Diophantine equations in separated variables and lacunary polynomials

Dijana Kreso

Institute for Analysis und Number Theory, Graz University of Technology, Steyrergasse 30/II, 8010 Graz, Austria, and
Department of Mathematics, University of Salzburg, Hellbrunnerstrasse 34/I, 5020 Salzburg, Austria.
e-mail: kreso@math.tugraz.at

Abstract: We study Diophantine equations of type $f(x) = g(y)$, where f and g are lacunary polynomials. According to a well known finiteness criterion, for a number field K and nonconstant $f, g \in K[x]$, the equation $f(x) = g(y)$ has infinitely many solutions in S-integers x, y only if f and g are representable as a functional composition of lower degree polynomials in a certain prescribed way. The behaviour of lacunary polynomials with respect to functional composition is a topic of independent interest, and has been studied by several authors. In this paper, we utilize known results on the latter topic, and develop new ones, in relation to Diophantine applications.

Keywords: Diophantine equations, lacunary polynomials, polynomial decomposition.

1 Introduction

The possible ways of writing a polynomial as a composition of lower degree polynomials were studied by several authors, starting with Ritt in the 1920's in his classical paper [15]. Ritt's and later results have applications to number theory, complex analysis, arithmetic dynamics, finite geometries, etc. See e.g. [16] and [21] for an overview of the theory and applications.

The behaviour of lacunary polynomials with respect to functional composition has been studied by several authors, at least since the 1940's when Erdős and Rényi independently investigated this topic. By a lacunary polynomial we mean a polynomial with a fixed number of nonconstant terms whose degrees of the terms and the coefficients may vary. We write $a_1x^{n_1} + a_2x^{n_2} + \cdots + a_\ell x^{n_\ell} + a_{\ell+1}$ with $a_1a_2\cdots a_\ell \neq 0$ for a lacunary polynomial with ℓ nonconstant terms. Lacunary polynomials have been studied from various viewpoints (reducibility, distribution of roots, applications to cryptography, etc.) and have played an important role in various algebraic and arithmetical investigations (see [16, chap. 5 & chap. 6]). In the last decade, various results are shown about the behaviour of lacunary polynomials (and rational functions) with respect to functional composition, see e.g. [8, 9, 19, 20]. The methods in these papers rely mainly on modified Puiseux expansions and on lower bounds for approximations by sums of S-units in function fields, and are developed by Zannier [19, 20].

On the other hand, Diophantine equations of type $f(x) = g(y)$ have been of long-standing interest to number theorists. By Siegel's classical theorem, it follows that an irreducible algebraic curve defined over a number field has only finitely many S-integral

points, unless it has genus zero and no more than two points at infinity. Ever since Siegel's theorem, one of the driving questions was to classify the polynomials f, g for which the equation $f(x) = g(y)$ has infinitely many solutions in S-integers x, y. The classification was completed by Bilu and Tichy [1] in 2000, by building on the work of Ritt, Fried and Schinzel. It turns out that such f and g must be representable as a composition of lower degree polynomials in a certain prescribed way.

Here, in the light of the above results, we are interested in Diophantine equations of type $f(x) = g(y)$, where f and g are lacunary. Some results in this direction can be found in [10, 11, 14, 17]. Note that some classical Diophantine equations are of this type (Pell's equation, the defining equation of an elliptic curve, etc.).

For a field K, it is said that $f \in K[x]$ is *indecomposable* (over K) if $\deg f > 1$ and f can not be represented as a composition of lower degree polynomials in $K[x]$. Otherwise, f is *decomposable* (over K). Here is our first result.

Theorem 1.1. *Let K be a number field, S a finite set of places of K that contains all Archimedean places and $\mathcal{O}_S$ the ring of S-integers of K. The equation*

$$a_1x^{n_1} + a_2x^{n_2} + \cdots + a_\ell x^{n_\ell} + a_{\ell+1} = b_1y^{m_1} + b_2y^{m_2} + \cdots + b_k y^{m_k}, \tag{1.2}$$

where $\ell, k \geq 3$, $n_i, m_j \in \mathbb{N}$, $a_i, b_j \in K$, and

i) $n_i > n_j$ if $i > j$, $\gcd(n_1, \ldots, n_\ell) = 1$, $m_i > m_j$ if $i > j$, $\gcd(m_1, \ldots, m_k) = 1$,

ii) $a_1a_2 \cdots a_\ell b_1b_2 \cdots b_k \neq 0$,

iii) $b_1y^{m_1} + b_2y^{m_2} + \cdots + b_k y^{m_k}$ is indecomposable,

iv) $m_1 \geq 2\ell(\ell-1)$, $m_1 \neq k$ and $n_1 \neq \ell$, and either $m_1 \geq 2k+1$ or $n_1 \geq 2\ell+1$,

has infinitely many solutions $x, y \in K$ with a bounded $\mathcal{O}_S$-denominator if and only if

$$a_1x^{n_1} + \cdots + a_\ell x^{n_\ell} + a_{\ell+1} = (b_1x^{m_1} + \cdots + b_k x^{m_k}) \circ \mu(x) \tag{1.3}$$

for some linear $\mu \in K[x]$.

Note that if in (1.3) we have $\mu(0) = 0$, then $k = \ell$, $n_i = m_i$, $a_{\ell+1} = 0$ and $a_i = b_i\zeta$ for some $\zeta \in K \setminus \{0\}$ such that $\zeta^d = 1$, where $d = \gcd(m_1, m_2, \ldots, m_k)$, for all $i = 1, 2, \ldots, k$. If $\mu(0) \neq 0$, then it can be shown that $n_1 = m_1 \leq k + \ell$, see Proposition 4.3. In Section 5, we discuss how the assumptions in Theorem 1.1 arise, and in which way they can be relaxed at the cost of a more complicated formulation of the theorem. We also show a version of Theorem 1.1 when m_1 is a composite number and *iv)* is relaxed to $m_1 \geq 2\ell(\ell-1)$.

Note that *iii)* in Theorem 1.1 holds when m_1 is a prime (since if $f(y) = g(h(y))$, then $\deg f = \deg g \cdot \deg h$). Furthermore, *iii)* in Theorem 1.1 holds when $b_1m_1y^{m_1-1} + b_2m_2y^{m_2-1} + \cdots + b_km_ky^{m_k-1}$ is irreducible over K (since if $f(y) = g(h(y))$, then $f'(y) = g'(h(y))h'(y)$). Reducibility of lacunary polynomials has been studied by Schinzel in a series of twelve papers, which were then incorporated into his book [16]. Zannier [20] showed that if $K = \mathbb{C}$ and *iii)* does not hold, then $(m_1, m_2, \ldots, m_k) \in M$, where $M = M(b_1, b_2, \ldots, b_k)$ is a finite union of subgroups of $\mathbb{Z}^k$. In [3, 4], it is shown that *iii)* holds when $b_1, b_2, \ldots, b_k$ are nonzero integers, and either $m_2 = m_1 - 1$ and $\gcd(m_1, b_2) = 1$, or f is an odd polynomial, $m_2 = m_1 - 2$ and $\gcd(m_1, b_2) = 1$. (In the appendix we discuss an extension of the latter result to the case when the polynomial in *iii)* has coefficients in any unique factorization domain). Furthermore, Fried and Schinzel [7] showed that if $k = 2$ and $\gcd(m_1, m_2) = 1$, then *iii)* holds. When $k = 2$, we have the following result.

Theorem 1.4. *Let K be a number field, S a finite set of places of K that contains all Archimedean places and $\mathcal{O}_S$ the ring of S-integers of K. The equation*

$$a_1x^{n_1} + \cdots + a_\ell x^{n_\ell} + a_{\ell+1} = b_1y^{m_1} + b_2y^{m_2}, \tag{1.5}$$

where $\ell \geq 3$, $n_i, m_j \in \mathbb{N}$, $a_i, b_j \in K$, and

i) $n_i > n_j$ if $i > j$, $\gcd(n_1, \ldots, n_\ell) = 1$, $m_1 > m_2$, $\gcd(m_1, m_2) = 1$,

ii) $a_1a_2 \cdots a_\ell b_1 b_2 \neq 0$,

iii) $m_1 \geq \binom{\ell+2}{2} + \ell - 1$, $n_1 \geq 3$,

has infinitely many solutions $x, y \in K$ with a bounded $\mathcal{O}_S$-denominator if and only if

$$\begin{aligned} b_1x^{m_1} + b_2x^{m_2} &= e_1c(d_1x + d_0)x^{m_1-1} \\ a_1x^{n_1} + \cdots + a_\ell x^{n_\ell} + a_{\ell+1} &= e_1(c_1x + c_0)^{n_1}, \end{aligned} \tag{1.6}$$

for some $e_1, c, c_1, c_0, d_1, d_0 \in K \setminus \{0\}$.

We remark that the Equation 1.5 was studied in [11], where a version of Theorem 1.4 is shown under additional assumptions. In this paper, we utilize several new results, and in this way we improve the main result of [11], and moreover shorten and simplify the proof.

To the proof of Theorem 1.1 of importance is a result of Zannier [19], which states that for a field K with $\mathrm{char}(K) = 0$ and for $f \in K[x]$ with $\ell \geq 2$ nonconstant terms, which satisfies $f = g \circ h$ for some $g, h \in K[x]$, where h is not of type $ax^k + b$, we have $\deg g < 2\ell(\ell - 1)$. To the proof of Theorem 1.4, we show the following.

Proposition 1.7. *Let K be a field with $\mathrm{char}(K) = 0$. Assume that*

$$a_1x^{n_1} + \cdots + a_\ell x^{n_\ell} + a_{\ell+1} = (b_1x^{m_1} + b_2x^{m_2}) \circ h(x), \tag{1.8}$$

where $\ell \geq 3$, $n_i, m_j \in \mathbb{N}$, $a_i, b_j \in K$, $h \in K[x]$ and

i) $n_i > n_j$ when $i > j$, $\gcd(n_1, \ldots, n_\ell) = 1$, $m_1 > m_2$,

ii) $a_1a_2 \cdots a_\ell b_1 b_2 \neq 0$.

Then

$$m_1 < \binom{\ell+2}{2} + \ell - 1. \tag{1.9}$$

If $a_{\ell+1} \neq 0$, then moreover

$$m_1 < \binom{\ell+2}{2} + 2. \tag{1.10}$$

Our proof of Proposition 1.7, like Zannier's proof, involves applying Brownawell and Masser's inequality [2], which can be seen as a version of Schmidt's subspace theorem for function fields. We remark that the above Zannier's result was one of the main ingredients of Zannier's proof [20] of a conjecture of Schinzel, by which for $f \in \mathbb{C}[x]$ with ℓ nonconstant terms, which satisfies $f = g \circ h$ for some $g, h \in \mathbb{C}[x]$, the number of terms of h is bounded above by $B(\ell)$, where B is an explicitly computable function.

For a field K with $\mathrm{char}(K) = 0$ and $f \in K[x]$ with $\deg f > 1$, the Galois group of $f(x) - t$ over $K(t)$, where t is transcendental over K, seen as a permutation group of the roots of this polynomial, is called the *monodromy group* of f (over K). The *absolute*

monodromy group $\mathrm{Mon}(f)$ is the monodromy group of f over an algebraic closure $\overline{K}$ of K. Several properties of a polynomial depend only on its monodromy group. For example, f is indecomposable if and only if $\mathrm{Mon}(f)$ is a primitive permutation group. For details, see Section 3. From the main result of [1], we deduce that if K is a number field and $f, g \in K[x]$ with $\deg f \geq 3$ and $\deg g \geq 3$ have doubly transitive absolute monodromy groups, then the equation $f(x) = g(y)$ has infinitely many solutions with a bounded $\mathcal{O}_S$-denominator if and only if $f(x) = g(\mu(x))$ for some linear $\mu \in K[x]$. Here, as usual, S is a finite set of places of K that contains all Archimedean places and $\mathcal{O}_S$ the ring of S-integers of K. Turnwald [18] showed that the monodromy group of $a_1x^{n_1} + a_2x^{n_2} + a_3$ with $a_1a_2 \neq 0$, and $\gcd(n_1, n_2) = 1$, is symmetric, and symmetric groups of degree ≥ 2 are doubly transitive. Turnwald's result is one of our main ingredients to the proof of Theorem 1.4. The latter two results further allow us to show the following.

Theorem 1.11. *Let K be a number field, S a finite set of places of K that contains all Archimedean places and $\mathcal{O}_S$ the ring of S-integers of K. The equation*

$$a_1x^{n_1} + a_2x^{n_2} + a_3 = b_1y^{m_1} + b_2y^{m_2}, \tag{1.12}$$

where $n_i, m_j \in \mathbb{N}$, $a_i, b_j \in K$, and

i) $n_1 > n_2$, $\gcd(n_1, n_2) = 1$, $m_1 > m_2$, $\gcd(m_1, m_2) = 1$,

ii) $a_1a_2b_1b_2 \neq 0$,

iii) $m_1 \geq 3$, $n_1 \geq 3$,

has infinitely many solutions with a bounded $\mathcal{O}_S$-denominator if and only if

$$a_1x^{n_1} + a_2x^{n_2} + a_3 = (b_1x^{m_1} + b_2x^{m_2}) \circ \mu(x) \tag{1.13}$$

for some linear $\mu \in K[x]$. Furthermore, (1.13) with $\mu(0) \neq 0$ holds exactly when $n_1 = m_1 = 3$, and either

$$n_2 = m_2 = 2, \quad a_1^2b_2^3 + a_2^3b_1^2 = 0, \quad 27a_1^2a_3 + 4a_2^3 = 0,$$

or

$$n_2 = 2, \quad m_2 = 1, \quad 27a_1^4b_2^3 + a_2^6b_1 = 0, \quad 3a_2^3a_3b_1 + 3a_1^2b_2^3 + a_2^3b_2^2 = 0,$$

and (1.13) with $\mu(0) = 0$ holds holds exactly when

$$n_1 = m_1, \quad n_2 = m_2, \quad a_3 = 0, \quad a_1 = b_1\zeta^{m_1}, \ a_2 = b_2\zeta^{m_2} \text{ for some } \zeta \in K \setminus \{0\}.$$

We give a short proof of Theorem 1.11 as an outcome of our methods. This result generalizes the main result of Péter, Pintér and Schinzel [14], who proved it in the case when $K = \mathbb{Q}$ and $\mathcal{O}_S = \mathbb{Z}$. In so doing, they generalized several results in the literature. Schinzel [17] further extended the main result of Péter, Pintér and Schinzel [14], by removing the assumption on the coprimality of the degrees of the terms. This resulted in several more exceptional cases when the Equation 1.12 has infinitely many solutions with a bounded $\mathcal{O}_S$-denominator. To avoid tedious work, in our results we restrict to the case when the degrees of the terms are coprime.

Our results rely on the main result of Bilu and Tichy [1], which in turn relies on Siegel's classical theorem on integral points on curves, and are consequently ineffective.

The paper is organized as follows. In Section 2 we recall the finiteness criterion from [1]. In Section 3 we recall the monodromy method. Furthermore, from the finiteness criterion

we deduce a result about the finiteness of S-integer solutions of the equation $f(x) = g(y)$, where f and g have doubly transitive absolute monodromy groups. We recall results from the literature giving sufficent conditions for the monodromy group to be doubly transitive. In Section 4 we recall and prove several new results about decompositions of lacunary polynomials, and in particular we prove Proposition 1.7. In Section 5 we prove our main results using the results from Section 3 and Section 4.

2 Finiteness criterion

In this section we present the finiteness criterion of Bilu and Tichy [1].

Let K be a field of characteristic zero, $a, b \in K \setminus \{0\}$, $m, n \in \mathbb{N}$, $r \in \mathbb{N} \cup \{0\}$, $p \in K[x]$ be a nonzero polynomial (which may be constant) and $D_n(x, a)$ be the n-th Dickson polynomial with parameter a given by

$$D_n(x,a) = \sum_{j=0}^{\lfloor n/2 \rfloor} \frac{n}{n-j} \binom{n-j}{j} (-a)^j x^{n-2j}. \tag{2.1}$$

We remark that $D_n(x, a) = 2a^n T_n(x/(2\sqrt{a}))$ where $T_k(x) = \cos(k \arccos x)$ is the k-th Chebyshev polynomial of the first kind. For various properties of Dickson polynomials, see [1, Sec. 3]. Some of these properties will be recalled in Section 3.

Standard pairs of polynomials over K are listed in the following table.

kind	standard pair (or switched)	parameter restrictions
first	$(x^m, ax^r p(x)^m)$	$r < m, \gcd(r, m) = 1,\ r + \deg p > 0$
second	$(x^2, (ax^2 + b)p(x)^2)$	-
third	$(D_m(x, a^n), D_n(x, a^m))$	$\gcd(m, n) = 1$
fourth	$(a^{\frac{-m}{2}} D_m(x, a), -b^{\frac{-n}{2}} D_n(x, b))$	$\gcd(m, n) = 2$
fifth	$((ax^2 - 1)^3, 3x^4 - 4x^3)$	-

We further call the pair

$$\left(D_m\left(x, a^{n/d}\right), -D_n\left(x\cos(\pi/d), a^{m/d}\right)\right) \text{ (or switched)},$$

with $d = \gcd(m, n) \geq 3$ and $\cos(2\pi/d) \in K$, a *specific pair* over K. One easily sees that if $b, \cos(2\alpha) \in K$, then $D_n(x \cos\alpha, b) \in K[x]$.

Theorem 2.2. *Let K be a number field, S a finite set of places of K that contains all Archimedean places, $\mathcal{O}_S$ the ring of S-integers of K, and $f, g \in K[x]$ nonconstant. Then the following assertions are equivalent.*

- *The equation $f(x) = g(y)$ has infinitely many solutions with a bounded $\mathcal{O}_S$-denominator;*
- *We have*

$$f(x) = \phi(f_1(\lambda(x))) \quad \& \quad g(x) = \phi(g_1(\mu(x))), \tag{2.3}$$

where $\phi \in K[x]$, $\lambda, \mu \in K[x]$ are linear polynomials, and (f_1, g_1) is a standard or specific pair over K such that the equation $f_1(x) = g_1(y)$ has infinitely many solutions with a bounded $\mathcal{O}_S$-denominator.

Theorem 2.2 relies on Siegel's classical theorem on integral points on curves, and it is consequently ineffective.

3 Polynomial decomposition via Galois theory

Throughout this section, K is an arbitrary field with $\mathrm{char}(K) = 0$.

Recall that a polynomial $f \in K[x]$ with $\deg f > 1$ is called *indecomposable* (over K) if it cannot be written as the composition $f(x) = g(h(x))$ with $g, h \in K[x]$, $\deg g > 1$ and $\deg h > 1$. Otherwise, f is said to be *decomposable*. Any representation of f as a functional composition of polynomials of degree > 1 is said to be a *decomposition* of f.

Note that for decomposable $f \in K[x]$ we have that

$$f(x) = g(h(x)) \text{ for some } g, h \in K[x] \text{ such that } \deg g \geq 2, \deg h \geq 2, \ h \text{ is monic and } h(0) = 0. \tag{3.1}$$

Namely, if $f = g \circ h$ for some $g, h \in K[x]$ with $\deg g \geq 2$ and $\deg h \geq 2$, then there exists a linear $\mu \in K[x]$ such that $\mu \circ h$ is monic and $\mu(h(0)) = 0$. Furthermore, there exists $\mu^{\langle -1 \rangle} \in K[x]$ such that $\mu(x) \circ \mu^{\langle -1 \rangle}(x) = \mu(x)^{\langle -1 \rangle} \circ \mu(x) = x$. (By comparison of degrees one sees that no such polynomial exists when $\deg \mu > 1$). Clearly $f = \left(g \circ \mu^{\langle -1 \rangle}\right) \circ (\mu \circ h)$.

Proposition 3.2. *Let K be a field with $\mathrm{char}(K) = 0$ and $f \in K[x]$. Then f is indecomposable over K if and only if f is indecomposable over $\overline{K}$.*

Proposition 3.2 is due to Fried and McRae [6]. It is easy to prove it. Namely, let $f \in K[x]$ and assume that it is decomposable over $\overline{K}$. Then write $f = g \circ h$, where $g, h \in \overline{K}[x]$ are such that $\deg \geq 2, \deg h \geq 2$, h is monic and $h(0) = 0$, as in (3.1). Comparison of coefficients, starting from the highest-degree coefficient and proceeding inductively, yields $g, h \in K[x]$.

Recall the definition of the monodromy group of a polynomial from the introduction. By Gauss's lemma it follows that $f(X) - t \in K(t)[X]$ is irreducible over $K(t)$, so $\mathrm{Mon}(f)$ is a transitive permutation group. Since $\mathrm{char}(K) = 0$, $f(X) - t$ is also separable. Let x be a root of $f(X) - t$ in its splitting field L over $K(t)$. Then $t = f(x)$ and $\mathrm{Mon}(f) = \mathrm{Gal}(L/K(f(x)))$, where $\mathrm{Mon}(f)$ is viewed as a permutation group on the conjugates of x over $K(f(x))$.

A lot of information about a polynomial is encoded into its monodromy group. In particular, the following is well-known.

Lemma 3.3. *Let K be a field with $\mathrm{char}(K) = 0$ and $f \in K[x]$. Then f is indecomposable if and only if $\mathrm{Mon}(f)$ is primitive. Furthermore, $(f(x) - f(y))/(x - y) \in K[x, y]$ is irreducible over K if and only if $\mathrm{Mon}(f)$ is doubly transitive.*

Recall that a transitive permutation group G acting on a set X is called primitive if it preserves no nontrivial partition of X (trivial partitions are those consisting either of one set of size $\#X$ or of $\#X$ singletons). A permutation group G acting on a set X with $\#X \geq 2$ is called doubly transitive when, for any two ordered pairs of distinct elements (x_1, y_1) and (x_2, y_2) in X^2, there is $g \in G$ such that $y_1 = gx_1$ and $y_2 = gx_2$. Every doubly transitive permutation group is primitive. A symmetric group is doubly transitive if it is of degree at least two, and an alternating group is doubly transitive if it is of degree at least four. Find more about the Galois theoretic setup for addressing decomposition questions, developed by Ritt [15], in [18] and [21]. The first part of the Lemma 3.3 was observed already by Ritt, and the second by Fried [5].

Fried [5] showed that if K is a field with $\mathrm{char}(K) = 0$ and $f \in K[x]$ with $\deg f \geq 3$, then the following assertions are equivalent.

i) $(f(x) - f(y))/(x - y)$ is reducible over $\overline{K}$,

ii) either $f(x)$ is decomposable, or $f(x) = e_1 D_n(c_1 x + c_0, a) + e_0$, where $n > 3$ is a prime and $e_i, c_i, a \in K$, or $f(x) = e_1 D_3(c_1 x + c_0, 0) + e_0 = e_1(c_1 x + c_0)^3 + e_0$ and $e_i, c_i \in K$, where $D_n(x, a)$ is the Dickson polynomial of degree n with parameter a.

It can be shown that for $n \geq 2$, an n-th primitive root of unity $\zeta_n \in \overline{K}$, $\alpha_k = \zeta_n^k + \zeta_n^{-k}$ and $\beta_k = \zeta_n^k - \zeta_n^{-k}$ we have:

$$\begin{aligned} D_n(x,a) - D_n(y,a) &= (x-y) \prod_{k=1}^{(n-1)/2} (x^2 - \alpha_k xy + y^2 + \beta_k^2 a) \text{ when } n \text{ is odd,} \\ D_n(x,a) - D_n(y,a) &= (x-y)(x+y) \prod_{k=1}^{(n-2)/2} (x^2 - \alpha_k xy + y^2 + \beta_k^2 a) \text{ when } n \text{ is even.} \end{aligned} \tag{3.4}$$

If $a \neq 0$, then each quadratic factor in (3.4) is irreducible over $\overline{K}[x, y]$, while if $a = 0$, it is clearly reducible. Thus, $(D_3(x, a) - D_3(y, a))/(x - y)$ is reducible over $\overline{K}[x, y]$ if and only if $a = 0$. Note that if f is decomposable, then $(f(x) - f(y))/(x - y)$ is clearly reducible over K. If f is of composite degree and $f(x) = e_1 D_n(c_1 x + c_0, a) + e_0$ with $e_i, c_i, a \in K$, i.e. f is *linearly related to a Dickson polynomial*, then f is decomposable since $D_{mn}(x, a) = D_m(D_n(x, a), a^n)$ for $m, n \in \mathbb{N}$. These facts can be verified directly. For details, see Turnwald's paper [18]. So, if f is indecomposable, to eliminate the possibility that f with $\deg f \geq 4$ is linearly related to a Dickson polynomial, it is necessary and sufficient to assume that the absolute monodromy group of f is doubly transitive. Of relevance to us is the following corollary.

Corollary 3.5. *Let K be a field with $\mathrm{char}(K) = 0$ and let $f \in K[x]$ be such that the absolute monodromy group of f is doubly transitive. If $\deg f \geq 4$, then there do not exist $e_i, c_i, a \in K$ such that $e_1 c_1 a \neq 0$ and $f(x) = e_1 D_n(c_1 x + c_0, a) + e_0$. Furthermore, if $\deg f \geq 3$, there do not exist $e_i, c_i \in K$ such that $e_1 c_1 \neq 0$ and $f(x) = e_1(c_1 x + c_0)^k + e_0$.*

Proof. The statements follow from Lemma 3.3 and Equation 3.4. □

From Theorem 2.2 and Corollary 3.5 we deduce the following.

Proposition 3.6. *Let K be a number field, S a finite set of places of K that contains all Archimedean places and $\mathcal{O}_S$ the ring of S-integers of K. If $f, g \in K[x]$ are such that $\deg f \geq 3, \deg g \geq 3$ and the absolute monodromy groups of f and g are doubly transitive, the equation $f(x) = g(y)$ has infinitely many solutions with a bounded $\mathcal{O}_S$-denominator if and only if $f(x) = g(\mu(x))$ for some linear $\mu \in K[x]$.*

Proof. If the equation $f(x) = g(y)$ has infinitely many solutions with a bounded $\mathcal{O}_S$-denominator, then by Theorem 2.2 we have that

$$f(x) = \phi(f_1(\lambda(x))), \quad g(x) = \phi(g_1(\mu(x))), \tag{3.7}$$

for some $\phi, f_1, g_1, \lambda, \mu \in K[x]$ such that (f_1, g_1) is a standard pair over K and $\deg \lambda = \deg \mu = 1$.

Assume that the absolute monodromy groups of f and g are doubly transitive. It follows, in particular, that f and g are indecomposable.

Assume that $\deg \phi > 1$. Then from (3.7) it follows that $\deg f_1 = 1$ and $\deg g_1 = 1$, and $f(x) = g(\mu(x))$ for some linear $\mu \in K[x]$. If this holds, then the equation $f(x) =$

$g(y)$ clearly has infinitely many solutions with a bounded $\mathcal{O}_S$-denominator, e.g. set $x = \mu(t), y = t$, where $t \in \mathcal{O}_S$.

If $\deg \phi = 1$, then from (3.7) it follows that

$$f(x) = e_1 f_1(c_1 x + c_0) + e_0, \quad g(x) = e_1 g_1(d_1 x + d_0) + e_0, \tag{3.8}$$

for some $c_1, c_0, d_1, d_0, e_1, e_0 \in K$ such that $c_1 d_1 e_1 \neq 0$. Let $\deg f = \deg f_1 =: k$ and $\deg g = \deg g_1 =: l$. By assumption $k, l \geq 3$.

Note that (f_1, g_1) is not a standard pair of the second kind since $k, l > 2$.

Furthermore, (f_1, g_1) is not a standard pair of the fifth kind, since otherwise either $f_1(x) = (ax^2 - 1)^3$ or $g_1(x) = (ax^2 - 1)^3$, so by (3.8) either f or g are decomposable, a contradiction with the assumption.

Also, (f_1, g_1) is not a standard pair of the first kind, since by Corollary 3.5 and (3.8) neither $f_1(x) = x^k$ nor $g_1(x) = x^l$ is possible (since $k, l \geq 3$).

It also follows that (f_1, g_1) is not a standard pair of the third or of the fourth kind. Namely, otherwise $\gcd(k, l) \leq 2$, and since $k, l \geq 3$, it follows that either $k \geq 4$ or $l \geq 4$, which together with (3.8) contradicts Corollary 3.5.

In the same way, Corollary 3.5 implies that if (f_1, g_1) is a specific pair, then $(k, l) = (3, 3)$. In this case, $\gcd(k, l) = 3$, so $f_1(x) = D_3(x, a) = x^3 - 3xa$ and $g_1(x) = -D_3(1/2x, a) = -1/8x^3 + 3/2xa$, so $g_1(-2x) = f_1(x)$. Then from (3.8) it follows that $g(\mu(x)) = f(x)$ for some linear $\mu \in K[x]$. □

We can prove a version of Proposition 3.6 in the case when only of the polynomials f and g has a doubly transitive absolute monodromy group, but the proof would be more technical, and there would be several exceptional cases when the equation $f(x) = g(y)$ has infinitely many solutions in S-integers x, y. Our proof of Theorem 1.4 illustrates how to handle this case.

The following result, exhibiting sufficient conditions for a polynomial to have symmetric, and thus doubly transitive monodromy group, was shown by Turnwald [18]. For a polynomial f, the roots of the derivative f' are called *critical points*, and the values of f at critical points are called *critical values*. If for critical points β_i's of f, one has $f(\beta_i) \neq f(\beta_j)$ when $\beta_i \neq \beta_j$, then f is said to have *all distinct critical values*.

Proposition 3.9. *Let K be a field with $\mathrm{char}(K) = 0$. If $f \in K[x]$ has at least one simple critical point and all distinct critical values, then $\mathrm{Mon}(f)$ is a symmetric permutation group.*

One may find a proof and an extension of Proposition 3.9 in [12].

4 Lacunary polynomials

Throughout this section, K is a field with $\mathrm{char}(K) = 0$. By $f^{(k)}$ we denote the k-th derivative of f.

Lemma 4.1 (Hajós's lemma)**.** *Let K be a field with $\mathrm{char}(K) = 0$. If $f \in K[x]$ with $\deg f \geq 1$ has a root $\beta \neq 0$ of mutiplicity m, then f has at least $m + 1$ terms.*

A proof of Lemma 4.1 can be found in e.g. [16, p. 187]. This is the main idea: Assume that f has $\ell \leq m$ nonzero terms. Since the first m derivatives of f (i.e. $f^{(0)}, \ldots, f^{(m-1)}$) vanish at β, we get a system of ℓ equations with ℓ unknowns (coefficients of f), for which one easily finds that its determinant is nonzero (as it reduces to Vandermonde type of determinant), so the system has a unique solution (trivial one), but the coefficients of f are nonzero, a contradiction.

Lemma 4.2. *Let K be a field with $\operatorname{char}(K) = 0$, Assume that*

$$a_1 x^{n_1} + \cdots + a_\ell x^{n_\ell} + a_{\ell+1} = (b_1 x^{m_1} + \cdots + b_k x^{m_k} + b_{k+1}) \circ \mu(x),$$

where $\ell, k \geq 1$, $n_i, m_j \in \mathbb{N}$, $a_i, b_j \in K$, $\mu \in K[x]$ and

i) $n_i > n_j$ when $i > j$ and $m_i > m_j$ when $i > j$

ii) $a_1 a_2 \cdots a_\ell b_1 b_2 \cdots b_k \neq 0$

iii) $\deg \mu = 1$, $\mu(0) \neq 0$.

Then for $i = 2, 3, \ldots, \ell + 1$, the n_i-th derivative of $b_1 x^{m_1} + \cdots + b_k x^{m_k} + b_{k+1}$ has at least $n_{i-1} - n_i$ terms and the $(n_i + 1)$-st derivative of $b_1 x^{m_1} + \cdots + b_k x^{m_k} + b_{k+1}$ has a nonzero root of multiplicity $n_{i-1} - n_i - 1$. Finally, if $n_i \geq m_i$ for $i = 1, 2, \ldots, k$, then

$$n_1 = m_1 \leq k(k+1)/2.$$

Proof. Let $f(x) = a_1 x^{n_1} + \cdots + a_\ell x^{n_\ell} + a_{\ell+1}$ and $g(x) = b_1 x^{m_1} + \cdots + b_k x^{m_k} + b_{k+1}$. Let $n_{\ell+1} := 0$ and $m_{k+1} := 0$. Let further $\mu(x) = \alpha x + \beta$. By assumption $f(x) = g(\mu(x))$ and $\alpha, \beta \neq 0$.

Note that $f^{(n_i)}(x) - f^{(n_i)}(0) = x^{n_{i-1} - n_i} h_i(x)$ for some $h_i \in K[x]$ for all $i = 2, \ldots, \ell, \ell + 1$. Since $f^{(n_i)}(x) = \alpha^{n_i} g^{(n_i)}(\alpha x + \beta)$, the last expression can be rewritten as

$$\alpha^{n_i} g^{(n_i)}(x) - f^{(n_i)}(0) = (x - \beta)^{n_{i-1} - n_i} \hat{h}_i(x)$$

for some $\hat{h}_i \in K[x]$. So, $\beta \neq 0$ is a root of multiplicity $n_{i-1} - n_i$ of $\alpha^{n_i} g^{(n_i)}(x) - f^{(n_i)}(0)$. Thus, $\beta \neq 0$ is a root of multiplicity $n_{i-1} - n_i - 1$ of $g^{(n_i+1)}(x)$ for all $i = 2, \ldots, \ell, \ell + 1$.

By Lemma 4.1 it follows that $\alpha^{n_i} g^{(n_i)}(x) - f^{(n_i)}(0)$ has at least $n_{i-1} - n_i + 1$ terms, so $g^{(n_i)}(x)$ has at least $n_{i-1} - n_i$ terms.

If $n_i \geq m_i$ for $i = 1, 2, \ldots, k$, then $\alpha^{n_i} g^{(n_i)}(x) - f^{(n_i)}(0)$ has at most i terms. Then by Lemma 4.1 it follows that $n_{i-1} - n_i + 1 \leq i$ for all $i = 2, \ldots, k + 1$. By taking sum, we get

$$n_1 = \sum_{i=2}^{k+1} (n_{i-1} - n_i) \leq 1 + 2 + \cdots + k = \binom{k+1}{2}.$$

□

We remark that by Lemma 4.2, using the same notation, it follows that $n_1 = m_1 \leq \ell(k+1)$. Namely, $n_1 = (n_1 - n_2) + (n_2 - n_3) \cdots + (n_\ell - n_{\ell+1})$, and if $n_1 \geq \ell(k+1) + 1$, then there exists $i \in \{2, \ldots, \ell + 1\}$ such that $n_{i-1} - n_i \geq k + 2$. However, $g^{(n_i)}(x)$ clearly has at most $k + 1$ terms for any $i \in \{2, \ldots, \ell + 1\}$, a contradiction.

Lemma 4.2 is based on Zannier's Lemma 2 in [19]. Zannier studied the case when $f = g$. We remark that there is a small technical mistake in his proof, but that this mistake has no impact on the main results of the paper. By our Lemma 4.2 it follows that, in particular, if $f \in K[x]$ has $\ell \geq 1$ nonconstant terms and $f = f \circ \mu$ for some linear $\mu \in K[x]$ with $\mu(0) \neq 0$, then $\deg f \leq \binom{\ell+1}{2}$, while Zannier concluded that $\deg f \leq \binom{\ell}{2}$. In fact, much more holds, as the following lemma shows.

Lemma 4.3. *Let K be a field with $\operatorname{char}(K) = 0$ and let $f \in K[x]$ have $\ell \geq 1$ nonconstant terms and $g \in K[x]$ have $k \geq 1$ nonconstant terms. Assume that $f(x) = g(\mu(x))$ for some linear $\mu \in K[x]$ such that $\mu(0) \neq 0$. Then $\deg f = \deg g \leq k + \ell$. In particular, if $f = g$, then $\deg f \leq 2\ell$.*

Lemma 4.3 is shown by Gawron [10]. His proof is based on a classical result of Gessel and Viennot about matrices with binomial coefficients. Gawron studied the Equation 1.2 when $k = 3$ and $\ell \geq 4$, and when $k = \ell = 3$.

The following result is due to Zannier [19].

Theorem 4.4. *Let K be a field with $\mathrm{char}(K) = 0$ and let $f \in K[x]$ have $\ell \geq 1$ nonconstant terms. Assume that $f = g \circ h$, where $g, h \in K[x]$ and where h is not of type $ax^k + b$ for $a, b \in K$. If $\ell \geq 2$, then $\deg g < 2\ell(\ell - 1)$. If $\ell = 1$, then $\deg g = 1$.*

The main ingredients of Zannier's proof of Theorem 4.4 are Lemma 4.1 and the following result of Brownawell and Masser [2], which can be seen as a version of Schmidt's subspace theorem for function fields.

Theorem 4.5. *Let $K/k(x, y)$ be a function field of one variable of genus g, and let $z_1, \ldots, z_s \in K$ be not all constant and such that $1 + z_1 + \cdots + z_s = 0$. Suppose also that no proper subsum of the left side vanishes. Then*

$$\max(\deg(z_i)) \leq \binom{s}{2} (\#S + 2g - 2),$$

where S is a set of points of K containing all zeros and poles of the z_i's.

We will use this result later to prove Proposition 1.7.

Let $f \in K[x]$ with $\ell \geq 1$ nonconstant terms be decomposable. Write $f(x) = g(h(x))$ with $g, h \in K[x]$, $\deg \geq 2$, $\deg h \geq 2$, h monic and $h(0) = 0$, as in (3.1). Theorem 4.4 implies that if $\ell = 1$, then $h(x) = x^k$, and if $\ell \geq 2$, then either $\deg g < 2\ell(\ell - 1)$ or $h(x) = x^k$. Note that

$$a_1 x^{n_1} + a_2 x^{n_2} + \cdots + a_\ell x^{n_\ell} + a_{\ell+1} = f(x) = g(x) \circ x^k,$$

with distinct n_i's and $a_1 \cdots a_\ell \neq 0$, exactly when $k \mid n_i$ for all $i = 1, 2, \ldots, \ell$.

If $\ell = 2$ in Theorem 4.4, then if $f = g \circ h$, where $g, h \in K[x]$ and where h is not of type $ax^k + b$, then $\deg g \leq 3$. Fried and Schinzel [7] have shown that in this case $\deg g = 1$. In particular, if $\gcd(n_1, n_2) = 1$, then $a_1 x^{n_1} + a_2 x^{n_2} + a_3 \in K[x]$ is indecomposable. Moreover, the following holds.

Corollary 4.6. *Let K be a field with $\mathrm{char}(K) = 0$ and $f(x) = a_1 x^{n_1} + a_2 x^{n_2} + a_3 \in K[x]$, with $a_1 a_2 \neq 0$, $n_1 > n_2 \geq 1$, $\gcd(n_1, n_2) = 1$. Then $\mathrm{Mon}(f)$ is symmetric.*

Proof. Note that $f'(x) = x^{n_2 - 1} (a_1 n_1 x^{n_1 - n_2} + a_2 n_2)$, so f' has at least one simple root. Note that $xf'(x) = n_1(f(x) - a_3) + a_2(n_1 - n_2)x^{n_2}$. If $f(\alpha) = f(\beta)$ for distinct critical points α and β of f, then $\alpha^{n_2} = \beta^{n_2}$, and then from $f'(\alpha) = f'(\beta) = 0$ it follows that $\alpha^{n_1} = \beta^{n_1}$. Since $\gcd(n_1, n_2) = 1$, we have $\alpha = \beta$. The statement then follows from Proposition 3.9. □

We now prove Proposition 1.7.

Proof of Proposition 1.7. Assume first that $\deg h \geq 2$. Let $z = h(x)$. Then

$$a_1 x^{n_1} + \cdots + a_\ell x^{n_\ell} + a_{\ell+1} = b_1 z^{m_1} + b_2 z^{m_2}. \tag{4.7}$$

We will make use of Theorem 4.5. Assume that there exists a proper vanishing subsum of (4.7). Choose a vanishing subsum which involves $a_1 x^{n_1}$ and has no proper vanishing subsum, and further write this vanishing sum as $p(x) = q(z)$. Clearly, $\deg p = n_1$, the

number of terms of p is $\leq \ell$, and by comparison of the degrees we have $q(z) = b_1 z^{m_1}$. Thus, $p(x) = b_1 x^{m_1} \circ h(x)$. By Lemma 4.1, it follows that either h has no nonzero root, i.e. $h(x) = cx^k$ for some $k \in \mathbb{N}$ and $c \in K \setminus \{0\}$, or $m_1 \leq \ell - 1$. In the latter case, we get what we sought and more. In the former case, since $\gcd(n_1, \ldots, n_\ell) = 1$, it must be that $k = 1$, which contradicts the assumption $\deg h \geq 2$.

Assume henceforth that there exists no proper vanishing subsum of (4.7). Note that $x, z \in K(x)$. From (4.7) it follows that

$$\frac{a_1 x^{n_1}}{a_\ell x^{n_\ell}} + \cdots + 1 + \frac{a_{\ell+1}}{a_\ell x^{n_\ell}} - \frac{b_1 h(x)^{m_1}}{a_\ell x^{n_\ell}} - \frac{b_2 h(x)^{m_2}}{a_\ell x^{n_\ell}} = 0.$$

Note that the total number of zeros and poles of the terms in the above vanishing sum is at most $\deg h + 1$. By Theorem 4.5, it follows that

$$n_1 - n_\ell \leq \binom{\ell+2}{2}(\deg h + 1 + 2 \cdot 0 - 2) = \binom{\ell+2}{2}(\deg h - 1).$$

Write $b_1 x^{m_1} + b_2 x^{m_2} - a_{\ell+1} = b_1 \prod_{i=1}^{r}(x - \beta_i)^{e_i}$, with distinct β_i's and positive integers e_i. Then

$$a_1 x^{n_1} + \cdots + a_\ell x^{n_\ell} = b_1 \prod_{i=1}^{r}(h(x) - \beta_i)^{e_i}. \tag{4.8}$$

Since the factors in the product are coprime, it follows that x^{n_ℓ} divides $(h(x) - \beta_i)^{e_i}$ for some i, say i_0. Since by assumption $h(x) - \beta_{i_0}$ has at least one nonzero root (since $\deg h \geq 2$ and $\gcd(n_1, \ldots, n_\ell) = 1$), it follows that $n_\ell \leq (\deg h - 1) \cdot e_{i_0}$.

By Lemma 4.1, from $b_1 x^{m_1} + b_2 x^{m_2} - a_{\ell+1} = b_1 \prod_{i=1}^{r}(x - \beta_i)^{e_i}$ we have that $e_i \leq 2$ for all i if $a_{\ell+1} \neq 0$. If $a_{\ell+1} = 0$, then $\beta_{i_0} = 0$, $e_{i_0} = m_2$ and $e_i = 1$ for all i except for i_0. However, since $h(x) - \beta_{i_0}$ must have a nonzero root (again, since $\deg h \geq 2$ and $\gcd(n_1, \ldots, n_\ell) = 1$), it follows from (4.8) that $e_{i_0} \leq \ell - 1$. Thus, $n_\ell \leq (\ell - 1)(\deg h - 1)$.

Therefore,

$$\begin{aligned} n_1 \leq \binom{\ell+2}{2}(\deg h - 1) + n_\ell &\leq \binom{\ell+2}{2}(\deg h - 1) + (\ell - 1)(\deg h - 1) \\ &= (\deg h - 1)\left(\binom{\ell+2}{2} + \ell - 1\right), \end{aligned}$$

so in particular (1.9) holds. Clearly, if $a_{\ell+1} \neq 0$, then by what we showed above, the summand $\ell - 1$ in the sum above can be replaced by 2, so (1.10) holds.

Let now $\deg h = 1$. Clearly, if $h(0) = 0$, then $\ell = 2$, a contradiction with the assumption. Thus, $h(0) \neq 0$. Then the polynomial on the right hand side of (1.8) has a nonzero root of multiplicity m_2, and the one on the left hand side has no nonzero root of multiplicity greater than ℓ by Lemma 4.1. Thus, $m_2 \leq \ell$. Assume that $n_1 = m_1 \geq \binom{\ell+2}{2} + \ell - 1$, so

$$m_1 - m_2 \geq \binom{\ell+2}{2} - 1 \geq \ell + 2$$

since $\ell \geq 3$. Note that the coefficients of the polynomial on the right hand side in (1.8) next to $x^{m_1}, x^{m_1-1}, \ldots, x^{m_2+1}$ are all nonzero, since $\deg b_2 h(x)^{m_2} = m_2$, and $h(0) \neq 0$. However, since $m_1 - m_2 \geq \ell + 2$, this contradicts the assumption that on the left hand side in (1.8) we have at most $\ell + 1$ nonzero terms. □

In relation to Proposition 1.7, we remark that proving a version of this proposition with the polynomial $b_1x^{m_1}+b_2x^{m_2}$ replaced by a lacunary polynomial with $k \geq 3$ nonconstant terms, would require a different approach, as it would be harder to analyse when there exists a proper zero subsum of an analogue of (4.7).

Remark 4.9. Let K be a field and $f(x) \in K[x]$. By $\mathrm{Aut}(f)$ we denote the group of linear polynomials $\mu(x) \in K[x]$ for which $f \circ \mu = f$, and call this group the automorphism group of f. The elements of $\mathrm{Aut}(f)$ play a prominent role in the study of the image set $f(K)$, where K is a finite field. This classical topic has a rich tradition. In [13], jointly with Zieve I studied various properties of the automorphism group of a cover of curves over an arbitrary field. In the sequel, in relation to the above results, I will briefly state some corollaries in the case when f is a lacunary polynomial with coefficients in a field K with $\mathrm{char}(K) = 0$. We will rely on the results from [21] and [13]. The results in these papers are obtained using the monodromy method.

Let K be an algebraically field with $\mathrm{char}(K) = 0$ and let $f(x) = a_1x^{n_1} + \cdots + a_\ell x^{n_\ell} + a_{\ell+1} \in K[x]$ where $\ell \geq 1$ and $a_1 \cdots a_\ell \neq 0$. (The assumption that K is algebraically closed will not reflect on the results). Let further $d = \gcd(n_1, \ldots, n_\ell)$. Clearly, $f(x) = (a_1x^{n_1/d} + \cdots + a_\ell x^{n_\ell/d} + a_{\ell+1}) \circ x^d$, and $f(x) = f(\mu(x))$ for any $\mu(x) = \zeta x$ where $\zeta^d = 1$. Thus, $|\mathrm{Aut}(f)| \geq d$.

By [13, Lem. 6.3], we may write $f(x) = g(h(x))$ where $K(x)/K(h(x))$ is Galois with Galois group $\mathrm{Aut}(f)$. Since $\mathrm{char}(K) = 0$ and $K(x)/K(h(x))$ is Galois, it follows by [13, Lem. 2.8, Lem. 3.1] that $\mathrm{Mon}(h)$ is cyclic. This corresponds to saying that h is cyclic, that is $h(x) = \ell_1(x) \circ x^k \circ \ell_2(x)$ for some linear $\ell_1, \ell_2 \in K[x]$ and $k \in \mathbb{N}$, and $|\mathrm{Mon}(h)| = \deg h$, by [21, Lem. 3.6]. Then $|\mathrm{Aut}(f)| = |\mathrm{Mon}(h)| = \deg h$ by [13, Lem. 3.4].

Assume that $\ell_2(0) = 0$. Then $h(x) = ax^k + b$ for some $a \in K \setminus \{0\}$ and $b \in K$, and thus $k \mid d$, so $|\mathrm{Aut}(f)| = k \leq d$. Since also $|\mathrm{Aut}(f)| \geq d$, it follows that $|\mathrm{Aut}(f)| = d$. So, in this case there does not exist a linear $\mu \in K[x]$ with $\mu(0) \neq 0$, such that $f \circ \mu = f$.

Assume henceforth $\ell_2(0) \neq 0$. Since $f(x) = g(x) \circ \ell_1(x) \circ x^k \circ \ell_2(x)$, it follows that $f(x) - g(\ell_1(0))$ has a nonzero root of multiplicity k. By Lemma 4.1 it follows that $k \leq \ell$. Thus, $|\mathrm{Aut}(f)| \leq \ell$. If $\ell \leq d$, then in the same way as above we conclude that there does not exist a linear $\mu \in K[x]$ with $\mu(0) \neq 0$, such that $f \circ \mu = f$.

If f is indecomposable (and recall that by Lemma 3.2, f is indecomposable over K if and only if f is indecomposable over $\overline{K}$), then in particular $d = 1$. Furthermore, by [13, Cor. 6.6] we have that either $\mathrm{Aut}(f)$ is trivial or f is cyclic and $|\mathrm{Aut}(f)| = \deg f$. So, if f is indecomposable and $|\mathrm{Aut}(f)| > 1$, then $\deg f = |\mathrm{Aut}(f)| \leq \ell$ by the same argument as above.

5 Diophantine equations and lacunary polynomials

We now give a short proof of Theorem 1.11.

Proof of Theorem 1.11. The main statement follows from Proposition 3.6 and Corollary 4.6. Assume that (1.13) holds. Then the equation clearly has infinitely many solutions $x, y \in K$ with a bounded $\mathcal{O}_S$-denominator. Further assume without loss of generality that $n_2 \leq m_2$. By Lemma 4.2 it follows that if $\mu(0) \neq 0$, then $n_1 = m_1 \leq 3$. Thus, $n_1 = m_1 = 3$. By comparing coefficients one easily works out that only the listed cases are possible. If $\mu(0) = 0$, then the last statement clearly holds. □

We now prove Theorem 1.4.

Proof of Theorem 1.4. If the equation has infinitely many solutions with a bounded $\mathcal{O}_S$-denominator, then

$$a_1x^{n_1} + \cdots + a_\ell x^{n_\ell} + a_{\ell+1} = \phi(f_1(\lambda(x))), \tag{5.1}$$
$$b_1x^{m_1} + b_2x^{m_2} = \phi(g_1(\mu(x))), \tag{5.2}$$

for some $f_1, g_1, \phi, \lambda, \mu \in K[x]$ such that (f_1, g_1) is a standard pair over K and $\deg\lambda = \deg\mu = 1$.

Assume that $\deg\phi > 1$. Since $\gcd(m_1, m_2) = 1$, by Corollary 4.6 it follows that $b_1x^{m_1} + b_2x^{m_2}$ is indecomposable. Thus, $\deg g_1 = 1$ and hence $\phi(x) = b_1\sigma(x)^{m_1} + b_2\sigma(x)^{m_2}$ for some linear $\sigma \in K[x]$. Then

$$a_1x^{n_1} + \cdots + a_\ell x^{n_\ell} + a_{\ell+1} = (b_1x^{m_1} + b_2x^{m_2}) \circ \sigma(f_1(\lambda(x))).$$

By Proposition 1.7 it follows that $m_1 < \binom{\ell+2}{2} + \ell - 1$, which contradicts the assumption.

Thus $\deg\phi = 1$. Then

$$a_1x^{n_1} + \cdots + a_\ell x^{n_\ell} + a_{\ell+1} = e_1f_1(c_1x + c_0) + e_0, \tag{5.3}$$
$$b_1x^{m_1} + b_2x^{m_2} = e_1g_1(d_1x + d_0) + e_0, \tag{5.4}$$

for some $c_1, c_0, d_1, d_0, e_1, e_0 \in K$ such that $c_1d_1e_1 \neq 0$. In particular, $\deg f_1 = n_1$ and $\deg g_1 = m_1$. By assumption, $m_1 \geq 12$ and $n_1 \geq 3$. Note that by Corollary 4.6 and (5.4), the absolute monodromy group of g_1 is doubly transitive.

Now, (f_1, g_1) is not a standard pair of the second kind since $n_1 > 2$ and $m_1 > 2$.

Furthermore, (f_1, g_1) is not a standard pair of the fifth kind since $m_1 > 6$.

Also, (f_1, g_1) cannot be a standard pair of the third or of the fourth kind, nor a specific pair. Namely, recall that the absolute monodromy group of g_1 is doubly transitive, so the statement follows by Corollary 3.5, since $m_1 \geq 12$.

If (f_1, g_1) is a standard pair of the first kind, then either $g_1(x) = x^{m_1}$ or $f_1(x) = x^{n_1}$. Since the absolute monodromy group of g_1 is doubly transitive and $m_1 \geq 12$, by Corollary 3.5 it follows that it must be that $f_1(x) = x^{n_1}$. Hence,

$$a_1x^{n_1} + \cdots + a_\ell x^{n_\ell} + a_{\ell+1} - e_0 = e_1(c_1x + c_0)^{n_1},$$

so $c_0 \neq 0$ and $n_1 = \ell$. Then $g_1(x) = c'x^r p(x)^{n_1}$ for some $c' \in K\setminus\{0\}$, $r < n_1$, $\gcd(r, n_1) = 1$ and $r + \deg p > 0$. Since the absolute monodromy group of g_1 is doubly transitive and $m_1 \geq 12$, by Corollary 3.5 it follows that $\deg p > 0$. Then

$$b_1x^{m_1} + b_2x^{m_2} - e_0 = e_1g_1(d_1x + d_0) = e_1c'(d_1x + d_0)^r p(d_1x + d_0)^{n_1}.$$

Since $n_1 \geq 3$, by Lemma 4.1 it follows that $p(d_1x + d_0)$ has no nonzero root. Then, since $n_1 \geq 3$ and $\deg p > 0$, it follows that $e_0 = 0$ and that $(d_1x + d_0)^r$ has exactly two terms, so $r = 1$ and $d_0 \neq 0$. Thus, (1.6) holds.

When (1.6) holds, there are infinitely many solutions x, y with a bounded $\mathcal{O}_S$-denominator of the equation, since the equation $x^{n_1} = cy\mu(y)^{m_1-1}$ with linear $\mu \in K[x]$ has infinitely many solutions x, y with a bounded $\mathcal{O}_S$-denominator. Namely, if $q, s \in \mathbb{N}$ are such that $qn_1 = s+1$, then an infinite family of solutions is given by $x = c^q u\mu(c^s u^{n_1})^{m_1-1}$, $y = c^s u^{n_1}$, for $u \in \mathcal{O}_S$. □

To the proof of Theorem 1.1 we need one more lemma.

Lemma 5.5. *Let K be a number field. Assume that*

$$a_1x^{n_1} + \cdots + a_\ell x^{n_\ell} + a_{\ell+1} = (e_1 D_{n_1}(c_1x + c_0, \alpha) + e_0) \circ \mu(x),$$

where $\ell \geq 2$, $n_i \in \mathbb{N}$, $a_i, e_i, c_i, \alpha \in K$, $\mu \in K[x]$ and

i) $n_i > n_j$ if $i > j$,

ii) $a_1a_2 \cdots a_\ell \neq 0$, $e_1c_1\alpha \neq 0$,

iii) $\deg \mu = 1$ and $\mu(0) \neq 0$.

Then $n_{i-1} - n_i \leq 2$ for all $i = 2, 3, \ldots, \ell + 1$, and thus $n_1 \leq 2\ell$.

Proof. By Lemma 4.2, for $i = 2, \ldots, \ell+1$, the (n_i+1)-st derivative of $e_1D_{n_1}(c_1x+c_0, \alpha)+e_0$ has a nonzero root of multiplicity $n_{i-1} - n_i - 1$. Thus, the $(n_i + 1)$-st derivative of $D_{n_1}(c_1x + c_0, \alpha)$ has a nonzero root of multiplicity $n_{i-1} - n_i - 1$.

We now show that $D^{(k)}_{n_1}(x, \alpha)$ has only simple roots for all $k = 0, 1, \ldots, n_1 - 1$, so that $D^{(k)}_{n_1}(c_1x+c_0, \alpha)$ has only simple roots for all $k = 0, 1, \ldots, n_1-1$. Recall that $D_{n_1}(x, \alpha) = 2\alpha^{n_1/2}T_{n_1}(x/(2\sqrt{\alpha}))$ where $T_k(x) = \cos(k \arccos x)$ is the k-th Chebyshev polynomial of the first kind. The roots of $T_k(x) = \cos(k \arccos x)$ are $x_j := \cos(\pi(2j - 1)/(2k))$, $j = 1, 2, \ldots, k$. These are all simple and real, so the roots of $T^{(k)}_{n_1}(x)$ are simple and real for all $k = 0, 1, \ldots, n_1 - 1$, by Rolle's theorem. Since

$$D^{(k)}_{n_1}(x, \alpha) = \frac{2\alpha^{n_1/2}}{(2\sqrt{\alpha})^k} T^{(k)}_{n_1}(x/(2\sqrt{\alpha})),$$

it follows that $D^{(k)}_{n_1}(x, \alpha)$ has only simple roots for all $k = 0, 1, \ldots, n_1 - 1$. Note that the multiplicity of a nonzero root of $D^{(n_1)}_{n_1}(x, \alpha)$ is 0. Therefore, $n_{i-1} - n_i - 1 \leq 1$ for all $i = 2, \ldots, \ell + 1$, and

$$n_1 = (n_1 - n_2) + (n_2 - n_3) + \cdots + (n_\ell - n_{\ell+1}) \leq 2\ell.$$

□

The last statement of Lemma 5.5 is shown in [10], for the case $K = \mathbb{Q}$, by using Lemma 4.3.

Proof of Theorem 1.1. If the equation has infinitely many solutions with a bounded $\mathcal{O}_S$-denominator, then

$$a_1x^{n_1} + \cdots + a_\ell x^{n_\ell} + a_{\ell+1} = \phi(f_1(\lambda(x))), \tag{5.6}$$

$$b_1x^{m_1} + \cdots + b_k x^{m_k} = \phi(g_1(\mu(x))), \tag{5.7}$$

for some $f_1, g_1, \phi, \lambda, \mu \in K[x]$ such that (f_1, g_1) is a standard pair over K and $\deg \lambda = \deg \mu = 1$.

Assume that $\deg \phi > 1$. Since $b_1x^{m_1} + \cdots + b_kx^{m_k}$ is indecomposable it follows that $\deg g_1 = 1$, so that $\phi(x) = b_1\sigma(x)^{m_1} + \cdots + b_k\sigma(x)^{m_k}$ for some linear $\sigma \in K[x]$. Then

$$a_1x^{n_1} + \cdots + a_\ell x^{n_\ell} + a_{\ell+1} = (b_1x^{m_1} + \cdots + b_kx^{m_k}) \circ \sigma(f_1(\lambda(x))).$$

From Theorem 4.4 it follows that either $\sigma(f_1(\lambda(x))) = \zeta x^k + \nu$ for some $\zeta, \nu \in K$, or $m_1 < 2\ell(\ell - 1)$. The latter can not be by assumption. Note that if the former holds, then

$k \mid n_i$ for all $i = 1, 2, \ldots, \ell$. This contradicts the assumption on coprimality of n_i's, unless $k = 1$. If $k = 1$, then (1.3) holds, and the equation clearly has infinitely many solutions $x, y \in K$ with a bounded $\mathcal{O}_S$-denominator

Assume henceforth $\deg \phi = 1$. Then

$$a_1 x^{n_1} + \cdots + a_\ell x^{n_\ell} + a_{\ell+1} = e_1 f_1(c_1 x + c_0) + e_0, \tag{5.8}$$
$$b_1 x^{m_1} + \cdots + b_k x^{m_k} = e_1 g_1(d_1 x + d_0) + e_0, \tag{5.9}$$

for some $c_1, c_0, d_1, d_0, e_1, e_0 \in K$ such that $c_1 d_1 e_1 \neq 0$. In particular, $\deg f_1 = n_1$ and $\deg g_1 = m_1$. By assumption $m_1 \geq 12$ and $n_1 \geq 3$.

Note that (f_1, g_1) is not a standard pair of the second kind, since $n_1 > 2$ and $m_1 > 2$. Similarly, (f_1, g_1) is not a standard pair of the fifth kind since $m_1 > 6$.

Also, (f_1, g_1) is not a standard pair of the third or of the fourth kind, nor a specific pair. Namely, otherwise, by (5.8) and (5.9), and Lemma 5.5, it follows that $n_1 \leq 2\ell$ and $m_1 \leq 2k$, a contradiction with the assumption.

Finally, if (f_1, g_1) is a standard pair of the first kind, then either $f_1(x) = x^{n_1}$ or $g_1(x) = x^{m_1}$. Assume first that the former holds. Then

$$\begin{aligned} a_1 x^{n_1} + \cdots + a_\ell x^{n_\ell} + a_{\ell+1} - e_0 &= e_1 (c_1 x + c_0)^{n_1}, \\ b_1 x^{m_1} + \cdots + b_k x^{m_k} - e_0 &= e_1 c' (d_1 x + d_0)^r p(d_1 x + d_0)^{n_1}, \end{aligned} \tag{5.10}$$

where $p \in K[x]$, $r < n_1$, $\gcd(r, n_1) = 1$, $r + \deg p > 0$ and $c' \neq 0$. Clearly, $n_1 = \ell$ and $c_0 \neq 0$. By Lemma 4.1 it follows that either $p(d_1 x + d_0)$ has no nonzero root, or $n_1 \leq k$. If $n_1 > k$, then we have

$$b_1 x^{m_1} + \cdots + b_k x^{m_k} - e_0 = e_1 c (d_1 x + d_0)^r x^{m_1 - r},$$

for some $c \neq 0$. Then $r + 1 = k$.

Assume now that $g_1(x) = x^{m_1}$. Then

$$\begin{aligned} a_1 x^{n_1} + \cdots + a_\ell x^{n_\ell} + a_{\ell+1} - e_0 &= e_1 c' (c_1 x + c_0)^r p(c_1 x + c_0)^{m_1}, \\ b_1 x^{m_1} + \cdots + b_k x^{m_k} - e_0 &= e_1 (d_1 x + d_0)^{m_1}, \end{aligned} \tag{5.11}$$

where $p \in K[x]$, $r < m_1$, $\gcd(r, m_1) = 1$, $r + \deg p > 0$ and $c' \neq 0$. Clearly, $m_1 = k$ and $d_0 \neq 0$. By Lemma 4.1 it follows that either $p(c_1 x + c_0)$ has no nonzero root, or $m_1 \leq \ell$. The latter cannot be by assumption, so

$$a_1 x^{n_1} + \cdots + a_\ell x^{n_\ell} + a_{\ell+1} - e_0 = e_1 c (c_1 x + c_0)^r x^{n_1 - r},$$

for some $c \neq 0$. Then $r + 1 = \ell$.

Since $n_1 \neq \ell$ and $m_1 \neq k$ by assumption, we have that (f_1, g_1) is not a standard pair of the first kind. This completes the proof. □

We now discuss how the assumptions of Theorem 1.1 can be relaxed.

Instead of requiring that either $m_1 \geq 2k + 1$ or $n_1 \geq 2\ell + 1$, we could have required that either there exists $i \in \{2, 3, \ldots, \ell + 1\}$ such that $n_{i-1} - n_i > 2$ or that there exists $i \in \{2, 3, \ldots, k + 1\}$ such that $m_{i-1} - m_i > 2$. This follows by Lemma 5.5, since we used this assumption only to eliminiate the cases when $\deg \phi = 1$ and (f_1, g_1) is a either standard pair of the third or fourth kind, or a specific pair.

Instead of requiring that $n_1 \neq \ell$ and $m_1 \neq k$, we can list the cases that occur when $n_1 = \ell$ or $m_1 = k$, as was done in the last paragraphs of the proof of Theorem 1.1, and in Theorem 1.4.

If we assume that m_1 is a composite number, because of the assumption *iii*), we can immediately eliminate the case when $\deg\phi = 1$ and (f_1, g_1) is either a standard pair of the third or fourth kind, or a specific pair, since a Dickson polynomial of composite degree is decomposable. For details, see the paragraph below the Equation 3.4. Thus we do not need to assume that either $m_1 \geq 2k+1$ or $n_1 \geq 2\ell+1$. In the same way, we do not need to assume that $m_1 \neq k$, since this assumption serves to eliminate the case $b_1y^{m_1} + \cdots + b_ky^{m_k} - e_0 = e_1(d_1x + d_0)^{m_1}$. (This cannot be since on the left hand side we have an indecomposable polynomial, and on the right a decomposable polynomial, since m_1 is by assumption composite). Thus, if we assume that m_1 is composite and relax the assumption *iv*) to requiring that $m_1 \geq 2\ell(\ell-1)$, we have that the equation (1.2) has infinitely many solutions $x, y \in K$ with a bounded $\mathcal{O}_S$-denominator if and only if either (1.3) or (5.10) holds.

Appendix

In [3, 4], it is shown that $b_1x^{m_1} + b_2x^{m_2} + \cdots + b_kx^{m_k}$ with $m_i \in \mathbb{N}$ and $b_i \in \mathbb{Z}\setminus\{0\}$ is indecomposable when either $m_2 = m_1 - 1$ and $\gcd(m_1, b_2) = 1$, or f is an odd polynomial, $m_2 = m_1 - 2$ and $\gcd(m_1, b_2) = 1$. We now extend these results to the case when b_i's are in a unique factorization domain of characteristic zero. This is of interest in relation to Theorem 1.1.

Let R be an integral domain and L be its quotient field. Assume that $\mathrm{char}(L) = 0$. Let K be any extension of L.

For a nonconstant $f \in R[x]$, write $f(x) = g(h(x))$ with $g, h \in K[x]$, $\deg g \geq 2$, $\deg h \geq 2$, h monic and $h(0) = 0$, as in (3.1), Turnwald [18] showed that the coefficients of g and h belong to an integral closure of R in L by the following argument. The coefficients of g and h belong to L by the same argument as in the proof of Proposition 3.2 (see the text below it). Furthermore, if α is a root of g, then the monic polynomial $h(x) - \alpha$ divides $f(x) = g(h(x))$. So, the coefficients of $h(x) - \alpha$ are integral over R. Since α was an arbitrary root, the same holds for g. Thus, the coefficients of g and h belong to an integral closure of R in L. If R is a unique factorization domain, then R is integrally closed in L, so the coefficients of g and h belong to R, and the following holds.

Corollary 5.12. *Let R be a unique factorization domain and K any field extension of the quotient field of R. Assume that $\mathrm{char}(K) = 0$. Let $f \in R[x]$ be such that $f(x) = g(h(x))$ with $g, h \in K[x]$, $\deg g \geq 2$, $\deg h \geq 2$, h monic and $h(0) = 0$. Then $g, h \in R[x]$.*

In particular, if K is a number field of class number 1, R is the ring of algebraic integers of K and $f \in R[x]$ is such that $f(x) = g(h(x))$, where $g, h \in K[x]$, $\deg g \geq 2, \deg h \geq 2$, h monic and $h(0) = 0$, then $g, h \in R[x]$.

Turnwald [18] further showed that if number field K is of class number greater than 1 and R is the ring of algebraic integers of K, then for every prime q there exists $f \in R[x]$ of degree q^2 which is decomposable over K, but can not be represented as a composition of polynomials in $R[x]$.

We now prove the sought result. In the sequel, for a unique factorization domain R, $t \in \mathbb{Z}$ and $a \in R$, we say that t divides a in R, and write $t \mid a$ in R, when there exists $a' \in R$ such that $a = ta'$.

Proposition 5.13. *Let R be a unique factorization domain and K any field extension of the quotient field of R. Assume that $\mathrm{char}(K) = 0$. Let $f(x) = a_1x^{n_1} + \cdots + a_\ell x^{n_\ell} + a_{\ell+1} \in R[x]$, where n_i's are distinct positive integers with $n_i > n_j$ for $i > j$, and $a_1a_2\cdots a_\ell \neq 0$.*

Assume that $f(x) = g(h(x))$*, where* $g, h \in K[x]$*,* $\deg g \geq 2$ *and* $\deg h \geq 2$*. Then either* $h(x) = \zeta x^m + \nu$ *for some* $\zeta, \nu \in K$ *and* $m \mid n_i$ *for all* $i = 1, 2, \ldots, \ell$*, or* $\deg g \mid a_2$ *in* R*.*

In particular, if $\gcd(n_1, \ldots, n_\ell) = 1$ *and there does not exist integer* $t \geq 2$ *such that* $t \mid n_1$ *and* $t \mid a_2$ *in* R*, then* f *is indecomposable over* K*.*

Proof. Let $f(x) = g(h(x))$ with $g, h \in K[x]$, $\deg g \geq 2$, $\deg h \geq 2$, h monic and $h(0) = 0$, as in (3.1). By Corollary 5.12 it follows that $g, h \in R[x]$. Let $\deg h = m$ and $\deg g = t$. Let further $h(x) = b_1 x^{m_1} + b_2 x^{m_2} + \cdots + b_k x^{m_k}$ with $m_i \in \mathbb{N}$ and $b_i \in R \setminus \{0\}$. By assumption, $b_1 = 1$ and $m_1 = m$. If $h(x) = x^m$, then clearly $m \mid n_i$ for all $i = 1, 2, \ldots, \ell$. Assume that h is not a monomial, so that $k \geq 2$. Then by $f(x) = g(h(x))$, it follows that $f(x) = a_1 h(x)^t + p(x)$, where $p \in R[x]$, $\deg p \leq (t-1)m_1$. Then $a_2 = a_1 t b_2$ by comparison of coefficients on both sides next to x^{n_2}. Thus $t \mid a_2$ in R. Clearly, $t \mid n_1$ as well. □

Acknowledgements

I am thankful for the support of the Austrian Science Fund (FWF) through projects W1230 and FWF-24574.

References

[1] Yu.F. Bilu and R.F. Tichy, *The Diophantine equation* $f(x) = g(y)$, Acta Arith. **95** (2000), 261–288. 2, 4, 5

[2] W.D. Brownawell and D.W. Masser, *Vanishing sums in function fields*, Math. Proc. Cambridge Philos. Soc. **100** (1986), no. 3, 427–434. 3, 10

[3] A. Dujella and I. Gusić, *Indecomposability of polynomials and related Diophantine equations*, Q. J. Math. **57** (2006), 193–201. 2, 16

[4] A. Dujella, I. Gusić, and R.F. Tichy, *On the indecomposability of polynomials*, Österreich. Akad. Wiss. Math.-Natur. Kl. Sitzungsber. II **214** (2005), 81–88. 2, 16

[5] M.D. Fried, *Arithmetical properties of function fields. II. The generalized Schur problem*, Acta Arith. **25** (1973/74), 225–258. 6

[6] M.D. Fried and R.E. McRae, *On the invariance of chains of fields*, Illinois J. Math. **13** (1969), 165–171. 6

[7] M.D. Fried and A. Schinzel, *Reducibility of quadrinomials*, Acta Arith. **21** (1972), 153–171. 2, 10

[8] C. Fuchs, V. Mantova, and U. Zannier, *On fewnomials, integral points and a toric version of Bertini's theorem*, arXiv:1412.4548. 1

[9] C. Fuchs and U. Zannier, *Composite rational functions expressible with few terms*, J. Eur. Math. Soc. **14** (2012), 175–208. 1

[10] M. Gawron, *On decompositions of quadrinomials and related Diophantine equations*, arXiv:1512.02817. 2, 10, 14

[11] D. Kreso, *On common values of lacunary polynomials at integer points*, New York J. Math. **21** (2015), 987–1001. 2, 3

[12] D. Kreso and R.F. Tichy, *Diophantine equations and monodromy groups*, submitted. 8

[13] D. Kreso and M.E. Zieve, *On factorizations of maps between curves*, arXiv: 1405.4753. 12

[14] G. Péter, Á. Pintér, and A. Schinzel, *On equal values of trinomials*, Monatsh. Math. **162** (2011), 313–320. 2, 4

[15] J.F. Ritt, *Prime and composite polynomials*, Trans. Amer. Math. Soc. **23** (1922), 51–66. 1, 6

[16] A. Schinzel, *Polynomials with special regard to reducibility*, Cambridge University Press, 2000. 1, 2, 8

[17] ———, *Equal values of trinomials revisited*, Tr. Mat. Inst. Steklova **276** (2012), 255–261. 2, 4

[18] G. Turnwald, *On Schur's conjecture*, J. Austral. Math. Soc. Ser. A **58** (1995), 312–357. 4, 6, 7, 8, 16

[19] U. Zannier, *On the number of terms of a composite polynomial*, Acta Arith. **127** (2007), 157–167. 1, 3, 9, 10

[20] ———, *On composite lacunary polynomials and the proof of a conjecture of Schinzel*, Invent. Math. **174** (2008), 127–138. 1, 2, 3

[21] M.E. Zieve and P. Müller, *On Ritt's polynomial decomposition theorems*, arXiv:0807.3578. 1, 6, 12