GENERALIZED “SECOND RITT THEOREM” AND EXPLICIT SOLUTION OF THE POLYNOMIAL MOMENT PROBLEM.

F. PAKOVICH

Abstract. In the recent paper [13] was shown that any solution of “the polynomial moment problem”, which asks to describe polynomials P, Q satisfying $\int_a^b P^i dQ = 0$ for all $i \geq 0$, may be obtained as a sum of some “reducible” solutions related to “compositional right factors” of P. However, the methods of [13] do not permit to estimate the number of necessary reducible solutions or to describe them explicitly. In this paper we prove a version of “the second Ritt theorem” about polynomial solutions of the functional equation $P_1 \circ W_1 = P_2 \circ W_2$ for the more general functional equation $P_1 \circ W_1 = P_2 \circ W_2 = P_3 \circ W_3$, and on this base show that any solution of the polynomial moment problem may be obtained as a sum of at most *two* reducible solutions. We also describe these solutions in a very explicit form.

1. Introduction

About a decade ago, in the series of papers [2]–[5] 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

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

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., [3]–[6], [9], [13]–[20]).

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. [1]-[9], [23]).

The center problem for the Abel equation is connected with the polynomial moment problem in several ways. For example, it was shown in [4] that for the parametric version

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

of (2) the "infinitesimal" center conditions with respect to ε reduce to moment equations (41) with

$$P(z) = \int p(z)\mathrm{d}z.$$

On the other hand, it was shown in [7] that "at infinity" (under an appropriate projectivization of the parameter space) the system of equations on the coefficients of p and q describing the center set of (2) reduces to (1) with

$$P(z) = \int p(z)dz, \quad Q(z) = \int q(z)dz.$$

Many other results relating the center problem and the polynomial moment problem can be found in [7].

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

$$P = \tilde{P} \circ W, \qquad Q = \tilde{Q} \circ W, \tag{3}$$

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

$$\int_{W(a)}^{W(b)} \tilde{P}^i d\tilde{Q} = 0, \quad i \geq 0, \tag{4}$$

while equation (2) transforms to the equation

$$\frac{\mathrm{d}\tilde{y}}{\mathrm{d}w} = \tilde{P}'(w)\tilde{y}^2 + \tilde{Q}'(w)\tilde{y}^3. \tag{5}$$

Furthermore, if the polynomial W in (3) satisfies the equality

$$W(a) = W(b), \tag{6}$$

then it follows from the Cauchy theorem that (4) and therefore (1) holds. Similarly, since any solution $y(z)$ of equation (2) is the pull-back

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

of a solution $\tilde{y}(w)$ of equation (5), if W satisfies (6), then equation (2) has a center. This justifies the following definition: a center for equation (2) or a solution of system (41) is called *reducible* if there exist polynomials $\tilde{P}$, $\tilde{Q}$, W such that conditions (3), (6) 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 [7] and the bibliography therein).

By analogy with the composition conjecture 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, if a, b are not critical points of P ([9]), if P is indecomposable that is can not be represented as a composition of two polynomials of degree greater than one ([15]), and in some other special cases (see e. g. [4], [18], [19], [20]). 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 [14]. These counterexamples use polynomials P which admit "double decompositions" of the form

$$P = P_1 \circ W_1 = P_2 \circ W_2, \tag{7}$$

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 any polynomial Q, which can be represented as

$$Q = E \circ W_1 + F \circ W_2$$

for some polynomials E, F, satisfies (1) by linearity. On the other hand, it can be shown (see [14]) that if $\deg W_1$ and $\deg W_2$ are coprime, then condition (3) is not satisfied already for

$$Q = W_1 + W_2.$$

Notice that polynomial solutions of (7) are described by the following statement which is a bit more general form of the so called "second Ritt theorem" (see Section 2 below): if P_1, P_2, W_1, W_2 are polynomials satisfying (1), then there exist polynomials U, V, where

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

and polynomials σ_1, σ_2 of degree one such that up to a possible replacement of P_1 to P_2 and W_1 to W_2 either

$$P_1 = U \circ z^n \circ \sigma_1^{-1}, \qquad W_1 = \sigma_1 \circ z^s R(z^n) \circ V$$
$$P_2 = U \circ z^s R^n(z) \circ \sigma_2^{-1}, \qquad W_2 = \sigma_2 \circ z^n \circ V,$$

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

$$P_1 = U \circ T_n \circ \sigma_1^{-1}, \qquad W_1 = \sigma_1 \circ T_m \circ V,$$
$$P_2 = U \circ T_m \circ \sigma_2^{-1}, \qquad W_2 = \sigma_2 \circ T_n \circ V,$$

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

It was conjectured in [16] that actually *any* solution of (1) can be represented as a sum of reducible ones and recently this conjecture was proved in [13]. More precisely, it was proved in [13] that non-zero polynomials P, Q satisfy system (1) if and only if Q can be represented as a sum of polynomials Q_j such that

$$P = \tilde{P}_j \circ W_j, \quad Q_j = \tilde{Q}_j \circ W_j, \qquad W_j(a) = W_j(b) \tag{8}$$

for some polynomials $\tilde{P}_j, \tilde{Q}_j, W_j$.

In general, a polynomial P may have many compositional right factors W_j. For example, if $P = T_n$, then for any divisor d of n the equality

$$T_n = T_{n/d} \circ T_d$$

holds. Therefore, an important problem is to prove or disprove the existence of a number s such that any solution of the polynomial moment problem may be obtained as a sum of *at most* s reducible solutions, and somehow to describe these solutions. However, the methods of [13] do not permit to solve this problem and this fact makes a practical use of representation (8) rather difficult. In the paper we eliminate this defect and show that the number of different W_j necessary for constructing any solution always may be reduced to one or two. As a corollary of this result and the second Ritt theorem we obtain a very precise description of solutions of the polynomial moment problem. Our principal result is the following theorem.

Theorem 1.1. *A non-zero polynomials P, Q satisfy system (1) if and only if either there exist polynomials $\widetilde{P}$, $\widetilde{Q}$, W such that*

$$P = \widetilde{P} \circ W, \quad Q = \widetilde{Q} \circ W, \quad \textit{and} \quad W(a) = W(b);$$

or there exist polynomials Q_1, Q_2, R, W, U such that

$$P = U \circ z^{mn} R^n(z^n) \circ W, \quad Q = Q_1 \circ z^n \circ W + Q_2 \circ z^m R(z^n) \circ W,$$

and

$$W^n(a) = W^n(b), \quad R(W^n(a)) = 0,$$

where $n > 1$, $GCD(m,n) = 1$; or there exist polynomials U, W and Chebyshev polynomials T_n, T_m, T_{nm} such that

$$P = U \circ T_{nm} \circ W, \quad Q = Q_1 \circ T_n \circ W + Q_2 \circ T_m \circ W,$$

and

$$T_n(W(a)) = T_n(W(b)), \quad T_m(W(a)) = T_m(W(b)),$$

where $n > 1$, $m > 1$, and $GCD(m,n) = 1$.

Our main technical tool for proving Theorem 1.1 is the decomposition theory of polynomials. In more details, we prove a version of the second Ritt theorem for the equation

$$P = P_1 \circ W_1 = P_2 \circ W_2 = P_3 \circ W_3 \tag{9}$$

and on this base show that if a polynomial P has three compositional right factors W_1, W_2, W_3 such that $W_i(a) = W_i(b)$, $1 \leq i \leq 3$, then there exists a polynomial W such that W is a common compositional right factor of at least two of W_1, W_2, W_3, and $W(a) = W(b)$. This permits to reduce in a recursive way the number of summands in the representation $Q = \sum Q_j$ of a solution of the polynomial moment problem to one or two. Notice that our analogue of the second Ritt theorem seems to be interesting by itself and to the best of our knowledge is new.

The paper is organized as follows. In the second section we recall the description of polynomial solutions of equation (7) and prove some other related results. In the third section we establish an analogue of the second Ritt theorem for equation (9). Finally, in the fourth section on the base of the results obtained we prove Theorem 1.1.

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

2.1. **The second Ritt theorem.** In this subsection we collect some results concerning polynomial solutions of the equation

$$P_1 \circ W_1 = P_2 \circ W_2. \tag{10}$$

For more detailed account of the theory of decompositions of polynomials we refer the reader to the classical paper [21] as well as to the recent papers [12], [24] and the bibliography therein.

Polynomial solutions of equation (10) may be described by means of two theorems given below. The first one provides conditions implying that a solution of (10) can be obtained from a "smaller" solution by the operation of composition.

Theorem 2.1. ([10], [22]) *Let P_1, P_2, W_1, W_2 be polynomials such that* (10) *holds. Then there exist polynomials U, V, A, B, C, D, where*

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

such that

$$P_1 = U \circ A, \quad P_2 = U \circ B, \quad W_1 = C \circ V, \quad W_2 = D \circ V,$$

and

$$A \circ C = B \circ D. \qquad \square \tag{11}$$

Notice that since the monodromy group of a polynomial of degree n contains a cycle of length n, Theorem 2.1 follows from the fact that for a permutation group G of degree n, containing a cycle of length n, the lattice of imprimitivity systems of G is isomorphic to a sublattice of the lattice of divisors of n (see e.g. Theorem 2.3 of [11]). In particular, Theorem 10 remains true for any "double decompositions" (10) of a meromorphic function with a single pole on a Riemann surface into compositions of meromorphic functions. Besides, it extends in an obvious way to polynomial solutions of the functional equation

$$P_1 \circ W_1 = P_2 \circ W_2 = P_3 \circ W_3 \tag{12}$$

(see Theorem 3.1 below).

The second theorem, known as "the Second Ritt theorem", describes solutions of (10) which cannot be reduced to solutions of smaller degrees via Theorem 2.1.

Theorem 2.2. ([21]) *Let A, B, C, D be polynomials such that* (11) *holds and*

$$\mathrm{GCD}(\deg A, \deg B) = 1, \quad \mathrm{GCD}(\deg C, \deg D) = 1. \tag{13}$$

Then there exist polynomials $\sigma_1, \sigma_2, \mu, \nu$ of degree one such that, up to a possible replacement of A to B and C to D, either

$$A = \nu \circ z^n \circ \sigma_1^{-1}, \qquad C = \sigma_1 \circ z^s R(z^n) \circ \mu, \tag{14}$$

$$B = \nu \circ z^s R^n(z) \circ \sigma_2^{-1}, \qquad D = \sigma_2 \circ z^n \circ \mu, \tag{15}$$

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

$$A = \nu \circ T_n \circ \sigma_1^{-1}, \qquad C = \sigma_1 \circ T_m \circ \mu, \tag{16}$$

$$B = \nu \circ T_m \circ \sigma_2^{-1}, \qquad D = \sigma_2 \circ T_n \circ \mu, \tag{17}$$

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

Notice that in distinction with Theorem 2.1 the proof of Theorem 2.2 essentially uses the fact that the functions in (10) are polynomials, and reduces to the calculation of the genus g of the curve

$$A(x) - B(y) = 0, \tag{18}$$

since the condition $\mathrm{GCD}(\deg A, \deg B) = 1$ implies that this curve is irreducible, and that, in case if $g = 0$, it may be parametrized by polynomials.

Is is convenient to combine Theorem 2.1 and Theorem 2.2 as follows.

Theorem 2.3. *Let P_1, P_2, W_1, W_2 be polynomials such that* (10) *holds. Then there exist polynomials $U, V, A, B, C, D,$ where*

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

such that

$$P_1 = U \circ A, \quad P_2 = U \circ B, \quad W_1 = C \circ V, \quad W_2 = D \circ V,$$

and, up to a possible replacement of A to B and C to D, either

$$A = z^n \circ \sigma_1^{-1}, \quad C = \sigma_1 \circ z^s R(z^n), \quad B = z^s R^n(z) \circ \sigma_2^{-1}, \quad D = \sigma_2 \circ z^n, \tag{19}$$

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

$$A = T_n \circ \sigma_1^{-1}, \quad C = \sigma_1 \circ T_m, \quad B = T_m \circ \sigma_2^{-1}, \quad D = \sigma_2 \circ T_n, \tag{20}$$

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

Notice that although above theorems give a description of polynomial solutions of equation (10), they do not immediately imply a similar description of polynomial solutions of equation (12) since the functions U, V from Theorem 2.1 are different for different pairs of equations appearing in (12).

Let us mention the following well known corollary of Theorem 2.1.

Corollary 2.4. *Let P_1, P_2, W_1, W_2 be polynomials such that* (10) *holds. Assume additionally that* $\deg P_1 = \deg P_2$*. Then there exist a polynomial μ of degree one such that the equalities*

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

hold. In particular, if P_1, W_1 are 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. The first part of the corollary follows directly from Theorem 2.1. The second part follows from the first part since for any $d|n$, the equalities

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

hold and hence the equality $P_1 \circ W_1 = T_n$ (resp. $P_1 \circ W_1 = z^n$) implies the equality $P_1 \circ W_1 = T_d \circ T_{n/d}$ (resp. $P_1 \circ W_1 = z^d \circ z^{n/d}$), where $d = \deg P_1$. □

2.2. **Double decompositions involving Chebyshev polynomials or powers.** In this subsection we provide a description of solutions of (10) in the case where one of polynomials involved is a Chebyshev polynomial or a power. Since this description is closely related to Theorem 2.2, it is convenient to keep the notation of this theorem and to use the letters A, B, C, D instead of the letters of P_1, P_2, W_1, W_2, writing (10) in form (11). 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.

We start from collecting some basic properties of the Chebyshev polynomials. First, it follows easily from the formula

$$T_n(\cos \varphi) = \cos n\varphi \tag{21}$$

that if $n > 2$, then T_n has exactly two finite critical values 1 and -1, and local multiplicities of T_n at preimages of these points are $1, 1, 2, 2, \dots 2$ and $2, 2, \dots, 2$, if n is even, and $1, 2, 2, \dots 2$ and $1, 2, 2, \dots, 2$, if n is odd. Furthermore, this property characterizes Chebyshev polynomials up to the linear equivalence. Indeed, any polynomial P of degree n which has only two finite critical values c_1, c_2 and local multiplicities at $P^{-1}\{c_1\}$, $P^{-1}\{c_2\}$ as above satisfies the equation

$$n^2(y - c_1)(y - c_2) = (y')^2(z - a)(z - b),$$

where a, b are distinct complex numbers and $y(b)$ is equal either to c_1 or to c_2. On the other hand, (21) implies that that T_n satisfies the differential equation

$$n^2(y^2 - 1) = (y')^2(z^2 - 1), \quad y(1) = 1. \tag{22}$$

Therefore for appropriate polynomials μ, ν of degree 1 the polynomial $\mu \circ P \circ \nu$ also satisfies the equation (22) and hence $\mu \circ P \circ \nu = T_n$ by the uniqueness theorem for solutions of differential equations. Notice that this characterization of Chebyshev polynomials implies in particular that T_n is not linearly equivalent to z^n unless $n = 2$.

Further, (21) implies that Chebyshev polynomials satisfy

$$T_n(-z) = (-1)^n T_n(z), \quad n > 1. \tag{23}$$

In particular, if n odd, then

$$T_n(z) = zE_n(z^2) \tag{24}$$

for some polynomial E_n. Notice that for n odd, T_n satisfies the identity

$$T_n = \theta \circ zE_n^2(z) \circ \theta^{-1}, \tag{25}$$

where $\theta = 2z - 1$. Indeed,

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

implying the equality

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

which is equivalent to (25).

Finally, observe that T_n may not be represented in the form

$$T_m = \sigma \circ z^s R(z^n) \circ \mu, \quad s \geq 0, \quad n \geq 2, \tag{26}$$

where R is a polynomial and σ, μ are polynomials of degree one, unless $n = 2$. Indeed, if ζ is a critical point of the polynomial $z^s R(z^n)$, then for any i, $1 \leq i \leq n$, the number $\varepsilon^i \zeta$, where ε is nth primitive root of unity, also is its critical point. On the other hand, formula (21) implies that all critical points of T_m are on the real line. Therefore, all critical points of $z^s R(z^n) = \sigma^{-1} \circ T_m \circ \mu^{-1}$ also are on a single line implying that $n = 2$ and $\mu = \pm z$. In particular, if

$$T_n = \sigma \circ T_n \circ \mu, \tag{27}$$

for some polynomials of degree one σ, μ, then $\mu = \omega z$ and $\sigma = \omega^n z$, where $\omega = \pm 1$.

Proposition 2.5. *Let A, B, C, D be polynomials such that* (11) *holds.*

a) If $D = z^n$, then there exist a polynomial σ of degree one and polynomials S, U, $\deg U = \mathrm{GCD}(\deg A, \deg B)$, *such that*

$$A = U \circ z^{n/e} \circ \sigma^{-1}, \quad C = \sigma \circ z^s S(z^n), \quad B = U \circ z^{s/e} S^{n/e}, \tag{28}$$

where $s \geq 0$ and $e = \mathrm{GCD}(\deg C, \deg D)$, *b) If $A = z^n$, then there exist a polynomial σ of degree one and polynomials S, V,* $\deg V = \mathrm{GCD}(\deg C, \deg D)$, *such that*

$$C = z^{s/e} S(z^{n/e}) \circ V, \quad B = z^s S^n \circ \sigma^{-1}, \quad D = \sigma \circ z^{n/e} \circ V, \tag{29}$$

where $s \geq 0$ and $e = \mathrm{GCD}(\deg A, \deg B)$.

Proof. It follows from Theorem 2.1 taking into account the second part of Corollary 2.4 that it is enough to prove the proposition under the assumption that polynomials A, B, C, D satisfy (13). Furthermore, for $n = 1$ the proposition is obviously true so we may assume that $n \geq 2$.

Suppose that $D = z^n$. Then it follows from Theorem 2.2 that for polynomials A, B, C, D either (14), (15) or (16), (17) holds. Furthermore, for $n > 2$ the only first case is possible since for such n polynomials z^n and T_n are not linearly equivalent. Observe now that the equality

$$z^n = \sigma_2 \circ z^n \circ \mu$$

implies the equalities

$$\sigma_2 = \alpha z, \quad \mu = \beta z, \quad \alpha, \beta \in \mathbb{C}.$$

Therefore, if (14), (15) holds, then setting

$$U = \nu, \quad \sigma = \sigma_1, \quad S(z) = \beta^s R(\beta^n z)$$

we obtain (28).

On the other hand, if $n = 2$ and (16), (17) holds, then taking into account that the equality

$$z^2 = \sigma_2 \circ T_2 \circ \mu = \sigma_2 \circ \theta \circ z^2 \circ \mu$$

implies the equalities

$$\sigma_2 \circ \theta = \alpha z, \quad \mu = \beta z, \quad \alpha, \beta \in \mathbb{C},$$

and using identity (25), we can rewrite (16), (17) in the form

$$A = (\nu \circ \theta) \circ z^2 \circ \sigma_1^{-1}, \qquad C = \sigma_1 \circ (z E_m(z^2) \circ \beta z),$$
$$B = (\nu \circ \theta) \circ z E_m^2 \circ z/\alpha, \qquad D = (\alpha \beta^2 z) \circ z^2$$

and hence (28) holds for

$$U = \nu \circ \theta, \quad \sigma = \sigma_1, \quad S(z) = \beta E_m(\beta^2 z).$$

Similarly, if $A = z^n$ and (14), (15) holds, then $\nu = \alpha z$, $\alpha \in \mathbb{C}$, and setting

$$S = \alpha^{1/n} R, \quad V = \mu, \quad \sigma = \sigma_2,$$

we obtain (29). On the other hand, if $n = 2$ and (16), (17) holds, then

$$\nu \circ \theta = \alpha z, \quad \sigma_1 = \beta z, \quad \alpha, \beta \in \mathbb{C},$$

and writing (16), (17) in the form

$$A = z^2 \circ \sqrt{\alpha} z/\beta, \qquad C = \beta z \circ E_m(z^2) \circ \mu,$$
$$B = z \alpha E_m^2 \circ (\theta^{-1} \circ \sigma_2^{-1}), \qquad D = (\sigma_2 \circ \theta) \circ z^2 \circ \mu$$

we conclude that (29) holds for

$$\sigma = \sigma_2 \circ \theta, \quad V = \mu, \quad S(z) = \sqrt{\alpha} E_m. \qquad \square$$

Proposition 2.6. *Let A, B, C, D be polynomials such that* (11) *holds. Assume additionally that* $\deg C$ *is not a divisor of* $\deg D$*, and* $\deg D$ *is not a divisor of* $\deg C$.

a) If $C = T_m$ then there exist a polynomial μ of degree one and a polynomial U, $\deg U = \mathrm{GCD}(\deg A, \deg B)$, *such that either*

$$A = U \circ \varepsilon^{m/d} T_{n/d}, \quad B = U \circ T_{m/d} \circ \mu, \quad D = \mu^{-1} \circ \varepsilon T_n, \tag{30}$$

where $d = \mathrm{GCD}(\deg C, \deg D)$ *and* $\varepsilon = \pm 1$, *or*

$$A = U \circ \frac{z+1}{2} R^2\Big(\frac{z+1}{2}\Big), \quad B = U \circ z^2 \circ \mu, \quad D = \mu^{-1} \circ zR(z^2) \circ T_{m/2}, \tag{31}$$

where R is a polynomial,

b) If $B = T_m$, then there exist a polynomial μ of degree one and a polynomial U, $\deg U = \mathrm{GCD}(\deg C, \deg D)$, *such that either*

$$A = \varepsilon^m T_n \circ \mu, \quad C = \mu^{-1} \circ T_{m/d} \circ U, \quad D = \varepsilon T_{n/d} \circ U, \tag{32}$$

where $d = \mathrm{GCD}(\deg A, \deg B)$ *and* $\varepsilon = \pm 1$, *or*

$$A = T_{m/2} \circ (2zR^2(z) - 1) \circ \mu, \quad C = \mu^{-1} \circ z^2 \circ U, \quad D = zR(z^2) \circ U, \tag{33}$$

where R is a polynomial.

Proof. As in Proposition 2.5 we may assume that condition (13) holds. Furthermore, the requirement imposed on degrees of A and C implies that $n \geq 2$. If $D = T_2$ (resp. $A = T_2$), then it follows from Proposition 2.5, taking into account the equality $T_2 = \theta \circ z^2$ and the requirement imposed on degrees of A and C, that (31) (resp. (33)) holds. For $n > 2$ the proposition is proved in the paper [24], Lemma 3.16. Below we give an alternate proof. Denote the polynomial defined by the equality (11) by F.

Suppose that $C = T_m$. Observe that in order to prove the proposition it is enough to show that F is linearly equivalent to a Chebyshev polynomial. Indeed, in this case the second part of Corollary 2.4 implies the equalities

$$A = \nu_1 \circ T_n \circ \sigma, \quad T_m = \sigma^{-1} \circ T_m \circ \nu_2, \quad B = \nu_1 \circ T_m \circ \mu, \quad D = \mu^{-1} \circ T_n \circ \nu_2,$$

where ν_1, ν_2, σ, μ are polynomials of degree one. Therefore, $\nu_2 = \omega z$, $\sigma = \omega^m z$, where $\omega = \pm 1$ and hence (30) holds for $\varepsilon = \omega^n$.

If (16), (17) holds, then F clearly is equivalent to a Chebyshev polynomial. Otherwise, taking into account that z^n and T_n are not linearly equivalent for $n > 2$, we should have (14), (15). As it was observed above the equality

$$T_m = \sigma_1 \circ z^s R(z^n) \circ \mu \tag{34}$$

implies that $n = 2$. Hence m is odd and $T_m = zE_m(z^2)$. Further, since $zE_m(z^2)$ has no terms of degree $m-1$ and 0, it follows from equality (34) that $\sigma_1 = \alpha z$, $\mu = \beta z$, $\alpha, \beta \in \mathbb{C}$. It follows now from (14) and (34) that

$$F = \nu \circ z^2 \circ z^s R(z^n) \circ \mu = \nu \circ z^2 \circ z/\alpha \circ T_m \circ z/\beta \circ \mu =$$

$$= \nu \circ z/\alpha^2 \circ \theta^{-1} \circ T_2 \circ T_m \circ z/\beta \circ \mu$$

implying that F is linearly equivalent to a Chebyshev polynomial.

Suppose now that $B = T_m$. Again we only must show that F is linearly equivalent to a Chebyshev polynomial, and in case if (16) (17) holds this is obviously true. Otherwise, we should have (14), (15). Furthermore, the equality

$$T_m = \nu \circ z^s R^n(z) \circ \sigma_2^{-1}$$

implies that $n = 2$ for otherwise T_m would have critical points of the multiplicity greater than 2. Therefore, $\deg A = 2$. In particular, A has a unique finite critical value c, and m is odd. The calculation of the genus g of curve (18) (see e.g. Lemma 8.2 of [12]) shows that for such A and B the equality $g = 0$ holds if and only if $c = \pm 1$. In its turn, the equality $c = \pm 1$ implies that $A = \pm T_2 \circ \sigma_1^{-1}$ for some polynomial σ_1 of degree one. Furthermore, since (18) may be parametrized by the polynomials

$$\widetilde{C} = \sigma_1 \circ T_m, \quad \widetilde{D} = \pm T_2,$$

any other polynomial parametrization C, D of (18) such that

$$\deg C = \deg \widetilde{C}, \quad \deg C = \deg \widetilde{C},$$

has the form

$$C = \tilde{C} \circ \mu, \quad D = \tilde{D} \circ \mu,$$

where μ is a polynomial of degree one. Therefore, F is a linearly equivalent to a Chebyshev polynomial. $\square$

3. Polynomial solutions of $P_1 \circ W_1 = P_2 \circ W_2 = P_3 \circ W_3$

As it was mentioned above Theorem 2.3 of [11] implies immediately the following generalization of Theorem 2.1 to the equation

$$P_1 \circ W_1 = P_2 \circ W_2 = P_3 \circ W_3. \tag{35}$$

Theorem 3.1. *Let P_i, W_i, $1 \leq i \leq 3$, be polynomials of degrees p_i, w_i, $1 \leq i \leq 3$, respectively such that* (35) *holds. Then there exist polynomials U, V, W, and $\hat{P}_i, \hat{W}_i$, $1 \leq i \leq 3$, where*

$$\deg U = \mathrm{GCD}(p_1, p_2, p_3), \quad \deg V = \mathrm{GCD}(w_1, w_2, w_3),$$

such that

$$P_i = U \circ \hat{P}_i, \quad W_i = \hat{W}_i \circ V, \quad 1 \leq i \leq 3,$$

and

$$\hat{P}_1 \circ \hat{W}_1 = \hat{P}_2 \circ \hat{W}_2 = \hat{P}_3 \circ \hat{W}_3. \quad \square$$

Theorem 3.1 reduces the problem of describing of solutions of (35) to the case where

$$\mathrm{GCD}(p_1, p_2, p_3) = 1, \quad \mathrm{GCD}(w_1, w_2, w_3) = 1. \tag{36}$$

Notice that if the degree of one of P_1, P_2, P_3 is one, then (35), (36) imply that the degree of one of W_1, W_2, W_3 is also one, and vice versa. It is easy to see that in this case solutions of (35) have the form

$$\mu \circ (U \circ V) = (\mu \circ U) \circ (V \circ \nu) = (U \circ V) \circ \nu,$$

where U, V are arbitrary polynomials and μ, ν are polynomials of degree one. So, below we will assume that polynomials P_i, W_i, $1 \leq i \leq 3$, are non-linear.

The following statement essentially is proved in [24], Lemma 3.22. Since however the formulation given in [24] uses some additional restrictions on $n, s, \widehat{n}, \widehat{s}$ we provide an independent proof.

Proposition 3.2. *Let F, R, $\widehat{R}$ be polynomials and δ, γ be polynomials of degree one satisfying the equality*

$$F = z^s R(z^n) = \delta \circ z^{\widehat{s}} \widehat{R}^{\widehat{n}} \circ \gamma, \tag{37}$$

where $n \nmid s$ and $\widehat{n} \nmid \widehat{s}$. Then either $\delta(0) = 0$ and $\gamma(0) = 0$, or F is linearly equivalent to a Chebyshev polynomial T_f of odd degree.

Proof. Set $f = \deg F$ and write

$$\delta = \alpha z + \beta, \quad \gamma = \widehat{\alpha} z + \widehat{\beta},$$

where $\alpha, \beta, \widehat{\alpha}, \widehat{\beta} \in \mathbb{C}$.

Assume that $\beta \neq 0$. Then equality $F(\varepsilon z) = \varepsilon^s F(z)$, where ε is nth primitive root of unity leads to the equality

$$z^{\widehat{s}} \widehat{R}^{\widehat{n}} \circ \gamma \circ \varepsilon z + \omega_1 (z^{\widehat{s}} \widehat{R}^{\widehat{n}} \circ \gamma) = \omega_2, \tag{38}$$

where ω_1, ω_2 are non-zero complex numbers. Clearly, the function

$$U = \delta^{-1} \circ F = z^{\widehat{s}} \widehat{R}^{\widehat{n}} \circ \gamma$$

has at most $(f-1)/2 + 1$ zeros and the equality attains if and only if

$$n = 2, \quad s = 1, \tag{39}$$

and R is a polynomial with no multiple roots such that $R(0) \neq 0$. Furthermore, it follows from (38) that the number of ω_2/ω_1-points of U also is at most $(f-1)/2+1$.

By the Riemann-Hurwitz formula, the preimage $U^{-1}\{a_1, a_2, \dots, a_k\}$ of the set of all finite critical values $a_1, a_2, \dots, a_k$ of a polynomial U of degree f contains $(k-1)f + 1$ points. Therefore, the preimage $U^{-1}\{a, b\}$ of arbitrary points a, b contains at least $f+1$ points and the equality attains if and only if U has no critical values distinct from a, b. Thus, the assumption $\beta \neq 0$ implies that $F = \delta \circ U$ has only two finite critical values and local multiplicities of F at preimages of these values are $1, 2, 2, \dots 2$ implying that F is linearly equivalent to a Chebyhsev polynomial T_f of odd degree.

Further, if $\beta = 0$, then $\omega_2 = 0$ in equality (38) implying that the linear function $\kappa = \gamma \circ \varepsilon z \circ \gamma^{-1}$ transforms the set of zeros of the polynomial $z^{\widehat{s}} \widehat{R}^{\widehat{n}}$ to itself. Any linear function transforming a finite set of points of the complex plane to itself is a rotation. Furthermore, since all roots of the polynomial $z^{\widehat{s}} \widehat{R}^{\widehat{n}}$ distinct from zero have the multiplicity which is divisible by $\hat{n}$ while the multiplicity of zero is not divisible by $\hat{n}$ we conclude that $\kappa(0) = 0$ implying $\widehat{\beta} = 0$. $\square$

In order to lighten the notation below we will call a pair a polynomial B, D by "a right Ritt pair of the exponential type" (resp. by "a right Ritt pair of the dihedral type") if the degrees of B, D are coprime and, possibly after switching B and D, equalities (15) (resp. (17)) hold. Left Ritt pairs are defined similarly.

Our main result related to equation (35) is the following one.

Theorem 3.3. *Let P_i, W_i, $1 \leq i \leq 3$, be non-linear polynomials of degrees p_i, w_i, $1 \leq i \leq 3$, respectively satisfying (35) and (36). Then at least one P_i, $1 \leq i \leq 3$, is linearly equivalent to a Chebyshev polynomial or to a power, and at least one W_i, $1 \leq i \leq 3$, is linearly equivalent to a Chebyshev polynomial or to a power.*

Proof. Applying Theorem 2.3 to the equality

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

we can find polynomials $X_1, Y_1, A_1, B_1, C_1, D_1$ such that

$$\deg X_1 = \mathrm{GCD}(p_1, p_2), \quad \deg Y_1 = \mathrm{GCD}(w_1, w_2), \tag{40}$$

$$P_1 = X_1 \circ A_1, \quad P_2 = X_1 \circ B_1, \quad W_1 = C_1 \circ Y_1, \quad W_2 = D_1 \circ Y_1, \tag{41}$$

$$A_1 \circ C_1 = B_1 \circ D_1, \tag{42}$$

and either (19) or (20) holds.

Similarly, applying Theorem 2.3 to the equality

$$P_1 \circ W_1 = P_3 \circ W_3$$

we can find polynomials $X_2, Y_2, A_2, B_2, C_2, D_2$ such that

$$\deg X_2 = \mathrm{GCD}(p_1, p_3), \quad \deg Y_2 = \mathrm{GCD}(w_1, w_3), \tag{43}$$

$$P_1 = X_2 \circ A_2, \quad P_3 = X_2 \circ B_2, \quad W_1 = C_2 \circ Y_2, \quad W_3 = D_2 \circ Y_2, \tag{44}$$

$$A_2 \circ C_2 = B_2 \circ D_2, \tag{45}$$

and either (19) or (20) holds.

Finally, applying Theorem 2.3 to the equality

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

we can find polynomials $X_3, Y_3, A_3, B_3, C_3, D_3$ such that

$$\deg X_3 = \mathrm{GCD}(p_2, p_3), \quad \deg Y_3 = \mathrm{GCD}(w_2, w_3), \tag{46}$$

$$P_2 = X_3 \circ A_3, \quad P_3 = X_3 \circ B_3, \quad W_2 = C_3 \circ Y_3, \quad W_3 = D_3 \circ Y_3, \tag{47}$$

$$A_3 \circ C_3 = B_3 \circ D_3, \tag{48}$$

and either (19) or (20) holds.

Set $x_i = \deg X_i$, $a_i = \deg A_i$, $1 \leq i \leq 3$. Notice that (36) implies that

$$\mathrm{GCD}(x_i, x_j) = 1, \quad 1 \leq i, j \leq 3, \quad i \neq j. \tag{49}$$

Suppose at first that for at least one of equalities (42), (45), (48) condition (20) holds for some $m, n > 1$. Changing if necessary the numeration of P_i, W_i, $1 \leq i \leq 3$, without loss of generality we may assume that

$$A_1 = T_m \circ \mu_1, \quad C_1 = \mu_1^{-1} \circ T_n, \quad B_1 = T_n \circ \mu_2, \quad D_1 = \mu_2^{-1} \circ T_m, \tag{50}$$

where μ_1, μ_2 are polynomials of degree one, $\mathrm{GCD}(n, m) = 1$, and the number m is odd.

Consider the equality

$$P_1 = X_1 \circ A_1 = X_2 \circ A_2. \tag{51}$$

Since x_1, x_2 are coprime, if $a_1 | a_2$, then $x_2 = 1$ and hence P_1, P_3 form a left Ritt pair. Similarly, if $a_2 | a_1$, then $x_1 = 1$ and hence P_1, P_2 form a left Ritt pair. In both case at least one of P_1, P_2, P_3 is linearly equivalent to a Chebyshev polynomial or to a power. On the other hand, if $a_1 \nmid a_2$, $a_2 \nmid a_1$, then applying Proposition 2.6, a) to (51) and taking into account that m is odd and x_1, x_2 are coprime we conclude that P_1 is linearly equivalent to a Chebyshev polynomial. Analyzing now in the same way the equation

$$W_2 = C_3 \circ Y_3 = D_1 \circ Y_1 \tag{52}$$

we conclude that at least one of W_1, W_2, W_3 is linearly equivalent to a Chebyshev polynomial or to a power.

Assume now that for all equalities (42), (45), (48) up to a possible replacement of A_i to C_i and B_i to D_i, $1 \leq i \leq 3$, condition (19) holds. Then without loss of generality we may assume that

$$A_1 = z^n \circ \mu_1, \quad B_1 = \mu_1^{-1} \circ z^{s_1} R_1^n(z), \quad C_1 = z^{s_1} R_1^n(z) \circ \mu_2, \quad D_1 = \mu_2^{-1} \circ z^n,$$

where μ_1, μ_2 are polynomials of degree one, R_1 is a polynomial, and n, s_1 satisfy $\mathrm{GCD}(n, s_1) = 1$. If $a_1 | a_2$ or $a_2 | a_1$, then we conclude as above that at least one of P_1, P_2, P_3 is linearly equivalent to a Chebyshev polynomial or to a power. So assume that $a_1 \nmid a_2$, $a_2 \nmid a_1$. In particular, this implies that $n > 1$. Applying Proposition 2.5, a) to (51) and taking into account that x_1, x_2 are coprime we conclude that

$$X_1 = \mu \circ z^{s_2/d} R_2^{n/d}, \quad X_2 = \mu \circ z^{n/d} \circ \delta, \quad A_2 = \delta^{-1} \circ z^{s_2} R_2(z^n) \circ \mu_1, \tag{53}$$

where δ, μ are polynomials of degree one, R_2 is a polynomial, and $d = \mathrm{GCD}(n, s_2)$. Notice that $n \nmid s_2$ since otherwise $a_1 | a_2$.

By the assumption either

$$A_2 = z^{\widehat{n}} \circ \nu_1, \quad C_2 = \nu_1^{-1} \circ z^{\widehat{s}} \widehat{R}(z^{\widehat{n}}), \quad B_2 = z^{\widehat{s}} \widehat{R}^{\widehat{n}} \circ \nu_2, \quad D_2 = \nu_2^{-1} \circ z^{\widehat{n}}, \tag{54}$$

or

$$A_2 = z^{\widehat{s}} \widehat{R}^{\widehat{n}} \circ \nu_1, \quad C_2 = \nu_1^{-1} \circ z^{\widehat{n}}, \quad B_2 = z^{\widehat{n}} \circ \nu_2, \quad D_2 = \nu_2^{-1} \circ z^{\widehat{s}} \widehat{R}(z^{\widehat{n}}), \tag{55}$$

where $\widehat{R}$ is a polynomial, ν_1, ν_2 are polynomials of degree one, and $\mathrm{GCD}(\widehat{n}, \widehat{s}) = 1$. Assume that (54) holds. Then it follows from (53), (54) that

$$z^{s_2} R_2(z^n) = \delta \circ z^{\widehat{n}} \circ \gamma, \tag{56}$$

where $\gamma = \nu_1 \circ \mu_1^{-1}$. Since $n > 1$, the polynomial in the left part of equality (56) has no term of degree $a_2 - 1$ implying $\gamma(0) = 0$. On the other hand, it follows from $n \nmid s_2$ that $s_2 > 0$ implying $\delta(0) = 0$. Therefore,

$$P_1 = X_2 \circ A_2 = \mu \circ z^{n/d} \circ \delta \circ z^{\widehat{n}} \circ \nu_1$$

is linearly equivalent to a power.

Further, if (55) holds, then it follows from (53), (54) that

$$z^{s_2} R_2(z^n) = \delta \circ z^{\widehat{s}} \widehat{R}^{\widehat{n}} \circ \gamma,$$

where $\gamma = \nu_1 \circ \mu_1^{-1}$. Moreover, $\widehat{n} \nmid \widehat{s}$ since $\mathrm{GCD}(\widehat{n}, \widehat{s}) = 1$. Therefore, if A_2 is not linearly equivalent to a Chebyshev polynomial of odd degree, then by Lemma 3.2 the equality $\delta(0) = 0$ holds, and

$$P_3 = X_2 \circ B_2 = \mu \circ z^{n/d} \circ \delta \circ z^{\widehat{n}} \circ \nu_2$$

is linearly equivalent to a power. On the other hand, if A_2 is linearly equivalent to a Chebyshev polynomial of odd degree, then applying Proposition 2.6, a) to (51) we conclude as above that P_1 is linearly equivalent to a Chebyshev polynomial.

Similarly, applying Proposition 2.5, b) to equation (52) and taking into account that y_1, y_3 are coprime we conclude that

$$C_3 = \mu_2^{-1} \circ z^{s_3} R_3^n(z) \circ \kappa, \quad Y_3 = \kappa^{-1} \circ z^{n/e} \circ \nu, \quad Y_1 = z^{s_3/e} R_3(z^{n/e}) \circ \nu, \tag{57}$$

where κ, ν are polynomials of degree one, R_3 is a polynomial, and $e = \mathrm{GCD}(n, s_3)$. Furthermore, either

$$A_3 = z^{\widetilde{n}} \circ \eta_1, \quad C_3 = \eta_1^{-1} \circ z^{\widetilde{s}} \widetilde{R}(z^{\widetilde{n}}), \quad B_3 = z^{\widetilde{s}} \widetilde{R}^{\widetilde{n}} \circ \eta_2, \quad D_3 = \eta_2^{-1} \circ z^{\widetilde{n}}, \tag{58}$$

or

$$A_3 = z^{\widetilde{s}}\widetilde{R}^{\widetilde{n}} \circ \eta_1, \quad C_3 = \eta_1^{-1} \circ z^{\widetilde{n}}, \quad B_3 = z^{\widetilde{n}} \circ \eta_2, \quad D_3 = \eta_2^{-1} \circ z^{\widetilde{s}}\widetilde{R}(z^{\widetilde{n}}), \tag{59}$$

where $\widetilde{R}$ is a polynomial, η_1, η_2 are polynomials of degree one, $\widetilde{n} > 1$, and $\widetilde{n} \nmid \widetilde{s}$.

Assume that (58) holds. Then it follows from (57), (58) that

$$z^{s_3} R_3(z^n) = \gamma \circ z^{\widetilde{s}}\widetilde{R}^{\widetilde{n}} \circ \kappa^{-1},$$

where $\gamma = \mu_2 \circ \eta_1^{-1}$. If C_3 is not linearly equivalent to a Chebyshev polynomial of odd degree, then by Lemma 3.2 the equality $\kappa^{-1}(0) = 0$ holds, and

$$W_3 = D_3 \circ Y_3 = \eta_2^{-1} \circ z^{\widetilde{n}} \circ \kappa^{-1} \circ z^{n/e} \circ \nu$$

is linearly equivalent to a power. On the other hand, if C_3 is linearly equivalent to a Chebyshev polynomial of odd degree, then we conclude as above that W_2 is linearly equivalent to a Chebyshev polynomial.

Further, if (59) holds, then it follows from (57), (59) that

$$z^{s_3} R_3(z^n) = \gamma \circ z^{\widetilde{n}} \circ \kappa^{-1},$$

where $\gamma = \mu_2 \circ \eta_1^{-1}$ implying as above that $\kappa^{-1}(0) = 0$. Hence

$$W_2 = C_3 \circ Y_3 = \eta_1^{-1} \circ z^{\widetilde{n}} \circ \kappa^{-1} \circ z^{n/e} \circ \nu$$

is linearly equivalent to a power. $\square$

Remark. Notice that Theorem 3.3 reduces the study of equation (35) to the study of the equations

$$\begin{aligned} z^n \circ A &= B \circ z^m = U \circ V \\ z^n \circ A &= B \circ T_m = U \circ V \\ T_n \circ A &= B \circ z^m = U \circ V \\ T_n \circ A &= B \circ T_m = U \circ V, \end{aligned} \tag{60}$$

and using Proposition 2.5 and Proposition 2.6 one can obtain a description of solutions of these equations in the spirit of Theorem 2.2. For examples, one can show that any solution of (60) has the form

$$U = z^{\frac{r_2 m}{d_2}} R_2^n(z^{\frac{m}{d_2}}), \quad V = z^{\frac{r_1 n}{d_1}} R_1^{\frac{n}{d_1}}(z^m),$$

$$A = z^{\frac{r_1 r_2 m}{d_1 d_2}} R_1^{\frac{r_2 m}{d_1 d_2}}(z^m) R_2(z^{\frac{r_1 n m}{d_1 d_2}} R_1^{\frac{mn}{d_1 d_2}}(z^m))), \quad B = z^{\frac{r_1 r_2 n}{d_1 d_2}} R_1^{\frac{n}{d_1}} R_2^n(z^{\frac{r_1 n}{d_1 d_2}} R_1^{\frac{mn}{d_1 d_2}}),$$

where R_1, R_2 are polynomials, $\mathrm{GCD}(r_1, m) = 1$, $\mathrm{GCD}(r_2, n) = 1$, and $d_1 d_2 = \mathrm{GCD}(n, m)$. However, we do not need this more precise version of Theorem 3.3 for our purposes.

4. Proof of Theorem 1.1

We start by proving the following statement.

Proposition 4.1. *Let P and P_i, W_i, $1 \leq i \leq 3$, be polynomials such that*

$$P = P_1 \circ W_1 = P_2 \circ W_2 = P_3 \circ W_3$$

and

$$W_1(a) = W_1(b), \quad W_2(a) = W_2(b), \quad W_3(a) = W_3(b). \tag{61}$$

Then there exist distinct i_1, i_2, $1 \leq i_1, i_2 \leq 3$, *and polynomials* $\widetilde{W}_{i_1}$, $\widetilde{W}_{i_2}$, W *such that*

$$W_{i_1} = \widetilde{W}_{i_1} \circ W, \quad W_{i_2} = \widetilde{W}_{i_2} \circ W, \quad \text{and} \quad W(a) = W(b).$$

Proof. It follows easily from Theorem 3.1 that without loss of generality we may assume that conditions (36) hold. Furthermore, in view of condition (61) the polynomials W_i, $1 \leq i \leq 3$, are non-linear implying by (36) that the same is true for the polynomials P_i, $1 \leq i \leq 3$. Finally, observe that if w_i, $1 \leq i \leq 3$, is a divisor of w_j, $1 \leq j \leq 3$, $i \neq j$, then the theorem is true. Indeed, in this case it follows from Theorem 2.1 that the polynomial W_j is a polynomial in W_i and we may set $i_1 = i$, $i_2 = j$, $W = W_i$. Thus, in the following we may assume that w_i, $1 \leq i \leq 3$, is not a divisor of w_j, $1 \leq j \leq 3$, unless $i = j$.

We will keep the notation of Theorem 3.3. By Theorem 3.3 without loss of generality we may assume that either $W_1 = T_m$ or $W_1 = z^n$. If $W_1 = T_m$, then Proposition 2.6, a) implies that there exists polynomials δ_i, $i = 2, 3$, of degree one such that either

$$W_i = \delta_i \circ zR_i(z^2) \circ T_{m/2}, \tag{62}$$

where R_i is a polynomial, or

$$W_i = \delta_i \circ T_{m_i}. \tag{63}$$

If for at least one i, $i = 2, 3$, equality (62) holds, then we must have

$$T_{m/2}(a) = T_{m/2}(b)$$

since otherwise (61), (62) imply equalities

$$T_2(\hat{a}) = T_2(\hat{b}), \quad \hat{a}R_i(\hat{a}^2) = \hat{b}R_i(\hat{b}^2),$$

where $\hat{a} = T_{m/2}(a)$, $\hat{b} = T_{m/2}(b)$, which are clearly impossible. Therefore, if for at least one i, $i = 2, 3$, equality (62) holds, we can set $i_1 = 1$, $i_2 = i$, $W = T_{m/2}$. On the other hand, if for both i, $i = 2, 3$, equality (63) holds, then an easy calculation (see e.g. [17], p. 281) shows that the statement of the proposition is true.

Suppose now that $W_1 = z^n$. Observe that we may assume that the right Ritt pair C_3, D_3 from (48) is of the exponential type. Indeed, the degree of at least one of C_3, D_3 is odd. Therefore, if the pair C_3, D_3 is of the Chebyshev type, then as in the proof of Theorem 3.3 we conclude that either W_2 or W_3 is linearly equivalent to a Chebyshev polynomial, and in this case the statement of the proposition is already proved. So, assume that $C_3 = \mu \circ z^r$ where μ is a polynomial of degree one (the case of switched C_3, D_3 may be considered similarly).

Applying Proposition 2.5, a) to the equality $P_1 \circ W_1 = P_2 \circ W_2$ we conclude that there exists a polynomial S and a polynomial δ of degree one such

$$W_2 = \delta \circ z^s S(z^n). \tag{64}$$

Since $W_2 = C_3 \circ Y_3$, this implies that for any primitive nth root of unity ε the equality

$$\delta^{-1} \circ C_3 \circ Y_3(\varepsilon z) = \varepsilon^s \delta^{-1} \circ C_3 \circ Y_3$$

holds and therefore by Corollary 2.4

$$\delta^{-1} \circ C_3 = \varepsilon^k \delta^{-1} \circ C_3 \circ \gamma, \quad Y_3(\varepsilon z) = \gamma^{-1} \circ Y_3$$

for some polynomial γ of degree one. Since $C_3 = \mu \circ z^r$, the first of the equalities above implies easily that $\gamma(0) = 0$ and then the second equality implies that

$$Y_3 = z^e F(z^n), \quad W_2 = C_3 \circ Y_3 = \mu \circ z^{re} F^r(z^n)$$

for some polynomial F and $e > 0$. It follows now from (61) that

$$a^n = b^n = c, \quad a^{re} F^r(c) = b^{re} F^r(c).$$

Therefore, either $\mathrm{GCD}(n, re) = d > 1$ and $a^d = b^d$, or $F(c) = 0$. In the first case we can set $i_1 = 1, i_2 = 2$, $W = z^d$. In the second case $Y_3(a) = Y_3(b) = 0$ and we can set $i_1 = 2, i_2 = 3$, $W = Y_3$. $\Box$

Proposition 4.1 permits to reduce the number of reducible solutions in the representation $Q = \sum_j Q_j$, where Q_j satisfy (8), to one or two. Indeed, in the notation of Proposition 4.1 we may replace the sum of two reducible solutions Q_{i_1} Q_{i_2}, $1 \leq i_1, i_2 \leq 3$, by the unique reducible solution

$$(\widetilde{Q}_{i_1} \circ \widetilde{W}_{i_1} + \widetilde{Q}_{i_2} \circ \widetilde{W}_{i_2}) \circ W$$

and continuing in the same way we will eventually represent $Q = \sum_j Q_j$ as a sum of only two reducible solutions. Furthermore, if Q itself is not reducible, then Theorem 2.3 implies that, possibly after switching W_1 and W_2, either

$$W_1 = \sigma_1 \circ z^s R(z^n) \circ W, \quad W_2 = \sigma_2 \circ z^n \circ W,$$

or

$$W_1 = \sigma_1 \circ T_m \circ W, \quad W_2 = \sigma_2 \circ T_n \circ W,$$

where W, R are polynomials, σ_1, σ_2 are polynomials of degree 1, and $\mathrm{GCD}(s, r) = 1$. Moreover, it easy to see that in the first case the equalities

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

imply that $c = W^n(a) = W^n(b)$ is a root of R.

References

[1] M. Blinov, M. Briskin, Y. Yomdin, *Local center conditions for a polynomial Abel equation and cyclicity of its zero solution*, in "Complex analysis and dynamical systems II", Contemp. Math., AMS, Providence, RI, 65–82 (2005).

[2] M. Briskin, J.-P. Françoise, Y. Yomdin, *Une approche au problème du centre-foyer de Poincaré,* C. R. Acad. Sci. Paris, Sér. I, Math., vol. **326**, no. 11, 1295–1298 (1998).

[3] M. Briskin, J.-P. Françoise, Y. Yomdin, *Center conditions, compositions of polynomials and moments on algebraic curve*, Ergodic Theory Dyn. Syst., vol. **19**, no. 5, 1201–1220 (1999).

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

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

[6] M. Briskin, J.-P. Françoise, Y. Yomdin, *Generalized moments, center-focus conditions and compositions of polynomials*, in "Operator Theory, System Theory and Related Topics", Oper. Theory Adv. Appl., vol. **123**, 161–185 (2001).

[7] M. Briskin, N. Roytvarf, Y. Yomdin, *Center conditions at infinity for Abel differential equations*, to appear in Annals of Mathematics, available at `http://annals.math.princeton.edu/issues/AcceptedPapers.html`

[8] M. Briskin, Y. Yomdin, *Tangential version of Hilbert 16th problem for the Abel equation*, Moscow Math. J., vol. **5**, no. 1, 23–53 (2005).

[9] C. Christopher, *Abel equations: composition conjectures and the model problem*, Bull. Lond. Math. Soc., vol. **32**, no. 3, 332–338 (2000).

[10] H. Engstrom, *Polynomial substitutions,* Amer. J. Math. 63, 249-255 (1941).

[11] M. Muzychuk, F. Pakovich, *Jordan-Holder theorem for imprimitivity systems and maximal decompositions of rational functions*, `arXiv:0712.3869v2`
[12] F. Pakovich, *Prime and composite Laurent polynomials,* `arXiv:0710.3860v5`. To appear in Bull. Sci. Math..
[13] F. Pakovich, M. Muzychuk, *Solution of the polynomial moment problem*, `arXiv:0710.4085`. To appear in Proc. London Math. Soc..
[14] F. Pakovich, *A counterexample to the "composition conjecture"*, Proc. Amer. Math. Soc., vol. **130**, no. 12, 3747–3749 (2002).
[15] F. Pakovich, *On the polynomial moment problem*, Math. Research Letters, vol. **10**, 401–410 (2003).
[16] F. Pakovich, *Polynomial moment problem*, Addendum to the paper [23].
[17] F. Pakovich, *On polynomials orthogonal to all powers of a Chebyshev polynomial on a segment*, Israel J. Math, vol. **142**, 273–283 (2004).
[18] F. Pakovich, *On polynomials orthogonal to all powers of a given polynomial on a segment*, Bull. Sci. Math., vol. **129**, no. 9, 749–774 (2005).
[19] F. Pakovich, N. Roytvarf, Y. Yomdin, *Cauchy type integrals of algebraic functions*, Israel J. Math., vol. **144**, 221–291 (2004).
[20] N. Roytvarf, *Generalized moments, composition of polynomials and Bernstein classes*, in "Entire Functions in Modern Analysis: B. Ya. Levin Memorial Volume", Israel Math. Conf. Proc., vol. **15**, 339–355 (2001).
[21] J Ritt, *Prime and composite polynomials*, American M. S. Trans. 23, 51-66 (1922).
[22] P. Tortrat, *Sur la composition des polynômes*, Colloq. Math. 55, No.2, 329-353 (1988).
[23] Y. Yomdin, *Center problem for Abel equation, compositions of functions and moment conditions*, Moscow Math. J., vol. **3**, no. 3, 1167–1195 (2003).
[24] M.Zieve, P. Müller, *On Ritt's polynomial decomposition theorem*, preprint, arXiv:0807.3578v1.

Department of Mathematics, Ben-Gurion University of the Negev, P.O.B. 653, Beer-Sheva, Israel
E-mail address: `pakovich@cs.bgu.ac.il`