COMPOSITIO MATHEMATICA

Generalized 'second Ritt theorem' and explicit solution of the polynomial moment problem

F. Pakovich

Compositio Math. **149** (2013), 705–728.

doi:10.1112/S0010437X12000620

FOUNDATION
COMPOSITIO
MATHEMATICA

LONDON
MATHEMATICAL
SOCIETY

Compositio Math. 149 (2013) 705–728
doi:10.1112/S0010437X12000620

Generalized 'second Ritt theorem' and explicit solution of the polynomial moment problem

F. Pakovich

Abstract

In the recent paper by Pakovich and Muzychuk [*Solution of the polynomial moment problem*, Proc. Lond. Math. Soc. (3) **99** (2009), 633–657] it was shown that any solution of 'the polynomial moment problem', which asks to describe polynomials Q orthogonal to all powers of a given polynomial P on a segment, may be obtained as a sum of so-called 'reducible' solutions related to different decompositions of P into a composition of two polynomials of lower degrees. However, the methods of that paper do not permit us to estimate the number of necessary reducible solutions or to describe them explicitly. In this paper we provide a description of polynomial solutions of the functional equation $P_1 \circ W_1 = P_2 \circ W_2 = \cdots = P_r \circ W_r$, and on this base describe solutions of the polynomial moment problem in an explicit form suitable for applications.

1. Introduction

About a decade ago, in the series of papers [BFY98, BFY99, BFY00a, BFY00b] the following 'polynomial moment problem' was posed: for a given complex polynomial P and complex numbers a, b describe polynomials Q satisfying the system of equations

$$\int_a^b P^k \, dQ = 0, \quad k \geqslant 0. \tag{1}$$

Despite its rather classical and simple setting this problem turned out to be quite difficult and was intensively studied in many recent papers (see, e.g., [BFY99, BFY00a, BFY00b, BFY01, Chr00, Pak03b, Pak02, Pak03a, Pak04, Pak05, PM09, PRY04, Roy01]).

The main motivation for the study of the polynomial moment problem is its relation with the center problem for the Abel differential equation

$$\frac{dy}{dz} = p(z)y^2 + q(z)y^3 \tag{2}$$

with polynomial coefficients p, q in the complex domain. For given $a, b \in \mathbb{C}$ the center problem for the Abel equation is to find necessary and sufficient conditions on p, q which imply the equality $y(b) = y(a)$ for any solution $y(z)$ of (2) with $y(a)$ small enough. This problem is closely related to the classical center-focus problem of Poincaré and has been studied in many recent papers (see e.g. [BBY05, BFY98, BFY99, BFY00a, BFY00b, BFY01, BRY10, BY05, Chr00, Yom03]).

The interrelation between the center problem for the Abel equation and the polynomial moment problem is provided by the result of [BRY10] which states that 'at infinity' (under an

Received 9 October 2011, accepted in final form 8 May 2012, published online 29 January 2013.
2010 Mathematics Subject Classification 30E99 (primary), 14H30, 34C99 (secondary).
Keywords: polynomial moment problem, second Ritt theorem, polynomial decompositions, center problem.
This research was supported by ISF, Grant 639/09.

appropriate projectivization of the parameter space) the system of equations on coefficients of p and q describing the center set of (2) reduces to (1), where

$$P(z)=\int p(z)\,dz,\quad Q(z)=\int q(z)\,dz. \tag{3}$$

Notice also that for the parametric version

$$\frac{dy}{dz}=p(z)y^2+\varepsilon q(z)y^3$$

of (2) the 'infinitesimal' center conditions with respect to ε also reduce to (1), where P and Q are defined as above (see [BFY00a]). Other results relating the center problem and the polynomial moment problem may be found in [BRY10].

There exists a natural condition on P and Q which reduces (1) and (2) to similar equations with respect to polynomials of lower degrees. Namely, suppose that there exist polynomials $\widetilde{P},\widetilde{Q},W$, $\deg W>1$, such that

$$P=\widetilde{P}\circ W,\quad Q=\widetilde{Q}\circ W, \tag{4}$$

where the symbol $\circ$ denotes a superposition of functions: $f_1\circ f_2=f_1(f_2)$. Then after the change of variable $z\to W(z)$ the equations (1) transform to the equations

$$\int_{W(a)}^{W(b)}\widetilde{P}^k\,d\widetilde{Q}=0,\quad k\geqslant 0, \tag{5}$$

while (2) transforms to the equation

$$\frac{d\widetilde{y}}{dw}=\widetilde{P}'(w)\widetilde{y}^2+\widetilde{Q}'(w)\widetilde{y}^3. \tag{6}$$

Further, if the polynomial W in (4) satisfies the equality

$$W(a)=W(b), \tag{7}$$

then it follows from the Cauchy theorem that all integrals in (5) vanish, implying that all integrals in (1) also vanish. Similarly, since any solution $y(z)$ of (2) is the pull-back

$$y(z)=\widetilde{y}(W(z))$$

of a solution $\widetilde{y}(w)$ of (6), if W satisfies (7), then (2) has a center. A center for (2) or a solution of system (1) is called *reducible* if there exist polynomials $\widetilde{P},\widetilde{Q},W$ such that conditions (4), (7) hold. The main conjecture concerning the center problem for the Abel equation ('the composition conjecture for the Abel equation') states that any center for the Abel equation is reducible (see [BRY10] and the bibliography therein).

By analogy with the composition conjecture for the Abel equation it was suggested ('the composition conjecture for the polynomial moment problem') that any solution of (1) is reducible. This conjecture was shown to be true in many cases. For instance, it is true if a,b are not critical points of P [Chr00], if P is indecomposable (that is P cannot be represented as a composition of two polynomials of lower degrees [Pak03a]), and in some other special cases (see e.g. [BFY00a, Pak05, PRY04, Roy01]). Nevertheless, in general the composition conjecture for the polynomial moment problem fails to be true.

A class of counterexamples to the composition conjecture for the polynomial moment problem was constructed in [Pak02]. These counterexamples use polynomials P which admit 'double

decompositions' of the form

$$P = P_1 \circ W_1 = P_2 \circ W_2, \tag{8}$$

where P_1, P_2, W_1, W_2 are non-linear polynomials. If P is such a polynomial and, in addition, the equalities

$$W_1(a) = W_1(b), \quad W_2(a) = W_2(b)$$

hold, then for any polynomials V_1, V_2 the polynomial

$$Q = V_1 \circ W_1 + V_2 \circ W_2$$

satisfies (1) by linearity. On the other hand, it can be shown (see [Pak02]) that if $\deg W_1$ and $\deg W_2$ are coprime, then condition (4) is not satisfied already for $Q = W_1 + W_2$.

Notice that the description of polynomial solutions of (8) reduces to the case where

$$\mathrm{GCD}(\deg P_1, \deg P_2) = 1, \quad \mathrm{GCD}(\deg W_1, \deg W_2) = 1. \tag{9}$$

Namely, if P_1, P_2, W_1, W_2 are polynomials such that (8) holds, then there exist polynomials $U, V, \widetilde{P}_1, \widetilde{P}_2, \widetilde{W}_1, \widetilde{W}_2$, where

$$\deg U = \mathrm{GCD}(\deg P_1, \deg P_2), \quad \deg V = \mathrm{GCD}(\deg W_1, \deg W_2),$$

such that

$$P_1 = U \circ \widetilde{P}_1, \quad P_2 = U \circ \widetilde{P}_2, \quad W_1 = \widetilde{W}_1 \circ V, \quad W_2 = \widetilde{W}_2 \circ V,$$

and

$$\widetilde{P}_1 \circ \widetilde{W}_1 = \widetilde{P}_2 \circ \widetilde{W}_2$$

(see Theorem 2.1 below). On the other hand, polynomial solutions of (8) satisfying (9) are described explicitly by the so-called 'second Ritt theorem', which states that for any such solution there exist polynomials $\nu, \mu, \sigma_1, \sigma_2$ of degree one such that up to a possible replacement of P_1 by P_2 and W_1 by W_2 either

$$P_1 = \nu \circ z^n \circ \sigma_1^{-1}, \qquad W_1 = \sigma_1 \circ z^s R(z^n) \circ \mu, \tag{10}$$

$$P_2 = \nu \circ z^s R^n(z) \circ \sigma_2^{-1}, \quad W_2 = \sigma_2 \circ z^n \circ \mu, \tag{11}$$

where R is a polynomial and $s \geqslant 0$, or

$$P_1 = \nu \circ T_n \circ \sigma_1^{-1}, \quad W_1 = \sigma_1 \circ T_m \circ \mu, \tag{12}$$

$$P_2 = \nu \circ T_m \circ \sigma_2^{-1}, \quad W_2 = \sigma_2 \circ T_n \circ \mu, \tag{13}$$

where T_n, T_m are the Chebyshev polynomials.

It was conjectured in [Pak03b] that any solution of (1) can be represented as a *sum* of reducible ones, and recently this conjecture was proved in [PM09]. In more detail, it was proved in [PM09] that non-zero polynomials P, Q satisfy system (1) if and only if

$$Q = \sum_{i=1}^{r} Q_i \tag{14}$$

where Q_i, $1 \leqslant i \leqslant r$, are polynomials such that

$$P = P_i \circ W_i, \quad Q_i = V_i \circ W_i, \quad W_i(a) = W_i(b) \tag{15}$$

for some polynomials P_i, V_i, W_i, $1 \leqslant i \leqslant r$. Although this result in a sense solves the problem, it does not provide any explicit description of polynomials P and Q satisfying (14), (15). On the

other hand, in view of the results of [BRY10] relating (1) with the center equations for the Abel equation, such a description would be highly desirable.

The problem of the explicit description of the solutions of the polynomial moment problem naturally leads to the following two problems.

First, since the number r in (14) may be greater than 2, it is necessary to give a description of polynomial solutions of the equation

$$P_1 \circ W_1 = P_2 \circ W_2 = \cdots = P_r \circ W_r \tag{16}$$

for $r > 2$. Notice that, in the same way as in the case $r = 2$, this problem reduces to the case where

$$\mathrm{GCD}(\deg P_1, \deg P_2, \dots, \deg P_r) = 1, \tag{17}$$

and

$$\mathrm{GCD}(\deg W_1, \deg W_2, \dots, \deg W_r) = 1 \tag{18}$$

(see Theorem 3.1 below). However, since conditions (17), (18) do not imply that the degrees of polynomials P_i, $1 \leqslant i \leqslant r$, as well as of Q_i, $1 \leqslant i \leqslant r$, are *pairwise* coprime, the Ritt theorem cited above does not provide any immediate information about solutions of (16)–(18).

Second, since a solution of the polynomial moment problem may be represented in the form of a sum of reducible solutions not in a unique way, it is desirable to find a canonical form for such a representation, in particular, to find a representation for which the number r is minimal.

In this paper we solve both problems above. Our first result is an analogue of the second Ritt theorem for the functional equation (16). Recall that two polynomials U, V are called linearly equivalent if $U = \mu \circ V \circ \nu$ for some polynomials μ, ν of degree one.

Theorem 1.1. *Let P_i, W_i, $1 \leqslant i \leqslant r$, be polynomials satisfying (16). If, additionally, (17) holds, then at least one P_i, $1 \leqslant i \leqslant r$, is linearly equivalent either to a Chebyshev polynomial or to a power. Similarly, if (18) holds, then at least one W_i, $1 \leqslant i \leqslant r$, is linearly equivalent either to a Chebyshev polynomial or to a power.*

Notice that although in distinction with the second Ritt theorem this result does not provide a full description of all polynomials involved in (16), it still implies their 'partial' description sufficient for applications (see § 4.1).

Theorem 1.1 permits us to bound the number of necessary reducible solutions in the representation $Q = \sum_{i=1}^{r} Q_i$ and to show that, roughly speaking, any non-reducible solution of the polynomial moment problem may be represented either as a sum of two reducible solutions related to double decomposition (8), where P_1, P_2, W_1, W_2 are given by (10)–(13), or as a sum of three reducible solutions related to the 'triple' decomposition

$$P_1 \circ W_1 = P_2 \circ W_2 = P_3 \circ W_3, \tag{19}$$

with

$$W_1 = T_{2n}, \quad W_2 = T_{2m}, \quad W_3 = zR(z^2) \circ T_{mn},$$

and

$$P_1 = \frac{z+1}{2} R^2\left(\frac{z+1}{2}\right) \circ T_m, \quad P_2 = \frac{z+1}{2} R^2\left(\frac{z+1}{2}\right) \circ T_n, \quad P_3 = z^2,$$

where R is an arbitrary polynomial (see § 4.2).

Theorem 1.2. *Let P, Q be non-constant complex polynomials and a, b distinct complex numbers such that the equalities in (1) hold. Then, either Q is a reducible solution of (1), or there exist polynomials P_i, Q_i, V_i, W_i, $1 \leqslant i \leqslant r$, such that*

$$Q = \sum_{i=1}^{r} Q_i, \quad P = P_i \circ W_i, \quad Q_i = V_i \circ W_i, \quad W_i(a) = W_i(b),$$

and one of the following conditions holds:

(i) $r = 2$ *and*

$$P = U \circ z^{sn} R^n(z^n) \circ V, \quad W_1 = z^n \circ V, \quad W_2 = z^s R(z^n) \circ V,$$

where R, U, V are polynomials, $n > 1$, $s > 0$, $\mathrm{GCD}(s, n) = 1$;

(ii) $r = 2$ *and*

$$P = U \circ T_{nm} \circ V, \quad W_1 = T_n \circ V, \quad W_2 = T_m \circ V,$$

where U, V are polynomials, $n > 1$, $m > 1$, $\mathrm{GCD}(m, n) = 1$;

(iii) $r = 3$ *and*

$$P = U \circ z^2 R^2(z^2) \circ T_{m_1 m_2} \circ V,$$
$$W_1 = T_{2m_1} \circ V, \quad W_2 = T_{2m_2} \circ V, \quad W_3 = (zR(z^2) \circ T_{m_1 m_2}) \circ V,$$

where R, U, V are polynomials, $m_1 > 1, m_2 > 1$ are odd, and $\mathrm{GCD}(m_1, m_2) = 1$.

The paper is organized as follows. In the second section we recall the description of polynomial solutions of (8). In the third section we prove Theorem 1.1. In the fourth section we establish an analogue of the second Ritt theorem for (19). Finally, in the fifth section we show that for any polynomial P and $a, b \in \mathbb{C}$ the minimal number r of compositional right factors W_i, $1 \leqslant i \leqslant r$, of P such that $W_i(a) = W_i(b)$, $1 \leqslant i \leqslant r$, and any compositional right factor W of P satisfying $W(a) = W(b)$ is a polynomial in one of W_i, $1 \leqslant i \leqslant r$, does not exceed three, and prove Theorem 1.2.

2. Polynomial solutions of $P_1 \circ W_1 = P_2 \circ W_2$

2.1 Imprimitivity systems and decompositions of rational functions

In this subsection we recall some definitions, related to decompositions of a rational function F into a composition of rational functions of lower degrees, and the fundamental correspondence between equivalence classes of decompositions of F and imprimitivity systems of the monodromy group of F. For a more detailed account of algebraic structures related to decompositions of rational functions see e.g. [MP11, § 2.1].

Let $G \subseteq S_n$ be a transitive permutation group acting on the set $X = \{1, 2, \dots, n\}$. A subset B of X is called a *block* of G if for each $g \in G$ the set B^g is either disjoint or equal to B (see e.g. [Wie64]). For a block B the sets B^g, $g \in G$, form a partition of X into a disjoint union of blocks of equal cardinality, which is called an *imprimitivity system* of G. If F is a rational function, then the *monodromy group* G_F of F is defined as a permutation group acting on the set $F^{-1}\{z_0\}$, where z_0 is a regular value of F and the action is induced by the analytical continuation of branches of the algebraic function inverse to F.

The structure of decompositions of a rational function F into a composition of rational functions of lower degrees is defined by the structure of imprimitivity systems of its monodromy group G_F. Namely, if $F = A \circ B$ is a decomposition of F and $x_1, x_2, \dots, x_r$ are preimages of z_0

under the map $A:\mathbb{CP}^1\to\mathbb{CP}^1$, then the sets $X_i=B^{-1}\{x_i\}$, $1\leqslant i\leqslant r$, form an imprimitivity system $\mathcal{E}$ of G_F corresponding to the decomposition $A\circ B$. Furthermore, if $\mathcal{E}$ and $\widetilde{\mathcal{E}}$ are imprimitivity systems corresponding to the decompositions $A\circ B$ and $\widetilde{A}\circ\widetilde{B}$ of F respectively, then $\widetilde{\mathcal{E}}$ is a refinement of $\mathcal{E}$ if and only if there exists a rational function U such that

$$\widetilde{A}=A\circ U,\quad U\circ\widetilde{B}=B.$$

In particular, $\mathcal{E}=\widetilde{\mathcal{E}}$ if and only if there exists a rational function of degree one μ such that

$$\widetilde{A}=A\circ\mu,\quad \widetilde{B}=\mu^{-1}\circ B. \tag{20}$$

In the last case the decompositions $F=A\circ B$ and $F=\widetilde{A}\circ\widetilde{B}$ are called equivalent.

It is easy to see that any decomposition $F=A\circ B$ of a *polynomial* F into a composition of rational functions is equivalent to a decomposition $F=\widetilde{A}\circ\widetilde{B}$, where $\widetilde{A}$, $\widetilde{B}$ are *polynomials*. Taking into account this fact, we will always assume below that all the functions considered are polynomials and will use the following modification of the general definition of equivalence: two decompositions of a polynomial F into a composition of polynomials $F=A\circ B$ and $F=\widetilde{A}\circ\widetilde{B}$ are called equivalent if there exists a polynomial of degree one μ such that (20) holds. Clearly, under this notation the correspondence between equivalence classes of decompositions of a polynomial F and imprimitivity systems of the monodromy group of F remains true.

2.2 Reduction and the second Ritt theorem

The description of polynomial solutions of the equation

$$P_1\circ W_1=P_2\circ W_2 \tag{21}$$

may be reduced to the case where

$$\mathrm{GCD}(\deg P_1,\deg P_2)=1,\quad \mathrm{GCD}(\deg W_1,\deg W_2)=1 \tag{22}$$

owing to the statement given below. Since in the following we will need a generalization of this statement, we provide its complete proof.

Theorem 2.1 [Eng41, Tor88]. *Let P_1,P_2,W_1,W_2 be polynomials such that (21) holds. Then there exist polynomials $U,V,\widetilde{P}_1,\widetilde{P}_2,\widetilde{W}_1,\widetilde{W}_2$, where*

$$\deg U=\mathrm{GCD}(\deg P_1,\deg P_2),\quad \deg V=\mathrm{GCD}(\deg W_1,\deg W_2),$$

such that

$$P_1=U\circ\widetilde{P}_1,\quad P_2=U\circ\widetilde{P}_2,\quad W_1=\widetilde{W}_1\circ V,\quad W_2=\widetilde{W}_2\circ V,$$

and

$$\widetilde{P}_1\circ\widetilde{W}_1=\widetilde{P}_2\circ\widetilde{W}_2.$$

Proof. Set $P=P_1\circ W_1=P_2\circ W_2$. Since P is a polynomial, its monodromy group G_P contains a cycle σ of length $n=\deg P$, corresponding to a loop around infinity, and without loss of generality we may assume that this cycle coincides with the cycle $\sigma=(12\cdots n)$. Furthermore, since any σ-invariant partition of the set $\{1,2,\dots,n\}$ coincides with the set I_d consisting of residue classes modulo d for some $d|n$, any imprimitivity system of G_P also has such a form. In view of the correspondence between decompositions of P and imprimitivity systems of G_P this implies easily that in order to prove the theorem it is enough to show that if I_{d_1} and I_{d_2} are imprimitivity systems of G_P for some divisors d_1,d_2 of n, then the sets $I_{\mathrm{LCM}(d_1,d_2)}$ and $I_{\mathrm{GCD}(d_1,d_2)}$ also are imprimitivity systems of G_P.

In order to prove the first part of the last statement observe that for any element $x \in X$ the intersection of two blocks B_1, B_2 containing x obviously is a block and, if $B_1 \in I_{d_1}$, $B_2 \in I_{d_2}$, then $B_1 \cap B_2$ coincides with a residue class modulo $\mathrm{LCM}(d_1, d_2)$. The easiest way to prove the second part is to observe that I_d is an imprimitivity system for G_P if and only if the d-dimensional subspace V_d of $\mathbb{C}^n$, consisting of vectors whose coordinates are d-periodical, is invariant with respect to the permutation representation ρ_{G_P} of G_P on $\mathbb{C}^n$, where by definition for $g \in G_P$ and $\vec{v} = (a_1, a_2, \dots, a_n)$ the vector $\vec{v}^g$ is defined by the formula $\vec{v}^g = (a_{1^g}, a_{2^g}, \dots, a_{n^g})$ (see [PM09, § 3.1]). Clearly, if V_{d_1} and V_{d_2} are ρ_{G_P}-invariant, then the subspace $V_{d_1} \cap V_{d_2}$ also is ρ_{G_P}-invariant. On the other hand, it is easy to see that $V_{d_1} \cap V_{d_2} = V_{\mathrm{GCD}(d_1,d_2)}$. □

Let us mention the following well-known corollaries of Theorem 2.1.

Corollary 2.2. *Let P_1, P_2, W_1, W_2 be polynomials such that (21) holds. Assume additionally that $\deg W_1 | \deg W_2$ or equivalently that $\deg P_2 | \deg P_1$. Then there exists a polynomial S such that*

$$P_1 = P_2 \circ S, \quad W_2 = S \circ W_1.$$

In particular, if $\deg W_1 = \deg W_2$, then there exists a polynomial μ of degree one such that

$$P_1 = P_2 \circ \mu, \quad W_1 = \mu^{-1} \circ W_2.$$

Proof. Indeed, if $\deg W_1 | \deg W_2$, then the degree of the polynomial $\widetilde{W}_1$ from Theorem 2.1 is one and hence the equality $W_2 = S \circ W_1$ holds for $S = \widetilde{W}_2 \circ \widetilde{W}_1^{-1}$. Now the equality

$$P_1 \circ W_1 = P_2 \circ W_2 = P_2 \circ S \circ W_1$$

implies that $P_1 = P_2 \circ S$. □

Recall that the Chebyshev polynomials may be defined by the formula

$$T_n(\cos \varphi) = \cos n\varphi, \quad n \geqslant 1. \tag{23}$$

Notice that this definition implies that all critical points of T_n are simple and real. Furthermore, it implies the equalities

$$T_n(-z) = (-1)^n T_n(z), \quad n \geqslant 1, \tag{24}$$

and

$$T_{mn} = T_m \circ T_n = T_n \circ T_m, \quad n, m \geqslant 1.$$

Corollary 2.3. *Let P_1, W_1 be polynomials such that $P_1 \circ W_1 = z^n$. Then there exists a polynomial μ of degree one such that*

$$P_1 = z^d \circ \mu, \quad W_1 = \mu^{-1} \circ z^{n/d}$$

for some $d|n$. Similarly, if $P_1 \circ W_1 = T_n$, then there exists a polynomial μ of degree one such that

$$P_1 = T_d \circ \mu, \quad W_1 = \mu^{-1} \circ T_{n/d}$$

for some $d|n$.

Proof. Clearly, any of the equalities $P_1 \circ W_1 = z^n$ and $P_1 \circ W_1 = T_n$ implies that $d = \deg P_1$ is a divisor of n. On the other hand, for any $d|n$, the equalities

$$z^n = z^d \circ z^{n/d}, \quad T_n = T_d \circ T_{n/d}$$

hold. Therefore, Corollary 2.3 follows from Corollary 2.2 applied to the equalities $P_1 \circ W_1 = T_d \circ T_{n/d}$ and $P_1 \circ W_1 = z^d \circ z^{n/d}$. □

An explicit description of polynomials satisfying (21) and (22) is given by the following statement, known as the second Ritt theorem (see [Rit22] as well as [BT00, Fri73, Pak09, Sch82, Tor88, Zan93, ZM08]).

Theorem 2.4 [Rit22]. *Let P_1, P_2, W_1, W_2 be polynomials such that (21) and (22) hold. Then there exist polynomials $\sigma_1, \sigma_2, \mu, \nu$ of degree one such that, up to a possible replacement of P_1 by P_2 and W_1 by W_2, either*

$$P_1 = \nu \circ z^s R^n(z) \circ \sigma_1^{-1}, \quad W_1 = \sigma_1 \circ z^n \circ \mu, \tag{25}$$

$$P_2 = \nu \circ z^n \circ \sigma_2^{-1}, \quad W_2 = \sigma_2 \circ z^s R(z^n) \circ \mu, \tag{26}$$

where R is a polynomial, $n \geqslant 1$, $s \geqslant 0$, and $\mathrm{GCD}(s, n) = 1$, or

$$P_1 = \nu \circ T_m \circ \sigma_1^{-1}, \quad W_1 = \sigma_1 \circ T_n \circ \mu, \tag{27}$$

$$P_2 = \nu \circ T_n \circ \sigma_2^{-1} \quad W_2 = \sigma_2 \circ T_m \circ \mu, \tag{28}$$

where T_n, T_m are the Chebyshev polynomials, $n, m \geqslant 1$, and $\mathrm{GCD}(n, m) = 1$.

We will call solutions of the first type provided by Theorem 2.4 *cyclic* and solutions of the second type *dihedral*. Notice that any solution of the form (27), (28) with $m = 2$ is dihedral and cyclic at the same time. Indeed, (24) implies that for odd n the equality

$$T_n(z) = zE_n(z^2) \tag{29}$$

holds for some polynomial E_n. Furthermore, $T_2 = \theta \circ z^2$, where $\theta = 2z - 1$, and hence

$$zE_n(z^2) \circ \theta \circ z^2 = T_n \circ T_2 = T_2 \circ T_n = \theta \circ T_n^2 = \theta \circ zE_n^2(z) \circ z^2.$$

Since the last equality implies the equality

$$zE_n(z^2) \circ \theta = \theta \circ zE_n^2(z),$$

we conclude that

$$T_n = \theta \circ zE_n^2(z) \circ \theta^{-1}, \quad T_{2n} = \theta \circ z^2 E_n^2(z^2). \tag{30}$$

Therefore, the equality

$$T_n \circ T_2 = T_2 \circ T_n$$

may be written in the form

$$(\theta \circ zE_n^2(z) \circ \theta^{-1}) \circ (\theta \circ z^2) = (\theta \circ z^2) \circ zE_n(z^2). \tag{31}$$

Actually, any solution of (21) and (22) which is cyclic and dihedral at the same time has the form (27), (28) with $m \leqslant 2$. Indeed, since all critical points of T_m are simple, T_m may not be linearly equivalent to z^m for $m > 2$.

3. Polynomial solutions of $P_1 \circ W_1 = P_2 \circ W_2 = \cdots = P_r \circ W_r$

3.1 Reduction to the case of coprime degrees

Similarly to the description of the solutions of (21), the description of the solutions of the equation

$$P_1 \circ W_1 = P_2 \circ W_2 = \cdots = P_r \circ W_r, \tag{32}$$

where P_i, W_i, $1 \leqslant i \leqslant r$, are polynomials of degrees p_i, w_i, $1 \leqslant i \leqslant r$, respectively, reduces to the case where

$$\mathrm{GCD}(p_1, p_2, \ldots, p_r) = 1, \tag{33}$$

and

$$\mathrm{GCD}(w_1, w_2, \dots, w_r) = 1. \tag{34}$$

Theorem 3.1. *Let $P_i, W_i, 1 \leqslant i \leqslant r$, be polynomials such that (32) holds. Then there exist polynomials U, V, and $\widetilde{P}_i, \widetilde{W}_i, 1 \leqslant i \leqslant r$, where*

$$\deg U = \mathrm{GCD}(p_1, p_2, \dots, p_r), \quad \deg V = \mathrm{GCD}(w_1, w_2, \dots, w_r),$$

such that

$$P_i = U \circ \widetilde{P}_i, \quad W_i = \widetilde{W}_i \circ V, \quad 1 \leqslant i \leqslant r,$$

and

$$\widetilde{P}_1 \circ \widetilde{W}_1 = \widetilde{P}_2 \circ \widetilde{W}_2 = \dots = \widetilde{P}_r \circ \widetilde{W}_r.$$

Proof. The proof is the same as in the case where $r = 2$ since if $B_i \in I_{d_i}, 1 \leqslant i \leqslant r$, are blocks containing an element $x \in X$, then $\bigcap_{i=1}^{r} B_i$ is a block which coincides with a residue class modulo $\mathrm{LCM}(d_1, d_2, \dots d_r)$, and

$$\bigcap_{i=1}^{r} V_{d_i} = V_{\mathrm{GCD}(d_1, d_2, \dots d_r)}. \qquad \square$$

3.2 Proof of Theorem 1.1

The proof is by induction on r. For $r = 2$ the statement follows from Theorem 2.4. Assume now that the statement is true for $r - 1$ and show that then it is true for r, where $r \geqslant 3$. For brevity, we will use the notation $A \sim B$ for linearly equivalent polynomials A and B.

Assume first that (33) holds. For $i, 1 \leqslant i \leqslant r$, set

$$x_i = \mathrm{GCD}(p_1, p_2, \dots p_{i-1}, p_{i+1}, \dots p_r).$$

If at least one $x_i, 1 \leqslant i \leqslant r$, is equal to one, then the equality

$$P_1 \circ W_1 = P_2 \circ W_2 = \dots = P_{i-1} \circ W_{i-1} = P_{i+1} \circ W_{i+1} = \dots = P_r \circ W_r \tag{35}$$

by the induction assumption implies that at least one $P_j, 1 \leqslant j \leqslant r, j \neq i$, is linearly equivalent either to a Chebyshev polynomial or to a power. Therefore, we may assume that

$$x_i > 1, \quad 1 \leqslant i \leqslant r. \tag{36}$$

Furthermore, since condition (33) implies that at least one of the numbers $p_i, 1 \leqslant i \leqslant r$, is odd, without loss of generality we may assume that p_r is odd. This implies that the numbers x_i, $1 \leqslant i \leqslant r - 1$, also are odd.

By Theorem 3.1 there exist a polynomial X_r, $\deg X_r = x_r$, and polynomials $\widetilde{P}_i, 1 \leqslant i \leqslant r - 1$, such that

$$P_i = X_r \circ \widetilde{P}_i, \quad 1 \leqslant i \leqslant r - 1,$$

and

$$\widetilde{P}_1 \circ W_1 = \widetilde{P}_2 \circ W_2 = \dots = \widetilde{P}_{r-1} \circ W_{r-1}. \tag{37}$$

Moreover, by the induction assumption at least one of polynomials $\widetilde{P}_i, 1 \leqslant i \leqslant r - 1$, is linearly equivalent either to a Chebyshev polynomial or to a power, and without loss of generality we may assume that this is $\widetilde{P}_1$.

Since (33) implies that $\mathrm{GCD}(x_r, p_r) = 1$, it follows from Theorems 2.1 and 2.4 applied to the equality

$$P_r \circ W_r = X_r \circ (\widetilde{P}_1 \circ W_1)$$

that either

$$P_r \sim T_{p_r}, \quad X_r \sim T_{x_r},$$

or

$$P_r \sim z^{p_r}, \quad X_r \sim z^s R^{p_r}(z),$$

or

$$P_r \sim z^s R^{x_r}(z), \quad X_r \sim z^{x_r},$$

where R is a polynomial and $s \geqslant 0$. Clearly, in the first two cases P_r is linearly equivalent either to a Chebyshev polynomial or to a power. Therefore, we may assume that $X_r \sim z^{x_r}$.

In the similar way as above we may find polynomials X_{r-1}, $\deg X_{r-1} = x_{r-1}$, and $\widehat{P}_i$, $1 \leqslant i \leqslant r$, $i \neq r-1$, such that

$$P_i = X_{r-1} \circ \widehat{P}_i, \quad 1 \leqslant i \leqslant r, \ i \neq r-1,$$

and

$$\widehat{P}_1 \circ W_1 = \widehat{P}_2 \circ W_2 = \cdots = \widehat{P}_{r-2} \circ W_{r-2} = \widehat{P}_r \circ W_r. \tag{38}$$

Furthermore, applying Theorems 2.1 and 2.4 to the equality

$$P_{r-1} \circ W_{r-1} = X_{r-1} \circ (\widehat{P}_1 \circ W_1),$$

we conclude as above that if P_{r-1} is not linearly equivalent either to a Chebyshev polynomial or to a power, then $X_{r-1} \sim z^{x_{r-1}}$.

Consider now the equality

$$P_1 = X_r \circ \widetilde{P}_1 = X_{r-1} \circ \widehat{P}_1 \tag{39}$$

and show that if

$$X_r \sim z^{x_r}, \quad X_{r-1} \sim z^{x_{r-1}}, \tag{40}$$

and $\widetilde{P}_1$ is linearly equivalent either to a Chebyshev polynomial or to a power, then P_1 is linearly equivalent to a power.

Since x_{r-1} is an odd number greater than one, and z^n is not linearly equivalent to T_n for $n > 2$, it follows from Theorems 2.1 and 2.4 applied to (39) that there exist polynomials W, $\widetilde{R}$ and polynomials α, β, γ of degree one such that either

$$X_r = \alpha \circ z^{x_r} \circ \beta, \qquad \widetilde{P}_1 = \beta^{-1} \circ z^s \widetilde{R}(z^{x_r}) \circ W, \tag{41}$$

$$X_{r-1} = \alpha \circ z^s \widetilde{R}^{x_r}(z) \circ \gamma, \quad \widehat{P}_1 = \gamma^{-1} \circ z^{x_r} \circ W, \tag{42}$$

or

$$X_r = \alpha \circ z^s \widetilde{R}^{x_{r-1}}(z) \circ \beta, \quad \widetilde{P}_1 = \beta^{-1} \circ z^{x_{r-1}} \circ W, \tag{43}$$

$$X_{r-1} = \alpha \circ z^{x_{r-1}} \circ \gamma, \qquad \widehat{P}_1 = \gamma^{-1} \circ z^s \widetilde{R}(z^{x_{r-1}}) \circ W, \tag{44}$$

where $s \geqslant 0$. Furthermore, since (33) implies the equality $\mathrm{GCD}(x_{r-1}, x_r) = 1$, it follows from (36) that $s > 0$.

Observe now that if a polynomial P of the form $z^s R^m(z)$, where $m > 1$, $s > 0$, is linearly equivalent to a power, then R is a monomial. Indeed, since a power has a unique critical point, the inequality $m > 1$ implies that R has at most one zero. Furthermore, since the multiplicity

of the unique critical point of a power z^n coincides with n, it follows from $s>0$ that whenever $\deg R>0$ the unique zero of R coincides with the origin. Therefore, it follows from (40)–(43) that without loss of generality we may assume that

$$X_r=\alpha\circ z^{x_r}\circ\beta,\qquad \widetilde{P}_1=\beta^{-1}\circ z^{x_{r-1}}\circ W, \tag{45}$$

$$X_{r-1}=\alpha\circ z^{x_{r-1}}\circ\gamma,\quad \widehat{P}_1=\gamma^{-1}\circ z^{x_r}\circ W, \tag{46}$$

where W is a polynomial and α,β,γ are polynomials of degree one.

If $\widetilde{P}_1$ is linearly equivalent to a power, then it follows from the second equality in (45) by the chain rule that the only critical value of W is zero, implying that $W=z^t\circ\omega$ for some polynomial of degree one ω and $t\geqslant 0$. Therefore, in this case $P_1=X_r\circ\widetilde{P}_1$ is linearly equivalent to a power. On the other hand, the above assumptions yield that $\widetilde{P}_1$ may not be linearly equivalent to a Chebyshev polynomial, for otherwise Corollary 2.3 applied to the second equality in (45) would imply that $z^{x_{r-1}}$ is linearly equivalent to $T_{x_{r-1}}$, in contradiction to the assumption that x_{r-1} is an odd number greater than one. Therefore, if (33) holds, then at least one P_i, $1\leqslant i\leqslant r$, is linearly equivalent either to a Chebyshev polynomial or to a power.

In order to prove that (34) implies that at least one W_i, $1\leqslant i\leqslant r$, is linearly equivalent either to a Chebyshev polynomial or to a power we use similar arguments. Namely, for i, $1\leqslant i\leqslant r$, define

$$y_i=\mathrm{GCD}(w_1,w_2,\dots w_{i-1},w_{i+1},\dots w_r).$$

As above, if at least one y_i, $1\leqslant i\leqslant r$, is equal to one, then (35) by the induction assumption implies that at least one W_j, $1\leqslant j\leqslant r$, $j\neq i$, is linearly equivalent either to a Chebyshev polynomial or to a power. Therefore, we may assume that $y_i>1$ for all i, $1\leqslant i\leqslant r$. Furthermore, we may assume that w_r and y_i, $1\leqslant i\leqslant r-1$, are odd.

Using Theorem 3.1, we conclude that there exist a polynomial Y_r, $\deg Y_r=y_r$, and polynomials $\widetilde{W}_i$, $1\leqslant i\leqslant r-1$, such that

$$W_i=\widetilde{W}_i\circ Y_r,\quad 1\leqslant i\leqslant r-1,$$

and

$$P_1\circ\widetilde{W}_1=P_2\circ\widetilde{W}_2=\dots=P_{r-1}\circ\widetilde{W}_{r-1}, \tag{47}$$

where by the induction assumption we may assume that $\widetilde{W}_1$ is linearly equivalent either to a Chebyshev polynomial or to a power. Furthermore, since (34) implies that $\mathrm{GCD}(y_r,w_r)=1$ it follows from Theorems 2.1 and 2.4 applied to the equality

$$(P_1\circ\widetilde{W}_1)\circ Y_r=P_r\circ W_r$$

that W_r is linearly equivalent either to a Chebyshev polynomial or to a power unless $Y_r\sim z^{y_r}$.

Continuing to argue as above we reduce the proof of the theorem to the analysis of the equality

$$W_1=\widetilde{W}_1\circ Y_r=\widehat{W}_1\circ Y_{r-1}, \tag{48}$$

where

$$Y_r\sim z^{y_r},\quad Y_{r-1}\sim z^{y_{r-1}}, \tag{49}$$

and $\widetilde{W}_1$ is linearly equivalent either to a Chebyshev polynomial or to a power.

Observe now that if a polynomial of the form $z^sR(z^m)$, where $m>1$, $s>0$, is linearly equivalent to a power, then R is a monomial. Indeed, comparing the coefficients of z^{n-1} of

both parts of the equality

$$z^s R(z^m) = \mu \circ z^n \circ \nu, \tag{50}$$

we conclude that $\nu(0) = 0$ whenever $\deg R > 0$. It follows now from $s > 0$ that $\mu(0) = 0$, implying that R is a monomial. Therefore, applying Theorems 2.1 and 2.4 to (48) and arguing as in the analysis of (39) we conclude that there exist a polynomial W and polynomials α, β, γ of degree one such that

$$\widetilde{W}_1 = W \circ z^{y_{r-1}} \circ \beta, \quad Y_r = \beta^{-1} \circ z^{y_r} \circ \alpha, \tag{51}$$

$$\widehat{W}_1 = W \circ z^{y_r} \circ \gamma, \quad Y_{r-1} = \gamma^{-1} \circ z^{y_{r-1}} \circ \alpha. \tag{52}$$

If $\widetilde{W}_1$ is linearly equivalent to a power, then the first equality in (51) implies that W has a unique critical value and that the corresponding critical point is zero, for otherwise $\widetilde{W}_1$ would have more than one critical point. Therefore, $W = \omega \circ z^t$ for some polynomial of degree one ω and $t \geqslant 0$, implying that $W_1 = \widetilde{W}_1 \circ Y_r$ is linearly equivalent to a power. On the other hand, $\widetilde{W}_1$ may not be linearly equivalent to a Chebyshev polynomial since otherwise Corollary 2.3 applied to the first equality in (51) would imply that $z^{y_{r-1}} \sim T_{y_{r-1}}$, in contradiction to the assumption that y_{r-1} is an odd number greater than one. □

4. The second Ritt theorem for triple decompositions

4.1 Decompositions involving Chebyshev polynomials or powers

By Theorem 1.2, if polynomials P_i, W_i, $1 \leqslant i \leqslant r$, satisfy (32) and (34), then one of W_i, $1 \leqslant i \leqslant r$, is linearly equivalently either to a Chebyshev polynomial or to a power. In this subsection we will show that this implies some strong restrictions on a possible form of other W_i appearing in (32). More precisely, we will describe a possible form of polynomials W satisfying the equations

$$P_1 \circ z^n = P_2 \circ W \tag{53}$$

or

$$P_1 \circ T_n = P_2 \circ W \tag{54}$$

for some polynomials P_1, P_2. Notice that if the number n in (53) and (54) is a divisor of $\deg W$, then Corollary 2.2 applied to (53) (respectively to (54)) implies that $W = R \circ z^n$ (respectively that $W = R \circ T_n$), where R is a polynomial. Therefore, we must consider only the case where $n \nmid \deg W$.

Two lemmas below may be deduced easily from [Pak09, Theorem 6.4] and [ZM08, Lemma 3.16] correspondingly. For the reader's convenience we provide short independent proofs. Notice that Lemma 4.1 is proved without the assumption $n \nmid \deg W$; however, for Lemma 4.2 this assumption is essential.

Lemma 4.1. *Let P, P_1, P_2, W be polynomials satisfying the equation*

$$P = P_1 \circ z^n = P_2 \circ W. \tag{55}$$

Then there exist polynomials R, U and a polynomial σ of degree one such that

$$W = \sigma \circ z^s R(z^n), \quad P = U \circ z^{sn/e} R^{n/e}(z^n), \tag{56}$$

where $s \geqslant 0$ and $e = \mathrm{GCD}(n, \deg W)$.

Proof. Observe first that without loss of generality we may assume that

$$\mathrm{GCD}(\deg P_1, \deg P_2) = 1, \quad \mathrm{GCD}(n, \deg W) = 1. \tag{57}$$

Indeed, by Theorem 2.1 there exist polynomials A, B, C, D, U, V where

$$\deg U = \mathrm{GCD}(\deg P_1, \deg P_2), \quad \deg V = e,$$

such that

$$P_1 = U \circ A, \quad z^n = C \circ V, \quad P_2 = U \circ B, \quad W = D \circ V, \quad A \circ C = B \circ D.$$

Furthermore, it follows from the first part of Corollary 2.3 that without loss of generality we may assume that

$$C = z^{n/e}, \quad V = z^e.$$

Set $\widetilde{P} = A \circ C = B \circ D$. If the lemma is true under assumption (57), then

$$D = \sigma \circ z^l R(z^{n/e}), \quad \widetilde{P} = z^{ln/e} R^{n/e}(z^{n/e}),$$

where $\mathrm{GCD}(l, n/e) = 1$. Therefore, since

$$P = U \circ \widetilde{P} \circ z^e, \quad W = D \circ z^e,$$

the equalities in (56) hold with $s = le$.

In order to prove Lemma 4.1 under assumption (57) apply Theorem 2.4 to (55). If the collection P_1, P_2, W, z^n is a cyclic solution of (21), then there exist a polynomial R_1 and polynomials $\sigma_1, \sigma_2, \nu, \mu$ of degree one such that either the equalities

$$P_1 = \nu \circ z^m \circ \sigma_1^{-1}, \qquad z^n = \sigma_1 \circ z^s R_1(z^m) \circ \mu,$$
$$P_2 = \nu \circ z^s R_1^m(z) \circ \sigma_2^{-1}, \quad W = \sigma_2 \circ z^m \circ \mu,$$

or the equalities

$$P_1 = \nu \circ z^s R_1^n(z) \circ \sigma_1^{-1}, \quad z^n = \sigma_1 \circ z^n \circ \mu, \tag{58}$$
$$P_2 = \nu \circ z^n \circ \sigma_2^{-1}, \qquad W = \sigma_2 \circ z^s R_1(z^n) \circ \mu, \tag{59}$$

hold. Furthermore, since the lemma is true if $n = 1$ or $\deg W = 1$, we may assume that $n > 1$, $\deg W > 1$, implying that $s > 0$ by (57). Therefore, since (50) for $m > 1, s > 0$ implies that R is a monomial, without loss of generality we may assume that (58) and (59) hold. Since $n \geqslant 2$, the second equality in (58) implies that $\mu(0) = 0$, and hence (58) and (59) imply (56).

Finally, if P_1, P_2, W, z^n is a dihedral solution of (21), then, since the equality $z^n = \sigma \circ T_n \circ \mu$ implies that $n = 2$ and $\mu(0) = 0$, the lemma follows from (29) and the second equality in (30). □

LEMMA 4.2. *Let P, P_1, P_2, W be polynomials satisfying the equation*

$$P = P_1 \circ T_n = P_2 \circ W, \tag{60}$$

where $n \nmid \deg W$. Then there exist a polynomial U and a polynomial σ of degree one such that either

$$W = \sigma \circ T_m, \quad P = U \circ T_t, \tag{61}$$

where $t = \mathrm{LCM}(n, m)$, or

$$W = \sigma \circ zS(z^2) \circ T_{n/2}, \quad P = U \circ z^2 S^2(z^2) \circ T_{n/2}, \tag{62}$$

for some polynomial S.

Proof. Using the second part of Corollary 2.3 it is easy to show in the same way as in the proof of Lemma 4.1 that without loss of generality we may assume that condition (57) holds. Furthermore, $n \geqslant 2$ by $n \nmid \deg W$. If $n = 2$, then, since $T_2 = \theta \circ z^2$, where $\theta = 2z - 1$, the lemma follows from Lemma 4.1 taking into account that we can set $s = 1$ in (56) in view of the condition $n \nmid \deg W$. Therefore, we may assume that $n > 2$.

Observe first that if

$$T_m = \sigma \circ z^s R(z^n) \circ \mu, \tag{63}$$

where σ and μ are polynomials of degree one, $n \geqslant 2$, and $\deg R > 0$, then $\mu(0) = 0$ and $n = 2$. Indeed, it is easy to see that the set of critical points of the polynomial $z^s R(z^n)$ is invariant with respect to the rotation $z \to \varepsilon z$, where ε is an nth primitive root of unity. On the other hand, since all critical points of T_m are on the real line, it follows from (63) that all critical points of $z^s R(z^n)$ are on the line $\mu\{\mathbb{R}\}$. This implies easily that $\mu(0) = 0$ and $n = 2$.

Furthermore, observe that the equality

$$T_n = \sigma \circ T_n \circ \mu, \tag{64}$$

where σ and μ are polynomials of degree one and $n \geqslant 2$, implies that

$$\mu = \pm z. \tag{65}$$

Indeed, by (24) any Chebyshev polynomial has the form $z^s R(z^2)$, where s is equal to zero or one, implying by the above remark that $\mu(0) = 0$ in (64). Now the comparison of coefficients of both parts of (64) implies that $\mu = \pm z$, for otherwise T_n would have a form $z^s R(z^n)$ for some $n > 2$ and $s \geqslant 0$.

Now apply Theorem 2.4 to (60). If P_1, P_2, W, T_n is a dihedral solution of (21), then, since (64) implies (65), it is easy to see taking into account (24) that the lemma is true. Otherwise, taking into account that z^n and T_n are not linearly equivalent for $n > 2$, we conclude that there exist polynomials $\sigma_1, \sigma_2, \nu, \mu$ of degree one such that

$$P_1 = \nu \circ z^{n_1} \circ \sigma_1^{-1}, \qquad T_n = \sigma_1 \circ z^{s_1} R_1(z^{n_1}) \circ \mu, \tag{66}$$

$$P_2 = \nu \circ z^{s_1} R_1^{n_1}(z) \circ \sigma_2^{-1}, \quad W = \sigma_2 \circ z^{n_1} \circ \mu, \tag{67}$$

where R_1 is a non-constant polynomial.

If $n_1 = 1$, then the lemma is true. On the other hand, if $n_1 > 1$, then $s_1 > 0$ by (57), and the second equality in (66) implies that $n_1 = 2$ and $\mu(0) = 0$. Therefore, $W = \sigma \circ T_2$, where σ is a polynomial of degree one. Finally, since (57) implies that n is odd, it follows from (29) and the second equality in (66) that $\sigma_1(0) = 0$ and hence

$$P = P_1 \circ T_n = \nu \circ z^2 \circ \sigma_1^{-1} \circ T_n = U \circ T_2 \circ T_n = U \circ T_{2n},$$

where U is a polynomial of degree one. □

Notice that the proofs of Lemmas 4.1 and 4.2 given above actually describe not only possible forms of W but also possible forms of P_1 and P_2. Notice also that in a similar way one can obtain descriptions of the solutions of (21) in the case where a *left* compositional factor of P is linearly equivalent to a Chebyshev polynomial or to a power.

4.2 Ritt's theorem for triple decompositions

In this subsection we apply the previous results to a description of the solutions of the equation

$$P_1 \circ W_1 = P_2 \circ W_2 = P_3 \circ W_3 \tag{68}$$

in the spirit of the second Ritt theorem. Having in mind applications to the polynomial moment problem, we restrict ourselves by the description of W_1, W_2, W_3 under the condition

$$\mathrm{GCD}(\deg W_1, \deg W_2, \deg W_3) = 1. \tag{69}$$

First of all, observe that for any solution P_1, P_2, W_1, W_2 of (21) and any decomposition $W_1 = A \circ B$ we obtain an 'induced' solution of (68) setting $P_3 = P_1 \circ A, W_3 = B$. Furthermore, it follows from Corollary 2.2 that any solution of (68) for which $\deg W_3 | \deg W_1$ holds may be obtained in such a way. In order to exclude such solutions we will assume that

$$\deg W_i \nmid \deg W_j, \quad i \neq j, 1 \leqslant j \leqslant 3. \tag{70}$$

Further, in view of Theorem 1.1 without loss of generality we may assume that either $W_1 = z^n$ or $W_1 = T_n$, where in the first case $n > 1$ by (70), while in the second case without loss of generality we may assume that $n > 2$ since $T_2 \sim z^2$.

Proposition 4.3. *Let $P_1, P_2, P_3, W_1, W_2, W_3$ be polynomials such that (68)–(70) hold. If $W_1 = z^n$, where $n > 1$, then there exist polynomials μ_1, μ_2 of degree one such that either*

$$W_2 = \mu_1 \circ z^m \circ z^{s_2} R_2(z^n), \quad W_3 = \mu_2 \circ z^{s_1} R_1(z^m) \circ z^{s_2} R_2(z^n), \tag{71}$$

where R_1, R_2 are polynomials, $m > 1, \mathrm{GCD}(s_1, m) = 1, \mathrm{GCD}(s_2, n) = 1$, or $n = 2$ and

$$W_2 = \mu_1 \circ T_{m_1} \circ zR(z^2), \quad W_3 = \mu_2 \circ T_{m_2} \circ zR(z^2), \tag{72}$$

where R is a polynomial, and $m_1 > 1, m_2 > 1$ are odd numbers satisfying $\mathrm{GCD}(m_1, m_2) = 1$.

On the other hand, if $W_1 = T_n$, where $n > 2$, then there exist polynomials μ_1, μ_2 of degree one such that either

$$W_2 = \mu_1 \circ T_{m_1}, \quad W_3 = \mu_2 \circ T_{m_2}, \tag{73}$$

where $m_1 > 1, m_2 > 1$, or $W_1 = T_{2m_1}$ and

$$W_2 = \mu_1 \circ T_{2m_2}, \quad W_3 = \mu_2 \circ zR(z^2) \circ T_{m_1 m_2}, \tag{74}$$

where R is a polynomial, and $m_1 > 1, m_2 > 1$ are odd numbers satisfying $\mathrm{GCD}(m_1, m_2) = 1$.

Proof in the case $W_1 = z^n$. It follows from Theorems 2.1 and 2.4 applied to the equality

$$P_2 \circ W_2 = P_3 \circ W_3$$

that without loss of generality we may assume that either

$$W_2 = z^m \circ W, \quad W_3 = z^{s_1} R_1(z^m) \circ W, \tag{75}$$

where R_1, W are polynomials and $\mathrm{GCD}(s_1, m) = 1$, or

$$W_2 = T_{m_1} \circ W, \quad W_3 = T_{m_2} \circ W, \tag{76}$$

where W is a polynomial and $\mathrm{GCD}(m_1, m_2) = 1$. Moreover, condition (70) implies that $m > 1$.

Further, it follows from

$$P_1 \circ z^n = P_2 \circ W_2 \tag{77}$$

that

$$P_2 \circ W_2 = P_2 \circ (W_2 \circ \varepsilon),$$

where ε is a primitive nth root of unity, and applying to this equality Corollary 2.2 we see that

$$W_2 = \sigma \circ W_2 \circ \varepsilon z, \tag{78}$$

where σ is a polynomial of degree one.

If (75) has place, then (78) implies that

$$z^m \circ W = (\sigma \circ z^m) \circ (W \circ \varepsilon z)$$

and applying Corollary 2.2 once again we conclude that there exists a polynomial μ of degree one such that the equalities

$$z^m = \sigma \circ z^m \circ \mu^{-1}, \tag{79}$$

and

$$W = \mu \circ W \circ \varepsilon z \tag{80}$$

hold. Since $m > 1$, (79) implies that $\mu(0) = 0$ and the comparison of coefficients of the parts of (80) yields that

$$W = z^{s_2} R_2(z^n), \tag{81}$$

where R_2 is a polynomial and $s_2 \geqslant 0$, implying (71). Furthermore, $\mathrm{GCD}(s_2, n) = 1$ by (69).

Assume now that (76) holds. As above, (78) implies that

$$T_{m_1} \circ W = (\sigma \circ T_{m_1}) \circ (W \circ \varepsilon z),$$

and applying to this equality Corollary 2.2 we conclude that there exists a polynomial μ of degree one such that the equalities $T_{m_1} = \sigma \circ T_{m_1} \circ \mu^{-1}$ and (80) hold. Since (64) implies (65), this yields that $\mu = \pm z$. If $\mu = z$, then it follows from (80) that $W = R_2(z^n)$ for some polynomial R_2, in contradiction to (70). On the other hand, if $\mu = -z$, then (80) yields that

$$W = z^{n/2} R_2(z^n), \tag{82}$$

implying that $n/2 = 1$ by (69). Therefore, $n = 2$ and (72) holds. Furthermore, m_1 and m_2 are odd by (70).

Remark. It follows immediately from Lemma 4.1 that $W = \mu \circ z^s R(z^n)$, where R is a polynomial and μ is a polynomial of degree one. However, the proofs of (81) and (82) require additional considerations given above. Notice also that (78) may be used for an alternative proof of Lemma 4.1.

Proof in the case $W_1 = T_n$. It follows from Lemma 4.2 applied to the equalities

$$P_1 \circ T_n = P_2 \circ W_2, \quad P_1 \circ T_n = P_3 \circ W_3$$

that without loss of generality we may assume that either

$$W_2 = T_{m_1}, \quad W_3 = T_{m_2}, \tag{83}$$

or

$$W_2 = zR_1(z^2) \circ T_{n/2}, \quad W_3 = zR_2(z^2) \circ T_{n/2} \tag{84}$$

for some polynomials R_1, R_2, or

$$W_2 = T_m, \quad W_3 = zR_1(z^2) \circ T_{n/2}, \tag{85}$$

where R_1 is a polynomial such that

$$W_3 \neq \sigma \circ T_l \tag{86}$$

for a polynomial σ of degree one and a Chebyshev polynomial T_l. Furthermore, in the last case

$$P = V \circ T_t, \tag{87}$$

where V is a polynomial and $t = \mathrm{LCM}(n, m)$.

Clearly, (83) corresponds to (73) while (84) is impossible in view of the conditions $n>2$ and (69). Assume now that (85) and (86) hold. Since in this case $n/2$ divides both $\deg W_1$ and $\deg W_3$ it follows from (69) that $\mathrm{GCD}(n/2,m)=1$. Similarly, $\mathrm{GCD}(n,m/2)=1$, since, in view of (86), Lemma 4.2 applied to the equality

$$P_2\circ T_m=P_3\circ W_3$$

implies that

$$W_3=zR_2(z^2)\circ T_{m/2} \tag{88}$$

for some polynomial R_2. Therefore, $n/2$ and $m/2$ are odd, $\mathrm{GCD}(n/2,m/2)=1$, and (87) takes the form

$$P=V\circ T_{nm/2}. \tag{89}$$

Applying now Lemma 4.2 to the equality

$$P=V\circ T_{nm/2}=P_3\circ W_3$$

and taking into account (86) we conclude that

$$W_3=zR(z^2)\circ T_{nm/4},\quad P=U\circ z^2R^2(z^2)\circ T_{nm/4} \tag{90}$$

for some polynomials R and U. Furthermore, since both numbers n and m are even each of them is greater than 2 by (70). Changing now n to $2m_1$ and m to $2m_2$ we obtain (74). □

5. Explicit solution of the polynomial moment problem

5.1 Lemma about values of Chebyshev polynomials

In this subsection we prove the following technical lemma.

LEMMA 5.1. *Let T_{m_1},T_{m_2},T_{m_3} be the Chebyshev polynomials and a, b complex numbers.*

(a) *Assume that*

$$T_{m_1}(a)=T_{m_1}(b),\quad T_{m_2}(a)=T_{m_2}(b),\quad T_{m_3}(a)=T_{m_3}(b). \tag{91}$$

Then there exists a pair of distinct indices i_1,i_2, $1\leqslant i_1,i_2\leqslant 3$, such that for $l=\mathrm{GCD}(m_{i_1},m_{i_2})$ the equality $T_l(a)=T_l(b)$ holds.

(b) *Assume that*

$$T_{m_1}(a)=0,\quad T_{m_2}(a)=0, \tag{92}$$

where m_1,m_2 are odd numbers such that $\mathrm{GCD}(m_1,m_2)=1$. Then $a=0$.

Proof. Choose $\alpha,\beta\in\mathbb{C}$ such that $\cos\alpha=a$, $\cos\beta=b$. Then the equalities in (91) imply the equalities

$$m_1\alpha=\varepsilon_1m_1\beta+2\pi k_1,\quad m_2\alpha=\varepsilon_2m_2\beta+2\pi k_2,\quad m_3\alpha=\varepsilon_3m_3\beta+2\pi k_3, \tag{93}$$

where $\varepsilon_1=\pm1$, $\varepsilon_2=\pm1$, $\varepsilon_3=\pm1$, and $k_1,k_2,k_3\in\mathbb{Z}$. Clearly, among the numbers $\varepsilon_1,\varepsilon_2,\varepsilon_3$ at least two are equal, and without loss of generality we may assume that $\varepsilon_1=\varepsilon_2$. Multiplying now the first equality in (93) by u and adding the second equality multiplied by v, where u,v are integers satisfying $um_1+vm_2=l$, where $l=\mathrm{GCD}(m_1,m_2)$, we see that $l\alpha=\varepsilon_1l\beta+2\pi k_4$, where $k_4\in\mathbb{Z}$, implying that $T_l(a)=T_l(b)$.

Similarly, the equalities in (92) imply the equalities

$$m_1\alpha=\pi/2+\pi k_1,\quad m_2\alpha=\pi/2+\pi k_2,\quad k_1,k_2\in\mathbb{Z}, \tag{94}$$

and the equality

$$\alpha = (u+v)\pi/2 + \pi k_3, \quad k_3 \in \mathbb{Z}, \tag{95}$$

where u, v are integers satisfying

$$um_1 + vm_2 = 1. \tag{96}$$

Moreover, since m_1, m_2 are odd, (96) implies that the numbers u, v have different parity. Therefore, (95) implies that $a = \cos\alpha = 0$. □

Notice that the above argument shows that if $a \neq b$ and $\mathrm{GCD}(m_1, m_2) = 1$ in (91), then the equality $\varepsilon_1 = \varepsilon_2$ in (93) is impossible. Therefore, a, b, $a \neq b$, is a solution of the system

$$T_{m_1}(a) = T_{m_1}(b), \quad T_{m_2}(a) = T_{m_2}(b), \tag{97}$$

where $\mathrm{GCD}(m_1, m_2) = 1$, if and only if $a = \cos\alpha$, $b = \cos\beta$, where $\alpha, \beta, \alpha \neq \beta$, is a solution of the system

$$\alpha - \beta = \frac{2\pi k_1}{m_1}, \quad \alpha + \beta = \frac{2\pi k_2}{m_2},$$

for some $k_1 \in \mathbb{Z}$, $k_2 \in \mathbb{Z}$. In particular, the equalities in (97) for $a \neq b$ imply the equalities

$$T_{m_1 m_2}(a) = \pm 1, \quad T_{m_1 m_2}(b) = \pm 1.$$

5.2 Proof of Theorem 1.2

Proposition 5.2. *Let P be a polynomial and W_i, $1 \leqslant i \leqslant r$, compositional right factors of P such that $W_i(a) = W_i(b)$, $1 \leqslant i \leqslant r$, where $r > 3$. Then there exists a pair of distinct indices i_1, i_2, $1 \leqslant i_1, i_2 \leqslant r$, such that the equalities*

$$W_{i_1} = \widetilde{W}_{i_1} \circ Z, \quad W_{i_2} = \widetilde{W}_{i_2} \circ Z, \quad Z(a) = Z(b) \tag{98}$$

hold for some polynomials $\widetilde{W}_{i_1}, \widetilde{W}_{i_2}, Z$.

Proof. Clearly, we may assume that

$$\deg W_i \nmid \deg W_j, \quad i \neq j, 1 \leqslant j \leqslant r, \tag{99}$$

since otherwise Corollary 2.2 applied to the equality

$$P_i \circ W_i = P_j \circ W_j \tag{100}$$

implies that $W_j = R \circ W_i$ for some polynomial R, and hence (98) holds for $i_1 = i, i_2 = j$, and $Z = W_i$. Furthermore, without loss of generality we may assume that (18) holds. Indeed, if

$$\mathrm{GCD}(\deg W_1, \deg W_2, \dots, \deg W_r) = w > 1,$$

then there exists a polynomial W of degree w and polynomials $\widehat{W}_1, \widehat{W}_2, \dots, \widehat{W}_r$ such that

$$W_1 = \widehat{W}_1 \circ W, \quad W_2 = \widehat{W}_2 \circ W, \dots, W_r = \widehat{W}_r \circ W, \tag{101}$$

$$P_1 \circ \widehat{W}_1 = P_2 \circ \widehat{W}_2 = \dots = P_r \circ \widehat{W}_r, \tag{102}$$

and

$$\widehat{W}_1(\widehat{a}) = \widehat{W}_1(\widehat{b}), \quad \widehat{W}_2(\widehat{a}) = \widehat{W}_2(\widehat{b}), \dots, \widehat{W}_r(\widehat{a}) = \widehat{W}_r(\widehat{b}), \tag{103}$$

where

$$\widehat{a} = W(a), \quad \widehat{b} = W(b).$$

If the statement is true under condition (18), then there exists a pair of indices i_1, i_2, $1 \leqslant i_1, i_2 \leqslant r$, such that

$$\widehat{W}_{i_1} = \widetilde{W}_{i_1} \circ U, \quad \widehat{W}_{i_2} = \widetilde{W}_{i_2} \circ U, \quad U(\widehat{a}) = U(\widehat{b})$$

for some polynomials $\widetilde{W}_{i_1}, \widetilde{W}_{i_2}$, and U. Therefore, (98) holds for the same pair i_1, i_2 and $Z = U \circ W$.

By Theorem 1.1 we may assume that either $W_1 = z^n$ or $W_1 = T_n$. Assume that $W_1 = z^n$ and show that in this case the statement is true already if $r > 2$. Namely, we will show that if $W_1 = z^n$ and W_2, W_3 are arbitrary polynomials such that

$$P = P_i \circ W_i, \quad W_i(a) = W_i(b), \quad 1 \leqslant i \leqslant 3,$$

for some polynomials P_1, P_2, P_3, then (98) holds for some i_1, i_2, $1 \leqslant i_1, i_2 \leqslant 3$. Observe that the same argument as above shows that it is enough to prove this statement under the assumption

$$\mathrm{GCD}(\deg W_1, \deg W_2, \deg W_3) = 1 \tag{104}$$

since by Corollary 2.3 without loss of generality we may assume that the polynomial $\widehat{W}_1$ in (101) is a power.

By Proposition 4.3, if (104) holds, then without loss of generality we may assume that either (71) holds, or $n = 2$ and (72) holds. If (71) holds, then the equalities $W_1(a) = W_1(b), W_2(a) = W_2(b)$ imply that either the number $a^n = b^n$ is a root of R_2, or

$$a^{ms_2} = b^{ms_2}. \tag{105}$$

In the first case (98) holds for $i_1 = 2, i_2 = 3$, and $Z = z^{s_2} R_2(z^n)$. On the other hand, in the second case we conclude that $a^t = b^t$, where $t = \mathrm{GCD}(ms_2, n)$, implying that (98) holds for $i_1 = 1, i_2 = 2$, and $Z = z^t$.

If $n = 2$ and (72) holds, then the equality $W_1(a) = W_1(b)$ implies that $b = -a$. Therefore, it follows from $W_2(a) = W_2(b)$ taking into account (24) and the oddness of m_1 that

$$T_{m_1}(aR(a^2)) = T_{m_1}(bR(b^2)) = 0. \tag{106}$$

Similarly, $W_3(a) = W_3(b)$ implies that

$$T_{m_2}(aR(a^2)) = T_{m_2}(bR(b^2)) = 0. \tag{107}$$

Applying now Lemma 5.1(b) to (106) and (107) we conclude that

$$aR(a^2) = bR(b^2) = 0,$$

implying that (98) holds for $i_1 = 2, i_2 = 3$, and $Z = zR(z^2)$,

Assume now that $W_1 = T_n$ and $r > 3$. It follows from Lemma 4.2 that without loss of generality we may assume that each W_j, $2 \leqslant j \leqslant r$, is either a Chebyshev polynomial or has the form $zR(z^2) \circ T_{n/2}$ for some polynomial R. Furthermore, since $r > 3$, at least two polynomials from the set W_j, $2 \leqslant j \leqslant r$, either both are Chebyshev polynomials or both have the form $zR(z^2) \circ T_{n/2}$. Therefore, we may assume that either

$$W_2 = T_{m_1}, \quad W_3 = T_{m_2}, \tag{108}$$

or

$$W_2 = zR_1(z^2) \circ T_{n/2}, \quad W_3 = zR_2(z^2) \circ T_{n/2} \tag{109}$$

for some polynomials R_1, R_2.

If (108) holds, then (98) is satisfied by Lemma 5.1(a). On the other hand, (109) implies (102) and (103), where

$$\widehat{W}_1 = T_2, \quad \widehat{W}_2 = zR_1(z^2), \quad \widehat{W}_3 = zR_2(z^2),$$

and

$$\widehat{a} = T_{n/2}(a), \quad \widehat{b} = T_{n/2}(b).$$

Since $\widehat{W}_1 = T_2 = \theta \circ z^2$, where $\theta = 2z - 1$, it is already proved that there exists a pair of indices i_1, i_2, $1 \leqslant i_1, i_2 \leqslant r$, such that

$$\widehat{W}_{i_1} = \widetilde{W}_{i_1} \circ U, \quad \widehat{W}_{i_2} = \widetilde{W}_{i_2} \circ U, \quad U(\widehat{a}) = U(\widehat{b})$$

for some polynomials $\widetilde{W}_{i_1}, \widetilde{W}_{i_2}$, and U. Therefore, (98) holds for the same pair i_1, i_2 and $Z = U \circ T_{n/2}$. This finishes the proof. □

By the main result of [PM09], if P, Q is a solution of (1), then there exist polynomials P_i, Q_i, V_i, W_i, $1 \leqslant i \leqslant r$, such that

$$Q = \sum_{i=1}^{r} Q_i$$

and

$$P = P_i \circ W_i, \quad Q_i = V_i \circ W_i, \quad W_i(a) = W_i(b), \quad 1 \leqslant i \leqslant r. \tag{110}$$

Therefore, Theorem 1.2 is a corollary of the following result.

Theorem 5.3. *For any polynomial P and $a, b \in \mathbb{C}$ the minimal number r of compositional right factors W_i, $1 \leqslant i \leqslant r$, of P such that $W_i(a) = W_i(b)$, $1 \leqslant i \leqslant r$, and any compositional right factor W of P satisfying $W(a) = W(b)$ is a polynomial in one of W_i, $1 \leqslant i \leqslant r$, does not exceed three.*

Furthermore, if $r = 2$, then either

$$P = U \circ z^{sn} R^n(z^n) \circ V, \quad W_1 = z^n \circ V, \quad W_2 = z^s R(z^n) \circ V, \tag{111}$$

where R, U, V are polynomials, $n > 1$, $s > 0$, $\mathrm{GCD}(s, n) = 1$, or

$$P = U \circ T_{nm} \circ V, \quad W_1 = T_n \circ V, \quad W_2 = T_m \circ V, \tag{112}$$

where U, V are polynomials, $n > 1$, $m > 1$, $\mathrm{GCD}(m, n) = 1$.

On the other hand, if $r = 3$, then

$$\begin{gathered} P = U \circ z^2 R^2(z^2) \circ T_{m_1 m_2} \circ V, \\ W_1 = T_{2m_1} \circ V, \quad W_2 = T_{2m_2} \circ V, \quad W_3 = (zR(z^2) \circ T_{m_1 m_2}) \circ V, \end{gathered} \tag{113}$$

where R, U, V are polynomials, $m_1 > 1, m_2 > 1$ are odd, and $\mathrm{GCD}(m_1, m_2) = 1$.

Proof. Since any polynomial up to the linear equivalence has only a finite number of compositional right factors, we may find a finite number of compositional right factors W_i, $1 \leqslant i \leqslant r$, of P such that $W_i(a) = W_i(b)$, $1 \leqslant i \leqslant r$, and any compositional right factor W of P satisfying $W(a) = W(b)$ is a polynomial in one of W_i, $1 \leqslant i \leqslant r$. Furthermore, if the number r is minimal, then Proposition 5.2 implies that $r \leqslant 3$.

If $r = 2$, then it follows from Theorems 2.1 and 2.4 that either (111) or (112) holds. On the other hand, if $r = 3$, then it follows from Theorem 3.1, Theorem 1.1, and Proposition 4.3 that without loss of generality we may assume that either $W_1 = z^n$ and one of conditions (71) or (72) holds, or $W_1 = T_n$ and one of conditions (73) or (74) holds. However, as was shown in the proof

of Proposition 5.2, the equality $W_1 = z^n$ contradicts the minimality of r for $r > 2$. Furthermore, (73) contradicts the minimality of r by Lemma 5.1(a). Therefore, taking into account the second formula in (90), we conclude that if $r = 3$, then (113) holds. □

In conclusion we make several comments concerning relations of solutions of the third type listed in the formulation of Theorem 1.2 with other types of solution, assuming for simplicity that $V = z$. First, it follows from $W_1(a) = W_1(b)$ that either

$$T_{m_1}(a) = T_{m_1}(b) \tag{114}$$

or

$$T_{m_1}(a) = -T_{m_1}(b). \tag{115}$$

However, if (114) holds, then we may replace $Q_1 + Q_3$ by

$$(V_1 \circ T_2 + V_3 \circ zR_1(z^2) \circ T_{m_2}) \circ T_{m_1},$$

obtaining a solution of the second type. A similar argument shows that Q reduces to a solution of the second type unless the equality

$$T_{m_2}(a) = -T_{m_2}(b) \tag{116}$$

holds. Finally, unless

$$a \neq -b, \tag{117}$$

we may replace $Q_1 + Q_2$ by

$$(V_1 \circ T_{m_1} + V_2 \circ T_{m_2}) \circ T_2,$$

obtaining a solution of the first type.

The remarks above show that a solution of the third type reduces to other types of solution unless conditions (115)–(117) are satisfied. Keeping the notation of Lemma 5.1 it is easy to see that (115) and (116) imply the equalities

$$m_1\alpha = \pi + \varepsilon_1 m_1\beta + 2\pi k_1, \quad m_2\alpha = \pi + \varepsilon_2 m_2\beta + 2\pi k_2, \tag{118}$$

where $\varepsilon_1 = \pm 1$, $\varepsilon_2 = \pm 1$, $k_1, k_2 \in \mathbb{Z}$. Further, if $\varepsilon_1 = \varepsilon_2$, then

$$\alpha = (u + v)\pi + \varepsilon_1\beta + 2\pi k_3, \quad k_3 \in \mathbb{Z},$$

where u, v satisfy (96). Since (96) for odd m_1, m_2 implies that the numbers u, v have different parities we conclude that in this case $a = -b$. Therefore, solutions of the third type which cannot be reduced to solutions of other types are obtained from the system

$$\alpha - \beta = \frac{\pi}{m_1} + \frac{2\pi k_1}{m_1}, \quad \alpha + \beta = \frac{\pi}{m_2} + \frac{2\pi k_2}{m_2},$$

for some $k_1 \in \mathbb{Z}$, $k_2 \in \mathbb{Z}$. In particular, if conditions (115)–(117) are satisfied, then, since m_1, m_2 are odd, the equalities

$$T_{m_1m_2}(a) = \pm 1, \quad T_{m_1m_2}(b) = \pm 1 \tag{119}$$

hold. Therefore, since $W_3 = zR(z^2) \circ T_{m_1m_2}$ and

$$T_{m_1m_2}(a) = T_{m_2}(T_{m_1}(a)) = T_{m_2}(-T_{m_1}(b)) = -T_{m_1m_2}(b), \tag{120}$$

it follows from $W_3(a) = W_3(b)$ that necessarily

$$R(1) = 0. \tag{121}$$

Finally, observe that in general a solution of the third type may not be obtained as a sum of only two reducible solutions. Consider for example the following in a sense the simplest possible solution of the third type:

$$P = z^2R^2(z^2) \circ T_{m_1m_2}, \quad Q = T_{2m_1} + T_{2m_2} + zR(z^2) \circ T_{m_1m_2}, \tag{122}$$

where $R(z) = z - 1$, and a, b satisfy conditions (115)–(117). Assume additionally that m_1, m_2 are different prime numbers greater than three, and show that such Q can not be represented as a sum of two reducible solutions.

Observe first that P is not linearly equivalent to a Chebyshev polynomial since ± 1 are critical values of $T_{m_1m_2}$ and at the same time are critical points of the polynomial $z^2R^2(z^2) = z^2(z^2-1)^2$, implying that P has critical points of multiplicity four. Further, show that up to the linear equivalence compositional right factors of P are T_2, T_{m_1}, T_{m_2}, $T_{2m_1m_2}, T_{2m_2}$, $T_{2m_1}, T_{m_1m_2}$, or $z(z^2-1) \circ T_{m_1m_2}$. Indeed, all the polynomials above are clearly right factors of P. On the other hand, since m and n are odd, it follows from Lemma 4.2 applied to the equality

$$P = z^2(z^2-1)^2 \circ T_{m_1m_2} = U \circ W$$

that if W is a compositional right factor of P, then either $m_1m_2|\deg W$ or W is linearly equivalent to a Chebyshev polynomial. In the first case Corollary 2.2 yields that $W = V \circ T_{m_1m_2}$, where V is a right factor of $z^2(z^2-1)^2$, implying that W is linearly equivalent either to $T_{2m_1m_2}$ or $z(z^2-1) \circ T_{m_1m_2}$. On the other hand, taking into account that m_1, m_2 are prime numbers greater than three and $\deg z^2(z^2-1)^2 = 6$, in the second case W is linearly equivalent either to one of the Chebyshev polynomials listed above or to a Chebyshev polynomial whose order is divisible by three. However, the last case is not possible, for otherwise T_3 also would be a right factor of P and Lemma 4.2 applied to the equality

$$P = \frac{z+1}{2}\left(\frac{z-1}{2}\right)^2 \circ T_{2m_1m_2} = F \circ T_3$$

would imply that P is linearly equivalent to a Chebyshev polynomial.

Since a and b satisfy conditions (115)–(117), and (119) and (120) hold, among compositional right factors W of P only the polynomials $T_{2m_1}, T_{2m_2}, T_{2m_1m_2}$, and $z(z^2-1) \circ T_{m_1m_2}$ satisfy the condition $W(a) = W(b)$. Therefore, taking into account that $T_{2m_1m_2}$ is a polynomial in T_{2m_1} as well as a polynomial in T_{2m_2}, we conclude that if Q may be represented as a sum of at most two reducible solutions, then Q has the form

$$Q = V_1 \circ W_1 + V_2 \circ W_2, \tag{123}$$

where W_1, W_2 are different polynomials from the set

$$S = \{T_{2m_1}, T_{2m_2}, z(z^2-1) \circ T_{m_1m_2}\}$$

and $V_1, V_2 \in \mathbb{C}[z]$.

Denote by W_3 the polynomial from the set S distinct from W_1, W_2. Since $Q = W_1 + W_2 + W_3$ by (122), it follows from (123) that the equality

$$W_3 = (V_1 - 1) \circ W_1 + (V_2 - 1) \circ W_2$$

holds. However, this equality is impossible since any two polynomials W_1, W_2 from S have a common compositional right factor which is not a compositional right factor of W_3.

References

BT00 Y. Bilu and R. Tichy, *The Diophantine equation $f(x) = g(y)$*, Acta Arith. **95** (2000), 261–288.

BBY05 M. Blinov, M. Briskin and Y. Yomdin, *Local center conditions for the Abel equation and cyclicity of its zero solution*, in *Complex analysis and dynamical systems II: a conference in honor of Professor Lawrence Zalcman's sixtieth birthday, June 9–12, 2003, Nahariya, Israel*, Contemporary Mathematics, vol. 382 (American Mathematical Society, Providence, RI, 2005), 65–82.

BFY98 M. Briskin, J.-P. Françoise and Y. Yomdin, *Une approche au problème du centre-foyer de Poincaré*, C. R. Acad. Sci. Paris, Sér. I, Math. **326** (1998), 1295–1298.

BFY99 M. Briskin, J.-P. Françoise and Y. Yomdin, *Center conditions, compositions of polynomials and moments on algebraic curve*, Ergodic Theory Dynam. Systems **19** (1999), 1201–1220.

BFY00a M. Briskin, J.-P. Françoise and Y. Yomdin, *Center condition II: parametric and model center problems*, Israel J. Math. **118** (2000), 61–82.

BFY00b M. Briskin, J.-P. Françoise and Y. Yomdin, *Center condition III: Parametric and model center problems*, Israel J. Math. **118** (2000), 83–108.

BFY01 M. Briskin, J.-P. Françoise and Y. Yomdin, *Generalized moments, center-focus conditions and compositions of polynomials*, in *Operator theory, system theory and related topics*, Operator Theory: Advances and Applications, vol. 123 (Birkhäuser, Basel, 2001), 161–185.

BRY10 M. Briskin, N. Roytvarf and Y. Yomdin, *Center conditions at infinity for Abel differential equations*, Ann. of Math. (2) **172** (2010), 437–483.

BY05 M. Briskin and Y. Yomdin, *Tangential version of Hilbert 16th problem for the Abel equation*, Mosc. Math. J. **5** (2005), 23–53.

Chr00 C. Christopher, *Abel equations: composition conjectures and the model problem*, Bull. Lond. Math. Soc. **32** (2000), 332–338.

Eng41 H. Engstrom, *Polynomial substitutions*, Amer. J. Math. **63** (1941), 249–255.

Fri73 M. Fried, *On a theorem of Ritt and related diophantine problems*, J. Reine Angew. Math. **264** (1973), 40–55.

MP11 M. Muzychuk and F. Pakovich, *Jordan–Holder theorem for imprimitivity systems and maximal decompositions of rational functions*, Proc. Lond. Math. Soc. (3) **102** (2011), 1–24.

Pak02 F. Pakovich, *A counterexample to the 'composition conjecture'*, Proc. Amer. Math. Soc. **130** (2002), 3747–3749.

Pak03a F. Pakovich, *On the polynomial moment problem*, Math. Res. Lett. **10** (2003), 401–410.

Pak03b F. Pakovich, *Polynomial moment problem*, Mosc. Math. J. **3** (2003), Addendum to [Y. Yomdin, *Center problem for Abel equation, compositions of functions and moment conditions*, Mosc. Math. J. **3** (2003), 1167–1195].

Pak04 F. Pakovich, *On polynomials orthogonal to all powers of a Chebyshev polynomial on a segment*, Israel J. Math **142** (2004), 273–283.

Pak05 F. Pakovich, *On polynomials orthogonal to all powers of a given polynomial on a segment*, Bull. Sci. Math. **129** (2005), 749–774.

Pak09 F. Pakovich, *Prime and composite Laurent polynomials*, Bull. Sci. Math. **133** (2009), 693–732.

PM09 F. Pakovich and M. Muzychuk, *Solution of the polynomial moment problem*, Proc. Lond. Math. Soc. (3) **99** (2009), 633–657.

PRY04 F. Pakovich, N. Roytvarf and Y. Yomdin, *Cauchy type integrals of algebraic functions*, Israel J. Math. **144** (2004), 221–291.

Rit22 J. Ritt, *Prime and composite polynomials*, Trans. Amer. Math. Soc. **23** (1922), 51–66.

Roy01 N. Roytvarf, *Generalized moments, composition of polynomials and Bernstein classes*, in *Entire functions in modern analysis: Boris Levin memorial conference*, Israel Mathematical Conference Proceedings, vol. 15 (Bar-Ilan University, Ramat-Gan, Israel, 2001), 339–355.

Sch82 A. Schinzel, *Selected topics on polynomials* (University of Michigan Press, Ann Arbor, MI, 1982).

Tor88 P. Tortrat, *Sur la composition des polynômes*, Colloq. Math. **55** (1988), 329–353.

Wie64 H. Wielandt, *Finite permutation groups* (Academic Press, Berlin, 1964).

Yom03 Y. Yomdin, *Center problem for Abel equation, compositions of functions and moment conditions*, Mosc. Math. J. **3** (2003), 1167–1195.

Zan93 U. Zannier, *Ritt's second theorem in arbitrary characteristic*, J. Reine Angew. Math. **445** (1993), 175–203.

ZM08 M. Zieve and P. Müller, *On Ritt's polynomial decomposition theorem*, Preprint (2008), math.AG/0807.3578v1.

F. Pakovich pakovich@math.bgu.ac.il
Department of Mathematics, Ben-Gurion University of the Negev, P.O.B. 653, Beer-Sheva, Israel