Formal Power Series and Algebraic Combinatorics
Séries Formelles et Combinatoire Algébrique
Tianjin, China 2007

Complete decomposition of Dickson-type recursive polynomials and a related Diophantine equation

Thomas Stoll

Abstract. We characterize decomposition over $\mathbb{C}$ of polynomials $f_n(x)$ defined by the generalized Dickson-type recursive relation

$$f_0(x) = B, \qquad f_1(x) = x, \qquad f_{n+1}(x) = xf_n(x) - af_{n-1}(x) \qquad (n \geq 1),$$

where $B, a \in \mathbb{Q}$ or $\mathbb{R}$. This parametric class of polynomials includes *Fibonacci*, *Pell*, *Fermat*, *Dickson*, *Lucas (w-)*, *Pell-Lucas*, *Fermat-Lucas polynomials* as well as *Chebyshev polynomials of the first* and *second kind.* As an application of the decomposition result, we show that the Diophantine equation

$$f_n^{(a,B)}(x) = f_m^{(\hat{a},\hat{B})}(y)$$

with $f_n^{(a,B)}, f_m^{(\hat{a},\hat{B})} \in \mathbb{Q}[x]$ and $\min(m,n) \geq 3$ has only finitely many rational solutions (x,y) with a bounded denominator, except in a few explicitly stated exceptions. This vastly extends work of A. Dujella/R. F. Tichy (*Diophantine equations for second order recursive sequences of polynomials*, Quart. J. Math. **52** (2001), 161–169) and A. Dujella/I. Gusić (*Decomposition of a recursive family of polynomials*, Monatsh. Math., to appear). In particular, a complete answer to a question posed by the latter authors is presented.

Résumé. Nous caractérisons la décomposition sur $\mathbb{C}$ de polynômes $f_n(x)$ définis par la relation de récurrence de type Dickson généralisée :

$$f_0(x) = B, \qquad f_1(x) = x, \qquad f_{n+1}(x) = xf_n(x) - af_{n-1}(x) \qquad (n \geq 1),$$

où $B, a \in \mathbb{Q}$ ou $\mathbb{R}$. Cette classe de polynômes paramétriques inclut les *polynômes de Fibonacci*, *Pell*, *Fermat*, *Dickson*, *Lucas (w-)*, *Pell-Lucas*, *Fermat-Lucas* ainsi que les *polynômes de Tchebychev de première et deuxième espèces.* Une application de notre résultat permet de montrer que l'équation diophantienne

$$f_n^{(a,B)}(x) = f_m^{(\hat{a},\hat{B})}(y)$$

avec $f_n^{(a,B)}, f_m^{(\hat{a},\hat{B})} \in \mathbb{Q}[x]$ et $\min(m,n) \geq 3$ n'admet qu'un nombre fini de solutions rationnelles (x,y) avec dénominateur borné, à quelques exceptions près que nous donnons explicitement. Ceci prolonge les travaux de A. Dujella et R. F. Tichy (*Diophantine equations for second order recursive sequences of polynomials*, Quart. J. Math. **52** (2001), 161–169) et de A. Dujella/I. Gusić (*Decomposition of a recursive family of polynomials*, Monatsh. Math., à paraître). En particulier, nous répondons entièrement à la question posée par les deux derniers auteurs sus-cités.

1. Introduction

1.1. Indecomposability and Diophantine equations. The theory of polynomial decompositions dates back to the ground-breaking work of J. F. Ritt [**10, 11**]. Ritt's main results split into two parts. First, he identified all decompositions of polynomials over $\mathbb{C}$ as being prime decompositions up to linear transformations and bidecompositions. Secondly, in the so-called "Ritt's second theorem", he specified which bidecompositions are indeed possible.

2000 *Mathematics Subject Classification.* Primary 11B39; Secondary 11D45.

Key words and phrases. Polynomial decomposition, Dickson-type recursive polynomials, Sturm-Liouville differential equation, Diophantine equations.

Research supported by the Austrian Science Foundation (FWF), project S9604, "Analytic and Probabilistic Methods in Combinatorics".

In what follows, by a (binary) *decomposition* of $f \in \mathbb{C}[x]$ we mean a representation $f = r \circ q$ with some non-constant polynomials $r, q \in \mathbb{C}[x]$, where the operation is the usual functional composition. If $\deg r, \deg q > 1$, then the decomposition is called a *non-trivial* decomposition. We call r the *left* and q the *right component* of the decomposition. It is clear, that $(\mathbb{C}[x], \circ)$ forms a non-commutative monoid, where the units are exactly the polynomials over $\mathbb{C}$ of degree 1. Two decompositions $f = r_1 \circ q_1 = r_2 \circ q_2$ are called *equivalent* if there is a unit κ such that $r_2 = r_1 \circ \kappa$ and $q_2 = \kappa^{-1} \circ q_1$. A polynomial f is called *decomposable* over $\mathbb{C}$ if it has at least one non-trivial decomposition, and *prime* (or *indecomposable*) otherwise. It is well-known, that indecomposability over $\mathbb{Q}$ or $\mathbb{R}$ implies indecomposability over $\mathbb{C}$ (see [**13**, p.14]).

Several refinements on Ritt's results have been obtained (see [**1, 12**]) and some of the rather complicated original proofs based on Riemann surface theory have been considerably simplified (see [**3**]). Decomposition results have shown to give access to the finiteness problem for Diophantine equations of the form $f(x) = g(y)$ with $f, g \in \mathbb{Q}[x]$ in unknowns $(x, y) \in \mathbb{Q}^2$. In 2000, Bilu and Tichy [**2**] succeeded in fully joining polynomial decomposition theory with the classical finiteness theorem of Siegel [**14**] on finiteness of integral points of curves of genus > 0. They obtained the following remarkable theorem.

THEOREM 1.1 (Bilu/Tichy [**2**]). *Let $f(x), g(x) \in \mathbb{Q}[x]$ be non-constant polynomials. Then the following two assertions are equivalent:*

(a) *The equation $f(x) = g(y)$ has infinitely many rational solutions with a bounded denominator.*

(b) *We have*

$$f = \varphi \circ \mathfrak{f}_1 \circ \kappa_1 \qquad \text{and} \qquad g = \varphi \circ \mathfrak{g}_1 \circ \kappa_2,$$

where $\kappa_1, \kappa_2 \in \mathbb{Q}[x]$ are linear, $\varphi(x) \in \mathbb{Q}[x]$, and $(\mathfrak{f}_1, \mathfrak{g}_1)$ is a standard pair over $\mathbb{Q}$ such that the equation $\mathfrak{f}_1(x) = \mathfrak{g}_1(y)$ has infinitely many rational solutions (x, y) with a bounded denominator.

We say that the equation $f(x) = g(y)$ has *infinitely many rational solutions with a bounded denominator*, if there is $\nu \in \mathbb{Z}^+$ such that that $f(x) = g(y)$ has infinitely many rational solutions (x, y) with $\nu x, \nu y \in \mathbb{Z}$. The list of *standard pairs*, which is referred to in Theorem 1.1, includes five different pairs of polynomials $(\mathfrak{f}_1, \mathfrak{g}_1)$. For the sake of clarity, we define them separately in the next subsection (see (1.1)–(1.5)).

1.2. Standard pairs. In the sequel, let γ, δ denote some non-zero rational numbers, r, q, s and t some non-negative integers and $v(x) \in \mathbb{Q}[x]$ a non-zero polynomial (which may also be constant). Furthermore, denote by $D_s(x, \gamma)$ the *Dickson polynomial of the first kind* (for short: *Dickson polynomial*) of degree s defined by

$$D_s(x,\gamma) = \sum_{i=0}^{\lfloor s/2 \rfloor} \frac{s}{s-i} \binom{s-i}{i} (-\gamma)^i x^{s-2i},$$

which can equivalently be defined by a three-term recursion (see (1.6) below). For basic properties of these polynomials we refer to the monograph of Lidl *et al.* [**9**].

A standard pair of the *first* kind is of the type

$$(x^q, \gamma x^r v(x)^q) \tag{1.1}$$

(or switched), where $0 \le r < q$, $\gcd(r, q) = 1$ and $r + \deg v > 0$.

A standard pair of the *second* kind is given by

$$(x^2, (\gamma x^2 + \delta) v(x)^2) \tag{1.2}$$

(or switched).

A standard pair of the *third* kind is

$$(D_s(x, \gamma^t), D_t(x, \gamma^s)) \tag{1.3}$$

with $s, t \ge 1$ and $\gcd(s, t) = 1$.

A standard pair of the *fourth* kind is

$$(\gamma^{-s/2} D_s(x, \gamma), -\delta^{-t/2} D_t(x, \delta)) \tag{1.4}$$

(or switched) with $s, t \ge 1$ and $\gcd(s, t) = 2$.

A standard pair of the *fifth* kind is of the form

$$((\gamma x^2 - 1)^3, 3x^4 - 4x^3) \tag{1.5}$$

(or switched).

According to Theorem 1.1, to get finiteness of the number of solutions $(x, y) \in \mathbb{Q}^2$ with a bounded denominator (thus, in particular, of solutions $(x, y) \in \mathbb{Z}^2$), one can show that at least one of the polynomials f, g is indecomposable. In recent years, much interest has been focused on using the criterion of Theorem 1.1 to Diophantine equations of the form $p_m(x) = p_n(y)$ and, again more generally, to $p_m(x) = g(y)$, where $\{p_k\}_{k\geq 0}$ denotes some specific polynomial family and $g(x)$ is an arbitrary polynomial over $\mathbb{Q}$. However, as a principle, the main difficulty consists in proving a uniform indecomposability theorem for $\{p_k\}$.

1.3. Dickson-type recursive families. The aim of the present talk is to give a complete investigation of decomposition of so-called *Dickson-type recursive polynomials* over $\mathbb{R}$, which depend on two real parameters a and B. These polynomials generalize the Dickson polynomials $D_n(a, x)$ appearing in the definition of the standard pairs of the *third* (1.3) and *fourth* kind (1.4). Recall an alternative definition of the Dickson polynomials [**9**, Lemma 2.3],

$$D_0(x,a) = 2, \qquad D_1(x,a) = x, \qquad D_{n+1}(x,a) = xD_n(x,a) - aD_{n-1}(x,a), \qquad n \geq 1, \tag{1.6}$$

for any $a \in \mathbb{C}$. It is well-known that Dickson polynomials are decomposable for all $m, n \geq 2$, i.e.,

$$D_{mn}(x,a) = D_m(x,a^n) \circ D_n(x,a) = D_n(x,a^m) \circ D_m(x,a). \tag{1.7}$$

Note that several combinatorial polynomial families and their dilates form subclasses of the Dickson polynomials. Mention, for instance, the *Lucas (w-)polynomials* $L_k(x)$ and *Pell-Lucas polynomials* $Q_k(x/2)$ for $a = -1$, the *Chebyshev polynomials of the first kind* $2\,T_k(x/2)$ for $a = 1$ and the *Fermat-Lucas polynomials* $FL_k(x/3)$ for $a = 2$ (see [**19**]).

A generalized Dickson-type recursive relation is obtained by a perturbation of the zero instance in the Dickson recurrence (1.6).

Definition 1.2. Polynomials $f_k \in \mathbb{R}[x]$ (resp. $\mathbb{Q}[x]$) with

$$\begin{aligned} f_0(x) &= B, \\ f_1(x) &= x, \\ f_{n+1}(x) &= xf_n(x) - af_{n-1}(x), \qquad n \geq 1, \end{aligned} \tag{1.8}$$

where $B, a \in \mathbb{R}$ (resp. $\mathbb{Q}$) are called *Dickson-type recursive polynomials* over $\mathbb{R}$ (resp. $\mathbb{Q}$).

In the framework of (1.8) one again encounters well-known polynomial families related to combinatorics. For $B = 1$, for example, we have *Fibonacci polynomials* $F_k(x)$ resp. *Pell polynomials* $P_k(x/2)$ if $a = -1$, *Chebyshev polynomials of the second kind* $U_k(x/2)$ if $a = 1$ and *Fermat polynomials* $\mathcal{F}_k(x/3)$ if $a = 2$ (see [**19**]). In fact, the polynomials $E_n(x, a)$ defined by

$$E_0(x,a) = 1, \qquad E_1(x,a) = x, \qquad E_{n+1}(x,a) = xE_n(x,a) - aE_{n-1}(x,a), \qquad n \geq 1, \tag{1.9}$$

with $a \in \mathbb{C}$ are the *Dickson polynomials of the second kind*, for which holds the formula [**9**, Definition 2.2],

$$E_n(x,a) = \sum_{i=0}^{\lfloor n/2 \rfloor} \binom{n-i}{i} (-a)^i x^{s-2i}. \tag{1.10}$$

Decomposability of Dickson-type recursive polynomials over $\mathbb{Q}$ and related Diophantine equations have been previously considered by Dujella and Tichy [**8**] for $B = 1$ and $a \in \mathbb{Z}$. Very recently, Dujella, Gusić and Tichy [**7**], and Dujella and Gusić [**5**] proved new criteria for indecomposability of polynomials over $\mathbb{Z}$ in terms of the degree and two leading coefficients. In [**6**], the latter authors applied their criteria to attack indecomposability concerning general Dickson-type recursive polynomials over $\mathbb{Q}$.

Theorem 1.3 (Dujella/Gusić [**6**]). *Let $a \in \mathbb{Q}$ and $B = b_1/b_2$, where we assume $\gcd(b_1, b_2) = 1$ and $b_2 > 0$; if $B = 0$ then we set $b_1 = 0$ and $b_2 = 1$. Suppose $\gcd(b_2, n) = 1$ and $\gcd(b_1 - 2b_2, n) = 1$. Then:*

(i) *If n is odd, then f_n is indecomposable.*
(ii) *$f_{2n}(x) = \mathfrak{h}_n(x^2)$ with $\mathfrak{h}_n := f_{2n}(\sqrt{x}) \in \mathbb{Q}[x]$ is the unique non-trivial decomposition of f_{2n}.*

From the theorem one has that for $B \in \{1, 3\}$ and $a \in \mathbb{Q}$ the polynomial f_n is indecomposable (n odd), and $f_n(x) = \mathfrak{h}_{n/2}(x^2)$ (n even) is the unique binary decomposition. Hence, in particular, a former result about indecomposability of Fibonacci polynomials is reobtained [**8**].

Despite the huge class of known decompositions (1.7) given by the Dickson polynomials, there are other sporadic decompositions of Dickson-type recursive polynomials over $\mathbb{Q}$ as pointed out by Dujella and Gusić [**6**, Example 1].

EXAMPLE 1.4. Let $B = -2$ and $a = -1$, then

$$f_8 = (x^2 - 4x - 2) \circ (x^4 + 2x^2). \tag{1.11}$$

Motivated by example (1.11), the authors posed the *question*, whether there exist other values for $B, a \in \mathbb{Q}$ and odd n such that f_n is decomposable. We give a complete answer for decomposability (up to equivalence) with $B, a \in \mathbb{R}$ and show that example (1.11) is, in principle, the only "non-trivial" decomposition*.

2. Main results

THEOREM 2.1. *The Dickson-type recursive polynomials f_n over $\mathbb{R}$ defined in (1.8) with $a \neq 0$, $B \neq 2$ are decomposable over $\mathbb{C}$ if and only if $n = 2k$ with $k \geq 2$. In that case,*

$$f_n = \mathfrak{h}_k \circ x^2 \tag{2.1}$$

and $\mathfrak{h}_k$ is decomposable over $\mathbb{C}$ if and only if $B = -2$, $n = 8$ such that

$$f_8 = (x^2 - 4a^2x - 2a^4) \circ (x^2 - 2ax) \circ x^2. \tag{2.2}$$

Moreover, all non-trivial decompositions of f_n are equivalent to (2.1) and (2.2).

We join Theorem 2.1 with Theorem 1.1 to study the finiteness problem for Diophantine equations of the form $f_n(x) = g(y)$, where $g \in \mathbb{Q}[x]$ is an arbitrary, but fixed polynomial. In what follows, let $\kappa(x)$ be some arbitrary linear polynomial over $\mathbb{Q}$.

THEOREM 2.2. *Let $g(x) \in \mathbb{Q}[x]$ with $m = \deg g \geq 3$. Suppose that the Diophantine equation*

$$f_n(x) = g(y) \tag{2.3}$$

with Dickson-type recursive polynomials f_n over $\mathbb{Q}$ with $a \neq 0$, $B \neq 2$, $n \geq 3$ has infinitely many rational solutions (x, y) with a bounded denominator. Then we are in one of the following cases.

(i) *$g(x) = f_n(\tilde{g}(x))$ for some polynomial $\tilde{g} \in \mathbb{Q}[x]$.*

(ii) *$\mathsf{n} = 2\mathsf{k}$, $\mathsf{k} \geq 2$ and $g(x) = \mathfrak{h}_{\mathsf{k}}(\tilde{g}(x))$, where $\tilde{g}$ is a polynomial over $\mathbb{Q}$, whose square-free part has at most two zeroes, such that $\tilde{g}$ takes infinitely many square values in $\mathbb{Z}$.*

(iii) *$\mathsf{n} = 3$, $B \neq -1$ and $g(x) = \beta^3 D_m(\kappa(x), \gamma^3)$, where $\beta, \gamma \in \mathbb{Q}$, $\gcd(m, 3) = 1$ such that*
$$3\gamma^m\beta^2 = (B + 1)a.$$

(iv) *$\mathsf{n} = 3$, $B = -1$ and $g(x) = \gamma\kappa(x)^r v(x)^3$, where $\gamma \in \mathbb{Q} \setminus \{0\}$, $r \in \{1, 2\}$ and $v(x) \in \mathbb{Q}[x]$.*

(v) *$\mathsf{n} = 4$, $B \neq -2$ and $g(x) = \beta^4 D_m(\kappa(x), \gamma^4) - \frac{1}{8}a^2(B - 2)^2$, where $\beta, \gamma \in \mathbb{Q}$, $\gcd(m, 4) = 1$ such that*
$$4\gamma^m\beta^2 = (B + 2)a.$$

(vi) *$\mathsf{n} = 4$, $B \neq -2$ and $g(x) = -\frac{(B+2)^2a^2}{16}\delta^{-m/2}D_m(\kappa(x), \delta) - \frac{1}{8}a^2(B - 2)^2$, where $\delta \in \mathbb{Q} \setminus \{0\}$, $\gcd(m, 4) = 2$.*

(vii) *$\mathsf{n} = 4$, $B = -2$ and $g(x) = \gamma\kappa(x)^r v(x)^4$, where $\gamma \in \mathbb{Q} \setminus \{0\}$, $r \in \{1, 3\}$ and $v(x) \in \mathbb{Q}[x]$.*

(viii) *$\mathsf{n} = 8$, $B = -2$ and $g(x) = \kappa(x)^4 - 4a^2\kappa(x)^2 - 2a^4$.*

Moreover, in each of the cases, there are infinitely many choices of the parameters such that (2.3) has infinitely many rational solutions with a bounded denominator.

Thus, informally speaking, in most cases $f_n(x) = g(y)$ has only finitely many rational solutions with a bounded denominator. Note that Theorem 2.2 is no equivalence statement, since parameters of $g(x)$ are not made explicit. However, the version of Theorem 2.3 is already sufficient to *fully* settle the finiteness problem for Diophantine equations in Dickson-type recursive polynomials.

We introduce the notation $f_n^{(a,B)}(x) = f_n(x)$ and $\mathfrak{h}_k^{(a,B)}(x) := f_{2k}^{(a,B)}(\sqrt{x})$ in order to specify parameters in the related recurrence (1.6). By setting $g(x) = f_m^{(\hat{a},\hat{B})}(x)$ and working through Cases (i)–(viii) of

*For some missing proofs and more details, we refer to the original paper of the author [**16**].

Theorem 2.2, we can identify all those cases where there are infinitely many solutions with a bounded denominator. Moreover, we can show, that the implied parameter restrictions are already sufficient to identify an infinite parametric solution family, such that we get an equivalence statement (“*if and only if*”). For the details of the proof of Theorem 2.3, we again refer to [**16**].

Theorem 2.3. *The Diophantine equation*

$$f_n^{(a,B)}(x) = f_m^{(\hat{a},\hat{B})}(y) \tag{2.4}$$

with $a, \hat{a}, B, \hat{B} \in \mathbb{Q}$ and $m \geq n \geq 3$ has infinitely many rational solutions (x, y) with a bounded denominator if and only if *we are in one of the following cases ($\gamma \in \mathbb{Q} \setminus \{0\}$, $s, t \in \mathbb{Z}^+$):*

(I) $\mathsf{m} = 6,\ \mathsf{n} = 3$ *and* $\hat{B} = -5/2,\ 4a(B+1) = 21\hat{a}^2,\ \hat{a} \neq 0;$

(II) $\mathsf{m} = 3\mathsf{t},\ \mathsf{n} = 3$ *and* $\hat{B} = 2,\ (B+1)a = 3\hat{a}^t,\ t \geq 2,\ B \neq 2,\ \hat{a} \neq 0;$

(III) $\gcd(\mathsf{m}, 3) = 1,\ \mathsf{n} = 3$ *and* $\hat{B} = 2 \neq B,\ (B+1)a = 3\gamma^m,\ \hat{a} = \gamma^3 \neq 0;$

(IV) $\mathsf{m} > \mathsf{n} \geq 3$ *and* $B = \hat{B} = 2,\ a^t = \hat{a}^s,\ \hat{a} \neq 0,\ mt = ns.$

(V) $\mathsf{m} > \mathsf{n} \geq 3$ *and* $a = \hat{a} = 0;$

(VI) $\mathsf{m} > \mathsf{n} = 3$ *and* $B = -1,\ \hat{a} = 0,\ a \neq 0;$

(VII) $\mathsf{m} = \mathsf{n}$ *and* $f_n^{(a,B)} \equiv f_m^{(\hat{a},\hat{B})}.$

Remark 2.4. Observe that with the assumptions of (I) we have the identity

$$f_6^{(\hat{a},-5/2)}(x) = f_3^{(a,B)}(x^2 - \hat{a}/2) = x^6 + \frac{3}{2}\hat{a}x^4 - \frac{9}{2}\hat{a}^2x^2 + \frac{5}{2}\hat{a}^3,$$

such that (2.4) has infinitely many solutions in case (I) by trivial means. Besides this sporadic case, all of (II)–(VII) are well-known: From case (II) we retrieve the equation $D_3(x, \hat{a}^t) = D_{3t}(y, \hat{a})$, where $(x, y) = (D_t(u, \hat{a}), u)$ denotes an infinite family of solutions. In case (III) we get $D_3(x, \gamma^m) = D_m(y, \gamma^3)$ with $(x, y) = (D_m(u, \gamma), D_3(u, \gamma))$ being an infinite family of solutions. Case (IV) is based on the identity $D_n(D_s(x, \gamma), \gamma^s) = D_m(D_t(x, \gamma), \gamma^t)$. Cases (V) and (VI) plainly correspond to the equations $x^n = y^m$ and $x^3 = y^m$, respectively, whereas (VII) is trivial. We have plugged in various parameter restrictions into (I)–(VII) in order to avoid an overlapping of the seven cases.

Theorem 2.3 vastly generalizes two already known results for Diophantine equations with polynomials $f_k^{(a,B)}(x)$. First, for $a, \hat{a} \in \mathbb{Z} \setminus \{0\}$ with $a = \hat{a}$ we derive the finiteness result of Dujella and Tichy [**8**, Theorem 2] concerning Dickson polynomials of the second kind (1.9) (also termed *generalized Fibonacci polynomials*). Secondly, it has been proved by Dujella and Gusić [**6**, Theorem 3], that the equation (2.4) has only finitely many rational solutions with a bounded denominator, if the parameters satisfy certain conditions.

Corollary 2.5 (Dujella/Gusić [**6**]). *The Diophantine equation*

$$f_n^{(a,B)}(x) = f_m^{(\hat{a},\hat{B})}(y)$$

with $m, n \geq 3$, m, n odd, $a, \hat{a} \in \mathbb{Q}$ and $B = b_1/b_2$, $\hat{B} = \hat{b}_1/\hat{b}_2$ with

$$\gcd(b_2, n) = \gcd(b_1 - 2b_2, n) = \gcd(\hat{b}_2, m) = \gcd(\hat{b}_1 - 2\hat{b}_2, m) = 1$$

has only finitely many rational solutions (x, y) with a bounded denominator, except if $f_n^{(a,B)} \equiv f_m^{(\hat{a},\hat{B})}$ or $a = \hat{a} = 0$.

We point out that this result is weaker than the corresponding direction of Theorem 2.3, since none of the Cases (II), (III), (IV) and (VI) is covered.

3. Preliminaries

Let $\mathbb{K}$ be a field of constants with char $\mathbb{K} = 0$. First, we collect some standard results from polynomial decomposition theory, which will be needed in the sequel [**4, 12, 13**]. For more details we refer to [**16**].

Definition 3.1. Let $f = a_nx^n + a_{n-1}x^n + \cdots + a_0 \in \mathbb{K}[x]$ with $\deg f = n$. Then f is called *zerosymmetric* iff $a_0 = 0$, *monic* iff $a_n = 1$, and *normed* iff f is both zerosymmetric and monic.

By comparison of coefficients it is clear, that every non-constant polynomial f has exactly one decomposition $f = \kappa \circ \hat{f}$, where κ is a unit and $\hat{f}$ is normed. Furthermore, since $f = r \circ q = (r \circ \kappa^{-1}) \circ (\kappa \circ q)$, any decomposition is equivalent to a decomposition with a normed right component $\kappa \circ q$ of equal degree. In the next two propositions, we link decompositions of f to the degree of certain remainder polynomials (see [**4**, Ch. I. Par. 3.]).

PROPOSITION 3.2. *Let $f = r \circ q$, where r is monic and q is normed of degrees n and m, respectively. Then*

$$\deg(f - q^n) \leq mn - m.$$

PROPOSITION 3.3. *Let f be a monic polynomial and q a normed, non-constant polynomial of degrees mn and m, respectively. Suppose*

$$\deg(f - q^n) \leq mn - k$$

for some $1 \leq k < m$. Then there exists exactly one $\alpha \in \mathbb{K}$ such that

$$\deg(f - (q + \alpha x^{m-k})^n) \leq mn - k - 1. \tag{3.1}$$

Since $k < m$ and q is normed, the polynomial $q + \alpha x^{m-k}$ is normed, too, such that we may successively decrease the degree of the remainder polynomial, starting with $k = 1$. Obviously, $q = x^m$ is the only polynomial q with only one term such that $\deg(f - q^n) \leq mn - 1$. After applying Proposition 3.3 subsequently $(m - 1)$ times, we will come up with a sequence of numbers $\alpha_1, \alpha_2, \dots, \alpha_{m-1}$ (i.e., the numbers α indexed by k) and a polynomial

$$\hat{q}(x) = x^m + \alpha_1 x^{m-1} + \cdots + \alpha_{m-1} x \tag{3.2}$$

with $\deg \hat{q} = m$ and $\deg(f - \hat{q}^n) \leq mn - m$. By the construction, $\hat{q}$ is normed and uniquely determined by f and m. Therefore, by Proposition 3.2, if q is a normed right component of f then necessarily $q = \hat{q}$. This induces an indecomposability criterion for f with right components of fixed degree m.

LEMMA 3.4. *Let f be monic and $m \geq 2$ a positive integer. Denote by $\hat{q}(x)$ the unique polynomial of degree m given by (3.2). Furthermore, let*

$$f(x) = \beta_0 \hat{q}(x)^k + \beta_1 \hat{q}(x)^{k-1} + \cdots + \beta_l \hat{q}(x)^{k-l} + \mathcal{R}(x), \tag{3.3}$$

for some constants $\beta_j \in \mathbb{K}$, $0 \leq l < k$ with $\deg \mathcal{R} \leq mk - m$ and $m \nmid \deg \mathcal{R}$. Then f is indecomposable with right components of degree m.

PROOF. Observe that $\beta_0 = 1$ and

$$\begin{aligned} \mathcal{S}(x) &:= \hat{q}(x)^k + \beta_1 \hat{q}(x)^{k-1} + \cdots + \beta_l \hat{q}(x)^{k-l} \\ &= (x^k + \beta_1 x^{k-1} + \cdots + \beta_l x^{k-l}) \circ \hat{q}(x) =: s \circ \hat{q}. \end{aligned}$$

By Proposition 3.2 we have $\deg(\mathcal{S} - \hat{q}^k) \leq mk - m$. As $\deg \mathcal{R} \leq mk - m$ by assumption, this yields

$$\deg((\mathcal{S} + \mathcal{R}) - \hat{q}^k) = \deg((\mathcal{S} - \hat{q}^k) + \mathcal{R}) \leq mk - m.$$

By the argument following Proposition 3.3, if there is a decomposition of $\mathcal{S} + \mathcal{R}$ with a normed right component q of degree m then it is necessarily $\hat{q}$. Suppose $\mathcal{S} + \mathcal{R} = r \circ \hat{q}$. Since $\mathcal{S} = s \circ \hat{q}$, we get $\mathcal{R} = (r - s) \circ \hat{q}$ which is a contradiction since $m \nmid \deg \mathcal{R}$. Thus, $f = \mathcal{S} + \mathcal{R}$ is indecomposable with right components of degree m. □

4. Proof of Theorem 2.1

4.1. Sturm-Liouville type differential equation. We now turn back to the Dickson-type recursive polynomials f_n defined by (1.8). Let $a, B \in \mathbb{R}$, $a \neq 0$ and $B \neq 2$. We further may assume that $n \geq 4$ since otherwise f_n is trivially indecomposable by reasons of degrees. The polynomial family defined by

$$\tilde{f}_{-1}(x) = 0, \qquad \tilde{f}_0(x) = 1, \qquad \tilde{f}_{n+1}(x) = x\tilde{f}_n(x) - \delta_n \tilde{f}_{n-1}(x), \qquad n \geq 0, \tag{4.1}$$

with $\delta_0 = 0$, $\delta_1 = aB$ and $\delta_n = a$ for $n \geq 2$ denotes a canonical version for the polynomials f_n of (1.8). Indeed, it is easy to see that $\tilde{f}_n(x) = f_n(x)$ for $n \geq 1$. As already pointed out in [**5**], the polynomials $\tilde{f}_n$ form a quasi-orthogonal family of polynomials with a single dilated coefficient δ_1. More specifically, there is close connection to Chebyshev polynomials of the first kind, which are defined via $T_n(x) = \cos n\varphi$ with $x = \cos \varphi$.

Lemma 4.1. *For all $n \geq 1$ we have*

$$f_n(2\sqrt{a}x) = \frac{(\sqrt{a})^n}{x^2-1}\left((2x^2-B)T_n(x) + (B-2)xT_{n-1}(x)\right). \tag{4.2}$$

It is also possible to derive

$$f_n(2\sqrt{a}x) = (\sqrt{a})^n(2xU_{n-1}(x) - BU_{n-2}(x)), \tag{4.3}$$

where $U_n(x) = \sin n\varphi / \sin\varphi$ with $x = \cos\varphi$ denote the Chebyshev polynomials of the second kind. Since by (1.10),

$$U_n(x) = \sum_{i=0}^{\lfloor n/2 \rfloor} (-1)^i \binom{n-i}{i}(2x)^{n-2i},$$

we get the following explicit representation for f_n, which has already been proved in [**6**] by other means.

Proposition 4.2. *We have*

$$\begin{aligned} f_n(x) &= \sum_{i=0}^{\lfloor n/2 \rfloor} \frac{n+(B-2)i}{n-i}\binom{n-i}{i}(-a)^i x^{n-2i} \\ &= x^n - (n+B-2)ax^{n-2} + \frac{(n-3)(n+2B-4)}{2}a^2x^{n-4} \\ &\quad - \frac{(n-4)(n-5)(n+3B-6)}{6}a^3x^{n-6} \pm \dots \end{aligned} \tag{4.4}$$

The main tool to prove Theorem 2.1 relies on the fact that $f_n(x)$ satisfies a second-order linear differential equation of Sturm-Liouville type with polynomial factors of fixed degree. The method is reminiscent of Pólya–Sonin–Szegő [**18**, Th. 7.31.1] and has already been used by Tichy and the author to study two-interval monotonicity of continuous classical orthogonal polynomials [**15**].

Lemma 4.3. *The polynomials $y = f_n(x)$ with $a \neq 0$, $B \in \mathbb{R}$ satisfy the differential equation*

$$(A_4x^4 + aA_2x^2 + a^2A_0)y'' + (B_3x^3 + aB_1x)y' - (C_2x^2 + aC_0)y = 0, \tag{4.5}$$

where $A_4, A_2, A_0, B_3, B_1, C_2, C_0 \in \mathbb{R}$ with

$$\begin{aligned} A_4 &= B_3 = n(B-1), \\ A_2 &= -(n-1)B^2 - 2(2n+1)B + 4n, \\ A_0 &= 4(n-1)B^2 + 8B, \\ B_1 &= -3(n-1)B^2 + 2(4n-3)B - 8n, \\ C_2 &= n^3(B-1), \\ C_0 &= -n(n-1)(n-2)B^2 - 2n(3n-4)B - 8n. \end{aligned}$$

In order to use Szegős argument, we need the specific root behaviour of the polynomials $f_n(x)$, which has been stated in [**6**, Theorem 4].

Proposition 4.4. *The polynomials $f_n(x)$ with $a \neq 0$, $B \in \mathbb{R}$ have simple zeroes except in the following cases:*

(i) *$B = 0$ and $n = 2k$ (then $x = 0$ is a double root);*
(ii) *$B = -1/k$ and $n = 2k+1$ (then $x = 0$ is a triple root).*

Set $\varepsilon = 0$ if $n = 2k$, and $\varepsilon = -1/k$ if $n = 2k+1$. Then

(i) *If $B \geq \varepsilon$, $a > 0$ then all roots are real.*
(ii) *If $B \geq \varepsilon$, $a < 0$ then all roots are purely imaginary.*
(iii) *If $B < \varepsilon$, $a > 0$ then $n-2$ roots are real and two roots are purely imaginary conjugates.*
(iv) *If $B < \varepsilon$, $a < 0$ then $n-2$ roots are purely imaginary and two roots are real.*

Corollary 4.5. *The polynomials $f_n'(x)$ with $B \in \mathbb{R}$ have at least $n-3$ different real zeroes if $a > 0$, and at least $n-3$ different purely imaginary zeroes if $a < 0$.*

We now join Lemma 4.4 with Lemma 4.3 to obtain a uniform bound on the degree of the right component q of some possible decomposition $f_n = r \circ q$.

LEMMA 4.6. *Let $f_n = r \circ q$ with $r, q \in \mathbb{R}[x]$ and $\min(\deg r, \deg q) \geq 2$. Then*

$$\deg q \leq 6.$$

PROOF. Put $\sigma(x) = A_4x^4 + aA_2x^2 + a^2A_0$, $\tau(x) = B_3x^3 + aB_1x$ and $\lambda(x) = C_2x^2 + aC_0$. Moreover, define a function

$$h(x) = f_n(x)^2 - \frac{\sigma(x)}{\lambda(x)} f_n'(x)^2. \tag{4.6}$$

The denominator $\lambda(x)$ is a non-zero function because $C_2C_0 \neq 0$ for any $B \in \mathbb{R}$, $n \in \mathbb{Z}^+$. With use of the differential equation (4.5) we have

$$h'(x) = 2f_n(x)f_n'(x) - \left(\frac{\sigma(x)}{\lambda(x)}\right)' f_n'(x)^2 - \frac{2f_n'(x)}{\lambda(x)} \left(\lambda(x)f_n(x) - \tau(x)f_n'(x)\right) = \omega(x)(f_n'(x))^2, \tag{4.7}$$

where

$$\omega(x) = \frac{(2\tau(x) - \sigma'(x))\lambda(x) + \sigma(x)\lambda'(x)}{\lambda(x)^2} = -\frac{4a(B-2)^2\omega_1(x)}{n\left(n^2(B-1)x^2 - a(Bn-2B+4)(Bn-B+2)\right)^2}$$

with

$$\omega_1(x) = n(n^2-1)(B-1)x^3 - a(Bn^2 - 3Bn + 2B + 6n)(Bn - B + 2)x. \tag{4.8}$$

On the real line, the function $\omega(x)$ changes at most three times its sign, namely, at $x = 0$ and at possibly two more real zeroes of $\omega_1(x)$. First, let $a > 0$. Denote by $\xi_1, \xi_2, \ldots, \xi_m$ the pairwise different real zeroes of $f_n'(x)$. Then by Corollary 4.5, $m \geq n - 3$ and by (4.6) we get

$$h(\xi_j) = f_n(\xi_j)^2, \qquad 1 \leq j \leq m.$$

By (4.7) also $h'(x)$ changes at most three times its sign. This implies that $|f_n(\xi_j)|$ increases and decreases on at most 4 consecutive real intervals. Taking into account that for the possibly two additional roots of $f_n'(x)$, say η_1, η_2, there could be some index $1 \leq k \leq m$ such that $f(\eta_1) = f(\eta_2) = f(\xi_k)$, we conclude that uniformly in $\zeta \in \mathbb{C}$ there holds

$$\deg \gcd(f_n - \zeta, f_n') \leq 4 + 2 = 6. \tag{4.9}$$

Suppose a non-trivial decomposition $f_n = r \circ q$. Denote by ζ a root of r', which exists by $\deg r \geq 2$. Then both the polynomials $f_n(x) - r(\zeta)$ and $f_n'(x)$ are divisible by $q(x) - \zeta$. Therefore,

$$\deg q = \deg(q - \zeta) \leq \deg \gcd(f_n - \zeta, f_n') \leq 6,$$

which completes the proof of the lemma for $a > 0$. Finally, let $a < 0$. By (4.4) we have $f_n(\sqrt{a}x) = (\sqrt{a})^n f_n(x)$ and exactly the same arguments as above apply. This finishes the proof of the lemma. □

4.2. The small cases. In order to use Lemma 3.4 we require the upper-most coefficients of f_n given in (4.4). Lemma 4.6 says that if there is a non-trivial decomposition $f_n = r \circ q$ then necessarily $\deg q \in \{2, 3, 4, 5, 6\}$. In what follows, set $k = \deg r \geq 2$. We show, how the procedure works in the cases $\deg q = 3, 4$. The other cases are similar [**16**]. Note that since one gets no more decompositions with normed right components, when coefficients of r and q are allowed to be in $\mathbb{C}$, this investigation already completes the proof of Theorem 2.1.

The case $\deg q = 3$:

Proposition 3.3 gives $\alpha_1 = 0$ and $\deg(f - x^{3k}) = 3k - 2$. Therefore by (3.1) and (4.4),

$$\alpha_2 = \frac{\mathrm{lcoeff}(f_{3k}(x) - x^{3k})}{k} = -\frac{a(B + 3k - 2)}{k}$$

and

$$\hat{q}(x) = x^3 - \frac{a(B + 3k - 2)}{k} x.$$

It is sufficient to show that the remainder polynomial $\mathcal{R} = f_{3k} - \hat{q}^k$ has exact degree $3k-4$. Note that by construction it has degree at most $3k-4$. Therefore we only have to calculate the coefficient $[x^{3k-4}]$, i.e.,

$$\begin{aligned}\mathcal{R}(x) &= \left(\frac{(3k-3)(3k+2B-4)}{2}a^2 - \binom{k}{2}\frac{a^2(B+3k-2)^2}{k^2}\right)x^{3k-4} + \text{terms of lower order}\\ &= -\frac{a^2(B-2)^2(k-1)}{2k}x^{3k-4} + \text{terms of lower order.}\end{aligned}$$

Since the leading coefficient of $\mathcal{R}(x)$ is non-zero for $a \neq 0$, $B \neq 2$ and $3 \nmid \deg \mathcal{R} = 3k-4$, a decomposition with a polynomial q of degree 3 is impossible by Lemma 3.4.

The case $\deg q = 4$:

In the same spirit as before we obtain

$$\hat{q} = x^4 - \frac{x^2 a(B+4k-2)}{k}. \tag{4.10}$$

However, since f_{4k} is an even polynomials, $f_{4k} - \hat{q}^k$ in general has degree divisible by 4, so that we have to do some further expansion concerning (3.3). To begin with, write

$$f_{4k} = \hat{q}^k + \beta_1 \hat{q}^{k-1} + \mathcal{R}(x). \tag{4.11}$$

It is a direct calculation to check

$$\beta_1 = -\frac{a^2\left((k-1)B^2 - (6k-4)B - 4(k-1)^2\right)}{2k} \tag{4.12}$$

and

$$\mathcal{R}(x) = -\frac{a^3(B-2)^2(k-1)}{6k^2}((2k-1)B + 2k + 2)x^{4k-6} + \text{terms of lower order.}$$

The leading coefficient of $\mathcal{R}(x)$ equals zero if and only if

$$B = -(2k+2)/(2k-1). \tag{4.13}$$

In such case (4.11) with (4.12) and some simplification gives

$$f_{4k} = \hat{q}^k + \frac{2a^2k}{(2k-1)^2}(4k^2 - 19k + 13)\hat{q}^{k-1} + \mathcal{R}(x)$$

with

$$\mathcal{R}(x) = \frac{a^4 k(4k-5)(8k^4 - 78k^3 + 204k^2 - 208k + 69)}{(2k-1)^4}x^{4k-8} + \text{terms of lower order.} \tag{4.14}$$

Let β_2 denote the leading coefficient of $\mathcal{R}$ as given above. It is easy to see that $\beta_2 \neq 0$ for all $k \in \mathbb{Z}^+$. Since $4 \mid (4k-8)$, we have to expand one more term. Write $f_{4k}(x) = \hat{q}^k + \beta_1\hat{q}^{k-2} + \beta_2\hat{q}^{k-2} + \tilde{\mathcal{R}}(x)$ with

$$\tilde{\mathcal{R}}(x) = \frac{36(4k+1)(k-2)(2k-3)a^5k}{5(2k-1)^4}x^{4k-10} + \text{terms of lower order.}$$

Since $4 \nmid (4k-10)$ there can only be a decomposition if $k=2$, which by (4.12), (4.13), (4.14) gives $B=-2$, $\beta_1 = -4a^2$ and $\beta_2 = -2a^4$. Finally by (4.10) we get $\hat{q}(x) = x^4 - 2ax^2$ and the decomposition $f_8 = (x^2 - 4a^2x - 2a^4) \circ (x^4 - 2ax^2)$, as asserted in (2.2).

5. Proof of Theorem 2.2

In view of Theorem 1.1, we have to deal with decompositions of f_n involving the standard pairs given by (1.1)–(1.5). Recall that by Theorem 2.1, the only non-trivial binary decompositions of f_n are equivalent to $f_{2k} = \mathfrak{h}_k \circ x^2$ and $f_8 = (x^2 - 4a^2x - 2a^4) \circ (x^4 - 2ax^2)$. From now on, assume the ground field to be $\mathbb{Q}$.

Let $\min(n, \deg g) \geq 3$, $a \neq 0$, $B \neq 2$ and suppose that the Diophantine equation

$$f_n(x) = g(y)$$

has infinitely many rational solutions (x,y) with a bounded denominator. Then by Theorem 1.1,

$$f_n = \varphi \circ \mathfrak{f}_1 \circ \kappa_1 \qquad \text{and} \qquad g = \varphi \circ \mathfrak{g}_1 \circ \kappa_2,$$

where κ_1, κ_2 are some rational units, $\varphi \in \mathbb{Q}[x]$ and $(\mathfrak{f}_1, \mathfrak{g}_1)$ is a standard pair as given by the list in Subsection 1.2, such that $\mathfrak{f}_1(x) = \mathfrak{g}_1(y)$ has infinitely many rational solutions with a bounded denominator. By Theorem 2.1, we have one of the following four cases:

(i) $\deg \varphi = n$,
(ii) $\deg \varphi = k$ with $n = 2k$ and $f_n = \mathfrak{h}_k \circ x^2$,
(iii) $\deg \varphi = 1$,
(iv) $\deg \varphi = 2$ with $n = 8$ and $f_8 = (x^2 - 4a^2 x - 2a^4) \circ (x^4 - 2ax^2)$.

Because of reasons of space, we here omit the treatment of (iv) (see [**16**]).

Case $\deg \varphi = n$**:**

By comparison of degrees, $f_n = \varphi \circ \kappa$ for some unit κ and thus

$$g = f_n \circ (\kappa^{-1} \circ \mathfrak{g}_1 \circ \kappa_2) = f_n \circ \tilde{g}$$

for some non-constant polynomial $\tilde{g} \in \mathbb{Q}[x]$. Of course, there are infinitely many solutions with a bounded denominator of $f_n(x) = f_n(\tilde{g}(y))$. This gives Case (i) in Theorem 2.2.

Case $\deg \varphi = k$ **with** $n = 2k$ **and** $f_n = \mathfrak{h}_k \circ x^2$**:**

Let $f_n = \varphi \circ \mathfrak{f}_1 \circ \kappa_1$ and κ be the unique unit such that $\varphi \circ \kappa = \mathfrak{h}_k$. Then $f_n = (\varphi \circ \kappa) \circ (\kappa^{-1} \circ \mathfrak{f}_1 \circ \kappa_1) = \mathfrak{h}_k \circ l_1$ and Theorem 2.1 yields $l_1 = x^2$. On the other hand,

$$g = \varphi \circ \mathfrak{g}_1 \circ \kappa_2 = (\varphi \circ \kappa) \circ (\kappa^{-1} \circ \mathfrak{g}_1 \circ \kappa_2) = \mathfrak{h}_k \circ l_2,$$

where $l_2 = \kappa^{-1} \circ \mathfrak{g}_1 \circ \kappa_2$. If the equation $x^2 = l_2(y)$ has infinitely many solutions with a bounded denominator, then by Siegel's theorem l_2 has at most two zeroes of odd multiplicity. This specifies to Case (ii) of Theorem 2.2.

Case $\deg \varphi = 1$**:**

In this case $\varphi(x) = \varphi_1 x + \varphi_0$ with $\varphi_1, \varphi_0 \in \mathbb{Q}$. Since φ is a unit we have to deal with $f_n = \varphi \circ \mathfrak{f}_1 \circ \kappa_1$ and $g = \varphi \circ \mathfrak{g}_1 \circ \kappa_2$, where $(\mathfrak{f}_1, \mathfrak{g}_1)$ is a standard pair with $\deg \mathfrak{f}_1 = n$. We now have to carry out a detailed analysis of the five standard pairs from Subsection 1.2.

To begin with, recall the standard pair of the *second* kind $(x^2, (\gamma x^2 + \delta) v(x)^2)$ given in (1.2). By assumption both $n \geq 3$ and $\deg g \geq 3$, such that the standard pair $(\mathfrak{f}_1, \mathfrak{g}_1)$ cannot be of the second kind.

Now, suppose $n \geq 5$.

Next we want to exclude decompositions involving the Dickson polynomials as imposed by the standard pairs of the *third* and *fourth* kind. Recall the definition of the standard pair of the third kind (1.3), i.e.,

$$(\mathfrak{f}_1, \mathfrak{g}_1) = (D_s(x, \gamma^t), D_t(x, \gamma^s)).$$

Suppose $f_n \circ \kappa = \varphi \circ D_s(x, \gamma^t)$ with a unit κ. Since D_s is an odd respectively even polynomial, according to whether s is even or odd, we have that κ is zerosymmetric and therefore

$$f_n(x) = \varphi_1 D_s(\beta x, \gamma^t) + \varphi_0 \tag{5.1}$$

for some rational numbers β, φ_1 and φ_0. By (4.4), (5.1) and $s = n$, we have the following coefficient equations for the powers x^n, x^{n-2} and x^{n-4}:

$$\begin{aligned} 1 &= \varphi_1 \beta^n, \\ -(n + B - 2)a &= -\varphi_1 n \gamma^t \beta^{n-2}, \\ \frac{(n-3)(n+2B-4)a^2}{2} &= \varphi_1 \frac{n(n-3)\gamma^{2t}}{2} \beta^{n-4}. \end{aligned}$$

A simple combination of these equations gives $B = 2$ which is a contradiction. On the other hand, let $(\gamma^{-s/2} D_s(x, \gamma), -\delta^{-t/2} D_t(x, \delta))$ be a standard pair of the *fourth* kind (1.4). Then the same argument with an altered coefficient φ_1 gives the contradiction. Hence, $(\mathfrak{f}_1, \mathfrak{g}_1)$ cannot be a standard pair of the third or fourth kind.

Next, suppose $(\mathfrak{f}_1, \mathfrak{g}_1) = ((\gamma x^2 - 1)^3, 3x^4 - 4x^3)$ (or switched) is a standard pair of the *fifth* kind (1.5). Since $n \geq 5$ and $(\gamma x^2 - 1)^3$ is even, we only have to treat the case

$$f_6(x) = \varphi_1 (\gamma (\beta x)^2 - 1)^3 + \varphi_0. \tag{5.2}$$

The coefficient equations for the powers x^6, x^4 and x^2 in (5.2) are

$$\begin{aligned} 1 &= \varphi_1\gamma^3\beta^6, \\ -(B+4)a &= -3\varphi_1\gamma^2\beta^4, \\ 3(B+1)a^2 &= 3\varphi_1\gamma\beta^2. \end{aligned}$$

This yields $(B+4)^2 = 9(B+1)$ and $B = (1 \pm 3\mathrm{i}\sqrt{3})/2 \notin \mathbb{Q}$, a contradiction. Thus, $(\mathfrak{f}_1, \mathfrak{g}_1)$ cannot be a standard pair of the fifth kind.

Finally, consider the standard pair of the *first* kind given by (1.1), namely $(x^q, \gamma x^r v(x)^q)$. By Corollary 4.5, the polynomial $f_n'(x)$ has zeroes of multiplicity at most three. Hence, for $n \geq 5$, there cannot be a representation with $f_n(\beta x) = \varphi_1 x^q + \varphi_0$. It remains to consider the second entry of the standard pair. Suppose

$$f_n(x) = \hat{\varphi}_1(\beta_1 x + \beta_0)^r \hat{v}(x)^q + \varphi_0, \tag{5.3}$$

where $\hat{\varphi}_1 = \varphi_1\gamma$, $\hat{v}(x) = v(\beta_1 x + \beta_0)$ with $\beta_0, \beta_1 \in \mathbb{Q}$ and $0 \leq r < q$, $\gcd(r,q) = 1$, $r + \deg \hat{v} > 0$ as demanded in (1.1). Then, again due to Corollary 4.5 and the fact that $q \geq 3$ by $\deg g \geq 3$, we here have to treat the following two cases:

Case (a): $\deg \hat{v} = 1$ and $q = 3, 4$,
Case (b): $\deg \hat{v} = 2$ and $q = 3$.

Observe that by $n = r + q \deg \hat{v} \geq 5$ we have the pairs $(r,q) = (1,4), (3,4), (2,3)$ in Case (a), and the pairs $(r,q) = (1,3), (2,3)$ in Case (b). We first exploit the fact that f_n is an even resp. odd polynomial. Set $\hat{v}(x) = \hat{v}_1 x + \hat{v}_0$ and consider the pairs of Case (a). The coefficients $[x^{n-1}]$ and $[x^{n-3}]$ on the right hand side of (5.3) vanish if and only if $\beta_0 = \hat{v}_0 = 0$. But then $f_n(x) = \hat{\varphi}_1(\beta_1 x)^r(\hat{v}_1 x)^q + \varphi_0$, a contradiction. Now, set $\hat{v}(x) = \hat{v}_2 x^2 + \hat{v}_1 x + \hat{v}_0$ and consider the pairs (q,r) of Case (b). Here, the coefficient equations $[x^{n-1}] = [x^{n-3}] = [x^{n-5}] = 0$ yield $\beta_0 = \hat{v}_1 = 0$ and again a contradiction. Hence, the standard pair $(\mathfrak{f}_1, \mathfrak{g}_1)$ cannot be of the first kind.

Next we consider the cases $n = 3, 4$. The only non-trivial decompositions with standard pairs can arise from standard pairs of the *third* or/and *fourth* kind, namely,

$$f_3(x) = \beta^3 D_3\left(\frac{x}{\beta}, \frac{(B+1)a}{3\beta^2}\right) \quad \text{for } B \neq -1, \tag{5.4}$$

$$f_4(x) = \beta^4 D_4\left(\frac{x}{\beta}, \frac{(B+2)a}{4\beta^2}\right) - \frac{a^2(B-2)^2}{8} \quad \text{for } B \neq -2, \tag{5.5}$$

and in the special cases $B \in \{-1, -2\}$ for standard pairs of the *first* kind, namely,

$$f_3(x) = x^3 \quad \text{for } B = -1, \tag{5.6}$$

$$f_4(x) = x^4 - 2a^2 \quad \text{for } B = -2. \tag{5.7}$$

In the case of (5.4) we always have $\gcd(m,3) \neq 2$ hence – at best – a standard pair of the third kind. Then

$$g(x) = \beta^3 D_m\left(\kappa(x), \left(\frac{(B+1)a}{3\beta^2}\right)^{3/m}\right),$$

where $m = \deg g \geq 3$ and κ is a rational unit. Consider the Diophantine equation $f_3(x) = g(y)$. Since $D_3(x, \gamma^m) = D_m(y, \gamma^3)$ has infinitely many rational solutions with a bounded denominator if $\gcd(m,3) = 1$ (take, by (1.7), $x = D_m(t,\gamma)$ and $y = D_3(t,\gamma)$ with $t \in \mathbb{Z}$), we get Case (iii) of Theorem 2.2.

Next, consider (5.5). If the representation involves a standard pair of the third kind (with $\gcd(m,4) = 1$) then in the same manner as before we retrieve Case (v). On the other hand, if $\gcd(m,4) = 2$ and we suppose a representation with a standard pair of the fourth kind, then

$$g(x) = \frac{(B+2)^2 a^2}{16}\left(-\delta^{-m/2} D_m(\kappa(x), \delta)\right) - \frac{a^2(B-2)^2}{8},$$

which corresponds to Case (vi) of Theorem 2.2. There is an infinite family of solutions (x,y) with bounded denominator: Assume, without loss of generality, that $m/2$ is odd. Then from Proposition 3.1 in [**2**] a parametric family of solutions (x,y) is given by $x = \gamma^{(2-m)/4} D_{m/2}(v,\gamma)$ and $y = uv$, where (u,v) is a solution of $\gamma^2 u^2 + \delta v^2 = 4\gamma\delta$.

Now, let $B = -1$ and consider (5.6). The corresponding equation for the standard pair is $x^3 = \gamma y^r v(y)^3$, where $r = 1$ or $r = 2$. Since $3 \cdot 1 - r \cdot (3 - r) = 1$ we have that an infinite family of solutions is given by $x = \gamma t^r v(\gamma^{3-r} t^3)$ and $y = \gamma^{3-r} t^3$, where $t \in \mathbb{Z}$. This is Case (iv) in Theorem 2.2. We similarly get Case (vii) from (5.7).

This concludes the investigation with polynomials $\varphi(x)$ with $\deg \varphi = 1$.

6. Epilogue

At the end of the talk, we finally will comment on a recent result of the author [**17**] regarding *perturbed Chebyshev polynomials*, which is obtained by a concrete implementation of the the decomposition algorithm (Lemma 3.4) and Grőbner bases calculations with Maple 10.

THEOREM 6.1. *Let f_n be defined by*

$$f_0(x) = b, \quad f_1(x) = x - c, \qquad f_{n+1}(x) = (x - d) f_n(x) - a f_{n-1}(x), \qquad n \geq 1,$$

with $a, b, c, d \in \mathbb{R}$, $a > 0$ and put $e = (c - d)/(2\sqrt{a})$. Then f_n is decomposable over $\mathbb{C}$ if and only if

$$(n, b, e) \in \left\{ (mk, 2, 0), (2k, b, 0), (8, -2, 0), (6, -\frac{11}{2}, \pm\frac{3\sqrt{3}}{2}), (6, -\frac{10}{3}, \pm\frac{2\sqrt{3}}{3}), (4, 2 - e^2, e) \right\}.$$

Moreover, in all cases the attained decompositions can be made explicit.

References

1. A. F. Beardon, T. W. Ng, *On Ritt's factorization of polynomials*, J. London Math. Soc. (2) **62** (2000), no. 1, 127–138. MR1771856 (2001k:30008)
2. Y. Bilu and R. F. Tichy, *The Diophantine equation $f(x) = g(y)$*, Acta Arith. **95** (2000), 261–288. MR1793164 (2001i:11031)
3. F. Binder, *Characterization of Polynomial Prime Decompositions: A Simplified Proof*, Contributions to General Algebra **9**, Hoelder-Pichler-Tempsky/Teubner, Wien-Stuttgart, 1995. MR1484426 (98h:12001)
4. F. Binder, *Polynomial decomposition*, Master's thesis, University of Linz, June 1995.
5. A. Dujella and I. Gusić, *Indecomposability of polynomials and related Diophantine equations*, Q. J. Math. **57** (2006), 193–201.
6. A. Dujella and I. Gusić, *Decomposition of a recursive family of polynomials*, Monatsh. Math., to appear, available at: `http://web.math.hr/~duje`.
7. A. Dujella, I. Gusić and R. F. Tichy, *On the indecomposability of polynomials*, Ősterreich. Akad. Wiss. Math.-Natur. Kl. Sitzungsber. II **214** (2005), 81–88.
8. A. Dujella and R. F. Tichy, *Diophantine equations for second order recursive sequences of polynomials*, Quart. J. Math. **52** (2001), 161–169. MR1838360 (2002d:11030)
9. R. Lidl, G. Mullen, G. Turnwald, *Dickson polynomials*, Pitman Monographs and Surveys in Pure and Applied Mathematics **65**, Longman Scientific & Technical, Harlow, 1993. MR1237403 (94i:11097)
10. J. F. Ritt, *Prime and composite polynomials*, Trans. Amer. Math. Soc. **23** (1922), no. 1, 51–66. Erratum: Trans. Amer. Math. Soc. **23** (1922), no. 4, 431. MR1501189, MR1501205
11. J. F. Ritt, *Equivalent rational substitutions*, Trans. Amer. Math. Soc. **26** (1924), no. 2, 221–229. MR1501274
12. A. Schinzel, *Selected Topics on Polynomials*, Ann Arbor, University of Michigan Press, 1982. MR0649775 (84k:12010)
13. A. Schinzel, *Polynomials with special regard to reducibility*, Encyclopedia of Mathematics and its Applications **77**, Cambridge University Press, 2000. MR1770638 (2001h:11135)
14. C. L. Siegel, *Űber einige Anwendungen Diophantischer Approximationen*, Abh. Preuss. Akad. Wiss. Phys.-Math. Kl. (1929), no. 1, 209–266.
15. Th. Stoll and R. F. Tichy, *Diophantine equations for classical continuous orthogonal polynomials*, Indag. Math. (N.S.) **14** (2003), no. 2, 263–274. MR2027780 (2004m:11051)
16. Th. Stoll, *Complete decomposition of Dickson-type recursive polynomials and a related Diophantine equation*, submitted to Trans. Amer. Math. Soc.; preprint available at: `http://dmg.tuwien.ac.at/stoll`.
17. Th. Stoll, *Decomposition of perturbed Chebyshev polynomials*, submitted to J. Comp. Appl. Math.; preprint available at: `http://dmg.tuwien.ac.at/stoll`.
18. G. Szegő, *Orthogonal polynomials*, American Mathematical Society Colloquium Publications, vol. **23**, Fourth edition, Providence, R.I., 1975. MR0372517 (51 #8724)
19. E. W. Weisstein, *Mathworld, a Wolfram Web Resource*, `http://mathworld.wolfram.com`, 1999–2006.

INSTITUTE OF DISCRETE MATHEMATICS AND GEOMETRY, TU VIENNA, WIEDNER HAUPTSTRASSE 8–10, A–1040 VIENNA, AUSTRIA

E-mail address: `stoll@dmg.tuwien.ac.at`

URL: `http://dmg.tuwien.ac.at/stoll`