Monatshefte für Mathematik (2022) 199:135–148
https://doi.org/10.1007/s00605-022-01737-7

On decompositions of binary recurrent polynomials

Dijana Kreso[1]

Received: 6 January 2021 / Accepted: 31 May 2022 / Published online: 6 July 2022

Abstract
Polynomial decomposition expresses a polynomial f as the functional composition $f = g \circ h$ of lower degree polynomials g and h, and has various applications. In this paper, we will show that for a minimal, non-degenerate, simple, binary, linearly recurrent sequence $(G_n(x))_{n=0}^{\infty}$ of complex polynomials whose coefficients in the Binet form are constants, if $G_n(x) = g(h(x))$, then apart from some exceptional situations that have to be taken into account, the degree of g is bounded by a constant independent of n. We will build on a general but conditional result of this type that already exists in the literature. We will then present one Diophantine application of the main result.

Keywords Polynomial decomposition · Linear recurrences · Diophantine equations

Mathematics Subject Classification 11R09 · 12E99 · 39B12

1 Introduction

In the 1920's, Ritt [12] studied the functional *decomposition* $f = f_1 \circ \cdots \circ f_m$ of a complex polynomial f into *indecomposable* complex polynomials $f_1, \ldots, f_m$. A complex polynomial f with $\deg f > 1$ is said to be indecomposable if it cannot be represented as a composition of two lower degree polynomials. Ritt gave a procedure for obtaining any decomposition of a complex polynomial from any other by applying certain transformations. Ritt's results about polynomial decomposition have applications to number theory, complex analysis, arithmetic dynamics, finite geometries, etc. @ See e.g. [11] for an overview of the theory and applications. Of our interest in this paper are decomposition properties of binary recurrent sequences of polynomials. This

Communicated by Umberto Zannier.

✉ Dijana Kreso
kreso@math.tugraz.at

[1] Institute of Analysis and Number Theory (Math A), Graz University of Technology - TU Graz, Kopernikusgasse 24/II, 8010 Graz, Austria

topic has been studied in several papers [6–8] and relevant results will be mentioned later in the introduction. For $A_0(x), A_1(x), G_0(x), G_1(x) \in \mathbb{C}[x]$, let $(G_n(x))_{n=0}^{\infty}$ be a minimal, non-degenerate and simple binary linearly recurrent sequence of polynomials defined by

$$G_{n+2}(x) = A_1(x)G_{n+1}(x) + A_0(x)G_n(x),\ n \geq 0, \quad \text{so that } G_n(x) = \pi_1\alpha_1^n + \pi_2\alpha_2^n, \tag{1.1}$$

for $\pi_1, \pi_2 \in L$, where $L/\mathbb{C}(x)$ is the splitting field of the characteristic polynomial of the recurrence and $\alpha_1, \alpha_2 \in L$ are its distinct roots (distinct since the recurrence is simple) such that $\alpha_1/\alpha_2 \notin \mathbb{C}^*$ (since the recurrence is non-degenerate), and furthermore $A_1, A_0, \pi_1\alpha_1^n, \pi_2\alpha_2^n \neq 0$ (by minimality).

To state our first result, we recall the definitions of *cyclic* and *dihedral* polynomials. These polynomials play a prominent role in Ritt's theory (more details will be given in Sect. 2). A polynomial h is said to be cyclic if $h(x) = \ell_1(x) \circ x^n \circ \ell_2(x)$ for some $n \geq 2$ and ℓ_1, ℓ_2 linear polynomials and dihedral if $h(x) = \ell_1(x) \circ T_n(x) \circ \ell_2(x)$ for some $n \geq 3$ and ℓ_1, ℓ_2 linear polynomials, where $T_n(x)$ is the n-th Chebychev polynomial of the first kind given by $T_{n+2}(x) = 2xT_{n+1}(x) - T_n(x)$, $T_0(x) = 1$, $T_1(x) = x$.

Theorem 1 *Consider the sequence* (1.1) *such that* $\pi_1, \pi_2 \in \mathbb{C}$. *Assume that for some* $n \geq 0$ *we have* $G_n(x) = g(h(x))$ *for* $g(x), h(x) \in \mathbb{C}[x]$, *where* h *is indecomposable and neither cyclic nor dihedral. Further asume that we do not have* $G_m(x) \in \mathbb{C}[h(x)]$ *for all* $m \geq 0$. *Then* $\deg g \leq C$ *for a constant* $C = C(\{A_i, G_i : i = 0, 1\}) > 0$, *independent of* n.

It is well known that $T_{mk}(x) = T_m(x) \circ T_k(x)$ for any $m, k \in \mathbb{N}$ and since for Chebychev polynomials of the first kind the coefficients in the Binet form are constants, already these polynomials illustrate that Theorem 1 would not hold if we allow h to be dihedral. Indeed, for dihedral $h(x) \in \mathbb{C}[x]$ of any degree there exists $n \geq 0$ such that $T_n(x) = g(h(x))$ for some $g(x) \in \mathbb{C}[x]$ whose degree depends on n. Furthermore, the sequence $T_n(h(x))$ with $h(x) \in \mathbb{C}[x]$ is of type (1.1) and its coefficients in the Binet form are constants, and we clearly cannot bound $\deg T_n$ independently of n. This illustrates why we also have to exclude the case when $G_m(x) \in \mathbb{C}[h(x)]$ for all $m \geq 0$. Also, for cyclic $h(x) \in \mathbb{C}[x]$ of any degree there exists a sequence $(G_n(x))_{n=0}^{\infty}$ satisfying (1.1), whose coefficients in the Binet form are constants, such that we do not have $G_m(x) \in \mathbb{C}[h(x)]$ for all m, but $G_n(x) = g(h(x))$ for some $n \geq 0$ and some $g(x) \in \mathbb{C}[x]$ whose degree depends on n. (Pick e.g. $\pi_1 = \pi_2 = 1$, $A_0(x) = x$, $A_1(x) = x + 1$. Then $G_{mk}(x) = x^{mk} + 1 = (x^m + 1) \circ x^k$ for any $k, m \in \mathbb{N}$.)

Corollary 2 *Let* $p(x), q(x) \in \mathbb{C}[x]$ *be such that* $p(x)^n + q(x)^n = g(h(x))$ *for some* $n \geq 0$ *and* $g(x), h(x) \in \mathbb{C}[x]$, *where* h *is indecomposable and neither cyclic nor dihedral. Then either* $p(x), q(x) \in \mathbb{C}[h(x)]$ *or* $\deg g \leq C$ *for a constant* $C = C(p, q) > 0$, *independent of* n.

In relation to Corollary 2, we remark that it is well known (see Lemma 5) and follows from Ritt's results that if the n-th power of a complex polynomial u is a *composite* of a complex polynomial h (more precisely, u is nonconstant and $u(x)^n \in \mathbb{C}[h(x)]$),

where h is indecomposable and neither dihedral nor cyclic, then u is a composite of h. Moreover, Ritt [12] gave a description of all $g(x), h(x) \in \mathbb{C}[x]$ whose composition is an n-th power of a complex polynomial. Cohen [3] described all rational functions $g(x), h(x) \in \mathbb{C}(x)$ whose composition is an n-th power in $\mathbb{C}(x)$. It would be of interest to give a full description of all $g(x), h(x) \in \mathbb{C}(x)$ whose composition is a sum of two n-th powers in $\mathbb{C}(x)$.

Theorem 1 relies on the main result of [8], which is a general but conditional result for an element of the sequence (1.1) to satisfy $G_n(x) = g(h(x))$, for $g(x), h(x) \in \mathbb{C}[x]$, where h is indecomposable and neither cyclic nor dihedral. To state this result precisely, assume that $G_n(x) = g(h(x))$, for $g(x), h(x) \in \mathbb{C}[x]$, where h is indecomposable. The polynomial $h(X) - h(x) \in \mathbb{C}(h(x))[X]$ is clearly separable and since $\deg h \geq 2$ by assumption, there exists $y \neq x$ such that $h(x) = h(y)$. Then $G_n(x) = G_n(y)$ and by equating the corresponding Binet forms, we obtain

$$\pi_1 \alpha_1^n + \pi_2 \alpha_2^n = \rho_1 \beta_1^n + \rho_2 \beta_2^n, \tag{1.2}$$

where α_1, α_2 are distinct roots of the characteristic polynomial of the sequence $(G_n(x))_{n=0}^{\infty}$, β_1, β_2 are distinct roots of the characteristic polynomial of the sequence $(G_n(y))_{n=0}^{\infty}$, $\pi_1, \pi_2 \in L_1$ and $\rho_1, \rho_2 \in L_2$, where L_1 and L_2 are the splitting fields of the corresponding characteristic polynomials over $\mathbb{C}(x)$ and $\mathbb{C}(y)$, respectively. According to [8, Thm. 1], there is a constant $C > 0$, independent of n, with the following property: If $G_n(x) = g(h(x))$ for some $n \geq 0$ and $g(x), h(x) \in \mathbb{C}[x]$, where h is indecomposable and neither cyclic nor dihedral, and (1.2) has no vanishing subsum, then $\deg g \leq C$. We say that there exists a vanishing subsum of (1.2) if there is a permutation σ of the set $\{1, 2\}$ such that $\pi_i \alpha_i^n = \rho_{\sigma(i)} \beta_{\sigma(i)}^n$ for $i = 1, 2$. With the above restrictions on h, one can show that this holds if and only if

$$\pi_1 \pi_2 A_0(x)^n = -\frac{G_1(x)^2 - G_0(x)G_1(x)A_1(x) - A_0(x)G_0(x)^2}{A_1(x)^2 + 4A_0(x)} A_0(x)^n \in \mathbb{C}[h(x)]. \tag{1.3}$$

See Sect. 2 for details. It appears to be difficult to classify all such G_0, G_1, A_0, A_1. In regard to this problem, we mention [10], where the authors solved the equation $g(x) f(x)^n = g(h(x))$ where f, g, h are unknown nonconstant complex polynomials, $n > 1$, $\deg h \geq 2$ and g is separable. We also mention [4], where the authors completely classified binomials which have a non-trivial factor which is a composition of two polynomials of degree > 1. We further mention that certain sufficient, but unfortunately not quite illuminating, conditions for (1.2) to have no vanishing subsum were presented in [8, Thm. 2]. Finally, we mention that the constant C can be effectively computed; this is done in the proof of [8, Thm. 1].

To the proof of Theorem 1, we will show that under the assumptions of the theorem, there does not exist a vanishing subsum of (1.2). We will build on the techniques from [8] and strengthen the arguments, in particular by utilizing a well known result of Fried (Theorem 6). We will complement Theorem 1 with the following result. It will be proved using a similar approach.

Proposition 3 *Consider the sequence* (1.1) *with* A_0 *constant and any of* G_0, G_1, A_1 *constant. Assume* $G_n(x) = g(h(x))$ *for some* $n \geq 0$ *and* $g(x), h(x) \in \mathbb{C}[x]$*, where* h *is indecomposable and neither cyclic nor dihedral. Further assume that we do not have* $G_m(x) \in \mathbb{C}[h(x)]$ *for all* $m \geq 0$*. Then* $\deg g \leq C$ *for a constant* $C = C(\{A_i, G_i : i = 0, 1\})$.

We will then present some well-understood sequences from the literature exhibiting the decomposition property from Theorem 1 and Proposition 3. These include Chebyshev polynomials of the first kind, Lucas polynomials, Fibonacci polynomials, Fermat polynomials, Chebyshev polynomials of the second kind, etc. See Sect. 3 for precise definitions and for further applications.

We remark that Zannier [15] proved a result similar to Theorem 1 for lacunary polynomials, i.e. polynomials with a fixed number of terms. Theorem 1 relies on the main result of [8], which is obtained using techniques similar to Zannier's. There are several applications of Zannier's result, see e.g. [8] for more details . We conclude this paper by illustrating one Diophantine application of Theorem 1. Consider a minimal, simple and non-degenerate sequence $(G_n(x))_{n=0}^{\infty}$ satisfying

$$G_{n+2}(x) = A_1(x)G_{n+1}(x) + A_0(x)G_n(x), \quad n \geq 0, \tag{1.4}$$

with $G_0(x), G_1(x), A_0(x), A_1(x) \in \mathbb{Q}[x]$, such that its coefficients in the Binet form are constants and that there is no $h(x) \in \mathbb{C}[x]$ such that $G_m(x) \in \mathbb{C}[h(x)]$ for all $m \geq 0$. Further consider another minimal, simple and non-degenerate sequence $(H_n(x))_{n=0}^{\infty}$ of the same type

$$H_{n+2}(x) = B_1(x)H_{n+1}(x) + B_0(x)H_n(x), \quad n \geq 0, \tag{1.5}$$

with $H_0(x), H_1(x), B_0(x), B_1(x) \in \mathbb{Q}[x]$, such that its coefficients in the Binet form are constants and that there is no $h(x) \in \mathbb{C}[x]$ such that $H_m(x) \in \mathbb{C}[h(x)]$ for all $m \geq 0$. Recall that $P(x) \in \mathbb{C}[x]$ is said to be a composite of a cyclic or dihedral polynomial if it is nonconstant and $P(x) = g(h(x))$, where h is either cyclic or dihedral and $g(x) \in \mathbb{C}[x]$.

Theorem 4 *Consider sequences* $(G_n(x))_{n=0}^{\infty}$ *and* $(H_n(x))_{n=0}^{\infty}$ *satisfying* (1.4) *and* (1.5)*, respectively. Then there exists a constant* $C = C(\{A_i, G_i : i = 0, 1\}) > 0$ *with the following property. If* $G_n(x)$ *and* $H_m(x)$ *with* $\deg G_n \geq \deg H_m > C$ *are not composites of either cyclic or dihedral polynomials, and the equation* $G_n(x) = H_m(y)$ *has infinitely many integer solutions* x, y*, then* $G_n(x) = H_m(\ell(x))$ *for a linear* $\ell(x) \in \mathbb{C}[x]$.

Theorem 4 is an almost immediate consequence of Theorem 1 and the main result of [2]. The latter result is a criterion for the finiteness of integer solutions of Diophantine equations of type $f(x) = g(y)$, where $f(x), g(x) \in \mathbb{Q}[x]$ are nonconstant polynomials. All details will be given in Sect. 5.

2 Auxiliary results

We now recall some basic facts about complex polynomial decomposition. For $f(x) \in \mathbb{C}[x]$ with $\deg f > 1$, we say that two decompositions $f = f_1 \circ \cdots \circ f_m$ and $f = g_1 \circ \cdots \circ g_n$ of f are *equivalent* if $m = n$ and there are linear $\mu_1, \ldots, \mu_{m-1} \in \mathbb{C}[x]$ such that $f_i \circ \mu_i = g_i$ and $\mu_i^{(-1)} \circ f_{i+1} = g_{i+1}$, $i = 1, 2, \ldots, m-1$. Here $\mu_i^{(-1)}$ denotes the inverse of μ with respect to functional composition which clearly exists exactly when μ is a linear polynomial. For a given polynomial f there may exist several *complete decompositions*, that is decompositions into indecomposable polynomials, but they are all related in the following way: any complete decomposition of f can be obtained from any other through a sequence of steps, each of which involves replacing two adjacent indecomposables by two others with the same composition. The only solutions of the equation $a \circ b = c \circ d$ in indecomposable complex polynomials, up to composing with linear polynomials, are the trivial $a \circ b = a \circ b$ and the non-trivial solutions $x^m \circ x^r P(x^m) = x^r P(x)^m \circ x^m$, $T_m(x) \circ T_n(x) = T_n(x) \circ T_m(x)$ where $P(x) \in \mathbb{C}[x]$, $r, m, n \in \mathbb{N}$ and T_n is the n-th Chebyshev polynomial defined in the introduction. These results are due to Ritt [12]. There are many interesting results on various topics (see e.g. [11] for an overview of such results) relying on Ritt's findings. In particular, the following corollary of one such more recent result will be repeatedly used in this paper, [1, Thm. 5.1] which, roughly speaking, states that 'most' pairs of complex polynomials have no *common composite*; f and h with $\deg f, \deg h > 1$ have a common composite if there are nonconstant u, v such that $u(f(x)) = v(h(x))$.

Lemma 5 *Assume that for some $f(x), g(x) \in \mathbb{C}[x]$ where f is either cyclic or dihedral, we have $f(g(x)) \in \mathbb{C}[h(x)]$ for an indecomposable $h(x) \in \mathbb{C}[x]$ which is neither cyclic nor dihedral. Then $g(x) \in \mathbb{C}[h(x)]$.*

Proof By [1, Thm. 5.1], it follows that if $g(x), h(x) \in \mathbb{C}[x]$ satisfy $\deg g > 1$, and h is indecomposable and neither cyclic nor dihedral, then g and h have a common composite if and only if either $g(x) \in \mathbb{C}[h(x)]$ or there are linear polynomials $\ell_1(x), \ell_2(x), \ell_3(x) \in \mathbb{C}[x]$ such that

$$g(x) = \ell_1(x) \circ x^m \circ \ell_3(x), \quad h(x) = \ell_2(x) \circ x^r P(x^m) \circ \ell_3(x),$$

where $r, m \in \mathbb{N}$, $P(x) \in \mathbb{C}[x]$, $\gcd(\deg g, \deg h) = 1$. In particular, if $\deg g > 1$, then g is either cyclic or $g(x) \in \mathbb{C}[h(x)]$. However, for a cyclic polynomial there is clearly a complete decomposition consisting only of cyclic polynomials (since $x^{mn} = x^m \circ x^n$ for any m, n), and for a dihedral polynomial there is clearly a complete decomposition consisting only of dihedral polynomials and possibly cyclic polynomials of degree 2 (since $T_{mn}(x) = T_m(x) \circ T_n(x)$ for any m, n, and $T_2(x) = 2x^2 - 1$ is cyclic). Moreover, if one complete decomposition of a complex polynomial consists only of cyclic and dihedral polynomials, then all complete decompositions consist only of cyclic and dihedral polynomials (see e.g. [11, Thm. 1.3, Lemma 3.6]). Thus, any complete decomposition of the polynomial $f(g(x))$, where f is either cyclic or dihedral and g is either cyclic or $\deg g = 1$, consists only of cyclic or dihedral polynomials. This implies that unless $g(x) \in \mathbb{C}[h(x)]$ or $\deg g = 0$, h must be either cyclic or dihedral, a contradiction. If g is constant, the statement trivially holds. □

Another famous result on the topic of polynomial decomposition that we will make use of in this paper is the following theorem due to Fried [5].

Theorem 6 *For $h(x) \in \mathbb{C}[x]$ the following assertions are equivalent.*

(i) $(h(x) - h(y))/(x - y)$ *is irreducible in* $\mathbb{C}[x, y]$,
(ii) h *is indecomposable and if* $n := \deg h$ *is an odd prime then* $h(x) \neq \alpha D_n(x + b, a) + c$ *with* $\alpha, a, b, c \in \mathbb{C}$, *with* $a = 0$ *if* $n = 3$, *where* $D_n(x, a)$ *is the* n*-th Dickson polynomial with parameter* a *satisfying*

$$D_n(x, 0) = x^n, \quad D_n(2ax, a^2) = 2a^n T_n(x), \ a \neq 0 \tag{2.1}$$

where T_n *denotes, as usual, the* n*-th Chebyshev polynomial of the first kind.*

Thus, for an indecomposable $h(x) \in \mathbb{C}[x]$ which is neither cyclic nor dihedral, we have that $(h(X) - h(Y)/(X - Y))$ is an irreducible polynomial in $\mathbb{C}[X, Y]$. A detailed exposition of Fried's proof of Theorem 6 can be found in [14], along with various properties of Dickson polynomials.

Next we recall a few auxiliary results recorded in [8] that we will use to prove Theorem 1. Consider the sequence (1.1) and assume $G_n(x) = g(h(x))$ for $g(x), h(x) \in \mathbb{C}[x]$, where h is indecomposable and neither cyclic nor dihedral. Let $y \neq x$ be a root of $h(X) - h(x) \in \mathbb{C}(x)[X]$ so that $h(x) = h(y)$ and consequently $G_n(x) = G_n(y)$. Then (1.2) holds. In [8], we showed that then either $\mathbb{C}(x) \cap \mathbb{C}(y) = \mathbb{C}(x)$ and h is cyclic, or $\mathbb{C}(x) \cap \mathbb{C}(y) = \mathbb{C}(h(x))$. Indeed, since $h(x) = h(y)$, we have $\mathbb{C}(h(x)) \subseteq \mathbb{C}(x) \cap \mathbb{C}(y) \subseteq \mathbb{C}(x)$. By Lüroth's theorem ([13, p. 13]) it follows that $\mathbb{C}(x) \cap \mathbb{C}(y) = \mathbb{C}(r(x))$ for some $r \in \mathbb{C}(x)$. Moreover, since h is a polynomial, r can be chosen to be a polynomial as well by [13, p. 16]. Then $h(x) \in \mathbb{C}[r(x)]$. Since h is indecomposable, it follows that either $\deg r = \deg h$ or $\deg r = 1$, i.e. @ either $\mathbb{C}(x) \cap \mathbb{C}(y) = \mathbb{C}(h(x))$ or $\mathbb{C}(x) \cap \mathbb{C}(y) = \mathbb{C}(x)$. If $\mathbb{C}(x) \cap \mathbb{C}(y) = \mathbb{C}(x)$, then $v(y) = x$ for some $v(x) \in \mathbb{C}(x)$ and hence $h(v(y)) = h(x) = h(y)$. We deduce that $v(x) \in \mathbb{C}[x]$ and $\deg v = 1$. One can show that such h must be cyclic (see [8, Lemma 4]), so that if h is not cyclic, then

$$\mathbb{C}(x) \cap \mathbb{C}(y) = \mathbb{C}(h(x)). \tag{2.2}$$

In [8] we then deduced that if h is not cyclic, there exists a vanishing subsum of (1.2) if and only if

$$\pi_1 \pi_2 A_0(x)^n \in \mathbb{C}(h(x)). \tag{2.3}$$

This fact will be used repeatedly in the following section. Note that

$$\pi_1 \pi_2 = -\frac{G_1(x)^2 - G_0(x)G_1(x)A_1(x) - A_0(x)G_0(x)^2}{A_1(x)^2 + 4A_0(x)} \in \mathbb{C}(x). \tag{2.4}$$

3 Proofs of main results

Proof of Theorem 1 Let $y \neq x$ be a root of $h(X) - h(x) \in \mathbb{C}(x)[X]$ so that $h(x) = h(y)$ and consequently $G_n(x) = G_n(y)$, so that (1.2) holds. By assumption we have $\pi_1, \pi_2, \rho_1, \rho_2 \in \mathbb{C}$.

Note that $\alpha_1+\alpha_2 = A_1(x), \alpha_1\alpha_2 = -A_0(x), \beta_1+\beta_2 = A_1(y)$ and $\beta_1\beta_2 = -A_0(y)$ by Vieta's formulae. Further note that α_1, α_2 are not necessarily polynomials, but $\alpha_1^m + \alpha_2^m$ is a polynomial for any $m \geq 0$. Moreover, we have

$$\alpha_1^m + \alpha_2^m = D_m(A_1(x), -A_0(x)) = \sum_{i=0}^{\lfloor \frac{m}{2} \rfloor} \frac{m}{m-j} \binom{m-j}{j} A_0(x)^j A_1(x)^{m-2j}, \quad (3.1)$$

where $D_m(X+Y, XY) = X^m + Y^m$ for $m \geq 0$ defines the m-th Dickson polynomial $D_m(x, a)$ with parameter a, encountered already in Theorem 6. Likewise,

$$\beta_1^m + \beta_2^m = D_m(A_1(y), -A_0(y)) \in \mathbb{C}[y], \ m \geq 0. \quad (3.2)$$

By [8, Thm. 1] it suffices to show that (1.2), that is $\pi_1\alpha_1^n + \pi_2\alpha_2^n = \rho_1\beta_1^n + \rho_2\beta_2^n$, has no vanishing subsum. Assume the contrary. Since h is by assumption not cyclic, we can further assume that $\mathbb{C}(x) \cap \mathbb{C}(y) = \mathbb{C}(h(x))$, as proved in [8, Lemma 4] and recalled in (2.2).

Since $\pi_1, \pi_2 \in \mathbb{C}$, note that either $\rho_1 = \pi_1$ and $\rho_2 = \pi_2$, or $\rho_1 = \pi_2$ and $\rho_2 = \pi_1$. Indeed,

$$G_0(x) = \pi_1 + \pi_2 =: c_1 \in \mathbb{C}, \quad \frac{2G_1(x) - G_0(x)A_1(x)}{A_1(x)^2 + 4A_0(x)} = (\pi_1 - \pi_2)^2 =: c_2 \in \mathbb{C}.$$

Then $G_0(y) = \rho_1 + \rho_2 = c_1$ and $\frac{2G_1(y)-G_0(y)A_1(y)}{A_1(y)^2+4A_0(y)} = (\rho_1 - \rho_2)^2 = c_2$ via $x \mapsto y$, and we easily deduce the claim. Assume without loss of generality that $\rho_1 = \pi_1$ and $\rho_2 = \pi_2$. We next show that the existence of a vanishing subsum of (1.2) implies $\pi_1 = \pi_2$.

We have that either $\pi_1\alpha_1^n = \pi_1\beta_1^n$ and $\pi_2\alpha_2^n = \pi_2\beta_2^n$, or $\pi_1\alpha_1^n = \pi_2\beta_2^n$ and $\pi_2\alpha_2^n = \pi_1\beta_1^n$. Assume first that the former holds. Then $\alpha_1^n + \alpha_2^n = \beta_1^n + \beta_2^n$, and thus by (3.1) and (3.2) we have that $\alpha_1^n + \alpha_2^n \in \mathbb{C}(x) \cap \mathbb{C}(y) = \mathbb{C}(h(x))$, and moreover clearly $\alpha_1^n + \alpha_2^n \in \mathbb{C}[h(x)]$. Since by assumption $G_n(x) = \pi_1\alpha_1^n + \pi_2\alpha_2^n \in \mathbb{C}[h(x)]$, it follows that $(\pi_1 - \pi_2)\alpha_1^n \in \mathbb{C}[h(x)]$ and $(\pi_1 - \pi_2)\alpha_2^n \in \mathbb{C}[h(x)]$. We conclude that either $\pi_1 = \pi_2$ or $\alpha_1^n, \alpha_2^n \in \mathbb{C}[h(x)]$. In the latter case we easily check that if $n > 0$, then we must have $\alpha_1, \alpha_2 \in \mathbb{C}[x]$. Then $\alpha_1, \alpha_2 \in \mathbb{C}[h(x)]$ by Lemma 5 and hence $G_m(x) \in \mathbb{C}[h(x)]$ for any $m \geq 0$, a contradiction. If $n = 0$, the theorem trivially holds. Now assume $\pi_1\alpha_1^n = \pi_2\beta_2^n$ and $\pi_2\alpha_2^n = \pi_1\beta_1^n$. Then

$$\begin{aligned} \alpha_1^n + \alpha_2^n &= \frac{(\pi_1 + \pi_2)(\pi_1\beta_1^n + \pi_2\beta_2^n) - \pi_1\pi_2(\beta_1^n + \beta_2^n)}{\pi_1\pi_2} \\ &= \frac{(\pi_1 + \pi_2)G_n(y) - \pi_1\pi_2(\beta_1^n + \beta_2^n)}{\pi_1\pi_2}. \end{aligned}$$

Since $\pi_1, \pi_2 \in \mathbb{C}$, by (3.1) and (3.2) we have $\alpha_1^n + \alpha_2^n \in \mathbb{C}(x) \cap \mathbb{C}(y) = \mathbb{C}(h(x))$, and moreover $\alpha_1^n + \alpha_2^n \in \mathbb{C}[h(x)]$. Since also $\pi_1\alpha_1^n + \pi_2\alpha_2^n \in \mathbb{C}[h(x)]$, it follows that either $\pi_1 = \pi_2$ or $\alpha_1^n, \alpha_2^n \in \mathbb{C}[h(x)]$, as in the former case. The latter possibility we exclude as before. It remains to consider the case $\pi_1 = \pi_2$.

If $\pi_1 = \pi_2 =: \pi$, then $G_n(x) = \pi(\alpha_1^n + \alpha_2^n) = \pi(\beta_1^n + \beta_2^n) = G_n(y)$. By assumption there exists a vanishing subsum of this sum, and we may assume without loss of generality that $\alpha_1^n = \beta_1^n$ and $\alpha_2^n = \beta_2^n$. Thus, $\alpha_1 = \zeta\beta_1$ and $\alpha_2 = \mu\beta_2$ for $\zeta, \mu \in \mathbb{C}$ such that $\zeta^n = \mu^n = 1$. Since then $A_0(x) = -\alpha_1\alpha_2 = -\zeta\beta_1\mu\beta_2 = \zeta\mu A_0(y)$, it follows that $A_0(x) \in \mathbb{C}(x) \cap \mathbb{C}(y) = \mathbb{C}(h(x))$. Moreover, clearly $A_0(x) \in \mathbb{C}[h(x)]$. Since then $A_0(x) = A_0(y)$, it follows that $\zeta\mu = 1$. A short calculation shows that

$$A_1(x) = \frac{\left(\zeta + \frac{1}{\zeta}\right) A_1(y) + \left(\zeta - \frac{1}{\zeta}\right) \sqrt{A_1(y)^2 + 4A_0(y)}}{2}, \tag{3.3}$$

and hence

$$A_1(x)^2 - \left(\zeta + \frac{1}{\zeta}\right) A_1(x)A_1(y) + A_1(y)^2 - \left(\zeta - \frac{1}{\zeta}\right)^2 A_0(x) = 0.$$

Denote

$$\begin{aligned} H_1(X, Y) :\ &= A_1(X)^2 - \left(\zeta + \frac{1}{\zeta}\right) A_1(X)A_1(Y) + A_1(Y)^2 \\ &\quad - \left(\zeta - \frac{1}{\zeta}\right)^2 A_0(X) \in \mathbb{C}[X, Y]. \end{aligned} \tag{3.4}$$

Recall that by assumption $h(x) = h(y)$. Since h is neither cyclic nor dihedral, by Theorem 6 it follows that $H(X, Y) = (h(X) - h(Y))/(X - Y) \in \mathbb{C}[X, Y]$ is irreducible. Since $H_1(x, y) = 0$, it follows that $H(X, Y) \mid H_1(X, Y)$. (We clearly also have

$$H(X, Y) \mid A_1(X)^2 - \left(\zeta + \frac{1}{\zeta}\right) A_1(X)A_1(Y) + A_1(Y)^2 - \left(\zeta - \frac{1}{\zeta}\right)^2 A_0(Y),$$

but this follows from (3.4) and $A_0(x) \in \mathbb{C}[h(x)]$, which is what we will use instead.) It follows that the highest homogenous part of $H(X, Y)$ divides the highest homogenous part of $H_1(X, Y)$. (A similar argument appeared in [15, Lemma 3].) If $\deg A_0 > 2 \deg A_1$, then

$$\frac{X^{\deg h} - Y^{\deg h}}{X - Y} \mid X^{\deg A_0},$$

which is clearly a contradiction. If $2 \deg A_1 > \deg A_0$, then

$$\frac{X^{\deg h} - Y^{\deg h}}{X - Y} \mid X^{2 \deg A_1} - \left(\zeta + \frac{1}{\zeta}\right) X^{\deg A_1} Y^{\deg A_1} + Y^{2 \deg A_1}.$$

It follows that $\delta^{2\deg A_1} - \left(\zeta + \frac{1}{\zeta}\right)\delta^{\deg A_1} + 1 = 0$ for all δ satisfying $\delta \neq 1$ and $\delta^{\deg h} = 1$. Thus for all such δ we have that either $\delta^{\deg A_1} = \zeta$ or $\delta^{\deg A_1} = \zeta^{-1}$. Then either $\zeta = \pm 1$ or $\{1, \zeta, 1/\zeta\}$ is a cyclic subgroup of order 3 of the group of k-th roots of unity, where $k = \deg h$. If $\zeta = \pm 1$, then $A_1(x) = \pm A_1(y)$ by (3.3), and hence $A_1(x) \in \mathbb{C}(x) \cap \mathbb{C}(y) = \mathbb{C}(h(x))$, and moreover clearly $A_1(x) \in \mathbb{C}[h(x)]$. Since then $A_0(x), A_1(x), G_0(x), G_1(x) \in \mathbb{C}[h(x)]$ from the recurrence relation it follows that $G_m(x) \in \mathbb{C}[h(x)]$ for all $m \geq 0$, a contradiction. In the latter case we have $\zeta^3 = 1$, and hence $\alpha_1^3 + \alpha_2^3 = \beta_1^3 + \beta_2^3$ from $\alpha_1 = \zeta\beta_1$ and $\alpha_2 = \frac{1}{\zeta}\beta_2$. By (3.1) and (3.2) we conclude that

$$A_1(x)^3 + 3A_0(x)A_1(x) = \alpha_1^3 + \alpha_2^3 \in \mathbb{C}(x) \cap \mathbb{C}(y) = \mathbb{C}(h(x)).$$

Now recall that h is indecomposable and thus from $\mathbb{C}(h(x)) \subseteq \mathbb{C}(A_1(x), h(x)) \subseteq \mathbb{C}(x)$ by Lüroth's theorem ([13, p. 13]) it follows that there are no intermediate fields between $\mathbb{C}(h(x))$ and $\mathbb{C}(x)$. Thus, either $\mathbb{C}(h(x)) = \mathbb{C}(A_1(x), h(x))$ or $\mathbb{C}(A_1(x), h(x)) = \mathbb{C}(x)$. Since $A_1(x)^3 + 3A_0(x)A_1(x) \in \mathbb{C}(h(x))$ and $A_0(x) \in \mathbb{C}(h(x))$ we have that $A_1(x)$ is a root of a cubic polynomial over $\mathbb{C}(h(x))$, and hence either $\mathbb{C}(A_1(x), h(x)) = \mathbb{C}(h(x))$ or $\deg h = [\mathbb{C}(x) : \mathbb{C}(h(x)] = [\mathbb{C}(A_1(x), h(x)) : \mathbb{C}(h(x))] \leq 3$. However, any polynomial of degree 2 is cyclic and of degree 3 either cyclic or dihedral ($ax^3 + bx + c + d \in \mathbb{C}[x]$ with $a \neq 0$ is cylic if $b^2 = 3ac$, and dihedral otherwise). If $\mathbb{C}(A_1(x), h(x)) = \mathbb{C}(h(x))$, then clearly $A_1(x) \in \mathbb{C}[h(x)]$ and then $G_m(x) \in \mathbb{C}[h(x)]$ for all $m \geq 0$, a contradiction.

If $2\deg A_1 = \deg A_0$, then

$$\frac{X^{\deg h} - Y^{\deg h}}{X - Y} \mid a_1^2\left(X^{2\deg A_1} - \left(\zeta + \frac{1}{\zeta}\right)X^{\deg A_1}Y^{\deg A_1} + Y^{2\deg A_1}\right)$$
$$-a_0\left(\zeta - \frac{1}{\zeta}\right)^2 Y^{2\deg A_1},$$

where a_1 is the leading coefficient of A_1 and a_0 is the leading coefficient of A_0. It follows that for any $\delta \neq 1$ such that $\delta^{\deg h} = 1$, we have

$$a_1^2\left(\delta^{2\deg A_1} - \left(\zeta + \frac{1}{\zeta}\right)\delta^{\deg A_1} + 1\right) - a_0\left(\zeta - \frac{1}{\zeta}\right)^2 = 0. \tag{3.5}$$

Since $A_0(x) \in \mathbb{C}[h(x)]$ and $\deg A_0 = 2\deg A_1 > 0$ (A_0 and A_1 are nonconstant since otherwise the sequence is constant, which would violate the minimality assumption), it follows that $\deg h \mid 2\deg A_1$. Therefore $\delta^{2\deg A_1} = 1$ and hence $\delta^{\deg A_1} = \pm 1$. We deduce

$$-a_1^2\left(\zeta + \frac{1}{\zeta} \pm 2\right) = a_0\left(\zeta + \frac{1}{\zeta} - 2\right)\left(\zeta + \frac{1}{\zeta} + 2\right)$$

Recall that ζ is an n-th root of unity. It follows that either $\zeta = \pm 1$, or $\zeta^3 = 1$ (and a_1 and a_0 are related in a certain way). In the former case, $A_1(x) = \pm A_1(y)$ by (3.3), and

hence $A_1(x) \in \mathbb{C}(x) \cap \mathbb{C}(y) = \mathbb{C}(h(x))$ and moreover $A_1(x) \in \mathbb{C}[h(x)]$, so as before we conclude that $G_m(x) \in \mathbb{C}[h(x)]$ for all $m \geq 0$, a contradiction. In the latter case, we conclude that $A_1(x)^3 + 3A_0(x)A_1(x) \in \mathbb{C}(h(x))$. We eliminate this possibility using the same argument as in the case $2 \deg A_1 > \deg A_0$. □

Proof of Corollary 2 If $p(q) = \pm q(x)$, or one of p and q is a zero polynomial, or $p(x)^m = q(x)^m$ for some $m \geq 1$, then the statement follows from Lemma 4, since $p(x)^n + q(x)^n$ is a constant times $p(x)^n$. Otherwise, consider the sequence (1.1) with $A_0(x) = -p(x)q(x)$, $A_1(x) = p(x)+q(x)$, $G_0(x) = 2$ and $G_1(x) = A_1(x)$, which is minimal, non-degenerate and simple, and $G_m(x) = p(x)^m + q(x)^m$ for all $m \geq 0$. By Theorem 1 it follows that either $G_m(x) \in \mathbb{C}[h(x)]$ for all $m \geq 0$ or $\deg g \leq C(p, q)$. If the former holds, then $p(x) + q(x) \in \mathbb{C}[h(x)]$ and $p(x)^2 + q(x)^2 \in \mathbb{C}[h(x)]$, so also $p(x)q(x) \in \mathbb{C}[h(x)]$, and thus $A_0(x), A_1(x) \in \mathbb{C}[h(x)]$. Furthermore, clearly either

$$p(x) = \frac{A_1(x) + \sqrt{A_1(x)^2 + 4A_0(x)}}{2}, \quad q(x) = \frac{A_1(x) - \sqrt{A_1(x)^2 + 4A_0(x)}}{2},$$

or vice versa. Since p and q are polynomials, we have that $A_1(x)^2 + 4A_0(x) = D(x)^2$ for some $D(x) \in \mathbb{C}[x]$. It follows that $D(x)^2 \in \mathbb{C}[h(x)]$. By Lemma 5 we have $D(x) \in \mathbb{C}[h(x)]$, and hence $p(x), q(x) \in \mathbb{C}[h(x)]$. □

Proof of Proposition 3 As in the proof of Theorem 1, let $y \neq x$ be a root of $h(X) - h(x) \in \mathbb{C}(x)[X]$ so that $h(x) = h(y)$ and consequently $G_n(x) = G_n(y)$. Then (1.2) holds. Also as in the proof of Theorem 1, we may assume that $\mathbb{C}(x) \cap \mathbb{C}(y) = \mathbb{C}(h(x))$ since h is not cyclic. As before, by [8, Thm. 1] it suffices to show that (1.2) has no vanishing subsum. We assume the contrary.

If A_0 and A_1 are constants, then clearly $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathbb{C}$, and consequently $\pi_1, \pi_2 \in \mathbb{C}[x]$ and $\rho_1, \rho_2 \in \mathbb{C}[y]$. Since there exists a vanishing subsum of (1.2), we have that either $\pi_1\alpha_1^n = \rho_1\beta_1^n$ and $\pi_2\alpha_2^n = \rho_2\beta_2^n$, or $\pi_1\alpha_1^n = \rho_2\beta_2^n$ and $\pi_2\alpha_2^n = \rho_1\beta_1^n$. In either case,

$$\pi_1\alpha_1^n, \pi_2\alpha_2^n \in \mathbb{C}(x) \cap \mathbb{C}(y) = \mathbb{C}(h(x))$$

and moreover clearly $\pi_1\alpha_1^n, \pi_2\alpha_2^n \in \mathbb{C}[h(x)]$. Thus $\pi_1, \pi_2 \in \mathbb{C}[h(x)]$ and hence $G_m(x) = \pi_1\alpha_1^m + \pi_2\alpha_2^m \in \mathbb{C}[h(x)]$ for all $m \geq 0$, a contradiction.

Now ssume $A_0(x) = a_0$ and $G_m(x) = c$ for $m \in \{0, 1\}$, with $a_0, c \in \mathbb{C}$. Then also $A_0(y) = a_0$ and $G_m(y) = c$ via $x \mapsto y$. Note that the statement of the theorem trivially follows for $n \leq 3$. We may thus assume $n > 3$. Since, by assumption, there exists a vanishing subsum of (1.2), by multiplication and Vieta's formulae it follows that $\pi_1\pi_2 A_0(x)^n = \rho_1\rho_2 A_0(y)^n$, and hence $\pi_1\pi_2 = \rho_1\rho_2$. Then also $\pi_1\pi_2\alpha_1^m\alpha_2^m = \rho_1\rho_2\beta_1^m\beta_2^m$ since $(-\alpha_1\alpha_2)^m = A_0(x)^m = a_0^m = A_0(y)^m = (-\beta_1\beta_2)^m$. Since we also have $G_m(x) = G_m(y) = c$, it follows that $\pi_1\alpha_1^m + \pi_2\alpha_2^m = \rho_1\beta_1^m + \rho_2\beta_2^m$. We conclude that either $\pi_1\alpha_1^m = \rho_1\beta_1^m$ and $\pi_2\alpha_2^m = \rho_2\beta_2^m$ or $\pi_1\alpha_1^m = \rho_2\beta_2^m$ and $\pi_2\alpha_2^m = \rho_1\beta_1^m$. Without loss of generality we may assume that the fomer holds. Since there exists a vanishing subsum of (1.2), we have that either $\pi_1\alpha_1^n = \rho_1\beta_1^n$ and

$\pi_2\alpha_2^n = \rho_2\beta_2^n$, or $\pi_1\alpha_1^n = \rho_2\beta_2^n$ and $\pi_2\alpha_2^n = \rho_1\beta_1^n$. We now show that in either case

$$D_{n-m}(A_1(x), -A_0(x)) = D_{n-m}(A_1(x), -a_0) = \alpha_1^{n-m} + \alpha_2^{n-m} \in \mathbb{C}[h(x)].$$

Recall that by assumption $n > 3$ and thus $n - m > 2$. In the former case, from $\pi_1\alpha_1^m = \rho_1\beta_1^m$ and $\pi_1\alpha_1^n = \rho_1\beta_1^n$, we conclude $\alpha_1^{n-m} = \beta_1^{n-m}$, and likewise from $\pi_2\alpha_2^m = \rho_2\beta_2^m$ and $\pi_2\alpha_2^n = \rho_2\beta_2^n$, that $\alpha_2^{n-m} = \beta_2^{n-m}$. Then $\alpha_1^{n-m} + \alpha_2^{n-m} = \beta_1^{n-m} + \beta_2^{n-m}$ and by (3.1) and (3.2) we conclude that $\alpha_1^{n-m} + \alpha_2^{n-m} \in \mathbb{C}(x) \cap \mathbb{C}(y) = \mathbb{C}(h(x))$, and hence $D_{n-m}(A_1(x), -A_0(x)) \in \mathbb{C}[h(x)]$. If on the other hand $\pi_1\alpha_1^n = \rho_2\beta_2^n$ and $\pi_2\alpha_2^n = \rho_1\beta_1^n$, then from $\pi_1\alpha_1^m = \rho_1\beta_1^m$ and $\pi_2\alpha_2^m = \rho_2\beta_2^m$ we deduce

$$\alpha_1^{n-m} + \alpha_2^{n-m} = \frac{\rho_2\beta_2^n}{\rho_1\beta_1^m} + \frac{\rho_1\beta_1^n}{\rho_2\beta_2^m} = \frac{G_0(y)G_{m+n}(y) - \rho_1\rho_2(\beta_1^{m+n} + \beta_2^{m+n})}{\rho_1\rho_2(-A_0(y))^m}.$$

By (2.4), it follows that $\rho_1\rho_2 \in \mathbb{C}(y)$, and thus by (3.1) and (3.2) we conclude that $\alpha_1^{n-m} + \alpha_2^{n-m} \in \mathbb{C}(x) \cap \mathbb{C}(y) = \mathbb{C}(h(x))$, and hence $D_{n-m}(A_1(x), -A_0(x)) = \alpha_1^{n-m} + \alpha_2^{n-m} \in \mathbb{C}[h(x)]$. Now, since $A_0(x) = a_0 \in \mathbb{C}$ and $n - m > 2$ by assumption, from (2.1) we have that $D_{n-m}(X, -a_0)$ is either dihedral (if $a_0 \neq 0$) or cyclic (if $a_0 = 0$). By Lemma 5, from $D_{n-m}(A_1(x), -a_0) \in \mathbb{C}[h(x)]$, it follows that $A_1(x) \in \mathbb{C}[h(x)]$. Since $\pi_1\pi_2 = \rho_1\rho_2 \in \mathbb{C}(x) \cap \mathbb{C}(y) = \mathbb{C}(h(x))$ and $A_0(x), A_1(x) \in \mathbb{C}[h(x)]$, by (2.4) it follows that

$$G_1(x)^2 - G_0(x)G_1(x)A_1(x) - a_0G_0(x)^2 \in \mathbb{C}[h(x)].$$

If $m = 0$ and thus $G_0(x) = c$, then $a_0G_0(x)^2$ is constant and $G_1(x)^2 - cG_1(x)A_1(x) \in \mathbb{C}[h(x)]$. Since also $A_1(x) \in \mathbb{C}[h(x)]$, we deduce that $(2G_1(x) - cA_1(x))^2 \in \mathbb{C}[h(x)]$. By Lemma 5 it follows that $2G_1(x) - cA_1(x) \in \mathbb{C}[h(x)]$ and hence $G_1(x) \in \mathbb{C}[h(x)]$. If $m = 1$, we analogously conclude that $G_0(x) \in \mathbb{C}[h(x)]$. Therefore $G_0(x), G_1(x), A_0(x), A_1(x) \in \mathbb{C}[h(x)]$ in either case, so $G_m(x) \in \mathbb{C}[h(x)]$ for all $m \geq 0$, a contradiction. □

4 Some remarks in relation to our main results

In Table 1 we list some well-studied binary recurrent sequences of polynomials that our main results can be applied to. All of these polynomials are generated by the Lucas polynomial sequence. Note that for each polynomial sequence in the second column we have $G_m(x) = \alpha_1^m + \alpha_2^m$ for all $m \geq 0$, where α_1, α_2 are such that $A_1(x) = \alpha_1 + \alpha_2$ and $A_0(x) = -\alpha_1\alpha_2$, and therefore Theorem 1 can be applied. All the sequences in the first column have constant G_0 and A_0, and therefore Proposition 3 can be applied.

Furthermore, consider the sequence

$$G_n(x) = (Ax + B)G_{n-1}(x) + DG_{n-2}(x),\ n \geq 1, \quad G_{-1}(x) = 0,\ G_0(x) = g_1 \neq 0, \tag{4.1}$$

where the coefficients $A, B, D \in \mathbb{C}$ satisfy $A, D \neq 0$ and do not depend on n. Fuchs, Pethő and Tichy [9] considered this sequence while studying a problem related to ours.

Table 1 $(G_n(x))_{n=0}^{\infty}$ satisfying $G_{n+2}(x) = A_1(x)G_{n+1}(x) + A_0(x)G_n(x),\ n \geq 0$

Sequence $(G_n(x))_{n=0}^{\infty}$ with $G_0(x) = 0$, $G_1(x) = 1$	Sequence $(G_n(x))_{n=0}^{\infty}$ with $G_0(x) = 2$, $G_1(x) = A_1(x)$	$A_1(x)$	$A_0(x)$
Fibonacci polynomials	Lucas polynomials	x	1
Pell polynomials	Pell–Lucas polynomials	$2x$	1
Fermat polynomials	Fermat–Lucas polynomials	$3x$	-2
Chebyshev polynomials of the second kind	Chebyshev polynomials of the first kind $2T_n(x)$	$2x$	-1
	Jacobsthal–Lucas polynomials	1	$2x$
	$x^n + 1$	$x + 1$	$-x$

Table 2 Standard pairs

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	$(x^2, \left(ax^2 + b\right)p(x)^2\right)$	–
Third	$\left(D_m(x, a^n), D_n(x, a^m)\right)$	$\gcd(m, n) = 1$
Fourth	$(a^{\frac{-m}{2}} D_m(x, a), -b^{\frac{-n}{2}} D_n(x, b))$	$\gcd(m, n) = 2$
Fifth	$\left((ax^2 - 1)^3, 3x^4 - 4x^3\right)$	–

Under certain assumptions, they gave a bound on the number of distinct $n, m \geq 0$ such that $G_n(x) = G_m(P(x))$ for a fixed nonconstant $P(x) \in \mathbb{C}[x]$. Note that $\deg G_m = m$, so Proposition 3 gives an upper bound on m and n such that $G_n(x) = G_m(P(x))$ for a fixed nonconstant polynomial $P \in \mathbb{C}[x]$ if P is not a composite of a cyclic or a dihedral polynomial, or such that $G_m(x)$ and $P(x)$ are composites of the same polynomial of degree > 1 for all $m \geq 0$.

5 Proof of Theorem 4

As mentioned in the introduction, Theorem 4 is an almost immediate consequence of Theorem 1 and the main result of [2]. To state the latter result we define the so called *standard pairs* of polynomials. In what follows $a, b \in \mathbb{Q}\backslash 0$, $m, n \in \mathbb{N}$, $r \in \mathbb{N} \cup \{0\}$, $p(x) \in \mathbb{Q}[x]$ is nonzero and $D_m(x, a)$ is the m-th Dickson polynomial with parameter a, defined in Theorem 6 (Table 2).

Theorem 7 *Let $f(x), g(x) \in \mathbb{Q}[x]$ be non-constant polynomials. Then the equation $f(x) = g(y)$ has infinitely many rational solutions with a bounded denominator if and only if $f(x) = \phi(f_1(\lambda(x)),\ g(x) = \phi(g_1(\mu(x)))$, where $\phi(x) \in \mathbb{Q}[x]$, $\lambda(x), \mu(x) \in \mathbb{Q}[x]$ are linear polynomials, and (f_1, g_1) is a standard pair over $\mathbb{Q}$ such that the equation $f_1(x) = g_1(y)$ has infinitely many rational solutions with a bounded denominator.*

The proof of Theorem 7 in [2] relies on Siegel's classical theorem on integral points on curves, and is consequently ineffective. Thus, Theorem 4 is also ineffective. We remark that among the ingredients in the proof of Theorem 7 were Ritt's decompositions results.

Proof of Theorem 4 Assume that the equation $G_n(x) = H_m(y)$ has infinitely many solutions in integers x, y. Then $G_n(x) = \phi(f_1(\lambda(x))$ and $H_m(x) = \phi(g_1(\mu(x)))$, where $\phi(x) \in \mathbb{Q}[x]$, $\lambda(x), \mu(x) \in \mathbb{Q}[x]$ are linear polynomials, and (f_1, g_1) is a standard pair over $\mathbb{Q}$, according to Theorem 7. Note that ϕ is nonconstant since G_n and H_m are by assumption nonconstant. From the table we see that if both $\deg f_1 > 1$ and $\deg g_1 > 1$, then either G_n or H_m is a composite of an either cyclic or dihedral polynomial, a contradiction. Since $\deg G_n \geq \deg H_m$ by assumption, it follows that either $\deg g_1 = 1$ and $\deg f_1 > 1$, or both f_1 and g_1 are linear polynomials. If the latter holds, then clearly $\phi(x) = H_m(\ell_1(x))$ for linear ℓ_1, and thus $G_n(x) = H_m(\ell(x))$ for linear $\ell(x) \in \mathbb{Q}[x]$. If $\deg g_1 = 1$ and $\deg f_1 > 1$, then clearly $\phi(x) = H_m(\ell(x))$ for linear $\ell(x) \in \mathbb{Q}[x]$, and hence $G_n(x) = H_m(\ell(f_1(\lambda(x)))$. Since by assumption there does not exist $h(x) \in \mathbb{C}[x]$ such that $G_m(x) \in \mathbb{C}[h(x)]$ for all $m \geq 0$ and G_n is also not a composite of a cyclic or a dihedral polynomial, by Theorem 1 it follows that $\deg H_m < C(\{A_i, G_i : i = 0, 1\})$. □

Acknowledgements Open access funding provided by Graz University of Technology. I am thankful for the support of the Austrian Science Fund (FWF) through project I4406 (joint project of the FWF and the NKFIH).

References

1. Beals, R.M., Wetherell, J.L., Zieve, M.E.: Polynomials with a common composite. Israel J. Math. **174**, 93–117 (2009)
2. Bilu, Y.F., Tichy, R.F.: The Diophantine equation $f(x) = g(y)$. Acta Arith. **95**, 261–288 (2000)
3. Cohen, S.D.: Composite rational functions which are powers. Proc. R. Soc. Edinb. Sect. A Math. **83**(1–2), 11–16 (1979)
4. Dvornicich, R., Zannier, U.: Composite factors of binomials and linear systems in roots of unity. Israel J. Math. **229**(1), 381–0391 (2019)
5. Fried, M.D.: On a conjecture of Schur. Mich. Math. J. **17**, 41–55 (1970)
6. Fuchs, C., Heintze, S.: Perfect powers in polynomial power sums. Contemp. Math. **768**, 89–104 (2021). (In: Lie Groups, Number Theory, and Vertex Algebras)
7. Fuchs, C., Karolus, C.: Composite values of polynomial power sums. Ann. Math. Blaise Pascal **26**, 1–24 (2019)
8. Fuchs, C., Karolus, C., Kreso, D.: Decomposable polynomials in second order linear recurrence sequences. Manuscr. Math. **159**(3), 321–346 (2019)
9. Fuchs, C., Pethő, A., Tichy, R.F.: On the Diophantine equation $G_n(x) = G_m(P(x))$. Monatsh. Math. **137**, 173–196 (2002)

10. Ganguli, H., Jankauskas, J.: On the equation $f(g(x)) = f(x)h(x)^m$ for composite polynomials. J. Aust. Math. Soc. **92**, 155–161 (2012)
11. Müller, P., Zieve, M.E.: On Ritt's polynomial decomposition theorems. arXiv:0807.3578
12. Ritt, J.F.: Prime and composite polynomials. Trans. Am. Math. Soc. **23**, 51–66 (1922)
13. Schinzel, A.: Polynomials with Special Regard to Reducibility. Cambridge University Press, Cambridge (2000)
14. Turnwald, G.: On Schur's conjecture. J. Aust. Math. Soc. Ser. A **58**, 312–357 (1995)
15. Zannier, U.: On the number of terms of a composite polynomial. Acta Arith. **127**(2), 157–167 (2007)