_0}{md} \right] = nJ.$$

To estimate the number of possible (d - 1)-tuples  $(h_2, \ldots, h_d) \in \mathbb{N}^{d-1}$  for each  $s \in \{0, -1, \ldots, -Jmd/\deg A_0 + 1\}$ , it obviously must hold that

$$h_i < J - \frac{|s| \deg A_0}{md} \le J,$$

so for each such *s* there are at most  $J^{d-1}$  such  $(h_2, \ldots, h_d)$ .

If s = 1 we have that

$$\nu_0(t(1/y)) = n \left[ \frac{-\deg \alpha_1}{m} + h_2(\deg \alpha_1 - \deg \alpha_2) + \dots + h_d(\deg \alpha_1 - \deg \alpha_d) \right]$$
  
$$\geq n \left[ \frac{-\deg \alpha_1}{m} + h_2 + \dots + h_d \right] \geq n \left[ \frac{-\deg A_0}{m} + h_2 + \dots + h_d \right],$$

hence, if s = 1, we must have  $h_i < J + \frac{\deg A_0}{m}$ . Then the number of possible (d - 1)-tuples  $(h_2, \ldots, h_d)$  is not greater than  $(J + \frac{\deg A_0}{m})^{d-1}$ .

We conclude that we may write

$$h(x) = h(1/y) = t_1(1/y) + \dots + t_L(1/y) + \sum_{\nu_0(t(1/y)) \ge J_n} t(1/y),$$
(3.5)

15

where L is bounded above by

$$L \le \left(J + \frac{\deg A_0}{m}\right)^{d-1} + J^d \frac{md}{\deg A_0}.$$
(3.6)

This now justifies the above formal expansions. They are well-defined in the ring  $\mathbb{C}(y)$ .

We now distinguish between two cases, namely that  $\{t_1, \ldots, t_L, h(x)\}$  is linearly dependent or linearly independent over  $\mathbb{C}$ , respectively (we will often simply write  $t_i$  instead of  $t_i(x)$ ).

*Case 1. Let us assume that the set*  $\{t_1, \ldots, t_L, h(x)\}$  *is linearly independent over*  $\mathbb{C}$ *.* 

With the intention of applying Proposition 2.4, let  $F = \mathbb{C}(y, \alpha_1(1/y)^{1/m})$  and write  $\varphi_1 = -t_1(1/y), \ldots, \varphi_L = -t_L(1/y)$  and  $\varphi_{L+1} = h(1/y)$ . Also, set  $\sigma = \sum_{i=1}^{L+1} \varphi_i = \sum_{v_0(t(1/y)) \ge Jn} t(1/y)$ . Observe that  $\varphi(T) = T^{m_0} - \alpha_1(1/y)^{m_0/m}$  is the minimal polynomial of  $\alpha_1(1/y)^{1/m}$  over  $\mathbb{C}(y)$ , where we use that the definition of  $m_0$  for  $\alpha_1$  as a polynomial in x over  $\mathbb{C}$  implies that  $\alpha_1(1/y)^{m_0/m}$  is not a power of an element in  $\mathbb{C}(y)$  for a smaller power. Since this is a Kummer extension we can apply Proposition 2.2 ([21, Theorem III.7.3]). Therefore, we get that only places in F above  $0, \infty$  and the inverses of non-zero roots of  $\alpha_1$  (as a polynomial in  $\mathbb{C}[x]$ ) ramify. Thus for the genus  $g_F$  of F we find  $2g_F - 2 \le m_0 \deg \alpha_1 \le m \deg \alpha_1$ . We define S to be the set of zeros and poles of the  $t_1, \ldots, t_L$  together with the poles of h(1/y). Observe that h(1/y) has poles at most at places above  $0, \infty$ . Therefore S may contain at most the places above  $0, \infty$  and the inverses of  $\alpha_1, \ldots, \alpha_d$ . This gives at most  $m_0(2 + \deg \alpha_1 + \cdots + \deg \alpha_d) \le m(2 + \deg A_0)$  elements in S.

Note that for any place *P* in *F* above 0 in  $\mathbb{C}(y)$  we have that

$$\nu_P(\sigma) = \nu_P\left(\sum_{\nu_0(t(1/y)) \ge Jn} t(1/y)\right) = e(P|0) \cdot \nu_0\left(\sum_{\nu_0(t(1/y)) \ge Jn} t(1/y)\right) \ge Jn.$$

Clearly,  $P \in S$ . We will also need to give an upper bound on the degree deg  $h(1/y) = [F : \mathbb{C}(h(1/y))] = \mathcal{H}(h(1/y))$ . Note that  $\mathcal{H}(h(1/y)) = (\deg h)\mathcal{H}(1/y) = (\deg h)[F : \mathbb{C}(1/y)] = (\deg h)[F : \mathbb{C}(x)] = m_0 \deg h \le m \deg h$ . Hence, deg  $h(1/y) = m_0 \deg h$ .

By Proposition 2.4 we find that

$$\sum_{\nu \in S} (\nu(\sigma) - \min_{i=1,\dots,L+1} \nu(\varphi_i)) \le \frac{1}{2} L(L+1)(|S| + 2g_F - 2) + \deg h(1/y)$$
$$\le \frac{1}{2} L(L+1) 2m_0(\deg A_0 + 1) + m_0 \deg h.$$
(3.7)

On the other hand, since  $\sigma = \sum_{i=1}^{L+1} \varphi_i$ , it follows that  $v(\sigma) - \min_{i=1,\dots,L+1} v(\varphi_i) \ge 0$ for every valuation  $v \in S$ . Moreover, for  $v_P(\sigma) \ge Jn$  and  $\min_{i=1,\dots,L+1} v_P(\varphi_i) \le 1$   $v_P(h(1/y)) \le m_0 v_0(h(1/y))) = -m_0 \deg h$  (by Lemma 2.7), we see that

$$Jn + m_0 \deg h \le \nu_P(\sigma) - \min_{i=1,\dots,L+1} \nu_P(\varphi_i) \le \sum_{\nu \in S} (\nu(\sigma) - \min_{i=1,\dots,L+1} \nu(\varphi_i)).$$

We conclude that

$$Jn + m_0 \deg h \le \sum_{\nu \in S} (\nu(\sigma) - \min_{i=1,...,L+1} \nu(\varphi_i))$$

$$\le L(L+1)m_0(\deg A_0 + 2) + m_0 \deg h,$$
(3.8)

and therefore, for n we get the upper bound

$$n \le mL(L+1)(\deg A_0 + 2)/J$$
 (3.9)

(recall that for  $J \in \mathbb{N}$  one may take any natural number to get an upper bound, and that *L* is bounded above by a constant depending only on *J*,  $m = \deg g$  and the recurrence sequence, but not on *n*).

*Case 2. Let us now consider the second case, namely that the set*  $\{t_1, \ldots, t_L, h(x)\}$  *is linearly dependent over*  $\mathbb{C}$ .

We may assume that the  $t_1, \ldots, t_L$  are linearly independent, since otherwise we just group together the terms in question properly. Therefore, in a relation of linear dependency, h(x) must appear and we may write h(x) as a linear combination of  $t_1(x), \ldots, t_L(x)$ , i.e. there are  $w_i \in \mathbb{C}$  such that

$$h(x) = \sum_{i=1}^{L} w_i t_i(x).$$
(3.10)

Recall, that the  $t_i$ 's are all of the shape (3.3), where *s* and the  $h_i$ 's are elements of a finite set of numbers. After possibly renumbering the terms, we may assume that  $w_i \neq 0$  exactly for  $i = 1, ..., l \leq L$  and we get a power sum representation of h(x) of the shape

$$h(x) = w_1 d_1 \delta_1^n + \dots + w_l d_l \delta_l^n,$$

where we can control the  $\delta_i$ 's, since they are elements of a finite set, namely

$$\delta_i \in \{\alpha_1^{s/m - (h_2 + \dots + h_i)} \alpha_2^{h_2} \dots \alpha_d^{h_d}; s \in A, h_i \in B\}$$

where  $A = \{0, 1\}$  and  $B = \{0, 1, ..., J + \deg A_0/m\}$  (for A only terms  $t_i$  with s = 0, 1 contribute, as we have already observed above). However, note that we have no control over the coefficients  $w_i d_i \in \mathbb{C}$ .

We pause a moment to investigate this relation. Remember that  $m_0$  was defined to be the least integer such that  $\alpha_1^{m_0/m} \in \mathbb{C}(x)$ . Thus we have  $m_0 = [F : \mathbb{C}(x)]$ . Observe that  $m_0$ 

is a divisor of *m*. We may then write *h* in the following form

$$h(x) = \sum_{j=0}^{m_0-1} \alpha_1^{j/m} \Lambda_j,$$

where  $\alpha_1^{j/m} \Lambda_j$  is the sum of the terms of the shape (3.3) for which  $sn \equiv j \pmod{m_0}$ ; in particular,  $\Lambda_j \in \mathbb{C}(x)$ . Since  $h \in \mathbb{C}[x]$ , we deduce that  $h(x) = \Lambda_0$ . Note that at least one  $t_i$  with s = 1 has to appear since otherwise h would be constant. Moreover, for  $G_n(x) = g(h(x))$  to be true, the term with s = 1 and  $h_2, \ldots, h_d = 0$  must appear, hence from the special shape of  $t_i$  it follows that we therefore necessarily have  $n \equiv 0 \pmod{m_0}$ . We shall write  $n = m_0 \ell$  from now on.

Putting  $w_i d_i = c_i$  and  $\delta_i^{m_0} = \gamma_i$  for i = 1, ..., l gives  $h(x) = c_1 \gamma_1^{\ell} + \cdots + c_l \gamma_l^{\ell}$ , which is the claim in Theorem 1.1.

# 3.2. Proof of Theorem 1.2

Define  $H_{\ell} = c_1 \gamma_1^{\ell} + \cdots + c_l \gamma_l^{\ell} \in \mathbb{C}[c_1, \dots, c_l](x)$  for any  $\ell \in \mathbb{N}$ , where *l* and the  $\gamma_i$  are determined in Theorem 1.1. Moreover, we set

$$g(x) = g_0 x^m + g_1 x^{m-1} + \dots + g_m \in \mathbb{C}[g_0, \dots, g_m][x].$$

We may write  $g \circ H_{\ell}$  as a finite sum of  $\ell$ -th-power terms:

$$g(H_{\ell}(x)) = g(c_1\gamma_1^{\ell} + \dots + c_l\gamma_l^{\ell}) = e_1\epsilon_1^{\ell} + \dots + e_k\epsilon_k^{\ell}.$$

Here, we can control the  $\epsilon_i$ 's and k, but not the  $e_i$ 's since they depend on the  $w_i$ 's in (3.10). In fact, we have that

$$\epsilon_i \in \{\gamma_{i_1} \dots \gamma_{i_r}; \ 0 \le r \le m, \ 1 \le i_j \le l, \ 1 \le j \le r\},\$$

and

$$k \leq 1 + l + l^2 + \dots + l^m = (l^{m+1} - 1)/(l - 1),$$

and the  $e_i$  are polynomial expressions in  $g_0, \ldots, g_m, c_1, \ldots, c_l$  with coefficients in  $\mathbb{Q}$ , which can be written down explicitly. Moreover, we can assume that  $\epsilon_i/\epsilon_j$  is not in  $\mathbb{C}$  for any  $1 \le i < j \le k$  because otherwise we can join the two terms with the cost that the  $e_i$ are polynomial-exponential equations in  $g_0, \ldots, g_m, c_1, \ldots, c_l$  and exponentials in  $\ell$  with base in  $\mathbb{C}$ , which again can be written down explicitly. Below we will have that all the  $\epsilon_i$ 's are polynomials over  $\mathbb{C}$  in which case we can put out the leading coefficient, which is another exponential expression in  $\ell$  with base in  $\mathbb{C}$ ; we can put these exponentials also inside the  $e_i$ 's by modifying the  $e_i$ 's and  $\epsilon_i$ 's accordingly. Now from the proof of Theorem 1.1 we know that if  $G_n(x) = g(h(x))$ , then either *n* is bounded above by (3.9) or  $n = m_0 \ell$  for some  $\ell \in \mathbb{N}$  and h(x) may be written as a power sum as above. In this case we get the equation

$$a_1 b_1^{m_0 \ell} \beta_1^{m_0 \ell} + \dots + a_d b_d^{m_0 \ell} \beta_d^{m_0 \ell} = G_{m_0 \ell}(x) = e_1 \epsilon_1^{\ell} + \dots + e_k \epsilon_k^{\ell}.$$
 (3.11)

We seek to apply Theorem 2.5 to this equation to, again, give an upper bound on possible indices  $n \in \mathbb{N}$  in this case, if possible. The last equation can be viewed as a homogeneous *S*-unit-equation over  $K = \mathbb{C}(x)$ . Application of Theorem 2.5 requires the equation in question not to have a proper vanishing subsum. Therefore we look at a minimal vanishing subsum of (3.11) and again we distinguish between two possible cases. If there is such a subsum consisting of at least three terms, we are able to apply the theorem and consequently get an upper bound on *n*. On the other hand, this is not the case if and only if each of the terms of the right hand side of equation (3.11) is identical to exactly one term on the other side (note that in this case each minimal vanishing subsum consists of exactly two terms, since it cannot consist of one term by minimality, and moreover, because of the non-degeneracy it is not possible that two terms on the same side of equation (3.11) coincide). Also, if we are in this exceptional situation, it follows that k = d and that there is a unique permutation  $\rho \in \mathscr{S}_d$  such that  $a_i \alpha_i^{m_0 \ell} = e_{\rho(i)} \epsilon_{\rho(i)}^{\ell}$  (if there was another permutation of this kind, we would again end up in the situation that two terms of the same side coincide).

Now, assume that there is a proper vanishing subsum of (3.11) consisting of at least three terms. Then we may write the equation in the form  $1 + v_1 + \cdots + v_n = 0$  (where  $2 \le n \le k + d - 1$ ). Since for zeros and poles of the  $v_i$ 's we can only have zeros and poles of the  $\alpha_i$ 's, we can take  $K = \mathbb{C}(x)$  and  $S_K$  the set of places of K containing  $\infty$  and the zeros of  $\alpha_1, \ldots, \alpha_d$ . Similarly as above it follows that  $|S_K| \le \deg A_0 + 1$  and clearly  $g_K = 0$ , hence by Brownawell and Masser's theorem (Theorem 2.5) it follows that

$$\max_{i=1,...,n} \mathcal{H}(v_i) \le \frac{1}{2}(k+d-1)(k+d-2)(|S_K|+2g_K-2)$$
$$\le \frac{1}{2}\left(\frac{L^{m+1}-1}{L-1}+d-1\right)^2 \deg A_0.$$
(3.12)

Assume first that the vanishing subsum contains  $\beta_i$  and  $\beta_j$  for  $1 \le i < j \le d$ . The case when it contains two of the  $\epsilon_i$ 's will be done afterwards. Now, we may obtain the equation of shape  $1 + v_1 + \cdots + v_n = 0$  by dividing the original one by  $a_j b_j^{m_0 \ell} \beta_j^{m_0 \ell}$ . Then we find the following lower bound (note that we have  $\mathcal{H}(\alpha_i/\alpha_j) \ge 1$ , by the non-degeneracy of the sequence)

$$\max_{i=1,\dots,n} \mathcal{H}(v_i) \ge \mathcal{H}((\alpha_i/\alpha_j)^{m_0\ell}) = m_0\ell \cdot \mathcal{H}(\alpha_i/\alpha_j) \ge m_0\ell = n \ge \ell.$$
(3.13)

19

Now assume that the vanishing subsum contains  $\epsilon_i$  and  $\epsilon_j$  for  $1 \le i < j \le k$ . Then as above (note now that we have  $\mathcal{H}(\epsilon_i/\epsilon_j) \ge 1$  because we have taken the  $\epsilon_i$ 's to be non-degenerate)

$$\max_{i=1,\dots,n} \mathcal{H}(v_i) \ge \mathcal{H}((\epsilon_i/\epsilon_j)^{\ell}) = \ell \cdot \mathcal{H}(\epsilon_i/\epsilon_j) \ge \ell.$$

Clearly, with  $\ell$  we also have an upper bound for  $n = m_0 \ell$ . Hence, by (3.12) and (3.13) we see, that again in this case there can only be finitely many  $n \in \mathbb{N}$  such that  $G_n(x) = g(h(x))$  for some polynomial  $h \in \mathbb{C}[x]$ , with an upper bound C' given by (3.12).

As we saw, the only remaining situation we have to consider is the situation that in equation (3.11) each term on the left hand side coincides with exactly one term on the right hand side. In particular, it holds that d = k. So let  $\rho \in \mathcal{S}_d$  be such that  $a_i \alpha_i^{m_0 \ell} = a_i b_i^{m_0 \ell} \beta_i^{m_0 \ell} = e_{\rho(i)} \epsilon_{\rho(i)}^{\ell}$  for all i = 1, ..., d, or equivalently

$$\left(\frac{\beta_i^{m_0}}{\epsilon_{\rho(i)}}\right)^\ell = \frac{e_{\rho(i)}}{a_i b_i^{m_0 \ell}} \tag{3.14}$$

for all i = 1, ..., d. Since  $a_i, b_i, e_{\rho(i)} \in \mathbb{C}$  are constant, it follows that  $\beta_i^{m_0}$  and  $\epsilon_{\rho(i)}$  are polynomials that coincide up to some constant factor. We have already mentioned above that we may assume that both polynomials have leading coefficient equal to one. Therefore it follows that they have to be equal so that the quotient is equal to one for all  $\ell$ . It follows that we have equalities  $a_i b_i^{m_0 \ell} = e_{\rho(i)}$  for i = 1, ..., d. These are polynomial-exponential equations in the unknowns  $g_0, ..., g_m, c_1, ..., c_l$  and  $\ell$  which define a subvariety as claimed in the theorem.

We have shown that there is a subvariety  $\mathcal{V}$  of  $\mathbb{A}^{l+m+1} \times \mathbb{G}_m^t$ , where l and t are explicitly bounded by the originally given data and which is given by polynomial-exponential equations in the polynomial unknowns  $g_0, \ldots, g_m, c_1, \ldots, c_l$  and the exponential unknown  $\ell$  which can be written down explicitly. If we then define  $G(x) = g_0 x^m + \cdots + g_m \in \mathbb{C}[\mathcal{V}][x]$ and  $H_\ell = c_1 d_1 \delta_1^\ell + \cdots + c_l d_l \delta_l^\ell \in \mathbb{C}[\mathcal{V}](x)$ , then by construction we have for all  $\ell \in \mathbb{N}$  that  $G_{m_0\ell}(x) = G \circ H_\ell$  as an equation in  $\mathbb{C}[\mathcal{V}](x)$  and the following holds: If  $G_n(x) = g \circ h$ with  $g, h \in \mathbb{C}[x]$ , deg g = m, deg h > 1, then either n is not greater than the maximum of the bounds given in (3.9) and C' or  $n = m_0\ell$  and there is a point  $P \in \mathcal{V}(\mathbb{C})$  such that g(x) = G(P, x) and  $h(x) = H_\ell(P, x)$ . Conversely, if  $P = (g_0, \ldots, g_m, c_1, \ldots, c_l, \ell) \in \mathcal{V}(\mathbb{C})$ is a given  $\mathbb{C}$ -rational point on  $\mathcal{V}$  and if we define g(x) = G(P, x) and  $h(x) = H_\ell(P, x)$ then we have  $G_{m_0\ell}(x) = g \circ h$  with deg g = m. By integrality it follows that  $h \in \mathbb{C}[x]$ . Clearly, deg h > 1. This establishes the theorem.

#### 4. Proof of the remarks and special cases

(a). We just have to apply [9, Theorem 1]. It follows that there is a constant C with deg  $g \le C$ . We apply our Theorem 1.1 for each m with  $2 \le m \le C$ . From this the conclusion follows.

(b). This follows directly by inspecting the proof. The equations for the varieties arise from (3.14). By assumption  $b_i = 1$ ,  $\beta_i$ ,  $\epsilon_j$  are monic and  $e_j$  is a polynomial in  $c_1, \ldots, c_l, g_0, \ldots, g_m$  with rational coefficients. We therefore get for  $\mathcal{V}$  a subvariety of  $\mathbb{A}^{l+m+1}$  and there is no  $\mathbb{G}_m$ -part.

(c). Assume that  $G_n(x) = g \circ h$  with deg g = m and n > C. Then by Theorem 1.1 it follows that  $n = m_0 \ell$  and that  $h(x) = c_1 \gamma_1^{\ell} + \cdots + c_l \gamma_l^{\ell}$ , where the  $\gamma_i$  are (up to a constant) of the shape

$$\left(\alpha_1^{s_i/m-(h_{i2}+\cdots+h_{id})}\alpha_2^{h_{i2}}\ldots\alpha_d^{h_{id}}\right)^{m_0}$$

where  $s_i \in A = \{0, 1\}, h_{ij} \in B = \{0, 1, \dots, J + \deg A_0/m\}$ . We put  $k = \deg \alpha_1$  and assume that  $1 \le k < m$ . In the case  $(h_{i2}, \dots, h_{id}) = (0, \dots, 0)$ , if s = 0 then  $\gamma_i$  is constant, and if s = 1 then  $\gamma_i = \xi \alpha_1^{m_0/m} \in \mathbb{C}[x]$ , where  $\xi \in \mathbb{C}$ . Assume that there is an *i* with  $(h_{i2}, \dots, h_{id}) \ne (0, \dots, 0)$  and let  $\mathbf{h} = \max_i \sum_{j=2}^d h_{ij}$ . Then  $\gamma_i$  (up to a constant) is of the shape

$$\left(\frac{\alpha_1^{s_i/m-(h_{i2}+\dots+h_{id})+\mathbf{h}}\alpha_2^{h_{i2}}\dots\alpha_d^{h_{id}}}{\alpha_1^{\mathbf{h}}}\right)^{m_0} = \left(\frac{p(x)}{\alpha_1^{\mathbf{h}}}\right)^{m_0},$$

where  $p(x) \in \mathbb{C}[x]$  is a polynomial with

$$\deg p = ks_i/m - k(h_{i2} + \dots + h_{id}) + \mathbf{h}k + h_{i2} \deg \alpha_2 + \dots + h_{id} \deg \alpha_d$$
$$< 1 + \mathbf{h}k + \sum_{j=2}^d h_{ij}(\deg \alpha_j - k) \le \mathbf{h}k.$$

Hence, subtracting possibly the terms with  $(h_2, \ldots, h_d) = (0, \ldots, 0)$  from h(x), we get a polynomial h'(x) which can be written as the sum of  $\ell$ -th powers of terms of the described shape, i.e.  $h'(x) = p'(x)/\alpha_1^{hm_0\ell}$ , where deg  $p' < hkm_0\ell$ . This gives a contradiction to  $h' \in \mathbb{C}[x]$ , except for the case p' = 0. Thus we may assume that only the summands with  $h_2 = \cdots = h_t = 0$  (and s = 0, 1) occur, that is  $h(x) = c_1 + c_2\alpha_1^{(m_0\ell)/m} = c_1 + c_2\alpha_1^{deg G_n/(mk)}$  (since  $k = \deg \alpha_1 > \deg \alpha_i$  for  $i = 2, \ldots, d$  we have that deg  $G_n = n \deg \alpha_1 = kn$ ). A similar argument (considering the valuation at 0) shows that h(x) must also be of this shape in the case deg  $\alpha_1 = k = m$ . Note that for the finitely many remaining cases when m < k one can apply Theorems 1.1 and 1.2, respectively.  $\Box$ 

(*d*). We argue as in (c). We therefore have that  $\gamma_i = \beta^{(s_i/m - (h_{i2} + \dots + h_{id}))m_1 + h_2m_2 + \dots + h_dm_d} = \beta^{k_i}$  for some  $k_i \in \mathbb{Z}$ . By integrality it follows that  $k_i \in \mathbb{N}$ . This shows the claim.

(*e*). We assume that  $a_1, \ldots, a_d \in K$  and  $\alpha_1, \ldots, \alpha_d \in K[x]$  so that  $G_n(x) \in K[x]$  for all  $n \ge 0$ , where *K* is a number field. An application of Theorem 1.1 implies that either  $n \le C$  or  $h(x) = c_1 \gamma_1^{\ell} + \cdots + c_l \gamma_l^{\ell}$  with  $n = m_0 \ell$ . We have  $\gamma_1, \ldots, \gamma_l \in K(x)$  and  $c_1, \ldots, c_l \in \mathbb{C}$ . Taking a transcendence basis of  $K(c_1, \ldots, c_l) \supseteq K$  and comparing coefficients in this basis shows that we may assume that  $c_1, \ldots, c_l$  are algebraic over *K*. Taking now a (field) basis of  $K(c_1, \ldots, c_l) \supseteq K$  and comparing coefficients in this basis shows that we may assume  $c_1, \ldots, c_l \in K$ . Since  $G_n(x) \in K[x]$  and  $h(x) \in K[x]$  determine *g*, we see that  $g(x) \in K[x]$  as well (for this the algorithm in [17, Section 3] can be used). This proves the claim.

(f). This follows immediately by fixing  $g(x) = x^m$  and then going through the proofs.  $\Box$ 

(g). Assume that  $h(x) = c_1 \gamma_1^{\ell} + \cdots + c_l \gamma_l^{\ell}$  with  $n = m_0 \ell$  appears as "inner" decomposition factor for fixed  $c_1, \ldots, c_l$  (independent of  $\ell$ ) for any  $\ell \in \mathbb{N}$ . Then, as already mentioned above, we can identify the varying powers by indeterminates and then use the algorithm provided in [4] to explicitly calculate this family of decompositions.

### References

- [1] Roberto M. Avanzi and Umberto Zannier. The equation f(X) = f(Y) in rational functions X = X(t), Y = Y(t). *Compos. Math.*, 139(3):263–295, 2003.
- [2] Yuri Bilu, Clemens Fuchs, Florian Luca, and Ákos Pintér. Combinatorial Diophantine equations and a refinement of a theorem on separated variables equations. *Publ. Math.*, 82(1):219–254, 2013.
- [3] Yuri Bilu and Robert Tichy. The Diophantine equation f(x) = g(y). Acta Arith., 95(3):261–288, 2000.
- [4] Arnaud Bodin. Decomposition of polynomials and approximate roots. *Proc. Am. Math. Soc.*, 138(6):1989–1994, 2010.
- [5] W. Dale Brownawell and David W. Masser. Vanishing sums in function fields. *Math. Proc. Camb. Philos. Soc.*, 11(3):427–434, 1986.
- [6] Pietro Corvaja and Umberto Zannier. Finiteness of integral values for the ratio of two linear recurrences. *Invent. Math.*, 149(2):431–451, 2002.

- [7] Martin Eichler. Einführung in die Theorie der algebraischen Zahlen und Funktionen. Number 27 in Lehrbücher und Monographien aus dem Gebiete der exakten Wissenschaften, Mathematische Reihe. Birkhäuser, 1963.
- [8] Clemens Fuchs. On the Diophantine equation  $G_n(x) = G_m(P(x))$  for third order linear recurring sequences. *Port. Math.* (*N.S.*), 61(1):1–24, 2004.
- [9] Clemens Fuchs, Christina Karolus, and Dijana Kreso. Decomposable polynomials in second order linear recurrence sequences. *Manuscr. Math.*, 159(3-4):321–346, 2019.
- [10] Clemens Fuchs, Vincenzo Mantova, and Umberto Zannier. On fewnomials, integral points, and a toric version of Bertini's theorem. J. Am. Math. Soc., 31(1):107–134, 2018.
- [11] Clemens Fuchs and Attila Pethő. Effective bounds for the zeros of linear recurrences in function fields. J. Théor. Nombres Bordeaux, 17(3):749–766, 2005.
- [12] Clemens Fuchs and Attila Pethő. Composite rational functions having a bounded number of zeros and poles. Proc. Am. Math. Soc., 139(1):31–38, 2011.
- [13] Clemens Fuchs, Attila Pethő, and Robert Tichy. On the Diophantine equation  $G_n(x) = G_m(P(x))$ . *Monatsh. Math.*, 137(3):173–196, 2002.
- [14] Clemens Fuchs, Attila Pethő, and Robert Tichy. On the Diophantine equation  $G_n(x) = G_m(P(x))$ : higher-order recurrences. *Trans. Am. Math. Soc.*, 355(11):4657–4681, 2003.
- [15] Clemens Fuchs, Attila Pethő, and Robert Tichy. On the Diophantine equation  $G_n(x) = G_m(y)$  with Q(x, y) = 0. In *Diophantine Approximation. Festschrift for Wolfgang Schmidt*, volume 16 of *Developments in Mathematics*, pages 199–209. Springer, 2008.
- [16] Clemens Fuchs and Umberto Zannier. Composite rational functions expressible with few terms. J. Eur. Math. Soc., 14(1):175–208, 2012.
- [17] James Rickards. When is a polynomial a composition of other polynomials? Am. Math. Mon., 118(4):358–363, 2011.
- [18] Helmut Salzmann, Theo Grundhöfer, Hermann Hähl, and Rainer Löwen. The classical fields. Structural features of the real and rational numbers, volume 112 of Encyclopedia of Mathematics and Its Applications. Cambridge University Press, 2007.

- [19] Andrzej Schinzel. Polynomials with special regard to reducibility, volume 77 of Encyclopedia of Mathematics and Its Applications. Cambridge University Press, 2000. With an appendix by Umberto Zannier.
- [20] Hans P. Schlickewei and Wolfgang M. Schmidt. The intersection of recurrence sequences. *Acta Arith.*, 72(1):1–44, 1995.
- [21] Henning Stichtenoth. Function Fields and Codes. Universitext. Springer, 1993.
- [22] Robert J. Walker. Algebraic curves. Dover Publications, 1962.
- [23] Umberto Zannier. On the integer solutions of exponential equations in function fields. *Ann. Inst. Fourier*, 54(4):849–874, 2004.
- [24] Umberto Zannier. On the number of terms of a composite polynomial. *Acta Arith.*, 127(2):157–167, 2007.
- [25] Umberto Zannier. On composite lacunary polynomials and the proof of a conjecture of Schinzel. *Invent. Math.*, 174(1):127–138, 2008.
- [26] Umberto Zannier. Addendum to the paper: "On the number of terms of a composite polynomial". *Acta Arith.*, 140(1):93–99, 2009.

CLEMENS FUCHS University of Salzburg Hellbrunnerstr. 34/I A-5020 Salzburg AUSTRIA clemens.fuchs@sbg.ac.at CHRISTINA KAROLUS University of Salzburg Hellbrunnerstr. 34/I A-5020 Salzburg AUSTRIA christina.karolus@sbg.ac.at