Ergod. Th. & Dynam. Sys. (2014), **34**, 1–20
doi:10.1017/etds.2012.143
© *Cambridge University Press, 2012*

On the trigonometric moment problem

AMELIA ÁLVAREZ†, JOSÉ LUIS BRAVO† and COLIN CHRISTOPHER‡

† *Departamento de Matemáticas, Universidad de Extremadura, Avda. Elvas s/n, 06006 Badajoz, Spain*
(e-mail: trinidad@unex.es)

‡ *School of Computing and Mathematics (Faculty of Science and Technology), University of Plymouth, Room 9, 2 Kirkby Place, Drake Circus, Plymouth, Devon, PL4 8AA, UK*

(*Received* 22 *February* 2012 *and accepted in revised form* 1 *August* 2012)

Abstract. The trigonometric moment problem arises from the study of one-parameter families of centers in polynomial vector fields. It seeks to classify the trigonometric polynomials Q which are orthogonal to all powers of a trigonometric polynomial P. We show that this problem has a simple and natural solution under certain conditions on the monodromy group of the Laurent polynomial associated to P. In the case of real trigonometric polynomials, which is the primary motivation of the problem, our conditions are shown to hold for all trigonometric polynomials of degree 15 or less. In the complex case, we show that there are a small number of exceptional monodromy groups up to degree 30 where the conditions fail to hold and show how counterexamples can be constructed in several of these cases.

1. *Introduction*

This work is motivated by the following problem proposed by Briskin *et al* [**3**]: given a trigonometric polynomial p, determine all trigonometric polynomials q, such that the one-parameter Abel equation

$$z' = p(w)z^2 + \epsilon q(w)z^3 \tag{1.1}$$

has a parametric center (i.e., for all ϵ, $z(0) = z(2\pi)$ for every trajectory close to $z = 0$). This problem in turn is closely related to the Poincaré center-focus problem for planar vector fields, as in many cases of interest there are transformations to the trigonometric Abel equation (1.1) (see [**5**]).

In particular, a necessary and sufficient condition in order for (1.1) to have a parametric center to first order in ϵ (see [**3**]) is

$$\int_0^{2\pi} P^k(w)\, dQ(w) = 0, \quad k = 0, 1, 2, \ldots, \tag{1.2}$$

https://doi.org/10.1017/etds.2012.143 Published online by Cambridge University Press

where P and Q are primitives of p and q. Given a trigonometric polynomial P, the trigonometric moment problem is to obtain all trigonometric polynomials Q such that (1.2) holds. Thus, the moment problem is a 'first-order' approach to the parametric centers. Moreover, Briskin *et al* [**4**] have recently proved that the moment problem is indeed equivalent to the parametric center problem 'at infinity'.

The trigonometric moment problem has been studied by Pakovich [**15**] and Pakovich *et al* [**18**]. The results obtained here are complementary to the ones obtained there, as we detail in each of the sections.

Concretely, we shall obtain sufficient conditions on P in order to solve the trigonometric moment problem. These conditions can be computed for any given trigonometric polynomial P in terms of the associated monodromy group. Moreover, since the number of possible monodromy groups for any given degree is finite, they can be computed (theoretically at least) up to any given degree. We have checked up to degree 15 and they hold for all trigonometric polynomials with real coefficients. The few exceptions we encounter have complex coefficients.

The moment problem has been extensively studied in the polynomial setting, thus, where p and q are polynomials instead of trigonometric polynomials (see, e.g., [**2–6, 8, 13, 14, 19**]). Recently it has been completely solved by Pakovich and Muzychuk [**17**] who show that Q satisfies (1.2) if and only if there exist polynomials P_k, Q_k, W_k, $k = 1, \ldots, l$, such that

$$W_k(0) = W_k(2\pi), \quad P(w) = P_k(W_k(w)), \quad k = 1, \ldots, l,$$
$$Q(w) = \sum_{k=1}^{l} Q_k(W_k(w)).$$

The preceding identities can be referred to as a 'weak composition condition'.

Inspired by this result, we study whether a similar result holds for the trigonometric moment problem. We fix a trigonometric polynomial P and try to obtain all trigonometric polynomials Q such that

$$\int_0^{2\pi} P^k(\theta)\, dQ(\theta) = 0, \quad k = 0, 1, 2, \ldots. \tag{1.3}$$

Working instead with respect to a complex variable $z = e^{i\theta}$, this problem is equivalent to the following: given a Laurent polynomial $P \in \mathcal{L}$, where $\mathcal{L}$ is the space of complex Laurent polynomials $\mathbb{C}[z, z^{-1}]$, find all $Q \in \mathcal{L}$ such that

$$\oint_{|z|=1} P^k(z)\, dQ(z) = 0, \quad k = 0, 1, 2, \ldots. \tag{A}$$

The main difference between this and the polynomial case is that (up to conjugation by a Möbius transformation) the factorization of Laurent polynomials can happen in two distinct ways: a Laurent polynomial P can be written as $\tilde{P}(z^n)$, where $\tilde{P} \in \mathcal{L}$, or as $\tilde{P}(W)$, where $\tilde{P} \in \mathbb{C}[z]$ and $W \in \mathcal{L}$ (see [**16**] or [**23**]).

These two types of factorization give rise to two different mechanisms which imply the vanishing of the moments (A). Our aim is to show that these two mechanisms are enough to solve the trigonometric moment problem for a large number of cases.

https://doi.org/10.1017/etds.2012.143 Published online by Cambridge University Press

Firstly, if P can be written as $\tilde{P}(z^l)$, $l > 1$, with $\tilde{P} \in \mathcal{L}$, then it is easy to see (Proposition 3.2) that if, for some $Q \in \mathcal{L}$, we write $Q(z) = \tilde{Q}(z^l) + R(z)$ where the coefficients of z^{nl} in $R \in \mathcal{L}$ vanish for all $n \in \mathbb{Z}$, then Q satisfies (A) if and only if

$$\oint_{|z|=1} \tilde{P}^k(z)\, d\tilde{Q}(z) = 0, \quad k = 0, 1, 2, \ldots. \tag{1.4}$$

Thus, the problem can be reduced to one of lower degree (1.4). We call this condition (B):

$$\begin{gathered} P = \tilde{P}(z^l), \quad Q = \tilde{Q}(z^l) + \sum_{l \nmid i} a_i z^i, \\ \oint_{|z|=1} \tilde{P}^k(z)\, d\tilde{Q}(z) = 0, \quad k = 0, 1, 2, \ldots. \end{gathered} \tag{B}$$

On the other hand, if P can be factorized as $P = P_k \circ W_k$ for some $P_k \in \mathbb{C}[z]$ and $W_k \in \mathcal{L}$, $k = 1, \ldots, l$, then a straightforward computation (Proposition 3.3) shows that (A) will be satisfied whenever we can write

$$Q = Q_1 \circ W_1 + \cdots + Q_l \circ W_l, \tag{1.5}$$

for some $Q_k \in \mathbb{C}[z]$. We call this condition (C):

$$\begin{gathered} P = P_k(W_k), \quad P_k, Q_k \in \mathbb{C}[z], \quad W_k \in \mathcal{L}, \quad k = 1, \ldots, l, \\ Q = Q_1 \circ W_1 + \cdots + Q_l \circ W_l. \end{gathered} \tag{C}$$

Our approach to these problems is via the monodromy group of the Laurent polynomial P. In particular, we find a condition (B^*) on the monodromy group which is satisfied if and only if $P = \tilde{P}(z^l)$ for some $l > 1$ (Lemma 2.4) and hence the problem is reducible to one of lower degree, and a condition (C^*) which if satisfied implies condition (C) for any Q satisfying (A) (Theorem 4.1).

In the following sections we show how the trigonometric moment problem can be translated in terms of the monodromy group of P and then, using the GAP program, show how all transitive permutation groups of degree 30 or less satisfy either condition (B^*) or (C^*) except for a relatively small number of exceptional groups. We then study three of the four simplest such groups in more detail (the other one has been studied by Pakovich *et al* in the paper [**18**]). We obtain corresponding Laurent polynomials, which are of degree 9, 10 and 16, respectively, and prove the existence of solutions not satisfying conditions (B) or (C).

In the final section we consider the case of real trigonometric polynomials, which is the most important case for applications. We show that in this case the monodromy group has additional structure and compute via GAP that all examples up to degree 30 fall into cases (B) or (C). We give a proof that this is also true whenever P has prime degree, but were unable to prove the general result, which we leave as a conjecture.

Restating Theorem 6.1 in terms of real trigonometric polynomials, we obtain the following result.

THEOREM 1.1. *Assume that P, Q are trigonometric polynomials with real coefficients up to degree* 15. *Then (1.3) holds if and only if either of the following conditions holds.*

https://doi.org/10.1017/etds.2012.143 Published online by Cambridge University Press

(1) *There exist a polynomial* $\tilde{P}$ *and an integer* $l > 1$, *such that* $P(\theta) = \tilde{P}(\sin(l\theta), \cos(l\theta))$. *In this case the terms in the Fourier expansion of* Q *in* $\cos(k\theta)$, $\sin(k\theta)$ *with* $l \nmid k$ *make no contribution to (1.3). Writing the remaining terms in* Q *as* $\tilde{Q}(\sin(l\theta), \cos(l\theta))$,

$$\int_0^{2\pi} \tilde{P}^i(\sin\theta, \cos\theta)\, d\tilde{Q}(\sin\theta, \cos\theta) = 0. \tag{1.6}$$

(2) *There exist polynomials* $\tilde{P}_k$ *and* $\tilde{Q}_k$ *and trigonometric polynomials* W_k *such that* $P(\theta) = \tilde{P}_k(W_k(\theta))$ *and* $Q(\theta) = \sum_k \tilde{Q}_k(W_k(\theta))$.

In case (1), condition (1.6) is of strictly smaller degree than (1.3). So we can solve the trigonometric moment problem by iterating this theorem.

2. *Preliminaries: decompositions of* P *and blocks of* G_P

Let us denote by $\mathcal{L}$ the ring of Laurent polynomials with complex coefficients. We shall consider $P \in \mathcal{L}$,

$$P(z) = \sum_{k=-m}^{n} a_k z^k,$$

where a_{-m} and a_n are non-zero and $n, m \geq 1$ (if $n = 0$ or $m = 0$, then the problem is solved in [**15**]).

A short, neat and simple proof of the next result can be found in [**15**, p. 25]. For more details, see [**16**] or [**23**, Lemma 2.1].

LEMMA 2.1. *If* $P = g \circ h$, *where* $P \in \mathcal{L}\backslash(\mathbb{C}[z] \cup \mathbb{C}[z^{-1}])$ *and* $g, h \in \mathbb{C}(z)$, *then there is a degree-one* $\mu \in \mathbb{C}(z)$ *such that* $G := g \circ \mu$ *and* $H := \mu^{-1} \circ h$ *satisfy one of the following cases:*

(1) $G \in \mathbb{C}[z]$ *and* $H \in \mathcal{L}$;
(2) $G \in \mathcal{L}$ *and* $H = z^k$ *for some* $k \in \mathbb{N}$.

Remark. The decompositions of the Laurent polynomial $P(z)$ induce decompositions on the trigonometric polynomial $P(e^{iz})$. Namely, if $P(z) = \tilde{P}(z^m)$, with $\tilde{P} \in \mathcal{L}$, then $P(e^{iz})$ is a trigonometric polynomial in $\sin(mz)$ and $\cos(mz)$. If $P(z) = \tilde{P}(W(z))$, with $\tilde{P} \in \mathbb{C}[z]$ and $W \in \mathcal{L}$, then $P(e^{iz}) = \tilde{P}(W(e^{iz}))$, thus, it is the composition of a polynomial and a trigonometric polynomial. We show in §6 that if we start with a real trigonometric polynomial, the decomposition can also be chosen to be expressible as the composition of a real polynomial with a real trigonometric polynomial.

Let $f \in \mathbb{C}(z)$ be a rational function. We say that $z_0 \in \mathbb{C}$ is a *critical point* of f if $f'(z_0) = 0$, and the value $f(z_0)$ is called a *critical value* of f. We will denote by Σ the set of all critical values of f. For $t \in \mathbb{C}\backslash\Sigma$, the set $f^{-1}(t)$ consists of m different points $z_i(t)$, $i = 1, \ldots, m$. By the implicit function theorem one can push locally each solution $z_i(t)$ to nearby values of t thus defining multi-valued analytic functions $z_i(t)$, $t \in \mathbb{C}\backslash\Sigma$. Each loop based at $t_0 \in \mathbb{C}\backslash\Sigma$ thus defines a permutation of the m roots $z_1(t_0), \ldots, z_m(t_0)$ of $f(z) = t_0$. These permutations depend only on the homotopy class of the loop and form a group G_f called the *monodromy group* of f, which is transitive

https://doi.org/10.1017/etds.2012.143 Published online by Cambridge University Press

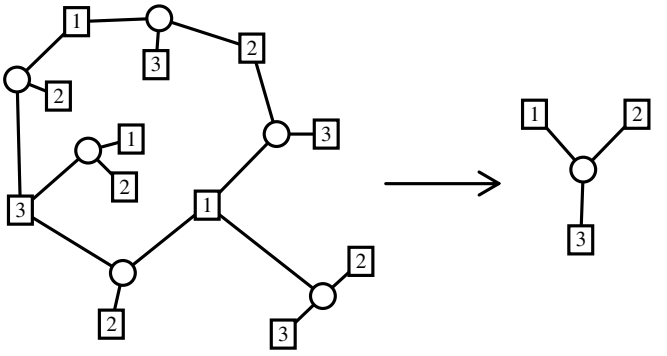


FIGURE 1. Constellation.

on the fiber $f^{-1}(t)$ (see, for example, [**24**]). Moreover, G_f is the Galois group of the Galois extension of $\mathbb{C}(t)$ by the m pre-images $z_1(t), \ldots, z_m(t)$ of $t \in \mathbb{C}\backslash\Sigma$ by f, that is,

$$G_f = \mathrm{Aut}(\mathbb{C}(z_1, \ldots, z_m)/\mathbb{C}(t)).$$

We recall that an extension $k \to L$ is said to be *Galois* if the degree of the extension coincides with the order of its automorphism group $G = \mathrm{Aut}(L/k) = \mathrm{Aut}_{k-\mathrm{alg}}(L, L)$:

$$[L : k] = |G|.$$

The automorphism group of a Galois extension is called the *Galois group* of the extension and is usually denoted by $\mathrm{Gal}(L/k)$, although we will use any of the previous notations when no confusion can arise. Any permutation $\sigma \in G_f$ is said to have *cycle shape* $(d_1)(d_2)\cdots(d_r)$ if σ is the product of r disjoint cycles $\sigma_1, \sigma_2, \ldots, \sigma_r$ with respective lengths $d_1 \geq d_2 \geq \cdots \geq d_r$.

Let $P \in \mathcal{L}$ be a Laurent polynomial and let $G_P = \mathrm{Gal}(L/\mathbb{C}(t))$ be its monodromy group, where $L = \mathbb{C}(z_1(t), \ldots, z_{n+m}(t))$ and $z_1, \ldots, z_{n+m}$ are the branches of P^{-1}. We shall number the branches of P^{-1} such that $\sigma_\infty = (1, 2, \ldots, n)(n+1, n+2, \ldots, n+m)$ is a permutation corresponding to a clockwise loop around infinity. A useful way to represent the monodromy group G_P of P is the so called *constellations*. Take $\Sigma = \{t_1, t_2, \ldots, t_r\}$, and let t_0 be a non-critical value. Consider the graph obtained by joining each of the critical values to t_0 with non-intersecting paths. Now take the pre-image of that 'star'. In Figure 1 we have denoted by circles the pre-images of the non-critical value, which can be identified with the branches, and by squares with a number the pre-images of the corresponding critical value. The permutation associated to a simple loop around one of the critical values can be obtained simply by rotating the branches connected with each pre-image of that critical value. This makes clear the relation between a critical value and a permutation associated to a simple loop around it: the critical value has associated critical points $w_1, w_2, \ldots, w_r$ with multiplicity $n_1, n_2, \ldots, n_r$ if and only if the cycle has cycle shape $(n_1)(n_2)\cdots(n_r)$. In Figure 1, the cycles associated to the critical values 1, 2 and 3 have shapes (3)(2), (2) and (3), respectively.

https://doi.org/10.1017/etds.2012.143 Published online by Cambridge University Press

The decompositions of a rational function induce imprimitivity systems in the monodromy group and vice versa. Let us describe this in more detail. A subset B of $X = \{1, 2, \ldots, n+m\}$ is called a *block* [**22**] of $G_P \subseteq S_{n+m}$ if for each $\sigma \in G_P$, either $\sigma(B) = B$ or $\sigma(B) \cap B = \varnothing$. Therefore, for a block B, $\mathcal{B} = \{\sigma(B) : \sigma \in G_P\}$ is a partition of X, which is called an *imprimitivity system* of G_P. There are always two *trivial* imprimitivity systems in G_P: the one generated by the block $B = \{1\}$, and the one generated by the block $B = X$. Let $G_{P,1}$ denote the subgroup of G_P which fixes the element 1; then the non-trivial block systems of G_P are in one-to-one correspondence with the subgroups H of G_P lying strictly between $G_{P,1}$ and G_P. Under this correspondence, the subgroups H are precisely the groups that stabilize the block which contains 1 in the imprimitivity system.

The non-trivial imprimitivity systems for a Laurent polynomial are described in the following result.

LEMMA 2.2. *Suppose that $n, m \neq 0$, and let $\mathcal{B}$ be a non-trivial imprimitivity system of G_P. Then one of the following cases holds.*

(a) *Every block $B \in \mathcal{B}$ is included in or disjoint with $\{1, \ldots, n\}$. In this case, there exists $d | \gcd(n, m)$ such that $\mathcal{B}$ coincides with the congruence classes modulo n/d in $\{1, \ldots, n\}$, and with the congruence classes modulo m/d in $\{n+1, \ldots, n+m\}$.*

(b) *Every block $B \in \mathcal{B}$ satisfies $B \cap \{1, \ldots, n\} \neq \varnothing$, $B \cap \{n+1, \ldots, n+m\} \neq \varnothing$. In this case, there exist $d | \gcd(n, m)$, $0 \leq r < d$, $k_B \in \mathbb{Z}$ such that*

$$B = \{i \in \{1, \ldots, n\} : i \equiv_d k_B\} \cup \{i \in \{n+1, \ldots, n+m\} : i \equiv_d k_B + r\},$$

that is, such that $B \cap \{1, \ldots, n\}$ is a congruence class modulo d in $\{1, \ldots, n\}$, and $B \cap \{n+1, \ldots, n+m\}$ is a congruence class modulo d in $\{n+1, \ldots, n+m\}$.

Proof. (a) Let $B \in \mathcal{B}$ be such that $B \subset \{1, \ldots, n\}$, the other case being analogous. Let $d = |B|$. Then, $\sigma_\infty^i(B)$ is also a block for $1 \leq i \leq n$, and $\{\sigma_\infty^i(B)\}_{1 \leq i \leq n}$ is a partition of $\{1, \ldots, n\}$ into subsets of the same cardinality. As a consequence, $\mathcal{B}$ restricted to $\{1, \ldots, n\}$ consists of the congruence classes modulo n/d.

Similarly, we can find $\bar{B} \in \mathcal{B}$ such that $\bar{B} \subset \{n+1, \ldots, n+m\}$, and, repeating the arguments, we obtain that $\mathcal{B}$ restricted to $\{n+1, \ldots, n+m\}$ is a congruence class modulo m/d.

(b) If $B \in \mathcal{B}$ satisfies $B \cap \{1, \ldots, n\} \neq \varnothing$, $B \cap \{n+1, \ldots, n+m\} \neq \varnothing$, then $\{\sigma_\infty^i(B)\}_{1 \leq i \leq n}$ defines one partition in $\{1, \ldots, n\}$ and another (related) in $\{n+1, \ldots, n+m\}$ of the same cardinality. Let

$$d = |\{1, \ldots, n\}|/|B \cap \{1, \ldots, n\}| = |\{n+1, \ldots, n+m\}|/|B \cap \{n+1, \ldots, n+m\}|.$$

Then each $B \in \mathcal{B}$ belongs to a congruence class modulo d in $\{1, \ldots, n\}$ and a congruence class modulo d in $\{n+1, \ldots, n+m\}$. □

Given a rational function $f(z)$ of degree m and Σ its set of critical values, we say that two *decompositions* $\tilde{f} \circ h$ and $\tilde{f}' \circ h'$ of f are *equivalent* if h and h' define the same field over every pre-image of $t \in \mathbb{C} \backslash \Sigma$ by $f(z)$. That is, if $\mathbb{C}(h(z_i)) = \mathbb{C}(h'(z_i))$ for every $i = 1, \ldots, m$. There exists a one-to-one correspondence between imprimitivity systems

https://doi.org/10.1017/etds.2012.143 Published online by Cambridge University Press

of G_f and equivalence classes of decompositions of f (see [**1**]). Moreover, for Laurent polynomials we have the following result.

COROLLARY 2.3. *Let $P(z)$ be a Laurent polynomial. There exists a one-to-one correspondence between imprimitivity systems of G_P and decompositions of P. More precisely, non-trivial imprimitivity systems are in a one-to-one correspondence with Laurent polynomials W such that $P = \tilde{P} \circ W$ for some $\tilde{P} \in \mathcal{L}$ up to equivalence by a Möbius transformation.*

Proof. Under the Galois correspondence, $\mathbb{C}(t)$ is the fixed field of G_P and $\mathbb{C}(z_1)$ is the fixed field of the group $G_{P,1}$. For any imprimitivity system $\mathcal{B}$ of G_P, we let $B \in \mathcal{B}$ denote the block containing the element 1. The group that fixes this block generates a fixed field $L_B \subseteq \mathbb{C}(z_1)$, which by Lüroth's theorem [**21**] is generated by a rational function $W \in \mathbb{C}(z_1)$. Since $\mathbb{C}(t) \subset \mathbb{C}(W)$, we must have $P(z_1) = t = \tilde{P}(W(z_1))$ for some rational function $\tilde{P}$ so that $P = \tilde{P} \circ W$. Clearly, distinct imprimitivity systems give distinct fixed fields and hence distinct factorizations. Any other generator of $\mathbb{C}(W(z_1))$ must be of the form $W_1 = \mu \circ W$, for some Möbius transformation μ.

Conversely, given a non-trivial decomposition $P = \tilde{P} \circ W$ we can form a chain of vector fields $\mathbb{C}(t) \subsetneq \mathbb{C}(W(z_1)) \subsetneq \mathbb{C}(z_1)$, by the Galois correspondence. This gives us a subgroup of G_P lying strictly between $G_{P,1}$ and G_P, and hence gives rise to an imprimitivity system. □

Moreover, we can determine the type of decomposition.

LEMMA 2.4. *Let P be a Laurent polynomial. The blocks of an imprimitivity system of G_P are contained in or disjoint with $\{1, \ldots, n\}$ if and only if the corresponding W of the decomposition of P is of the form $W(z) = z^k$.*

Proof. If $P = \tilde{P}(z^k)$, where $\tilde{P}$ is a Laurent polynomial, then we can find roots $\tilde{z}_j(t)$ of $\tilde{P} = t$. The roots $P(z) = t$ are just the solutions of $z^k = \tilde{z}_j$ for some j, and clearly the roots associated to each $\tilde{z}_j(t)$ form an imprimitivity system. Furthermore, if $\tilde{z}_j(t)$ tends to zero as t tends to infinity then the same is true for all elements of the block, and similarly if $\tilde{z}_j(t)$ tends to infinity as t tends to infinity. Hence the blocks are either contained in or disjoint from $\{1, \ldots, n\}$.

Conversely, suppose we have such a block system and let $P(z) = \tilde{P}(W(z))$ denote the corresponding decomposition. By construction, the blocks of the system correspond to roots of $W(z) = \tilde{z}_j(t)$, where $\tilde{z}_j(t)$ are the roots of $\tilde{P}(z) = t$. By Lemma 2.1, if we cannot choose $W(z) = z^k$ for some k after composition with a Möbius transformation, then $\tilde{P}$ must be a polynomial and $W(z)$ a non-trivial Laurent polynomial. Hence, as t tends to infinity, all the $\tilde{z}_j$ will tend to infinity, and therefore the roots of $W(z) = \tilde{z}_j(t)$ will include both those which tend to zero and those which tend to infinity as t tends to infinity, which contradicts the assumption on the blocks. □

In particular, if $\mathbb{B}$ denotes the set of all imprimitivity systems of G_P, then using Lemma 2.2 we have $P = \tilde{P}(z^l)$, $l > 1$, if and only if the following condition holds:

$$\exists \mathcal{B} \in \mathbb{B}\ \exists B \in \mathcal{B}, \quad \{1\} \subsetneq B \subseteq \{1, \ldots, n\}. \tag{B^*}$$

https://doi.org/10.1017/etds.2012.143 Published online by Cambridge University Press

3. *Sufficiency of the weak composition condition*

In this section we study how decompositions of the Laurent polynomials produce solutions of (A). First we transform the problem into a more algebraic one.

PROPOSITION 3.1. *Let $P, Q \in \mathcal{L}$. The following conditions are equivalent:*

(1) $\oint_{|z|=1} P^k(z)\, dQ(z) = 0$ *for every* $k \geq 0$.

(2) $\oint_{|z|=1} (dQ(z)/(P(z)-t)) \equiv 0$ *for every* $t \in \mathbb{C}$.

(3) $\oint_{|z|=1} (Q(z)\, dP(z)/(P(z)-t)) \equiv 0$ *for every* $t \in \mathbb{C}$.

(4) *Take t close to infinity and number the pre-images $z_i(t)$ of $P(z) = t$ such that $\{z_k(t)\}_{k=1,\dots,n}$ (respectively, $\{z_k(t)\}_{k=n+1,\dots,n+m}$) are the points close to infinity (respectively, zero). Then*

$$\sum_{k=1}^{n} m\, Q(z_k(t)) - \sum_{k=n+1}^{n+m} n\, Q(z_k(t)) \equiv 0 \quad \text{for every } t \in \mathbb{C}. \tag{3.7}$$

Remark. In the notation of Gavrilov and Movasati [**10**], Proposition 3.1 states that, for any given P, Q is a solution of the Laurent moment problem if and only if the zero-dimensional abelian integral of Q is identically null along the zero-dimensional cycle

$$C(t) = \sum_{k=1}^{n} m\, Q(z_k(t)) - \sum_{k=n+1}^{n+m} n\, Q(z_k(t)).$$

This problem has recently been studied for simple cycles $(z_i(t) - z_j(t))$ in [**7**] and, more generally, for polynomial P, in [**1, 11**].

Note that also in [**15, 17, 18**] the problem is transformed into the vanishing of a zero-dimensional abelian integral of Q for a certain cycle. This cycle is defined in terms of the constellations, so the explicit computation for a given polynomial group is not direct.

Proof. Firstly, since $\int_{|z|=1} P^k(z)\, dQ(z)$ are the coefficients of the Taylor series of

$$\oint_{|z|=1} \frac{dQ(z)}{P(z)-t}$$

at infinity, (1) and (2) are equivalent. Moreover, the coefficients of the Taylor series of

$$\oint_{|z|=1} \frac{Q(z)\, dP(z)}{P(z)-t}$$

at infinity are the same except for the first one, which, being just $\oint dQ$, is trivially satisfied. Thus (3) is also equivalent to (1) and (2).

Now let us prove that (3) and (4) are equivalent. Take t close to infinity. By the residue theorem,

$$\oint_{|z|=1} \frac{Q(z)\, dP(z)}{P(z)-t} = 2\pi i \left(\sum_{k=n+1}^{n+m} Q(z_k(t)) - \operatorname{Res}(QP'/(t-P), 0) \right).$$

Assume that (3) holds. For any $\sigma \in G_P$, by analytic continuation,

$$\sum_{k=n+1}^{n+m} Q(z_k(t)) - \sum_{k=n+1}^{n+m} Q(z_{\sigma(k)}(t)) = 0,$$

https://doi.org/10.1017/etds.2012.143 Published online by Cambridge University Press

where $\sigma(k)$ just expresses the action of G_P on the roots z_i. If we sum the previous formula over G_P, we obtain

$$\sum_{k=n+1}^{n+m} |G_P| Q(z_k(t)) - \sum_{k=1}^{n+m} \frac{|G_P| m}{n+m} Q(z_k(t)) = 0. \tag{3.8}$$

Dividing by $|G_P|$ and multiplying by $n+m$ gives

$$\sum_{k=n+1}^{n+m} n Q(z_k(t)) - \sum_{k=1}^{n} m Q(z_k(t)) = 0.$$

Conversely, assume that (3.7) holds (or, equivalently, (3.8)). Integrating around a simple cycle containing no critical point,

$$\sum_{k=1}^{n+m} Q(z_k(t)) = \operatorname{Res}(QP'/(t-P), 0) + \operatorname{Res}(QP'/(t-P), \infty).$$

Therefore

$$\begin{aligned}
&\oint_{|z|=1} \frac{Q(z)\, dP(z)}{P(z)-t} \\
&\quad = 2\pi i \left(\frac{m}{n+m} \sum_{k=1}^{n+m} Q(z_k(t)) - \operatorname{Res}(QP'/(t-P), 0) \right) \\
&\quad = 2\pi i \left(\frac{m}{n+m} \operatorname{Res}(QP'/(t-P), \infty) - \frac{n}{n+m} \operatorname{Res}(QP'/(t-P), 0) \right).
\end{aligned}$$

Since

$$\begin{aligned}
\frac{1}{P(z)-t} &= \frac{z^m}{a_{-m} + \sum_{k=1-m}^{n} a_k z^{k+m} - t z^m} \\
&= \frac{z^m}{a_{-m}} \sum_{l \geq 0} \left(\frac{1}{a_{-m}} \sum_{k=1-m}^{n} t z^m - a_k z^{k+m} \right)^l,
\end{aligned}$$

$\operatorname{Res}(QP'/(P-t), 0)$ is a polynomial in t. Using the change of variables, $z \to z^{-1}$, $\operatorname{Res}(QP'/(P-t), \infty)$ is also a polynomial in t. But as t tends to infinity, the integral $\oint_{|z|=1} Q(z)\, dP(z)/(P(z)-t)$ tends to zero, so it is zero. □

Now we study solutions of (A) when P is decomposable. The first case is when P is a composition with inner term a power of z. We show that in that case the problem can be reduced to one of lower degree.

PROPOSITION 3.2. *Suppose that $P(z) = \tilde{P}(z^l)$, $l \in \mathbb{N}$, $\tilde{P} \in \mathcal{L}$, and let us write $Q(z) = \tilde{Q}(z^l) + R(z)$, where $R(z)$ contains all the terms of $Q(z)$ that are not divisible by z^l. Then Q satisfies (A) if and only if*

$$\oint_{|z|=1} \tilde{P}^n(z)\, d\tilde{Q}(z) = 0, \quad n = 0, 1, 2, \ldots.$$

Remark. Let us recall that $P(z) = \tilde{P}(z^l)$ if and only if $B \subset \{1, \ldots, n\}$ for some block B of some imprimitivity system $\mathcal{B}$, therefore this problem can be reduced to one of lower degree if condition (B^*) holds.

https://doi.org/10.1017/etds.2012.143 Published online by Cambridge University Press

Proof. This follows easily by taking into account that

$$\oint_{|z|=1} \tilde{P}^k(z^l)\, dR(z) = 0, \quad k = 0, 1, \ldots,$$

as the function $\tilde{P}^k(z^l)R'(z)$ can have no poles of order one in the region $|z| \leq 1$. □

The second case is when P can be written as a composition with inner term a Laurent polynomial. In this case, the weak composition condition is sufficient.

PROPOSITION 3.3. *Suppose that* $P(z) = P_k(W_k(z))$ *with* $W_k \in \mathcal{L}\backslash(\mathbb{C}[z] \cup \mathbb{C}[z^{-1}])$ *for* $k = 1, \ldots, l$. *Then* $Q(z) = Q_1(W_1(z)) + \cdots + Q_l(W_l(z))$ *satisfies (A) for all choices of polynomials* $Q_k(z)$, $k = 1, \ldots, l$.

Proof. By Lemma 2.1, $P_i(z)$ must be a polynomial. Therefore, after the change of variable $u = W_i(z)$,

$$\oint_{|z|=1} P^k(z)\, dQ_i(W_i) = \oint_{W^{-1}(|z|=1)} P_i^k(z)\, dQ_i(z) = 0, \quad k = 0, 1, 2, \ldots,$$

whence the result, since both P_i and Q_i are polynomials. □

4. *Main result*

In this section we obtain a condition (C^*) on the monodromy group G_P which guarantees that every solution of (A) satisfies the weak composition condition (C) if condition (B^*) does not hold.

Take t_0 close to infinity and number the branches such that $z_1(t_0), \ldots, z_n(t_0)$ are points close to infinity and $z_{n+1}(t_0), \ldots, z_{n+m}(t_0)$ are points close to zero, and moreover, such that the permutation corresponding to a simple clockwise loop around infinity (not containing any other singular point) is $(1, 2, \ldots, n)(n+1, n+2, \ldots, n+m)$.

Let us define V as the vector space generated by the action of G_P on the coefficients of (3.7):

$$V = \langle \sigma(m, \overset{(n)}{\ldots}, m, -n, \overset{(m)}{\ldots}, -n) \colon \sigma \in G_P \rangle.$$

Since we are studying when Q satisfies the weak composition condition, we shall check how to describe compositions in terms of the monodromy group. Note that if B is a block of an imprimitivity system of the action of G_P, and $1 \in B$, then

$$R_B = \sum_{i \in B} Q(z_i(t))$$

is a function invariant by the action of G_B, the stabilizer of B by G_P. Let L_B be the fixed field of G_B; then $L_B = \mathbb{C}(W_B(z_1(t)))$ for some $W_B(z) \in \mathbb{C}(t)$ by Lüroth's theorem. Hence $R_B = Q_B(W_B(z_1(t)))$ for some $Q_B \in \mathbb{C}(z)$. Moreover, $Q_B \circ W_B \in \mathcal{L}$. If condition (B^*) does not hold, W cannot be equivalent to z^n, and hence W_B and Q_B can be chosen so that W_B is a Laurent polynomial and Q_B is a polynomial. Clearly W_B also appears as a factor in a decomposition of $P = P_B \circ W_B$, where P_B must also be a polynomial.

For each block B we define w_B to be the vector with $(w_B)_i = 1$ when $i \in B$, and 0 otherwise. We define W to be the space generated by all vectors w_B where B runs over all

https://doi.org/10.1017/etds.2012.143 Published online by Cambridge University Press

blocks which contain the element 1 including the trivial block $B = \{1, \ldots, n+m\}$, but not $\{1\}$.

THEOREM 4.1. *Let P be a proper Laurent polynomial ($P \notin \mathbb{C}[z]$, $P \notin \mathbb{C}[z^{-1}]$), such that it does not admit a decomposition of the form $P(z) = \tilde{P}(z^l)$ for any $l > 1$. Assume that*

$$(1, 0, \ldots, 0) \in V + W. \tag{C^*}$$

Then (A) holds if and only if there exist $P_1, \ldots, P_r, Q_1, \ldots, Q_r \in \mathbb{C}[z]$, $W_1, \ldots, W_r \in \mathcal{L}\backslash(\mathbb{C}[z] \cup \mathbb{C}[z^{-1}])$ such that $P(z) = P_i(W_i(z))$, $i = 1, \ldots, r$, and $Q(z) = Q_1(W_1(z)) + \cdots + Q_r(W_r(z))$.

Proof. If there exist $P_1, \ldots, P_r, Q_1, \ldots, Q_r \in \mathbb{C}[z]$, $W_1, \ldots, W_r \in \mathcal{L}\backslash(\mathbb{C}[z] \cup \mathbb{C}[z^{-1}])$ such that $P(z) = P_i(W_i(z))$, $i = 1, \ldots, r$, and $Q(z) = Q_1(W_1(z)) + \cdots + Q_r(W_r(z))$, then Q satisfies (A) by Proposition 3.3.

Now, suppose that P does not admit a decomposition of the form $P(z) = \tilde{P}(z^l)$, and that $(1, 0, \ldots, 0) \in V + W$. By Proposition 3.1,

$$\sum_{k=1}^{n} m\, Q(z_k(t)) - \sum_{k=n+1}^{n+m} n\, Q(z_k(t)) \equiv 0,$$

and by analytic continuation and linearity,

$$\sum_{k=1}^{n+m} v_i\, Q(z_i(t)) \equiv 0 \quad \text{for every } (v_1, \ldots, v_{n+m}) \in V. \tag{4.9}$$

Given a block B_i containing 1, by the argument above, we have

$$R_{B_i} := \sum_{i \in B} Q(z_i(t)) = Q_{B_i}(W_{B_i}(z_1)),$$

for some polynomial Q_{B_i} and Laurent polynomial W_{B_i}.

If $(1, 0, \ldots, 0) \in V + W$, then there exists a linear combination

$$(1, 0, \ldots, 0) = \sum_i \lambda_i \sigma_i(m, \ldots, m, -n, \ldots, -n) + \sum_j \mu_j w_{B_j}.$$

Therefore, by (4.9)

$$Q(z_1(t)) = \sum_j \mu_j R_{B_j}(z_1(t)) = \sum_j \mu_j Q_{B_j}(W_{B_j}(z)),$$

and each W_{B_j} appears as a factor in a decomposition of $P = P_{B_j} \circ W_{B_j}$ where P_{B_j} is a polynomial. □

5. *Laurent polynomials up to degree 30*

Lemma 2.4 and Theorem 4.1 give a sufficient condition on the monodromy group of P, such that we can solve the Laurent moment problem. That is, we can first check whether G_P satisfies condition (B^*). If so, then the problem is reducible to a problem of lower degree (and the process can be repeated). If not, we can check whether G_P satisfies condition (C^*).

https://doi.org/10.1017/etds.2012.143 Published online by Cambridge University Press

Since for every fixed degree $n = \deg(P)$ the monodromy group is a transitive permutation group of degree n, there are only a finite number of possible monodromy groups. Moreover, there is a complete list of transitive permutation groups (up to isomorphism) of degree at most 30 contained in the computational group theory program GAP [**9**].

Using GAP, for every transitive permutation group G of degree at most 30, we consider all possible candidates for a permutation corresponding to a loop around infinity, that is, we consider all permutations, g, which are a product of two cycles and that move n points (by transitivity, it is only necessary to consider these cycles up to conjugacy), and all the imprimitivity systems for that group. Then we can easily check whether condition (B^*) holds or, failing that, whether (C^*) holds.

Moreover, we want to see if they can be realized as monodromy groups of Laurent polynomials. Given a set of k generators of the group and for each generator a ramification point on the Riemann sphere, we can invoke Riemann's Existence Theorem to guarantee that this monodromy group is realizable by an algebraic function which is ramified at exactly these points, and whose monodromy around these points is given by the generators (see [**12**]). Furthermore, we can calculate the genus of the covering given by the algebraic function via the Riemann–Hurwitz formula. If the genus of the cover is zero for some choice of generators for which the generator around infinity is g as above then the associated function must be a Laurent polynomial.

The whole process can be automated, and we obtain the following results, where the first row gives the degree of the permutation group, the second the number of non-isomorphic permutation groups and the final row the number of exceptions. For the other possible degrees less than 30 there are no exceptions (we have not given the number of possible transitive groups for these degrees).

Degree	9	10	16	18	20	24	25	27	30
Groups	34	45	1954	983	1117	25 000	211	2392	5712
Exceptions	1	2	6	6	3	3	2	31	10

THEOREM 5.1. *Let $\mathcal{L}_{30}$ be the set of Laurent polynomials up to degree* 30*. For any $P \in \mathcal{L}_{30}$, if G_P is not one of the exceptional groups in the list above, then $Q \in \mathcal{L}$ satisfies (A) if and only if it is reducible via condition (B) to a set of moment equations of lower degree, or satisfies the weak composition condition (C).*

Each of the exceptional groups above can be realized as the monodromy group of a Laurent polynomial, although it is only possible to explicitly calculate these polynomials in simple cases. We have not been able to verify that each exceptional group does indeed give Laurent polynomials P and Q which satisfy (A) but neither (B) nor (C), but we give in detail below three of the four simplest cases of exceptional groups, showing how they indeed give such Q. A fourth case is considered by Pakovich *et al* [**18**].

For the three cases detailed below, we have computed explicitly all Laurent polynomials Q of bi-degree $(n-1, m)$ satisfying (A) but neither (B) nor (C). To do this we invoke [**15**, Theorem 7.1] which says that if

$$\oint_{|z|=1} P^k(z)\, dQ(z) = 0, \quad k = 0, 1, \ldots, (v-1)\deg(Q) + 1,$$

https://doi.org/10.1017/etds.2012.143 Published online by Cambridge University Press

where v is the number of distinct vectors in the orbit of $(1, \overset{(n)}{\ldots}, 1, 0, \overset{(m)}{\ldots}, 0)$, then (A) holds.

Remark. For groups of low degree (up to 9) we have tried to find how many of the transitive permutations groups can actually be realized as monodromy groups of polynomials or Laurent polynomials. Although our calculations are not complete, at least half of these groups are realizable as such, and so the small number of exceptional cases in the table above does indeed appear to be noteworthy.

5.1. *Group* $A_5(10)$. The two groups of degree 10 are S_5 acting on 10 elements, for which there is an example not satisfying the weak composition condition [**18**], and A_5 acting on 10 elements ($A_5(10)$), with two possible choices of the cycle of infinity (both having cycle shape (5)(5)). The two possible infinity cycles for the group $A_5(10)$ are, up to conjugation, (1, 2, 3, 6, 8)(4, 9, 7, 5, 10) and (1, 2, 9, 6, 7)(3, 8, 4, 10, 5).

The elements of $A_5(10)$ can have cycle shape (2)(2)(2)(2), (3)(3)(3) or (5)(5). Since there must be 10 critical points, and previous permutations have 4, 6, and 8 critical points associated, respectively, then the unique possibility is that there are exactly two critical values, one of cycle shape (2)(2)(2)(2) and the other (3)(3)(3). Therefore, choosing one of the critical values as zero, and taking the leading coefficient equal to one, one obtains

$$P(z) = \frac{(z^3 + a_2z^2 + a_1z + a_0)^3(z + d)}{z^5},$$
$$P(z) - \lambda = \frac{(z^4 + b_3z^3 + b_2z^2 + b_1z + b_0)^2(z^2 + c_1z + c_0)}{z^5}.$$

Now differentiating,

$$P'(z) = \frac{(z^3 + a_2z^2 + a_1z + a_0)^2 Q_1(z)}{z^6} = \frac{(z^4 + b_3z^3 + b_2z^2 + b_1z + b_0)Q_2(z)}{z^6}.$$

Since $z^3 + a_2z^2 + a_1z + a_0$ does not divide $z^4 + b_3z^3 + b_2z^2 + b_1z + b_0$, $Q_1(z) = z^4 + b_3z^3 + b_2z^2 + b_1z + b_0$. Therefore, we have the following equation in $a_0, a_1, a_2, \lambda, d, c_0, c_1$:

$$P(z) - \lambda - \left(\frac{P'(z)z^6}{(z^3 + a_2z^2 + a_1z + a_0)^2}\right)^2 \frac{z^2 + c_1z + c_0}{z^5} = 0.$$

Solving that equation, the solutions with $a_0 \neq 0$ are

$$P(z) = \frac{(z + d)R^3(z)}{z^5},$$

where

$$R(z) = \frac{(123 + 55\sqrt{5})d^3}{2} + \frac{(29 + 13\sqrt{5})d^2z}{2} - (2 + \sqrt{5})dz^2 + z^3,$$

or

$$R(z) = \frac{(123 - 55\sqrt{5})d^3}{2} + \frac{(29 - 13\sqrt{5})d^2z}{2} - (2 - \sqrt{5})dz^2 + z^3.$$

https://doi.org/10.1017/etds.2012.143 Published online by Cambridge University Press

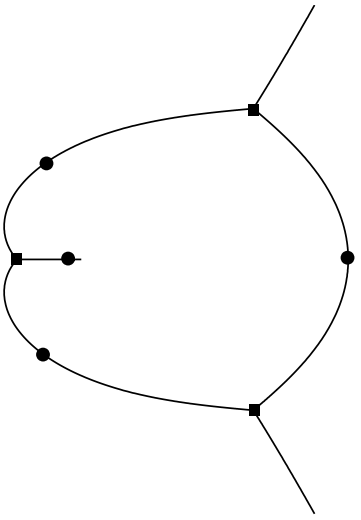


FIGURE 2. Constellation of $P(z)$.

We shall take the first solution and $d = 1$. It can be proved that its monodromy group is indeed $A_5(10)$, for instance, by computing its constellation (see Figure 2, where the circles and squares denote the pre-images of the two critical values). Moreover, as $A_5(10)$ has no non-trivial imprimitivity systems, P is indecomposable.

Now, we shall look for the solutions of the form

$$Q(z) = \sum_{i=-5}^{4} a_i z^i.$$

Imposing $\oint_{|z|=1} P^k \, dQ = 0$, for $k = 0, 1, \ldots, 5$, one obtains

$$\begin{aligned}
a_1 &= \frac{-7 + 3\sqrt{5}}{2} a_{-1} + 8(-38 + 17\sqrt{5}) a_{-2} + 3(-928 + 415\sqrt{5}) a_{-3} \\
&\quad + 4(445 - 199\sqrt{5}) a_{-4}, \\
a_2 &= \frac{-843 + 377\sqrt{5}}{2} a_{-2} + 3(-3571 + 1597\sqrt{5}) a_{-3} \\
&\quad + 24(-2889 + 1292\sqrt{5}) a_{-4}, \\
a_3 &= \frac{-15127 + 6765\sqrt{5}}{2} a_{-3} + 8(-12238 + 5473\sqrt{5}) a_{-4}, \\
a_4 &= \frac{-39603 + 17711\sqrt{5}}{2} a_{-4}, \quad a_{-5} = 0.
\end{aligned}$$

To prove that $\oint_{|z|=1} P^k \, dQ = 0$ for every $k \geq 0$, we use [**15**, Theorem 7.1]. This says that it is sufficient to check that $\oint_{|z|=1} P^k \, dQ = 0$ for every $0 \leq k \leq (v-1)\deg(Q) + 1 = 46$, where we have calculated (via GAP) that $v = 6$. This can be confirmed very easily via direct computer-aided computation (in our case with Mathematica and Maple).

https://doi.org/10.1017/etds.2012.143 Published online by Cambridge University Press

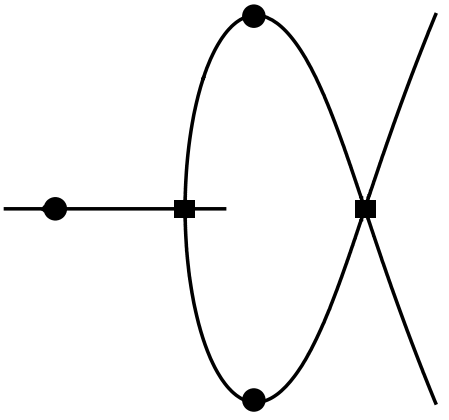


FIGURE 3. Constellation of $P(z)$.

Thus, discounting the constant solution, we have a four-dimensional vector space of solutions, Q, which do not satisfy the weak composition condition.

5.2. *Group* $E9 : D_8$. We now study the unique group of degree nine that we have obtained. For this group we obtain that the possible permutation corresponding to a loop around infinity has cycle shape (3)(6). Moreover, the permutations of $E9 : D_8$ have cycle shape (2)(2)(2), (2)(2)(2)(2), (3)(3)(3), (4)(4), (3)(6). After trying several combinations, considering two critical values with permutations associated with cycle shape (2)(2)(2) and (4)(4), and proceeding as in the group $A_5(10)$, we obtained the following Laurent polynomial with monodromy group $E9 : D_8$ with constellation shown in Figure 3 (again we denote the critical points corresponding to one of the critical values with squares and those corresponding to the other with circles):

$$P(z) = -\frac{(z-1)^4(2+z)(1+2z)^4}{2z^3}.$$

Although it is realizable with Laurent polynomials of degree nine, since the permutation corresponding to a loop around infinity has cycle shape (3)(6), the corresponding trigonometric polynomial has degree 12.

Now we check for the solutions $Q(z) = \sum_{k=-3}^{5} a_k z^k$, obtaining the three-dimensional space defined by the equations

$$a_{-2} = -a_4/2, \quad a_{-1} = -a_2 - 9a_4/2 + 5a_5/4, \quad a_3 = -15a_5/4, \quad a_{-3} = 0.$$

Again we use [**15**, Theorem 7.1], noting that v in this case is 6, and check that $\int_{|z|=1} P^k \, dQ = 0$ for every $0 \le k \le (v-1)\deg(Q) + 1 = 41$.

We note that P is indecomposable since the action of $E9 : D_8$ has no non-trivial imprimitivity system. Hence, discounting the constant solution and noting that a_1 can be chosen arbitrarily in the equations above, we obtain a four-dimensional space of solutions that do not satisfy the composition condition.

https://doi.org/10.1017/etds.2012.143 Published online by Cambridge University Press

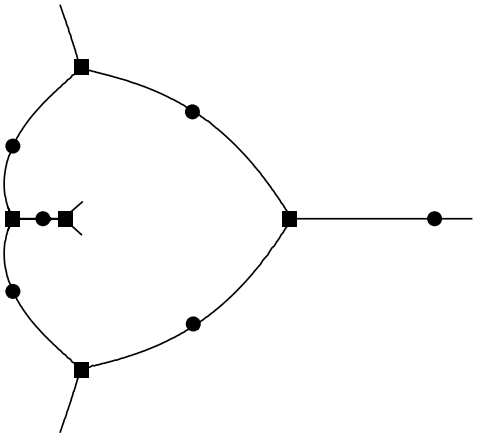


FIGURE 4. Constellation of $P(z)$.

5.3. *Group t16n195.* The simplest case where the action of the monodromy group has a non-trivial imprimitivity system is the group of degree 16 with number 195 in GAP. A Laurent polynomial having this group as its monodromy group (which is represented in Figure 4) is

$$\begin{aligned} P(z) = {} & -940848 + 665280\sqrt{2} + (89152 - 63040\sqrt{2})W(z) \\ & - (2376 - 1680\sqrt{2})W^2(z) + W^4(z), \end{aligned}$$

where

$$W(z) = \frac{-99 + 70\sqrt{2} + (48 - 34\sqrt{2})z + (8 - 6\sqrt{2})z^3 + z^4}{z^2}.$$

Since the group $t16n195$ has a unique non-trivial imprimitivity system, the decomposition above is the only one possible.

We seek a solution $Q(z) = \sum_{k=-8}^{7} a_k z^k$. However, since we can ignore the constant solution, and we already know that all linear combinations of W, W^2 and W^3 are solutions which satisfy the composition conjecture, we shall make the assumption that $a_{2k} = 0$ for $k = 0, 1, 2, 3$. The remaining solutions must therefore be exceptional ones.

A calculation in GAP shows that $v = 12$ in this case. Hence, by [**15**, Theorem 7.1], it is sufficient to calculate the integral up to $k = 155$. The solutions form a six-dimensional space. As the expressions are cumbersome, we only give two generators of this space:

$$Q_1 = 1/z^2 + (280 + 198\sqrt{2})z, \quad Q_2 = 1/z - (17 + 12\sqrt{2})z.$$

6. *Trigonometric polynomials with real coefficients*

In this section we consider trigonometric polynomials with real coefficients. In this case, the Laurent polynomial associated to the trigonometric polynomial via $z = \exp(i\theta)$, P, must satisfy the equation $\overline{P}(z) = P(1/z)$, where $\overline{P}(z) := \overline{P(\overline{z})}$. Conversely, any Laurent polynomial satisfying this equation must correspond to a real trigonometric polynomial. Every such polynomial must have bi-degree (n, n).

https://doi.org/10.1017/etds.2012.143 Published online by Cambridge University Press

It follows from the above that if $z(t)$ is a solution of $P(z) = t$ for $t \in \mathbb{R}$, $t \gg 0$, then so is $1/\overline{z}(t)$, where $\overline{z}(t) := \overline{z(\overline{t})}$. However, since the $z_i(t)$ are multi-valued, we will need to define the operation $\tau : f(t) \mapsto \overline{f}(t)$ with more care in order to specify it uniquely.

For $t \in \mathbb{R}$, $t \gg 0$, we label the roots as follows: $z_i = k\, w^i\, t^{1/n} + O(1)$ and $z_{n+i} = \overline{k}^{-1}\, w^{1-i}\, t^{-1/n} + O(1)$, where w is a primitive nth root of unity. The monodromy at infinity corresponds to the cycle $\sigma_\infty := (1, 2, \ldots, n)(n+1, n+2, \ldots, 2n)$, and we define the map $\tau(z_i(t)) = \overline{z}_i(t) = 1/z_{2n+1-i}$, $i = 1, \ldots, n$.

Clearly, τ extends to an element of the automorphism group $\tilde{G}_P$ of the field $\mathbb{C}(z_1, \ldots, z_n)$ over $\mathbb{R}(t)$. Since $|\tilde{G}_P|$ cannot exceed $|\mathbb{C}(z_1, \ldots, z_n) : \mathbb{R}(t)| = 2|G_P|$, we see that G_P is a normal subgroup of $\tilde{G}_P$ of index at most two.

We want to consider G_P by its action on the roots z_i. Unfortunately, the automorphism τ is not necessarily given by a permutation of the z_i. However, if $g \in G_P$, then the automorphism $\tau g \tau \in G_P$ gives the same permutation of the roots z_i as if we had taken τ to be represented by the permutation $\hat{\tau} = (1, 2n) \cdots (n, n+1)$.

Thus, working at the level of permutation groups, we define the group $\hat{G}_P$ to be the group $\langle G_P, \hat{\tau} \rangle$. In $\hat{G}_P$, the elements σ_∞ and τ generate a copy of the dihedral group D_{2n}.

It is easy to show that the calculations in §5 are unchanged if we replace G_P by $\hat{G}_P$. This is because the block structure for the two groups is the same. Furthermore, every element of $\hat{G}_P$ is either of the form g or $g\hat{\tau}$ for some g in G_P. Since $\hat{\tau}(1, \overset{(n)}{\ldots}, 1, 0, \overset{(n)}{\ldots}, 0) = (1, \overset{(2n)}{\ldots}, 1) - (1, \overset{(n)}{\ldots}, 1, 0, \overset{(n)}{\ldots}, 0)$, we see that any element of $V + W$ in Theorem 4.1 generated from $\hat{G}_P$ can in fact be generated from G_P.

Thus, in the real trigonometric case, we can apply our calculations to $\hat{G}_P$ rather than G_P, and assume the existence of $\hat{\tau}$. Adding this information into GAP, we find that all transitive permutation groups of degree 30 or less which contain a dihedral subgroup as above must satisfy condition (B^*) or (C^*).

THEOREM 6.1. *Let $\mathcal{L}^*_{30}$ be the set of Laurent polynomials up to degree 30 associated to real trigonometric polynomials via $z = \exp(i\theta)$.*

For any $P \in \mathcal{L}^*_{30}$, $Q \in \mathcal{L}$ satisfies (A) if and only if either it is reducible via condition (B) to a set of moment equations of lower degree, or it satisfies condition (C). In the first case, the reduced moment equations still satisfy the condition $\tilde{P}(z) = \overline{\tilde{P}(1/\overline{z})}$, and so we can iterate this process of reduction so that all Q satisfying (A) can be explained by these two processes.

CONJECTURE 6.2. *For every Laurent polynomial P obtained by a change of variables from a real trigonometric polynomial, a Laurent polynomial Q satisfies (A) if and only if it satisfies (B) or (C).*

We note that when condition (B) holds, and $P = \tilde{P}(z^k)$, then the decomposition corresponds to expressing the original polynomials in terms of $\cos(k\theta)$ and $\sin(k\theta)$. The condition $\overline{P}(z) = P(1/z)$ then implies that $\tilde{P}$ is a real polynomial.

When condition (C) holds, we want to show that this decomposition can be written in such a way as to reduce to a decomposition of the associated real trigonometric polynomials.

https://doi.org/10.1017/etds.2012.143 Published online by Cambridge University Press

Let $P(z) = \tilde{P}(W(z))$ be the decomposition, where we can choose $\tilde{P}$ to be a monic polynomial without loss of generality. From the condition $\overline{P}(1/z) = P(z)$ we see that the highest- and lowest-order terms of $W(z)$ must be in the form kz^r and $\overline{k}z^{-r}$ for some $k \neq 0$ and r. Now, it is easy to see that

$$\overline{P}(1/z) - P(z) = (\overline{W}(1/z) - W(z))((n/r)k^{n/r-1}z^{n-r} + \cdots).$$

Since this second term does not vanish, the first must be zero, and hence W is the Laurent polynomial associated to a real trigonometric polynomial. It is straightforward to show that $\overline{P}(z) = P(1/z)$ implies that $\tilde{P}$ must therefore be a real polynomial.

Now we shall prove that the conjecture is true when the degree of P is $2n$, with n a prime number.

THEOREM 6.3. *Suppose that* $\deg(P) = 2n$, *where* $n > 2$ *is a prime number. Then* $Q \in \mathcal{L}$ *satisfies (A) if and only if one of the following possibilities holds:*

(1) $P(z) = \tilde{P}(z^n)$, *and*

$$\oint_{|z|=1} \tilde{P}^k(z)\, d\tilde{Q}(z) = 0, \quad k = 0, 1, 2, \ldots,$$

where $\tilde{Q}(z^n)$ *is the sum of the monomials of* Q *divisible by* z^n.

(2) *There exist* $W \in \mathcal{L}\backslash(\mathbb{C}[z] \cup \mathbb{C}[z^{-1}])$, $\tilde{P}, \tilde{Q} \in \mathbb{C}[z]$, *such that* $P(z) = \tilde{P}(W(z))$, $Q(z) = \tilde{Q}(W(z))$.

Thus, (A) holds if and only if (B) or (C) holds.

Proof. By [**22**, Theorem 25.6] (or [**20**, Theorem 13.11.7]), since G_P contains a dihedral group as a regular subgroup then it is a B-group. This means that if there are no non-trivial blocks then the group is 2-transitive. In this case $W = \langle(1, \ldots, 1)\rangle$. If we sum up the vector $(1, \overset{(n)}{\ldots}, 1, -1, \overset{(n)}{\ldots}, -1)$ moved by the stabilizer of 1, we get a vector proportional to $(2n-1, -1, \overset{2n-1}{\ldots}, -1)$. Therefore, it is easy to prove that $(1, 0, \ldots, 0) \in V + W$ and so we are in case (2) above with $W = P$.

Suppose therefore, that a non-trivial block containing 1 is included in $\{1, 2, \ldots, n\}$, then in this case we can conclude that we are in case (1) by Theorem 4.1.

Suppose that there is no block containing 1 included in $\{1, 2, \ldots, n\}$. Then every block containing 1 is of the form $\{1, 1 + n + r\}$ for some $0 \leq r < n$. By the way that σ_∞ acts, the rest of the blocks are $\{i, i + n + r\}$, $1 \leq i \leq n$. If there are two such block systems, then taking the numbers $\{1, \ldots, 2n\}$ as vertices, and the blocks of the two block systems as edges, we get a graph which decomposes into a number of closed loops with an even number of edges (the vertices alternate between those in $\{1, \ldots, n\}$ and those in $\{n + 1, \ldots, 2n\}$, and the edges alternate between those corresponding to the two block groups). Since the group G_P takes the graph to itself, it is easy to see that the intersections of the set of vertices in each of these loops with $\{1, \ldots, n\}$ and $\{n + 1, \ldots, 2n\}$ give a block system with the block containing 1 lying within $\{1, 2, \ldots, n\}$. Hence, we are back in case (1) again.

Finally, we can suppose that we have just one block system, with blocks $B_i = \{i, i + n + r\}$, $1 \leq i \leq n$. Since $\{1, \ldots, n\}$ is not part of a block system, then there is at

https://doi.org/10.1017/etds.2012.143 Published online by Cambridge University Press

least one $\sigma \in G_P$ for which $\{1, \ldots, n\}$ has a non-empty image in both $\{1, \ldots, 2n\}$ and $\{n+1, \ldots, 2n\}$.

Let v_i be the vector with 1 in the ith position and -1 in the $(i+n+r)$th position. The element σ_∞ of G_P acts on the v_i as a cyclic group of order n. Since n is prime, there are only two rational invariant subspaces of the space generated by the v_i under the action of σ_∞. One is generated by $\sum v_i$ and the other is generated by all $\sum c_i v_i$ with $\sum c_i = 0$. Any $\sum d_i v_i$ with $\sum d_i \neq 0$ and with not all d_i the same must therefore generate the whole space under the action of σ_∞.

Let $v = (1, \overset{(n)}{\ldots}, 1, -1, \overset{(n)}{\ldots}, -1) = \sum v_i$; then since the action of σ respects the blocks, we see that $(\sigma(v) - v)/2 = \sum d_i v_i \in V$, where $d_i \in \{0, 1\}$. By our choice of σ, not all the d_i are zero nor are they all 1 and hence the element v_1 must also lie in V. Finally, let $v_{B_1} \in W$ be the vector associated to the block B_1; then we get $(1, 0, \ldots, 0) = (v_1 + v_{B_1})/2 \in V + W$. We are therefore in case (2). □

Acknowledgements. The authors are grateful to F. Pakovich for pointing out a mistake in the original version of this paper, and the referee for their comments. The first two authors are grateful to the University of Plymouth for its kind hospitality during the preparation of this work. The first and second authors were partially supported by Junta de Extremadura and FEDER funds and an MCYT/FEDER grant no. MTM2011-22751. The second author was partially supported by an MCYT/FEDER grant no. MTM2008-05460.

References

[1] A. Álvarez, J. L. Bravo and P. Mardešić. Vanishing abelian integrals on zero-dimensional cycles. *Preprint*, arXiv:1101.1777v2.

[2] M. Briskin, J. P. Françoise and Y. Yomdin. Center conditions, compositions of polynomials and moments on algebraic curves. *Ergod. Th. & Dynam. Sys.* **19**(5) (1999), 1201–1220.

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

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

[5] L. A. Cherkas. Number of limit cycles of an autonomous second-order system. *Differ. Uravn.* **12** (1975), 944–946.

[6] C. Christopher. Abel equations: composition conjectures and the model problem. *Bull. Lond. Math. Soc.* **32**(3) (2000), 332–338.

[7] C. Christopher and P. Mardešić. The monodromy problem and the tangential center problem. *Funktsional. Anal. i Prilozhen.* **44**(1) (2010), 27–43.

[8] J. P. Françoise, F. Pakovich, Y. Yomdin and W. Zhao. Moment vanishing problem and positivity: some examples. *Bull. Sci. Math.* **135**(1) (2011), 10–32.

[9] The GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.4.10; 2007, http://www.gap-system.org.

[10] L. Gavrilov and H. Movasati. The infinitesimal 16th Hilbert problem in dimension zero. *Bull. Sci. Math.* **131** (2007), 242–257.

[11] L. Gavrilov and F. Pakovich. Moments on Riemann surfaces and hyperelliptic Abelian integrals. *Preprint*, 15 July 2011, arXiv:1107.3029v1.

[12] G. Malle and H. Matzat. *Inverse Galois Theory*. Springer, Berlin, 1999.

https://doi.org/10.1017/etds.2012.143 Published online by Cambridge University Press

[13] F. Pakovich. Generalized 'second Ritt theorem' and explicit solution of the polynomial moment problem. *Preprint*, arXiv:0908.2508v3.
[14] F. Pakovich. On polynomials orthogonal to all powers of a given polynomial on a segment. *Israel J. Math.* **142** (2004), 273–283.
[15] F. Pakovich. On rational functions orthogonal to all powers of a given rational function on a curve. *Preprint*, arXiv:0910.2105v1.
[16] F. Pakovich. Prime and composite Laurent polynomials. *Bull. Sci. Math.* **133**(7) (2009), 693–732.
[17] F. Pakovich and M. Muzychuk. Solution of the polynomial moment problem. *Proc. Lond. Math. Soc.* **99**(3) (2009), 633–657.
[18] F. Pakovich, C. Pech and A. K. Zvonkin. Laurent polynomial moment problem: a case study. *Contemp. Math.* **532** (2010), 177–194.
[19] F. Pakovich, N. Roytvarf and Y. Yomdin. Cauchy type integrals of algebraic functions. *Israel J. Math.* **144** (2004), 221–291.
[20] W. R. Scott. *Group Theory*. Dover, New York, 1987.
[21] B. L. van der Waerden. *Algebra.* Vol. 1. Frederick Ungar, New York, 1970.
[22] H. Wielandt. *Finite Permutation Groups*. Academic Press, New York, 1964.
[23] M. E. Zieve. Decompositions of Laurent polynomials. *Preprint*, arXiv:0710.1902v1.
[24] H. Żołądek. *The Monodromy Group (Mathematics Institute of the Polish Academy of Science, Mathematical Monographs (New Series), 67)*. Birkhäuser, Basel, 2006.

https://doi.org/10.1017/etds.2012.143 Published online by Cambridge University Press