

Complete decomposition of Dickson-type polynomials and related Diophantine equations

Thomas Stoll

January 22, 2007

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

Abstract

We characterize decomposition over \mathbb{C} of polynomials $f_n^{(a,B)}(x)$ defined by the generalized Dickson-type recursive relation ($n \geq 1$),

$$f_0^{(a,B)}(x) = B, \quad f_1^{(a,B)}(x) = x, \quad f_{n+1}^{(a,B)}(x) = x f_n^{(a,B)}(x) - a f_{n-1}^{(a,B)}(x),$$

where $B, a \in \mathbb{Q}$ or \mathbb{R} . As a direct application of the uniform decomposition result, we fully settle the finiteness problem for the Diophantine equation

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

This extends and completes work of Dujella/Tichy and Dujella/Gusić concerning Dickson polynomials of the second kind. The method of the proof involves a new sufficient criterion for indecomposability of polynomials with fixed degree of the right component.

1 Introduction

1.1 Indecomposability and Diophantine equations

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. The theory of polynomial decompositions has a long history and dates back to the work of J. F. Ritt [21, 22]. 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 said to be *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 *indecomposable* (or *prime*) otherwise. It is well-known, that indecomposability over \mathbb{Q} or \mathbb{R} implies indecomposability over \mathbb{C} (see [24, p.14]).

Indecomposability results are closely related to finiteness statements for Diophantine equations of the form

$$f(x) = g(y) \tag{1.1}$$

with $f, g \in \mathbb{Q}[x]$ in unknowns $(x, y) \in \mathbb{Q}^2$. In 2000, Bilu and Tichy [3] succeeded in fully joining polynomial decomposition theory with the classical finiteness theorem of Siegel [25] on finiteness of integral points of curves of genus > 0 .

Theorem 1.1 (Bilu/Tichy [3]). *Let $f(x), g(x) \in \mathbb{Q}[x]$ be non-constant polynomials. Then the following two assertions are equivalent:*

(a) *The equation (1.1) has infinitely many rational solutions with a bounded denominator.*

(b) *We have*

$$f = \varphi \circ \mathbf{f}_1 \circ \kappa_1 \quad \text{and} \quad g = \varphi \circ \mathbf{g}_1 \circ \kappa_2,$$

where $\kappa_1, \kappa_2 \in \mathbb{Q}[x]$ are linear, $\varphi(x) \in \mathbb{Q}[x]$, and $(\mathbf{f}_1, \mathbf{g}_1)$ is a standard pair over \mathbb{Q} such that the equation $\mathbf{f}_1(x) = \mathbf{g}_1(y)$ 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 $(\mathbf{f}_1, \mathbf{g}_1)$ which are defined 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 (1.7) below).

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

$$(x^q, \gamma x^r v(x)^q) \quad (\text{or switched}), \quad (1.2)$$

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

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

$$(x^2, (\gamma x^2 + \delta) v(x)^2) \quad (\text{or switched}). \quad (1.3)$$

A standard pair of the *third* kind is

$$(D_s(x, \gamma^t), D_t(x, \gamma^s)) \quad (1.4)$$

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

A standard pair of the *fourth* kind is

$$(\gamma^{-s/2} D_s(x, \gamma), -\delta^{-t/2} D_t(x, \delta)) \quad (\text{or switched}), \quad (1.5)$$

with $s, t \geq 1$ and $\gcd(s, t) = 2$.

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

$$((\gamma x^2 - 1)^3, 3x^4 - 4x^3) \quad (\text{or switched}). \quad (1.6)$$

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 $p_m(x) = g(y)$, where $\{p_k\}_{k \geq 0}$ denotes some specific polynomial family and $g(x)$ is an arbitrary polynomial over \mathbb{Q} . The interested reader may consult [2, 12, 18, 19, 27] for equations with binomial coefficient polynomials, [13, 14, 15] for equations with Bernoulli polynomials, [2, 20] for power-sum polynomials, [15] for truncated Taylor polynomials of the exponential function and [1, 10, 11, 26, 29, 28] for polynomials in three-term recurrences. As a principle, the difficulty consists in proving a uniform indecomposability theorem for $\{p_k\}$. The novelty of the approach adopted in the present paper consists to first bound the right component by an analytical technique and then to cope with the small degree cases by a new sufficient criterion.

1.2 Dickson-type polynomials

Our method best fits for the so-called *Dickson-type 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* (1.4) and *fourth* kind (1.5). Recall an alternative definition of the Dickson polynomials [16, Lemma 2.3],

$$\begin{aligned} D_0(x, a) &= 2, \\ D_1(x, a) &= x, \\ D_{n+1}(x, a) &= xD_n(x, a) - aD_{n-1}(x, a), \quad n \geq 1, \end{aligned} \tag{1.7}$$

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

$$D_{mn}(x, a) = D_m(x, a^n) \circ D_n(x, a) = D_n(x, a^m) \circ D_m(x, a). \tag{1.8}$$

Note that several common polynomial families and their dilates form subclasses of the Dickson polynomials. Mention, for instance, the *Lucas polynomials* $L_k(x)$ and *Pell-Lucas polynomials* $Q_k(x/2)$ for $a = -1$, the *Chebyshev polynomials of the first kind* $2T_k(x/2)$ for $a = 1$ and the *Fermat-Lucas polynomials* $FL_k(x/3)$ for $a = 2$ (see [33]). A generalized Dickson-type recursive relation is obtained by a perturbation of the zero instance in the Dickson recurrence (1.7).

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

$$\begin{aligned} f_0(x) &= B, \\ f_1(x) &= x, \\ f_{n+1}(x) &= xf_n(x) - af_{n-1}(x), \quad n \geq 1, \end{aligned} \tag{1.9}$$

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

Note that the case $a = 0$ gives rise to $f_n(x) = x^n$, whose prime decompositions plainly correspond to permutations of the prime factors of n . As our focus is on finding more sophisticated decompositions, we are primarily concerned with polynomials with $B \neq 2$ and $a \neq 0$. In the framework of (1.9) one again encounters well-known polynomial families. 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 [33]). In fact, the polynomials $E_n(x, a)$ defined by

$$\begin{aligned} E_0(x, a) &= 1, \\ E_1(x, a) &= x, \\ E_{n+1}(x, a) &= xE_n(x, a) - aE_{n-1}(x, a), \quad n \geq 1, \end{aligned} \tag{1.10}$$

with $a \in \mathbb{C}$ are the *Dickson polynomials of the second kind* (see [16, Lemma 2.3]), for which holds the formula [16, Definition 2.2],

$$E_n(x, a) = \sum_{i=0}^{\lfloor n/2 \rfloor} \binom{n-i}{i} (-a)^i x^{s-2i}. \quad (1.11)$$

Decomposability of Dickson-type polynomials over \mathbb{Q} and related Diophantine equations have been previously considered by Dujella and Tichy [9] for $B = 1$ and $a \in \mathbb{Z}$. Very recently, Dujella, Gusić and Tichy [8], and Dujella and Gusić [6] proved new criteria for indecomposability of polynomials over \mathbb{Z} in terms of the degree and two leading coefficients. In [7], the latter authors applied their criteria to attack indecomposability concerning general Dickson-type recursive polynomials over \mathbb{Q} .

Theorem 1.3 (Dujella/Gusić [7]). *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 [9].

There are sporadic decompositions of Dickson-type polynomials over \mathbb{Q} as pointed out by Dujella and Gusić [7, Example 1].

Example 1.4. Let $B = -2$ and $a = -1$, then $f_8 = (x^2 - 4x - 2) \circ (x^4 + 2x^2)$.

Motivated by this example, 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.

2 Main results

Our main result is

Theorem 2.1. *The Dickson-type polynomials f_n over \mathbb{R} defined in (1.9) 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,*

$$f_n = \mathfrak{h}_k \circ x^2 \quad (2.1)$$

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

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

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

The method of proof is rather algorithmic and portions can very well be implemented with the aid of a computer algebra system. In a complementary work [31] we show, how one can use Gröbner

basis calculations performed with Maple 10 to cope with decomposition of so-called *perturbed Chebyshev polynomials*, which basically depend on one more parameter.

In the present paper, 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*

$$f_n(x) = g(y) \quad (2.3)$$

with Dickson-type 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) $n = 2k$, $k \geq 2$ and $g(x) = \mathfrak{h}_k(\tilde{g}(x))$, 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) $n = 3$, $B \neq -1$ 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) $n = 3$, $B = -1$ 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) $n = 4$, $B \neq -2$ 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) $n = 4$, $B \neq -2$ and $g(x) = -\frac{(B+2)^2 a^2}{16} \delta^{-m/2} D_m(\kappa(x), \delta) - \frac{1}{8}a^2(B - 2)^2$, where $\delta \in \mathbb{Q} \setminus \{0\}$, $\gcd(m, 4) = 2$.
- (vii) $n = 4$, $B = -2$ 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) $n = 8$, $B = -2$ 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 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 (1.7).

Theorem 2.3. *The Diophantine equation*

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

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) $m = 6, n = 3$ and $\hat{B} = -5/2, 4a(B+1) = 21\hat{a}^2, \hat{a} \neq 0$;
- (II) $m = 3t, n = 3$ and $\hat{B} = 2, (B+1)a = 3\hat{a}^t, t \geq 2, B \neq 2, \hat{a} \neq 0$;
- (III) $\gcd(m, 3) = 1, n = 3$ and $\hat{B} = 2 \neq B, (B+1)a = 3\gamma^m, \hat{a} = \gamma^3 \neq 0$;
- (IV) $m > n \geq 3$ and $B = \hat{B} = 2, a^t = \hat{a}^s, \hat{a} \neq 0, mt = ns$.
- (V) $m > n \geq 3$ and $a = \hat{a} = 0$;
- (VI) $m > n = 3$ and $B = -1, \hat{a} = 0, a \neq 0$;
- (VII) $m = n$ and $f_n^{(a,B)} \equiv f_m^{(\hat{a},\hat{B})}$.

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 all seven cases.

Theorem 2.3 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 [9, Theorem 2] concerning Dickson polynomials of the second kind (1.10) (also termed *generalized Fibonacci polynomials*).

Corollary 2.4 (Dujella/Tichy [9]). *The Diophantine equation $f_n^{(a,1)}(x) = f_m^{(a,1)}(y)$ with $m, n \geq 3, m \neq n$ and $a \in \mathbb{Z} \setminus \{0\}$ has only finitely many rational solutions (x, y) with a bounded denominator.*

It has been proved by Dujella and Gusić [7, 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 [7]). *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 $f_n^{(a,B)} = f_m^{(\hat{a},\hat{B})}$ 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.

The paper is organized as follows. In SECTION 3 we recall some basic facts from polynomial decomposition theory over fields of characteristic zero. SECTION 4 is devoted to the proof of

Theorem 2.1, which splits into two parts. First, in Subsection 4.1, a general investigation of right components of higher degree via a second-order differential equation technique is given. Thereafter, in Subsection 4.2, we carry out a detailed analysis of the “small” cases by means of an indecomposability criterion with right components of fixed degree (Lemma 3.4). Finally, in SECTION 5 we prove Theorem 2.2 and Theorem 2.3 by looking at the remaining decompositions involving the five standard pairs (1.2)–(1.6).

3 Preliminaries

Let \mathbb{K} be a field of constants with $\text{char } \mathbb{K} = 0$. First, we collect some standard results from polynomial decomposition theory, which will be needed in the sequel [4, 23, 24].

Definition 3.1. Let $f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in \mathbb{K}[x]$ 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*

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

Proof. Let $r = x^n + r_{n-1}x^{n-1} + \cdots$. Then

$$r \circ q = q^n + r_{n-1}q^{n-1} + \cdots$$

and $\deg(r \circ q - q^n) = \deg(r_{n-1}q^{n-1} + \cdots) \leq m(n-1)$. □

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

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

Proof. We have

$$\deg(f - (q + \alpha x^{m-k})^n) = \deg(f - q^n - nq^{n-1}\alpha x^{m-k} - \cdots),$$

where the omitted terms have degree $\leq (n-i)m + i(m-k) = mn - ik \leq mn - k - 1$ for $i \geq 2$. Therefore, since q is normed, inequality (3.1) holds if and only if $\alpha = \text{lcoeff}(f - q^n)/n \in \mathbb{K}$. □

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

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

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*

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

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

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

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 . \square

Lemma 3.4 is of particular use to exclude decompositions with right components of small degree in an improved way. Given a polynomial $f(x)$, one expands $f(x)$ regarding $\hat{q}(x)$ up to sufficiently large order (indicated by l) such that the remainder polynomial \mathcal{R} has the wanted properties. This procedure will be used in Subsection 4.2 to treat the ‘‘small’’ cases regarding Dickson-type polynomials.

4 Proof of Theorem 2.1

4.1 Sturm-Liouville type differential equation

We now turn back to the Dickson-type polynomials f_n defined by (1.9). Let $a, B \in \mathbb{R}$, $a \neq 0$ and $B \neq 2$. (In the sequel, some statements also hold for $B = 2$; we will make clear when this is the case.) We further may assume that $n \geq 4$ since otherwise f_n is trivially indecomposable by reasons of degrees. The polynomial family defined by

$$\begin{aligned} \tilde{f}_{-1}(x) &= 0, \\ \tilde{f}_0(x) &= 1, \\ \tilde{f}_{n+1}(x) &= x \tilde{f}_n(x) - \delta_n \tilde{f}_{n-1}(x), \quad n \geq 0, \end{aligned} \quad (4.1)$$

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 (1.9). Indeed, it is easy to see that $\tilde{f}_n(x) = f_n(x)$ for $n \geq 1$. As already pointed out in [6], 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 $x = \cos \varphi$. For later reference, we first state two well-known properties of these polynomials [17, p.104].

Proposition 4.1. For $n \geq 1$,

$$T_{n-1}(x) = 2xT_n(x) - T_{n+1}(x), \quad (4.2)$$

$$(1-x^2)T'_n(x) = n(T_{n-1}(x) - xT_n(x)). \quad (4.3)$$

The next lemma establishes the connection to Dickson-type polynomials.

Lemma 4.2. For all $n \geq 1$ we have

$$f_n(2\sqrt{ax}) = \frac{(\sqrt{a})^n}{x^2 - 1} ((2x^2 - B)T_n(x) + (B - 2)xT_{n-1}(x)). \quad (4.4)$$

Proof. Since $T_0(x) = 1$, $T_1(x) = x$ and $T_2(x) = 2x^2 - 1$, one easily checks that

$$\begin{aligned} (x^2 - 1) f_1(2\sqrt{ax}) &= \sqrt{a} ((2x^2 - B) \cdot x + (B - 2)x \cdot 1) = 2\sqrt{ax}, \\ (x^2 - 1) f_2(2\sqrt{ax}) &= a ((2x^2 - B) \cdot (2x^2 - 1) + (B - 2)x \cdot x) = 4ax^2 - aB. \end{aligned}$$

Thus, it remains to show that the right hand side of (4.4) satisfies the three-term relation in (4.1). By applying (4.2) twice, namely for $T_{n-2}(x)$ and $T_{n-1}(x)$, we have the identity

$$\begin{aligned} &2x(2x^2 - B)T_n(x) + 2x^2(B - 2)T_{n-1}(x) - (2x^2 - B)T_{n-1}(x) - (B - 2)xT_{n-2}(x) \\ &= 2x(2x^2 - B)T_n(x) + (2x^2B - 6x^2 + B)T_{n-1}(x) \\ &\quad - (B - 2)x(2xT_{n-1}(x) - T_n(x)) \\ &= T_n(x)(4x^3 - Bx - 2x) + T_{n-1}(x)(B - 2x^2) \\ &= T_n(x)(4x^3 - Bx - 2x) + (2xT_n(x) - T_{n+1}(x))(B - 2x^2) \\ &= T_{n+1}(x)(2x^2 - B) + T_n(x)(Bx - 2x). \end{aligned}$$

Multiplying by $(\sqrt{a})^{n+1}/(x^2 - 1)$ we get the $(n+1)$ -instance of (4.4). This completes the proof. \square

In the same style it is also possible to derive

$$f_n(2\sqrt{ax}) = (\sqrt{a})^n(2xU_{n-1}(x) - BU_{n-2}(x)), \quad (4.5)$$

where $U_n(x) = \sin n\varphi / \sin \varphi$ with $x = \cos \varphi$ denote the Chebyshev polynomials of the second kind. Since by (1.11),

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

we get the following explicit representation for f_n , which has already been proved in [7] by other means.

Proposition 4.3. *We have*

$$\begin{aligned}
f_n(x) &= \sum_{i=0}^{\lfloor n/2 \rfloor} \frac{n + (B-2)i}{n-i} \binom{n-i}{i} (-a)^i x^{n-2i} \\
&= x^n - (n+B-2)ax^{n-2} + \frac{(n-3)(n+2B-4)}{2} a^2 x^{n-4} \\
&\quad - \frac{(n-4)(n-5)(n+3B-6)}{6} a^3 x^{n-6} \pm \dots
\end{aligned} \tag{4.6}$$

The proof of 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, such that the degree of the right component can be bounded. The method is reminiscent of Pólya–Sonin–Szegő [32, Th. 7.31.1] and has already been used by Tichy and the author to study two-interval monotonicity of continuous classical orthogonal polynomials [26].

Lemma 4.4. *The polynomials $y = f_n(x)$ with $a \neq 0$, $B \in \mathbb{R}$ satisfy the differential equation*

$$(A_4 x^4 + aA_2 x^2 + a^2 A_0) y'' + (B_3 x^3 + aB_1 x) y' - (C_2 x^2 + aC_0) y = 0, \tag{4.7}$$

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

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

Proof. The proof is basically a straightforward calculation, so we only give the main steps. To begin with, we use Lemma 4.2 to express the first derivative of $f_n(x)$ in terms of $T_n(x)$, $T_{n-1}(x)$ and derivatives $T'_n(x)$ and $T'_{n-1}(x)$, i.e.,

$$\begin{aligned}
\frac{2(1-x^2)^2}{(\sqrt{a})^{n-1}} \cdot f'_n(2\sqrt{a}x) &= 2x(B-2)T_n(x) - (x^2+1)(B-2)T_{n-1}(x) \\
&\quad + (B-2x^2)(1-x^2)T'_n(x) - (B-2)x(1-x^2)T'_{n-1}(x).
\end{aligned}$$

We then apply (4.3) and shift indices back with the help of (4.2) so as to obtain an expression involving $T_n(x)$ and $T_{n-1}(x)$ only. Hence

$$\begin{aligned}
\frac{2(1-x^2)^2}{(\sqrt{a})^{n-1}} \cdot f'_n(2\sqrt{a}x) &= T_n(x) (2nx^3 + (2B-nB-4)x) \\
&\quad - T_{n-2}(x)x(B-2)(n-1) \\
&\quad + T_{n-1}(x) ((-2B+4-4n+nB)x^2 + nB-B+2) \\
&= T_n(x) (2nx^3 + (B-2n-2)x) \\
&\quad + T_{n-1}(x) (-nBx^2 + nB-B+2).
\end{aligned} \tag{4.8}$$

By the same means we get for the second derivative

$$\begin{aligned} \frac{4(1-x^2)^3}{(\sqrt{a})^{n-2}} \cdot f_n''(2\sqrt{a}x) &= (2nx^4 + (3B-6)x^2 + B - 2n - 2)T_n(x) \\ &\quad - (2nBx^3 + (4B - 2nB - 8)x)T_{n-1}(x) \\ &\quad + (2nx^3 + (B - 2n - 2)x)(1-x^2)T_n'(x) \\ &\quad - (nBx^2 - nB + B - 2)(1-x^2)T_{n-1}'(x), \end{aligned}$$

and

$$\begin{aligned} \frac{4(1-x^2)^3}{(\sqrt{a})^{n-2}} \cdot f_n''(2\sqrt{a}x) &= \\ &\quad T_n(x) \left(-2n(n-1)x^4 + (-2nB + 2n^2 + 2n + 3B - 6 + n^2B)x^2 \right. \\ &\quad \left. - n(nB - 2B + 4) \right) \\ &\quad + T_{n-1}(x) \left(-n(nB - 2n + B)x^3 \right. \\ &\quad \left. + (nB - 2n^2 - 3B + 6 + n^2B)x \right). \end{aligned} \tag{4.9}$$

We now solve the system (4.4), (4.8) to $T_n(x)$, $T_{n-1}(x)$ and plug these expressions into (4.9). Note that the determinant of the system is $-4n(B-1)x^2 + B(nB - B + 2)$ which does not vanish identically for any $B \in \mathbb{R}$, $n \in \mathbb{Z}^+$. Finally, we multiply the obtained equation by its common denominator, divide by $(1-x^2)^2$ and substitute $x \mapsto x/(2\sqrt{a})$ to obtain the statement of the Lemma. \square

In order to use Szegő's argument, we need the specific root behaviour of the polynomials $f_n(x)$, which has been stated in [7, Theorem 4].

Proposition 4.5. *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 4.6. *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 Proposition 4.5 with Lemma 4.4 to obtain a uniform bound on the degree of the right component q of some possible decomposition $f_n = r \circ q$.

Lemma 4.7. *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

$$h(x) = f_n(x)^2 - \frac{\sigma(x)}{\lambda(x)} f_n'(x)^2. \quad (4.10)$$

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 (4.7) we have

$$\begin{aligned} h'(x) &= 2f_n(x)f_n'(x) - \left(\frac{\sigma(x)}{\lambda(x)}\right)' f_n'(x)^2 - \frac{2f_n'(x)}{\lambda(x)} (\lambda(x)f_n(x) - \tau(x)f_n'(x)) \\ &= \omega(x)(f_n'(x))^2, \end{aligned} \quad (4.11)$$

where

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

with

$$\omega_1(x) = n(n^2 - 1)(B - 1)x^3 - a(Bn^2 - 3Bn + 2B + 6n)(Bn - B + 2)x. \quad (4.12)$$

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 $\xi_1, \xi_2, \dots, \xi_m$ the pairwise different real zeroes of $f_n'(x)$. Then by Corollary 4.6, $m \geq n - 3$ and by (4.10) we get

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

By (4.11) 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

$$\deg \gcd(f_n - \zeta, f_n') \leq 4 + 2 = 6. \quad (4.13)$$

Suppose a non-trivial decomposition $f_n = r \circ q$. Denote by ζ_0 a root of r' , which exists by $\deg r \geq 2$. Then both the polynomials $f_n(x) - r(\zeta_0)$ and $f_n'(x)$ are divisible by $q(x) - \zeta_0$. Therefore,

$$\deg q = \deg(q - \zeta) \leq \deg \gcd(f_n - r(\zeta_0), f_n') \leq 6,$$

which completes the proof of the lemma for $a > 0$. Finally, let $a < 0$. By (4.6) we have $f_n^{(a,B)}(\sqrt{ax}) = (\sqrt{a})^n f_n^{(1,B)}(x)$ and exactly the same arguments as above apply. This finishes the proof of the lemma. \square

One can improve the bound $\deg q \leq 6$ for f_n by distinguishing several cases on a , B and n , according to whether $\omega_1(x)$ in (4.12) indeed takes three real zeroes. However, the given uniform upper bound completely suffices our purposes for the calculations in Subsection 4.2.

4.2 The small cases

In order to use Lemma 3.4 we require the upper-most coefficients of f_n given in (4.6). Lemma 4.7 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 $k = \deg r \geq 2$.

The case $\deg q = 2$:

Since by (4.6) the coefficient $[x^{2k-1}]$ of $f_{2k}(x)$ equals zero, one step in Proposition 3.3 gives $\alpha_1 = 0$, $\hat{q} = x^2$ and thus (2.1). It remains to show that \mathfrak{h}_k is indecomposable whenever $k \neq 4$. For suppose a non-trivial decomposition $\mathfrak{h}_k = r_{\mathfrak{h}} \circ q_{\mathfrak{h}}$. This yields a non-trivial decomposition of $f_{2k} = r_{\mathfrak{h}} \circ (q_{\mathfrak{h}} \circ x^2)$. By Lemma 4.7 the degree of the right component $q_{\mathfrak{h}} \circ x^2$ is bounded by 6, such that we get all non-trivial decompositions of \mathfrak{h}_k by working out the cases $\deg q = 4$ and $\deg q = 6$ for the polynomials $f_{2k}(x)$. The indecomposability statement for \mathfrak{h}_k then follows from the single decomposition of $f_{2k}(x)$ for $k = 4$, $B = -2$ (see (4.19) below).

The case $\deg q = 3$:

As before, we have $\alpha_1 = 0$ and $\deg(f - x^{3k}) = 3k - 2$. Therefore by (3.1) and (4.6),

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

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.,

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

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

$$\hat{q} = x^4 - \frac{x^2 a(B + 4k - 2)}{k}. \quad (4.14)$$

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

$$f_{4k} = \hat{q}^k + \beta_1 \hat{q}^{k-1} + \mathcal{R}(x). \quad (4.15)$$

It is a direct calculation to check

$$\beta_1 = -\frac{a^2((k-1)B^2 - (6k-4)B - 4(k-1)^2)}{2k} \quad (4.16)$$

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

$$B = -(2k+2)/(2k-1). \quad (4.17)$$

In such case (4.15) with (4.16) 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

$$\mathcal{R}(x) = \frac{a^4k(4k-5)(8k^4-78k^3+204k^2-208k+69)}{(2k-1)^4}x^{4k-8} + \text{terms of lower order.} \quad (4.18)$$

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

$$f_{4k}(x) = \hat{q}^k + \beta_1\hat{q}^{k-1} + \beta_2\hat{q}^{k-2} + \tilde{\mathcal{R}}(x)$$

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 (4.16), (4.17), (4.18) gives $B=-2$, $\beta_1=-4a^2$ and $\beta_2=-2a^4$. Finally by (4.14) we get $\hat{q}(x) = x^4 - 2ax^2$ and the decomposition

$$f_8 = (x^2 - 4a^2x - 2a^4) \circ (x^4 - 2ax^2), \quad (4.19)$$

as asserted in (2.2).

The case $\deg q = 5$:

Here we have

$$\hat{q} = x^5 - \frac{a(B+5k-2)}{k}x^3 - \frac{a^2((k-1)B^2 - (8k-4)B - (10k^2 - 12k + 4))}{2k^2}x$$

and $f_{5k} = \hat{q}^k + \mathcal{R}(x)$ with

$$\mathcal{R}(x) = -\frac{a^3(B-2)^2(k-1)((2k-1)B-k+2)}{6k^2}x^{5k-6} + \text{terms of lower order.}$$

The leading coefficient of $\mathcal{R}(x)$ is zero if and only if $B = (k-2)/(2k-1)$. In that case, however, we get

$$\mathcal{R}(x) = -\frac{27(3k-1)(k-1)ka^4}{8(2k-1)^3}x^{5k-8} + \text{terms of lower order,}$$

and since $5 \nmid (5k-8)$ there cannot be a decomposition with $\deg q = 5$.

The case $\deg q = 6$:

The examination of the case $\deg q = 6$ is similar to $\deg q = 4$. Because of reasons of degree we have to expand more terms. More specifically, from Proposition 3.3 we retrieve

$$\hat{q} = x^6 - \frac{B + 6k - 2}{k} ax^4 + \frac{a^2}{2k^2} ((1 - k)B^2 + (10k - 4)B + 18k^2 - 16k + 4) x^2$$

and $f_{6k} = \hat{q}^k + \beta_1 \hat{q}^{k-1} + \mathcal{R}(x)$ with

$$\beta_1 = \frac{a^3}{6k^2} (- (2k^2 - 3k + 1)B^3 + 6(2k^2 - 3k + 1)B^2 - (30k^2 - 36k + 12)B - 4(k - 1)(3k^2 - 4k + 2)),$$

$$\mathcal{R}(x) = - \frac{a^4(B - 2)^2(k - 1) ((6k^2 - 5k + 1)B^2 + (8k - 4)B + 4k + 4)}{24k^3} x^{6k-8} + \text{terms of lower order.}$$

Since the discriminant of the quadratic numerator polynomial is

$$\Delta = (8k - 4)^2 - 4(6k^2 - 5k + 1)(4k + 4) = -48k^2(2k - 1) < 0,$$

there cannot be a decomposition with $\deg q = 6$, too.

This finishes the investigation for $\deg q \leq 6$. Since one gets no more decompositions with normed right components, when coefficients of r and q are allowed to be in \mathbb{C} , this completes the proof of Theorem 2.1.

5 Proof of Theorem 2.2 and 2.3

In view of Theorem 1.1, we have to deal with decompositions of f_n involving the standard pairs given by (1.2)–(1.6). 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,

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

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, 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 $f_8 = (x^2 - 4a^2x - 2a^4) \circ (x^4 - 2ax^2)$.

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 (1.2)–(1.6).

To begin with, recall the standard pair of the *second* kind $(x^2, (\gamma x^2 + \delta)v(x)^2)$ given in (1.3). 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 (1.4), 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 (4.6), (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 (1.5). Then the same argument with an altered coefficient φ_1 gives the contradiction. Hence, $(\mathbf{f}_1, \mathbf{g}_1)$ cannot be a standard pair of the third or fourth kind.

Next, suppose $(\mathbf{f}_1, \mathbf{g}_1) = ((\gamma x^2 - 1)^3, 3x^4 - 4x^3)$ (or switched) is a standard pair of the *fifth* kind (1.6). Since $n \geq 5$ and $(\gamma x^2 - 1)^3$ is even, we only have to treat the case

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

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 $B = (1 \pm 3i\sqrt{3})/2 \notin \mathbb{Q}$, a contradiction. Thus, $(\mathbf{f}_1, \mathbf{g}_1)$ cannot be a standard pair of the fifth kind.

Finally, consider the standard pair of the *first* kind given by (1.2), namely $(x^q, \gamma x^r v(x)^q)$. By Corollary 4.6, 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

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

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 (1.2). Then, again due to Corollary 4.6 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 $(\mathbf{f}_1, \mathbf{g}_1)$ 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,

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

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

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

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

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

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 (1.8), $x = D_m(t, \gamma)$ 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 [3] 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 $\deg \varphi = 1$.

Case $\deg \varphi = 2$ with $n = 8$ and $f_8 = (x^2 - 4a^2x - 2a^4) \circ (x^4 - 2ax^2)$:

Suppose the equation $f_8(x) = x^8 - 4ax^6 + 8a^3x^2 - 2a^4 = g(y)$ has infinitely many rational solutions with a bounded denominator. Then by Theorem 1.1,

$$f_8 = \varphi \circ \mathfrak{f}_1 \circ \kappa_1 \quad \text{and} \quad g = \varphi \circ \mathfrak{g}_1 \circ \kappa_2$$

with some standard pair $(\mathfrak{f}_1, \mathfrak{g}_1)$ such that $\mathfrak{f}_1(x) = \mathfrak{g}_1(y)$ has infinitely many rational solutions with a bounded denominator. By comparison of degrees we are looking for $(\mathfrak{f}_1, \mathfrak{g}_1)$ with $\deg \mathfrak{f}_1 = 4$ and $\deg \mathfrak{g}_1 \geq 2$. Let κ be the unique unit such that $\varphi \circ \kappa = x^2 - 4a^2x - 2a^4$. From $\kappa^{-1} \circ \mathfrak{f}_1 \circ \kappa_1 = x^4 - 2ax^2 = x^2(x^2 - 2a)$ one has that \mathfrak{f}_1 has a double root and two simple roots. By the conditions on the degrees and the fact that Dickson polynomials only have simple roots, there can only be a decomposition with a standard pair of the *second* kind with $g(x) = \varphi(\kappa_2(x)^2)$. Then, the Diophantine equation $f_8(x) = g(y)$ can be written as

$$x^2(x^2 - 2a)(x^2(x^2 - 2a) - 4a^2) = \kappa(y)^2(\kappa(y)^2 - 4a^2).$$

Here, an infinite parametric family of solutions is given by $x^2 = t^2 + 2a$ and $\kappa(y) = xt$. This is Case (viii) in Theorem 2.2.

This finishes the proof of Theorem 2.2.

Proof. (Proof of Theorem 2.3)

We work through Cases (i)–(viii) of Theorem 2.2.

Let $m, n \geq 3$, $f_n^{(a,B)} \neq f_m^{(\hat{a},\hat{B})}$ and suppose that $a, \hat{a} \neq 0$ and $B \neq 2$.

Case (i): We have to check the polynomial identity

$$g(x) = f_m^{(\hat{a},\hat{B})}(x) = f_n^{(a,B)}(\tilde{g}(x)), \quad (5.8)$$

where $\tilde{g}(x) \in \mathbb{Q}[x]$. We will say that we have a *solution* (of (5.8)), if we find parameters such that (5.8) holds true. If $\hat{B} = 2$ then $f_m^{(\hat{a},2)}(x) = D_m(x, \hat{a})$ and by (1.8),

$$f_n^{(a,B)}(\kappa(x)) = D_n(x, \hat{a}^t),$$

where $t = \deg \tilde{g}$ and $m = nt$. From (5.1), (5.4) and (5.5) we get $n = 3$, $m = 3t$ and $(B+1)a = 3\hat{a}^t$, which is a solution (Solution (II)). Let $\hat{B} \neq 2$. Then Theorem 2.1 implies

$$\tilde{g}(x) \in \{\beta_1(x^4 - 2x^2) + \beta_0, \beta_1x^2 + \beta_0, \beta_1x + \beta_0\}, \quad (5.9)$$

where $\beta_0, \beta_1 \in \mathbb{Q}$ and $\beta_1 \neq 0$. First, if $\tilde{g}(x) = \beta_1(x^4 - 2x^2) + \beta_0$ then $m = 8$ and $n = 2$, which is a contradiction. Secondly, let $\tilde{g}(x) = \beta_1x^2 + \beta_0$ and assume $m/2 = n \geq 5$. For $0 \leq j \leq \lfloor m/2 \rfloor$ put

$$c_{j,m}^{(a,B)} := \frac{m + (B-2)j}{m-j} \binom{m-j}{j} (-a)^j.$$

Then, by comparing coefficients $[x^{m-2i}]$ in (5.8) we get

$$c_{i,m}^{(\hat{a},\hat{B})} = \sum_{j=0}^{\lfloor i/2 \rfloor} c_{j,n}^{(a,B)} \binom{n-2j}{i-2j} \beta_1^{n-i} \beta_0^{i-2j}, \quad 0 \leq i \leq 5. \quad (5.10)$$

In particular, for $i = 0$ we have $\beta_1^n = 1$, such that (5.10) yields a system of five polynomial equations in unknowns $n, \beta_0, \beta_1, a, B, \hat{a}, \hat{B}$. With standard Gröbner techniques it can be shown that (5.10) has no admissible solution. (For the details of these and future calculations we refer to the MAPLE-worksheet [30]) It remains to consider $n = 3, 4$. If $n = 4$, $m = 8$ then $\hat{B} = -2$ and $B = 4 \pm 2\sqrt{3} \notin \mathbb{Q}$, a contradiction. If $n = 3$, $m = 6$ we have $\hat{B} = -5/2$ and $4a(B+1) = 21\hat{a}^2$, a solution (Solution (I) for $B \neq 2$), due to the polynomial identity

$$f_6^{(\hat{a},-5/2)}(x) = f_3^{(a,B)}(x^2 - \hat{a}/2).$$

Finally, consider $\tilde{g}(x) = \beta_1x + \beta_0$. By symmetry reasons we have $m = n$, $\beta_0 = 0$ and $\beta_1^{n-i} = 1$ for i even. But this contradicts with the fact that the polynomials $f_m^{(\hat{a},\hat{B})}(x)$ and $f_n^{(a,B)}(x)$ are supposed to be different.

Case (ii): We have to consider

$$g(x) = f_m^{(\hat{a},\hat{B})}(x) = \mathfrak{h}_k^{(a,B)}(\tilde{g}(x)),$$

where again (5.9). First, suppose $\tilde{g}(x) = \beta_1(x^4 - 2x^2) + \beta_0$ such that

$$\begin{aligned} x^8 - \hat{a}(\hat{B} + 6)x^6 + 5\hat{a}^2(\hat{B} + 2)x^4 - 2\hat{a}^3(3\hat{B} + 2)x^2 + \hat{a}^4\hat{B} \\ = (\beta_1(x^4 - 2x^2) + \beta_0)^2 - a(B+2)(\beta_1(x^4 - 2x^2) + \beta_0) + a^2B. \end{aligned}$$

This yields $\beta_1 = \pm 1$ and $\beta_0 = \mp 2$ or $\beta_0 = \mp 2 + (B+2)t$ with $t^2(B^2+4) = 6$. Since for $(B+2)t \in \{\pm 2, \pm 3\}$ we get $B \in \{-6 \pm 4\sqrt{2}, 4 \pm 2\sqrt{3}\}$, a contradiction, the polynomial $\tilde{g}(x) = \beta_1(x^4 - 2x^2) + \beta_0$ has always four simple zeroes. However, this is a contradiction to the assumption of Case (ii). Secondly, consider $f_m^{(\hat{a}, \hat{B})}(x) = \mathfrak{h}_k^{(a, B)}(\beta_1 x^2 + \beta_0)$. Then $m = n = 2k$ and

$$\sum_{j=0}^i c_{j,n}^{(a, B)} \binom{k-j}{i-j} \beta_1^{k-i} \beta_0^{i-j} = \begin{cases} c_{i,m}^{(\hat{a}, \hat{B})}, & \text{if } i \text{ even,} \\ 0, & \text{if } i \text{ odd.} \end{cases}$$

Suppose $n \geq 6$. The system for $0 \leq i \leq 6$ has no admissible solution (see [30]; note that $\beta_0 \neq 2a$). Let $n = 4$ and consider

$$x^4 - \hat{a}(\hat{B}+2)x^2 + \hat{a}^2 \hat{B} = (\beta_1 x^2 + \beta_0)^2 - a(B+2)(\beta_1 x^2 + \beta_0) + a^2 B.$$

Since $\hat{B} = -2$ implies $B = -2$ and $a = \pm \hat{a}$, which is not allowed, we have the only solution [30], $t \in \mathbb{Q}$,

$$\beta_1 = \pm 1, \quad aB = t, \quad t^2 = \hat{a}^2 \hat{B} + 4\hat{a}^2 - 4a^2, \quad \beta_0 = \mp \frac{\hat{a} \hat{B}}{2} \mp \hat{a} + \frac{t}{2} + a.$$

Therefore, $t = -2a$, $B = -2$ and $8a^2 = \hat{a}^2(\hat{B}^2 + 4)$, thus we have the Diophantine equation $x^4 - 2a^2 = y^4 - \hat{a}(\hat{B}+2)y^2 + \hat{a}^2 \hat{B}$, or equivalently,

$$x^4 = \left(y^2 - \frac{\hat{a}(\hat{B}+2)}{2} \right)^2,$$

which obviously has only finitely many rational solutions with a bounded denominator if $\hat{B} \neq -2$. The case $\tilde{g}(x) = \beta_1 x + \beta_0$ infers $f_m^{(\hat{a}, \hat{B})}(\tilde{\beta}_1 x^2 + \tilde{\beta}_0) = f_n^{(a, B)}(x)$ for some $\tilde{\beta}_1, \tilde{\beta}_0 \in \mathbb{Q}$, $\tilde{\beta}_1 \neq 0$. The argument given in the discussion of Case (i) applies, thus we get a solution (Solution (I)) for $B = 2$, too.

Finally, if $\hat{B} = 2$, then $n = 2k$, $m = k$ and $\mathfrak{h}_k^{(a, B)}(\kappa x) = D_k(x, \hat{a}^t)$ which similarly implies $k \leq 2$, a contradiction [30].

Case (iii): We have to check whether $f_m^{(\hat{a}, \hat{B})}(x) = \beta^3 D_m(\kappa(x), \gamma^3)$ has a solution. First, let $\hat{B} \neq 2$. From the discussion of (5.1) we get $m \leq 4$, thus $m = 4$ due to $\gcd(m, 3) = 1$. The only decomposition of $f_4^{(\hat{a}, \hat{B})}(x)$ in terms of a Dickson polynomial of degree 4 is of type (5.5), such that for some $\beta_1 \in \mathbb{Q} \setminus \{0\}$,

$$\beta^3 D_4(\kappa(x), \gamma^3) = \beta_1^4 D_4 \left(\frac{x}{\beta_1}, \frac{(\hat{B}+2)\hat{a}}{4\beta_1^2} \right) - \frac{\hat{a}^2(\hat{B}-2)^2}{8}. \quad (5.11)$$

Since $D_4(x, a) = x^4 - 4ax^2 + 2a^2$ is an even polynomial, we have $\kappa(x) = \beta_0 x$ with $\beta_0 \in \mathbb{Q}$. We now compare the coefficients of x^4 , x^2 and x^0 on both sides of (5.11). This gives the system of equations $\beta^3 \beta_0^4 = 1$, $-4\beta^3 \gamma^3 \beta_0^2 = -(\hat{B}+2)\hat{a}$ and $2\beta^3 \gamma^6 = \hat{a}^2 \hat{B}$, which has no solution for $\hat{a} \neq 0$ and $\hat{B} \neq 2$, a contradiction. Now, let $\hat{B} = 2$. Since by the well-known identity [3, eq. (6)], $D_m(x, \hat{a}) = \kappa_1^{-m} D_m(\kappa_1 x, \kappa_1^2 \hat{a})$, we get the solution $n = 3$, $\gcd(m, 3) = 1$, $(B+1)a = 3\beta^2 \gamma^m$, $\hat{a} = \gamma^3 \kappa_1^{-2}$ where $\beta, \gamma, \kappa_1 \in \mathbb{Q} \setminus \{0\}$ with $\beta^3 = \kappa_1^{-m}$ (Solution (III)).

Case (iv): By Proposition 4.5 we have $f_m^{(\hat{a}, \hat{B})}(x) = \gamma \kappa(x)^r v(x)^3$ with $\deg v \leq 1$. Since $\deg v = 0$ implies $m \leq 2$, a contradiction, we have $f_m^{(\hat{a}, \hat{B})}(x) = \gamma \kappa(x)^r (\beta_1 x + \beta_0)^3$ for some $\gamma, \beta_1, \beta_0 \in \mathbb{Q}$. But this is impossible by Proposition 4.5 and parity considerations for $m = r + 3$.

Case (v): Let $\hat{B} \neq 2$. Similarly to Case (iii) above, we get $m \leq 4$ and $m = 3$ by $\gcd(m, 4) = 1$. We conclude by (5.4) that for some $\beta_1 \in \mathbb{Q}$,

$$\beta^4 D_3(\kappa(x), \gamma^4) - \frac{a^2(B-2)^2}{8} = \beta_1^3 D_3\left(\frac{x}{\beta_1}, \frac{(\hat{B}+1)\hat{a}}{3\beta_1^2}\right). \quad (5.12)$$

However, since $D_3(x, a) = x^3 - 3ax$ is odd, the constant term in (5.12) vanishes if and only if $a = 0$ or $B = 2$, a contradiction. Since $\gcd(m, 4) = 1$ implies m odd, the same argument works also for $\hat{B} = 2$.

Case (vi): Again, if $\hat{B} \neq 2$, then $m \leq 4$, which contradicts $\gcd(m, 4) = 2$ and $m \geq 3$. If $\hat{B} = 2$ and $m \geq 6$, then the identity $D_m(x, \hat{a}) = \kappa_1^{-m} D_m(\kappa_1 x, \kappa_1^2 \hat{a})$ implies $-a^2(B-2)^2/8 = 0$ which is a contradiction.

Case (vii): By Proposition 4.5 we have $f_m^{(\hat{a}, \hat{B})}(x) = \gamma \kappa(x)^r v(x)^4$ with $\deg v = 0$, $r = 3$ such that $f_m^{(\hat{a}, \hat{B})}(x) = \hat{\gamma}(\beta_1 x)^3$ for some $\hat{\gamma}, \beta_1 \in \mathbb{Q}$. Hence $m = 3$ and $\hat{B} = -1$ and since $x^3 = y^4 - 2a^2$ has genus three there are only finitely many rational solutions with a bounded denominator in this case by Siegel's theorem.

Case (viii): In this case we have $f_m^{(\hat{a}, \hat{B})}(x) = \kappa(x)^4 - 4a^2 \kappa(x)^2 - 2a^4$, thus $m = 4$. By symmetry we have $\kappa(x) = \beta_1 x$ for some $\beta_1 \in \mathbb{Q}$. Comparing coefficients gives $\beta_1^4 = 1$, $-(\hat{B} + 2)\hat{a} = -4a^2 \beta_1^2$ and $\hat{a}^2 \hat{B} = -2a^4$, which yields $\hat{B} = -6 \pm 4\sqrt{2} \notin \mathbb{Q}$, a contradiction.

This finishes the investigation for $a, \hat{a} \neq 0$, $B \neq 2$.

Note that the case $a = \hat{a} = 0$ is trivial (Solution (V)). Suppose $\hat{a} = 0$ and $a \neq 0$. Then by Siegel's theorem and Proposition 4.5 we have

$$(n, B) \in \{(3, -1), (4, 0), (5, -1/2)\}.$$

Obviously, for $n = 3$, $B = -1$ the associated curve $x^m = y^3$ allows infinitely many rational solutions with a bounded denominator (Solution (VI)). Let $n = 4$, $B = 0$, namely, consider the equation $x^m = f_4^{(a, 0)}(y) = y^4 - 2ay^2$. Up to equivalence, we have the only decompositions

$$f_4^{(a, 0)}(y) = y \circ (y^4 - 2ay^2) = (y^2 - 2ay) \circ y^2 = (y^4 - 2ay^2) \circ y.$$

By $a \neq 0$, the left components of the second and third decomposition have at least two different roots, respectively. On the other hand, any left component of a decomposition of x^m can only have one (multiple) root. Therefore, by Theorem 1.1, we have $\deg \varphi = 1$ and we now directly exclude the only possible standard pair of the first kind with $m \geq 3$. Therefore, the equation $x^m = y^4 - 2ay^2$ has only finitely many rational solutions with a bounded denominator. We similarly conclude for the case $n = 5$, $B = -1/2$.

We finally consider the case where $B = \hat{B} = 2$ and $a, \hat{a} \neq 0$, i.e., the Diophantine equation

$$D_n(x, a) = D_m(y, \hat{a}).$$

This equation has infinitely many solutions with a bounded denominator if and only if $a^t = \hat{a}^s$ where $s, t \in \mathbb{Z}^+$ with $mt = ns$ (Solution (IV)).

This completes the proof of Theorem 2.3. □

References

- [1] Y. Bilu, Th. Stoll, R. F. Tichy, *Octahedrons with equally many lattice points*, Period. Math. Hungar. **40** (2000), no. 2, 229–238. MR1805319 (2001k:11192)
- [2] Y. Bilu, B. Brindza, P. Kirschenhofer, Á. Pintér, R. F. Tichy, *Diophantine equations and Bernoulli polynomials*, with an appendix by A. Schinzel, Compositio Math. **131** (2002), no. 2, 173–188. MR1898434 (2003a:11025)
- [3] Y. Bilu and R. F. Tichy, *The Diophantine equation $f(x) = g(y)$* , Acta Arith. **95** (2000), 261–288. MR1793164 (2001i:11031)
- [4] F. Binder, *Polynomial decomposition*, Master’s thesis, University of Linz, June 1995, available at: <http://www.algebra.uni-linz.ac.at/~xbx>.
- [5] T. S. Chihara, *An introduction to orthogonal polynomials*, Mathematics and its Applications, vol. **13**, Gordon and Breach Science Publishers, New York-London-Paris, 1978. MR0481884 (58 #1979)
- [6] A. Dujella and I. Gusić, *Indecomposability of polynomials and related Diophantine equations*, Q. J. Math. **57** (2006), 193–201.
- [7] A. Dujella and I. Gusić, *Decomposition of a recursive family of polynomials*, Monatsh. Math., to appear, available at: <http://web.math.hr/~duje>.
- [8] 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.
- [9] 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)
- [10] P. Kirschenhofer and O. Pfeiffer, *On a class of combinatorial Diophantine equations*, Sém. Lothar. Combin. **44** (2000), Art. B44h, 7 pp. (electronic). MR1814861 (2001m:05017)
- [11] P. Kirschenhofer and O. Pfeiffer, *Diophantine equations between polynomials obeying second order recurrences*, Period. Math. Hungar. **47** (2003), no. 1-2, 119–134. MR2025618 (2004k:11034)
- [12] M. Kulkarni and B. Sury, *On the Diophantine equation $x(x+1)(x+2)\dots(x+(m-1)) = g(y)$* , Indag. Math. (N.S.) **14** (2003), no. 1, 35–44. MR2015597 (2005b:11033)
- [13] M. Kulkarni and B. Sury, *Diophantine equations with Bernoulli polynomials*, Acta Arith. **116** (2005), no. 1, 25–34. MR2114902 (2005i:11038)
- [14] M. Kulkarni and B. Sury, *A class of Diophantine equations involving Bernoulli polynomials*, Indag. Math. (N.S.) **16** (2005), no. 1, 51–65. MR2138050 (2005m:11047)
- [15] M. Kulkarni and B. Sury, *On the Diophantine equation $1 + x + x^2/2! + \dots + x^n/n! = g(y)$* , Proceedings of the Int. Conf. on Diophantine equations on the occasion of the 60th birthday of T.N.Shorey, TIFR Mumbai, December 2005, to appear, available at: <http://www.isibang.ac.in/~sury>.
- [16] 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)
- [17] V. V. Prasolov, *Polynomials*, translated from the 2001 Russian second edition by Dimitry Leites. Algorithms and Computation in Mathematics, Springer, Berlin, 2004. MR2082772 (2005f:12001)
- [18] Cs. Rakaczki, *On the Diophantine equation $x(x-1)\dots(x-(m-1)) = \lambda y(y-1)\dots(y-(n-1)) + l$* , Acta Arith. **110** (2003), no. 4, 339–360. MR2011314 (2004k:11036)
- [19] Cs. Rakaczki, *On the Diophantine equation $F\binom{x}{n} = b\binom{y}{m}$* , Period. Math. Hungar. **49** (2004), no. 2, 119–132. MR2107991 (2005g:11046)
- [20] Cs. Rakaczki, *On the Diophantine equation $S_m(x) = g(y)$* , Publ. Math. Debrecen **65** (2004), no. 3-4, 439–460. MR2107960 (2005h:11067)
- [21] 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
- [22] J. F. Ritt, *Equivalent rational substitutions*, Trans. Amer. Math. Soc. **26** (1924), no. 2, 221–229. MR1501274
- [23] A. Schinzel, *Selected Topics on Polynomials*, Ann Arbor, University of Michigan Press, 1982. MR0649775 (84k:12010)

- [24] A. Schinzel, *Polynomials with special regard to reducibility*, Encyclopedia of Mathematics and its Applications **77**, Cambridge University Press, 2000. MR1770638 (2001h:11135)
- [25] C. L. Siegel, *Über einige Anwendungen Diophantischer Approximationen*, Abh. Preuss. Akad. Wiss. Phys.-Math. Kl. (1929), no. 1, 209–266.
- [26] 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)
- [27] Th. Stoll and R. F. Tichy, *The Diophantine equation $\alpha\binom{x}{m} + \beta\binom{y}{n} = \gamma$* , Publ. Math. Debrecen **64** (2004), no. 1-2, 155–165. MR2035894 (2004m:11042)
- [28] Th. Stoll and R. F. Tichy, *Diophantine equations involving general Meixner and Krawtchouk polynomials*, Quaest. Math. **28**, no. 1 (2005), 105–115. MR2136185 (2005m:11051)
- [29] Th. Stoll and R. F. Tichy, *Diophantine equations for Morgan-Voyce and other modified orthogonal polynomials*, Math. Slovaca, to appear, available at:
<http://dmg.tuwien.ac.at/stoll>.
- [30] Th. Stoll, *Calculation addendum*, available at:
<http://dmg.tuwien.ac.at/stoll>.
- [31] Th. Stoll, *Decomposition of perturbed Chebyshev polynomials*, preprint, available at:
<http://dmg.tuwien.ac.at/stoll>.
- [32] G. Szegő, *Orthogonal polynomials*, American Mathematical Society Colloquium Publications, vol. **23**, Fourth edition, Providence, R.I., 1975. MR0372517 (51 #8724)
- [33] E. W. Weisstein, *Mathworld, a Wolfram Web Resource*,
<http://mathworld.wolfram.com>, 1999–2007.