Math. Z. (2018) 288:299–310
https://doi.org/10.1007/s00209-017-1889-9

Mathematische Zeitschrift

CrossMark

On algebraic curves $A(x) - B(y) = 0$ of genus zero

Fedor Pakovich[1]

Received: 30 January 2016 / Accepted: 14 March 2017 / Published online: 12 May 2017

Abstract Using a geometric approach involving Riemann surface orbifolds, we provide lower bounds for the genus of an irreducible algebraic curve of the form $\mathcal{E}_{A,B}\,:\,A(x)-B(y)=0$, where $A, B \in \mathbb{C}(z)$. We also investigate "series" of curves $\mathcal{E}_{A,B}$ of genus zero, where by a series we mean a family with the "same" A. We show that for a given rational function A a sequence of rational functions B_i, such that $\deg B_i \to \infty$ and all the curves $A(x) - B_i(y) = 0$ are irreducible and have genus zero, exists if and only if the Galois closure of the field extension $\mathbb{C}(z)/\mathbb{C}(A)$ has genus zero or one.

Keywords Separated variable polynomials · Galois coverings · Rational points · Two-dimensional orbifolds

Mathematics Subject Classification 14H45 · 14G05 · 14H30 · 37F10

1 Introduction

The study of irreducible algebraic curves of genus zero having the form

$$\mathcal{E}_{A,B}\,:\,A(x)-B(y)=0, \tag{1}$$

where A and B are complex polynomials, has two main motivations. On the one hand, such curves have special Diophantine properties. Indeed, by the Siegel theorem, if an irreducible algebraic curve $\mathcal{C}$ with rational coefficients has infinitely many integer points, then $\mathcal{C}$ is of genus zero with at most two points at infinity. More generally, by the Faltings theorem, if $\mathcal{C}$ has infinitely many rational points, then $g(\mathcal{E}_{A,B}) \leq 1$. Therefore, since many interesting Diophantine equations have the form $A(x) = B(y)$, where $A, B \in \mathbb{Q}[z]$, the problem of description of curves $\mathcal{E}_{A,B}$ of genus zero is important for the number theory (see e.g. [3,7,13]).

✉ Fedor Pakovich
pakovich@math.bgu.ac.il

1 Department of Mathematics, Ben-Gurion University, P.O.B. 653, Beer-Sheva, Israel

On the other hand, for polynomials A and B with arbitrary complex coefficients the equality $g(\mathcal{E}_{A,B}) = 0$ holds if and only if there exist $C, D \in \mathbb{C}(z)$ satisfying the functional equation

$$A \circ C = B \circ D. \tag{2}$$

Since Eq. (2) describes situations in which a rational function can be decomposed into a composition of rational functions in two different ways, this equation plays a central role in the theory of functional decompositions of rational functions. Furthermore, functional Eq. (2) where C and D are allowed to be *entire* functions reduces to the case where $C, D \in \mathbb{C}(z)$ (see [2,18]). Thus, the problem of description of curves $\mathcal{E}_{A,B}$ of genus zero naturally appears also in the study of functional equations (see e.g. [7,17–19]).

Having in mind possible applications to Eq. (2) in rational functions, in this paper we study curves $\mathcal{E}_{A,B}$ allowing A and B to be arbitrary *rational* functions meaning by $\mathcal{E}_{A,B}$ the expression obtained by equating to zero the numerator of $A(x) - B(y)$. Notice that the curve $\mathcal{E}_{A,B}$ may turn out reducible. In this case its analysis is more complicated and has a different flavor (see e.g. [10]), so below we always will assume that considered curves $\mathcal{E}_{A,B}$ are irreducible.

For polynomial A and B the classification of curves $\mathcal{E}_{A,B}$ of genus zero with one point at infinity follows from the so-called "second Ritt theorem" [21] about polynomial solutions of (2). Namely, any such a curve has either the form

$$x^n - y^s R^n(y) = 0, \tag{3}$$

where R is an arbitrary polynomial and $\gcd(s, n) = 1$, or the form

$$T_n(x) - T_m(y) = 0, \tag{4}$$

where T_n, T_m are Chebyshev polynomials and $\gcd(n, m) = 1$. The classification of polynomial curves $\mathcal{E}_{A,B}$ of genus zero with at most two points at infinity was obtained in the paper of Bilu and Tichy [3], which continued the line of researches started by Fried (see [7–9]). In this case, in addition to the above curves we have the following possibilities:

$$x^2 - (1 - y^2)S^2(y) = 0, \tag{5}$$

where S is an arbitrary polynomial,

$$T_{2n}(x) + T_{2m}(y) = 0, \tag{6}$$

where $\gcd(n, m) = 1$, and

$$(3x^4 - 4x^3) - (y^2 - 1)^3 = 0. \tag{7}$$

Finally, the classification obtained in [3] was extended to the case where A and B are allowed to be Laurent polynomials in [17]. In this case, to the list above one has to add the possibility for R in (3) to be a Laurent polynomial, and the curve

$$\frac{1}{2}\left(y^n + \frac{1}{y^n}\right) - T_m(x) = 0, \tag{8}$$

where $\gcd(n, m) = 1$. Notice also that an explicit classification of curves (1) of genus *one* with one point at infinity for polynomial A and B was obtained by Avanzi and Zannier [1]. The above results essentially exhaust the list of general results concerning the problem of description of irreducible curves $\mathcal{E}_{A,B}$ of small genus.

All the curves $\mathcal{E}_{A,B}$ of genus zero listed above, except for (7), obviously share the following feature: in fact they are "series" of curves with the "same" A. We formalize this observation as follows. Say that a rational function A is a *basis of series of curves of genus zero* if there exists a sequence of rational functions B_i such that $\deg B_i \to \infty$ and all the curves $A(x) - B_i(y) = 0$ are irreducible and have genus zero. Clearly, a description of all bases of series is an important step in understanding of the general problem, and the main goal of the paper is to provide such a description in geometric terms.

Recall that for a rational function A its normalization $\widetilde{A}$ is defined as a holomorphic function of the lowest possible degree between compact Riemann surfaces $\widetilde{A} : \widetilde{S}_A \to \mathbb{CP}^1$ such that $\widetilde{A}$ is a Galois covering and $\widetilde{A} = A \circ H$ for some holomorphic map $H : \widetilde{S}_A \to \mathbb{CP}^1$. From the algebraic point of view, the passage from A to $\widetilde{A}$ corresponds to the passage from the field extension $\mathbb{C}(z)/\mathbb{C}(A)$ to its Galois closure. In these terms our main result about bases of series is the following statement.

Theorem 1 *A rational function A is a basis of series of curves of genus zero if and only if the Galois closure of $\mathbb{C}(z)/\mathbb{C}(A)$ has genus zero or one.*

Thus, the set of possible bases of series splits into two classes. Elements of the first class are "compositional left factor" of well known Galois coverings of $\mathbb{CP}^1$ by $\mathbb{CP}^1$ calculated for the first time by Klein [12]. In particular, up to the change $A \to \mu_1 \circ A \circ \mu_2$, where μ_1 and μ_2 are Möbius transformations, besides the functions

$$z^n, \qquad T_n, \qquad \frac{1}{2}\left(z^n + \frac{1}{z^n}\right), \quad n \geq 1, \tag{9}$$

this class contains only a finite number of functions which can be calculated explicitly. For instance, the polynomial $3x^4 - 4x^3$ appearing in (7) is an example of such a function, implying that curve (7) in fact also belongs to a series of curves of genus zero (see Sect. 5 below). Typical representatives of the second class, consisting of rational compositional left factors of Galois coverings of $\mathbb{CP}^1$ by a torus, are Lattès functions (see e.g. [15]), but other possibilities also exist.

The approach of the papers [1,3,17] to the calculation of $g(\mathcal{E}_{A,B})$ is based on the formula, given in [9], which expresses $g(\mathcal{E}_{A,B})$ through the ramifications of A and B. Namely, if $c_1, c_2, \ldots c_r$ is a union of critical values of A and B, and $f_{i,1}, f_{i,2}, \ldots, f_{i,u_i}$ (resp. $g_{i,1}, g_{i,2}, \ldots, g_{i,v_i}$) is a collection of local degrees of A (resp. B) at the points of $A^{-1}(\{c_i\})$ (resp. $B^{-1}(\{c_i\})$), then $g(\mathcal{E}_{A,B})$ may be calculated as follows:

$$2 - 2g(\mathcal{E}_{A,B}) = \sum_{i=1}^{r} \sum_{j_1=1}^{u_i} \sum_{j_2=1}^{v_i} \gcd(f_{i,j_1} g_{i,j_2}) - (r-2) \deg A \deg B. \tag{10}$$

However, the direct analysis of this formula is quite difficult already in the above cases, and the further progress requires even more cumbersome considerations. In this paper we propose a new approach to the problem and prove the following general result.

Theorem 2 *Let A be a rational function of degree n. Then for any rational function B of degree m such that the curve $\mathcal{E}_{A,B}$ is irreducible the inequality*

$$g(\mathcal{E}_{A,B}) > \frac{m - 84n + 168}{84} \tag{11}$$

holds, unless the Galois closure of $\mathbb{C}(z)/\mathbb{C}(A)$ has genus zero or one.

Our approach is based on techniques introduced in the recent paper [20]. This paper studies rational solutions of the functional equation

$$A \circ X = X \circ B \tag{12}$$

using Riemann surface orbifolds. For the first time orbifolds were used in the context of functional equations in the paper [5] devoted to commuting rational functions. However, in [5] orbifolds appear in a dynamical context as a certain characteristic of the Poincaré function, while in [20] an orbifold is attached directly to any rational function. The approach of [20] permits to obtain restrictions on possible ramifications of solutions of (2) in terms of the corresponding orbifolds, and to give transparent proofs of Theorems 1 and 2.

The paper is organized as follows. In the second section we recall basic facts about Riemann surface orbifolds and some results from the papers [17,20]. We also express the condition that the Galois closure of $\mathbb{C}(z)/\mathbb{C}(A)$ has genus zero or one in terms of orbifolds. In the third and the fourth sections we prove Theorems 2 and 1 correspondingly. Finally, in the fifth section we consider an example illustrating Theorem 1.

2 Fiber products, orbifolds, and Galois coverings

A pair $\mathcal{O} = (R, \nu)$ consisting of a Riemann surface R and a ramification function $\nu : R \to \mathbb{N}$ which takes the value $\nu(z) = 1$ except at isolated points is called a Riemann surface orbifold (see e.g. [14, Appendix E]). The Euler characteristic of an orbifold $\mathcal{O} = (R, \nu)$ is defined by the formula

$$\chi(\mathcal{O}) = \chi(R) + \sum_{z \in R} \left(\frac{1}{\nu(z)} - 1 \right), \tag{13}$$

where $\chi(R)$ is the Euler characteristic of R. If R_1, R_2 are Riemann surfaces provided with ramification functions ν_1, ν_2, and $f : R_1 \to R_2$ is a holomorphic branched covering map, then f is called *a covering map* $f : \mathcal{O}_1 \to \mathcal{O}_2$ *between orbifolds* $\mathcal{O}_1 = (R_1, \nu_1)$ *and* $\mathcal{O}_2 = (R_2, \nu_2)$ if for any $z \in R_1$ the equality

$$\nu_2(f(z)) = \nu_1(z) \deg_z f \tag{14}$$

holds, where $\deg_z f$ denotes the local degree of f at the point z. If for any $z \in R_1$ instead of equality (14) a weaker condition

$$\nu_2(f(z)) \mid \nu_1(z) \deg_z f \tag{15}$$

holds, then f is called *a holomorphic map* $f : \mathcal{O}_1 \to \mathcal{O}_2$ *between orbifolds*. $\mathcal{O}_1$ *and* $\mathcal{O}_2$.

A universal covering of an orbifold $\mathcal{O}$ is a covering map between orbifolds $\theta_{\mathcal{O}} : \widetilde{\mathcal{O}} \to \mathcal{O}$ such that $\widetilde{R}$ is simply connected and $\widetilde{\nu}(z) \equiv 1$. If $\theta_{\mathcal{O}}$ is such a map, then there exists a group $\Gamma_{\mathcal{O}}$ of conformal automorphisms of $\widetilde{R}$ such that the equality $\theta_{\mathcal{O}}(z_1) = \theta_{\mathcal{O}}(z_2)$ holds for $z_1, z_2 \in \widetilde{R}$ if and only if $z_1 = \sigma(z_2)$ for some $\sigma \in \Gamma_{\mathcal{O}}$. A universal covering exists and is unique up to a conformal isomorphism of $\widetilde{R}$, unless $\mathcal{O}$ is the Riemann sphere with one ramified point, or $\mathcal{O}$ is the Riemann sphere with two ramified points z_1, z_2 such that $\nu(z_1) \neq \nu(z_2)$. Furthermore, $\widetilde{R} = \mathbb{D}$ if and only if $\chi(\mathcal{O}) < 0$, $\widetilde{R} = \mathbb{C}$ if and only if $\chi(\mathcal{O}) = 0$, and $\widetilde{R} = \mathbb{CP}^1$ if and only if $\chi(\mathcal{O}) > 0$ (see [14, Appendix E] and [6, Section IV.9.12]). Abusing notation we will use the symbol $\widetilde{\mathcal{O}}$ both for the orbifold and for the Riemann surface $\widetilde{R}$.

Covering maps between orbifolds lift to isomorphisms between their universal coverings. More generally, the following proposition holds (see [20, Proposition 3.1]).

Proposition 1 *Let $f : \mathcal{O}_1 \to \mathcal{O}_2$ be a holomorphic map between orbifolds. Then for any choice of $\theta_{\mathcal{O}_1}$ and $\theta_{\mathcal{O}_2}$ there exist a holomorphic map $F : \widetilde{\mathcal{O}_1} \to \widetilde{\mathcal{O}_2}$ and a homomorphism $\phi : \Gamma_{\mathcal{O}_1} \to \Gamma_{\mathcal{O}_2}$ such that the diagram*

$$\begin{array}{ccc} \widetilde{\mathcal{O}_1} & \xrightarrow{F} & \widetilde{\mathcal{O}_2} \\ \downarrow{\scriptstyle \theta_{\mathcal{O}_1}} & & \downarrow{\scriptstyle \theta_{\mathcal{O}_2}} \\ \mathcal{O}_1 & \xrightarrow{f} & \mathcal{O}_2 \end{array} \tag{16}$$

is commutative and for any $\sigma \in \Gamma_{\mathcal{O}_1}$ the equality

$$F \circ \sigma = \phi(\sigma) \circ F \tag{17}$$

holds. The map F is defined by $\theta_{\mathcal{O}_1}$, $\theta_{\mathcal{O}_2}$, and f uniquely up to a transformation $F \to g \circ F$, where $g \in \Gamma_{\mathcal{O}_2}$. In the other direction, for any holomorphic map $F : \widetilde{\mathcal{O}_1} \to \widetilde{\mathcal{O}_2}$ which satisfies (17) for some homomorphism $\phi : \Gamma_{\mathcal{O}_1} \to \Gamma_{\mathcal{O}_2}$ there exists a uniquely defined holomorphic map between orbifolds $f : \mathcal{O}_1 \to \mathcal{O}_2$ such that diagram (16) is commutative. The holomorphic map F is an isomorphism if and only if f is a covering map between orbifolds. □

If $f : \mathcal{O}_1 \to \mathcal{O}_2$ is a covering map between orbifolds with compact support, then the Riemann-Hurwitz formula implies that

$$\chi(\mathcal{O}_1) = d\chi(\mathcal{O}_2), \tag{18}$$

where $d = \deg f$. For holomorphic maps the following statement is true (see [20, Proposition 3.2]).

Proposition 2 *Let $f : \mathcal{O}_1 \to \mathcal{O}_2$ be a holomorphic map between orbifolds with compact support. Then*

$$\chi(\mathcal{O}_1) \leq \chi(\mathcal{O}_2) \deg f \tag{19}$$

and the equality holds if and only if $f : \mathcal{O}_1 \to \mathcal{O}_2$ is a covering map between orbifolds. □

Let R_1, R_2 be Riemann surfaces, and $f : R_1 \to R_2$ a holomorphic branched covering map. Assume that R_2 is provided with ramification function ν_2. In order to define a ramification function ν_1 on R_1 so that f would be a holomorphic map between orbifolds $\mathcal{O}_1 = (R_1, \nu_1)$ and $\mathcal{O}_2 = (R_2, \nu_2)$ we must satisfy condition (15), and it is easy to see that for any $z \in R_1$ a minimal possible value for $\nu_1(z)$ is defined by the equality

$$\nu_2(f(z)) = \nu_1(z)\gcd(\deg_z f, \nu_2(f(z)). \tag{20}$$

In case if (20) is satisfied for any $z \in R_1$ we say that f is *a minimal holomorphic map between orbifolds* $\mathcal{O}_1 = (R_1, \nu_1)$ *and* $\mathcal{O}_2 = (R_2, \nu_2)$. Notice that any covering map obviously is a minimal holomorphic map.

With any holomorphic function $f : R_1 \to R_2$ between compact Riemann surfaces one can associate in a natural way two orbifolds $\mathcal{O}_1^f = (R_1, \nu_1^f)$ and $\mathcal{O}_2^f = (R_2, \nu_2^f)$, setting $\nu_2^f(z)$ equal to the least common multiple of local degrees of f at the points of the preimage $f^{-1}\{z\}$, and

$$\nu_1^f(z) = \nu_2^f(f(z))/\deg_z f.$$

By construction, f is a covering map between orbifolds $f : \mathcal{O}_1^f \to \mathcal{O}_2^f$. Furthermore, since the composition $f \circ \theta_{\mathcal{O}_1^f} : \widetilde{\mathcal{O}_1^f} \to \mathcal{O}_2^f$ is a covering map between orbifolds, it follows from the uniqueness of the universal covering that

$$\theta_{\mathcal{O}_2^f} = f \circ \theta_{\mathcal{O}_1^f}. \tag{21}$$

For rational functions A and B irreducible components of $\mathcal{E}_{A,B}$ correspond to irreducible components of the fiber product of A and B. In particular, if $\mathcal{E}_{A,B}$ is an irreducible curve and $\widetilde{\mathcal{E}}_{A,B}$ is its desingularization, then there exist holomorphic functions $p, q : \widetilde{\mathcal{E}}_{A,B} \to \mathbb{CP}^1$ such that

$$A \circ p = B \circ q, \tag{22}$$

and

$$\deg A = \deg q, \quad \deg B = \deg p \tag{23}$$

(see [17, Theorem 2.2 and Proposition 2.4]). Furthermore, the functions A, B, p, q possess "good" properties with respect to the associated orbifolds defined above. Namely, the following statement holds (see [20, Theorem 4.2 and Lemma 2.1]).

Theorem 3 *Let A, B be rational functions such that the curve $\mathcal{E}_{A,B}$ is irreducible, and $p, q : \widetilde{\mathcal{E}}_{A,B} \to \mathbb{CP}^1$ holomorphic functions such that equalities (22) and (23) hold. Then the commutative diagram*

$$\begin{array}{ccc} \mathcal{O}_1^q & \xrightarrow{p} & \mathcal{O}_1^A \\ \downarrow q & & \downarrow A \\ \mathcal{O}_2^q & \xrightarrow{B} & \mathcal{O}_2^A \end{array}$$

consists of minimal holomorphic maps between orbifolds. □

Of course, vertical arrows in the above diagram are covering maps and hence minimal holomorphic maps simply by definition. The meaning of the theorem is that the branching of q and A to a certain extent defines the branching of p and B. For example, Theorem 3 applied to functional Eq. (12) where A, X, B are rational functions such that $\mathcal{E}_{A,X}$ is irreducible, implies that $\chi(\mathcal{O}_2^X) \geq 0$ (see [20]).

For a rational function A the condition $\chi(\mathcal{O}_2^A) \geq 0$ is very restrictive, and is equivalent to the condition that the normalization of A has genus at most one.

Lemma 1 *Let A be a rational function. Then $g(\widetilde{S}_A) = 0$ if and only if $\chi(\mathcal{O}_2^A) > 0$, and $g(\widetilde{S}_A) = 1$ if and only if $\chi(\mathcal{O}_2^A) = 0$.*

Proof Let $f : S \to \mathbb{CP}^1$ be an arbitrary Galois covering of $\mathbb{CP}^1$. Then f is a quotient map $f : S \to S/\Gamma$ for some subgroup Γ of $Aut(S)$, and for any branch point z_i, $1 \leq i \leq r$, of f there exists a number d_i such that $f^{-1}\{z_i\}$ consists of $|G|/d_i$ points, at each of which the multiplicity of f equals d_i. Applying the Riemann-Hurwitz formula, we see that

$$2g(S) - 2 = -2|\Gamma| + \sum_{i=1}^{r} \frac{|\Gamma|}{d_i}(d_i - 1),$$

implying that

$$\chi(\mathcal{O}_2^f) = 2 + \sum_{i=1}^{r} \left(\frac{1}{d_i} - 1 \right) = \frac{2 - 2g(S)}{|\Gamma|}. \tag{24}$$

Thus, if $f : S \to \mathbb{CP}^1$ is a Galois covering, then $g(S) = 0$ if and only if $\chi(\mathcal{O}_2^f) > 0$, while $g(S) = 1$ if and only if $\chi(\mathcal{O}_2^f) = 0$.

Let now $A : \mathbb{CP}^1 \to \mathbb{CP}^1$ be an arbitrary rational function. Since the normalization $\widetilde{A} : \widetilde{S}_A \to \mathbb{CP}^1$ of A can be described as any irreducible component of the m-fold fiber product of A distinct from the diagonal components where two or more coordinates are equal (see [11, §I.G],), it follows from the construction of the fiber product (see e.g. [17, Section 2 and 3]) that

$$\mathcal{O}_2^A = \mathcal{O}_2^{\widetilde{A}}. \tag{25}$$

Thus, $g(\widetilde{S}_A) = 0$ if and only if $\chi(\mathcal{O}_2^A) > 0$, and $g(\widetilde{S}_A) = 1$ if and only if $\chi(\mathcal{O}_2^A) = 0$. □

If $\mathcal{O} = (\mathbb{CP}^1, \nu)$ is an orbifold such that $\chi(\mathcal{O}) = 0$, then (13) implies that the collection of ramification indices of $\mathcal{O}$ is either $(2, 2, 2, 2)$, or one of the following triples $(3, 3, 3)$, $(2, 4, 4)$, $(2, 3, 6)$. For all such orbifolds $\widetilde{\mathcal{O}} = \mathbb{C}$. Furthermore, the group $\Gamma_{\mathcal{O}}$ is generated by translations of $\mathbb{C}$ by elements of some lattice $L \subset \mathbb{C}$ of rank two and the transformation $z \to \varepsilon z$, where ε is nth root of unity with n equal to 2,3,4, or 6, such that $\varepsilon L = L$. For the collection of ramification indices $(2, 2, 2, 2)$ the complex structure of $\mathbb{C}/L$ may be arbitrary and the function $\theta_{\mathcal{O}}$ is the corresponding Weierstrass function $\wp(z)$. On the other hand, for the collections $(2, 4, 4)$, $(2, 3, 6)$, $(3, 3, 3)$ this structure is rigid and arises from the tiling of $\mathbb{C}$ by squares, equilateral triangles, or alternately colored equilateral triangles, respectively. Accordingly, the functions $\theta_{\mathcal{O}}$ may be written in terms of the corresponding Weierstrass functions as $\wp^2(z)$, $\wp'^2(z)$ and $\wp'(z)$ (see [6,15, Section IV.9.12]).

Similarly, if $\chi(\mathcal{O}) > 0$, then the collection of ramification indices of $\mathcal{O}$ is either (n, n) for some $n \geq 2$, or $(2, 2, n)$ for some $n \geq 2$, or one of the following triples $(2, 3, 3)$, $(2, 3, 4)$, $(2, 3, 5)$. In fact, formula (13) also allows $\mathcal{O}$ to be a non-ramified sphere or one of two orbifolds without universal covering. However, if $\mathcal{O} = \mathcal{O}_2^A$ for some rational function A, then these cases are impossible since for any rational function A both orbifolds $\mathcal{O}_1^A$, $\mathcal{O}_2^A$ have a universal covering (see [20, Lemma 4.2]), and $\mathcal{O}_2^A$ cannot be non-ramified. Further, $\widetilde{\mathcal{O}} = \mathbb{CP}^1$, and the group $\Gamma_{\mathcal{O}}$ is a finite subgroup of the automorphism group of $\mathbb{CP}^1$. Namely, to orbifolds with the collections of ramification indices (n, n), $(2, 2, n)$, $(2, 3, 3)$, $(2, 3, 4)$, and $(2, 3, 5)$ correspond the groups C_n, D_{2n}, A_4, S_4, and A_5. The corresponding functions $\theta_{\mathcal{O}}$ are Galois coverings of $\mathbb{CP}^1$ by $\mathbb{CP}^1$ and have degrees n, $2n$, 12, 24, and 60 (see [12]).

3 Proof of Theorem 2

First of all, observe that if $f : R \to \mathbb{CP}^1$ is a holomorphic function of degree n on a Riemann surface R of genus g, then

$$\chi(\mathcal{O}_2^f) > 4 - 2g - 2n. \tag{26}$$

Indeed, it follows from the definition that

$$\chi(\mathcal{O}_2^f) > 2 - c(f),$$

where $c(f)$ denotes the number of branch points of f. On the other hand, since the number $c(f)$ is less than or equal to the number of points $z \in R$ where $\deg_z f > 1$, the Riemann-Hurwitz formula

$$\chi(R) = \chi(\mathbb{CP}^1)n - \sum_{z \in R}(\deg_z f - 1)$$

implies that

$$c(f) \leq \chi(\mathbb{CP}^1)n - \chi(R).$$

Thus,

$$\chi(\mathcal{O}_2^f) > 2 + \chi(R) - \chi(\mathbb{CP}^1)n,$$

implying (26).

Let now $p, q : \widetilde{\mathcal{E}}_{A,B} \to \mathbb{CP}^1$ be holomorphic functions such that (22) and (23) hold. Since $B : \mathcal{O}_2^q \to \mathcal{O}_2^A$ is a minimal holomorphic map between orbifolds by Theorem 3, it follows from Proposition 2 that

$$\chi(\mathcal{O}_2^q) \leq m\chi(\mathcal{O}_2^A). \tag{27}$$

On the other hand, (13) implies that if $\chi(\mathcal{O}) < 0$, then in fact

$$\chi(\mathcal{O}) \leq -\frac{1}{42} \tag{28}$$

(where the equality is attained for the collection of ramification indices (2, 3, 7)). Therefore, if $\chi(\mathcal{O}_2^A) < 0$, then (28) and (26) imply the inequality

$$4 - 2g - 2n < -\frac{m}{42}$$

which in turn implies (11). □

4 Proof of Theorem 1

It follows from Theorem 2 and Lemma 1 that we only need to show that if $\chi(\mathcal{O}_2^A) \geq 0$, then A is a basis of series. Assume first that $\chi(\mathcal{O}_2^A) = 0$. Then the universal covering of $\mathcal{O}_2^A$ is $\mathbb{C}$, and the group $\Gamma_{\mathcal{O}_2^A}$ is generated by translations of $\mathbb{C}$ by elements of some lattice $L =< \omega_1, \omega_2 >$ and the transformation $z \to \varepsilon z$, where ε is an nth root of unity with n equal to 2,3,4, or 6, such that $\varepsilon L = L$. This implies that for any integer $m \geq 2$ the map $F : z \to mz$ satisfies condition (17) for the homomorphism $\phi : \Gamma_{\mathcal{O}_2^A} \to \Gamma_{\mathcal{O}_2^A}$ defined on the generators of $\Gamma_{\mathcal{O}_2^A}$ by the equalities

$$\phi(z + \omega_1) = z + m\omega_1, \quad \phi(z + \omega_1) = z + m\omega_1, \quad \phi(\varepsilon z) = \varepsilon z. \tag{29}$$

Therefore, by Proposition 1, there exists a rational functions R_m such that

$$\theta_{\mathcal{O}_2^A}(mz) = R_m \circ \theta_{\mathcal{O}_2^A},$$

and it is easy to see that $\deg R_m = m^2$. Furthermore, it follows from (18) that $\chi(\mathcal{O}_1^A) = 0$, implying that the group $\Gamma_{\mathcal{O}_1^A}$ is generated by translations by elements of some sublattice $\widetilde{L}$

of L and the transformation $z \to \varepsilon^l z$ for some $l \geq 1$. Thus, homomorphism (29) satisfies the condition

$$\phi(\Gamma_{\mathcal{O}_1^A}) \subseteq \Gamma_{\mathcal{O}_1^A}, \tag{30}$$

implying that there exists a rational function S_m of degree m^2 such that

$$\theta_{\mathcal{O}_1^A}(mz) = S_m \circ \theta_{\mathcal{O}_1^A}.$$

Since

$$\theta_{\mathcal{O}_2^A} = A \circ \theta_{\mathcal{O}_1^A}, \tag{31}$$

it follows now from the equalities

$$\theta_{\mathcal{O}_2^A}(mz) = R_m \circ \theta_{\mathcal{O}_2^A} = R_m \circ A \circ \theta_{\mathcal{O}_1^A}$$

and

$$\theta_{\mathcal{O}_2^A}(mz) = A \circ \theta_{\mathcal{O}_1^A}(mz) = A \circ S_m \circ \theta_{\mathcal{O}_1^A},$$

that

$$A \circ S_m = R_m \circ A.$$

Thus, whenever the curve $A(x) - R_m(y) = 0$ is irreducible, it has genus zero. Since $\mathcal{E}_{A,B}$ is irreducible whenever the degrees of A and B are coprime (see e.g. [17, Proposition 3.1]), taking any sequence $m_i \to \infty$ whose elements are coprime with deg A, we obtain a sequence $A(x) - R_{m_i}(y) = 0$ of irreducible curves of genus zero.

In the case $\chi(\mathcal{O}_2^A) > 0$ the proof is similar with appropriate modifications. First observe that in order to prove the theorem it is enough to show that for any A with $\chi(\mathcal{O}_2^A) > 0$ there exists a *single* pair of rational functions S and R such that

$$A \circ S = R \circ A \tag{32}$$

and

$$\gcd(\deg R, \deg A) = 1. \tag{33}$$

Indeed, (32) implies that

$$A \circ S^{\circ l} = R^{\circ l} \circ A.$$

Therefore, since equality (33) implies the equality $\gcd(\deg R^{\circ l}, \deg A) = 1$, the sequence $A(x) - R^{\circ l}(y) = 0$ consists of irreducible curves of genus zero. Further, since by Lemma 1 the group $\Gamma_{\mathcal{O}_2^A}$ belongs to the list C_n, D_{2n}, A_4, S_4, A_5, in order to show the existence of such a pairs for any A with $\chi(\mathcal{O}_2^A) > 0$ it is enough to show that for any group Γ from the above list there exists a rational function F of degree corpime with $|\Gamma|$ which is Γ-equivariant, that is satisfies the equality

$$F \circ \sigma = \sigma \circ F \tag{34}$$

for any $\sigma \in \Gamma$. Indeed, condition (34) means that the corresponding homomorphism in (17) satisfies $\phi(\sigma) = \sigma$ for any $\sigma \in \Gamma$, implying that $\phi(\widetilde{\Gamma}) = \widetilde{\Gamma}$ for any subgroup $\widetilde{\Gamma}$ of Γ, and we conclude as above that

$$\theta_{\mathcal{O}_2^A} \circ F = R \circ \theta_{\mathcal{O}_2^A}, \quad \theta_{\mathcal{O}_1^A} \circ F = S \circ \theta_{\mathcal{O}_1^A} \tag{35}$$

for some rational functions S and R such that (32) holds. Moreover, since $\deg\theta_{\mathcal{O}_2^A} = |\Gamma_{\mathcal{O}_2^A}|$ and $\deg R = \deg F$, it follows from (31) that equality (33) holds.

If $\Gamma_{\mathcal{O}_2^A} = C_n$, then up to the change $A \to \mu_1 \circ A \circ \mu_2$, where μ_1, μ_2 are Möbius transformations, $A = z^n$, and hence (3) already provides a necessary series of irreducible curves of genus zero. Similarly, if $\Gamma_{\mathcal{O}_2^A} = D_n$, then without loss of generality we may assume that either $A = T_n$ or

$$A = \frac{1}{2}\left(z^n + \frac{1}{z^n}\right)$$

(see e.g. Appendix of [16]), and hence the statement of the lemma follows from equalities (4) and (8). Finally, since $A_4 \subset S_4 \subset A_5$, in order to finish the proof it is enough to find a single A_5-equivariant function whose order is coprime with 60, and as such a function we can take for example the function

$$F = \frac{z^{11} + 66z^6 - 11z}{-11z^{10} - 66z^5 + 1} \tag{36}$$

of degree 11, constructed in the paper [4].

5 Example

Consider the rational function $A = 3z^4 - 4z^3$ appearing in (7). The critical values of this function are $0, -1, \infty$. The preimage of 0 consists of a critical point 0, whose multiplicity is 3, and the point $4/3$. The preimage of -1 consists of a critical point 1, whose multiplicity is 2, and the points $-\frac{1}{3} \pm i\frac{\sqrt{3}}{2}$. Finally, the preimage of ∞ consists of a single point ∞, whose multiplicity is 4. Thus,

$$\nu_2^A(-1) = 2, \quad \nu_2^A(0) = 3, \quad \nu_2^A(\infty) = 4,$$

and the value of ν_2^A at any other point equals 1. Correspondingly,

$$\nu_1^A\left(-\frac{1}{3} + i\frac{\sqrt{3}}{2}\right) = \nu_1^A\left(-\frac{1}{3} - i\frac{\sqrt{3}}{2}\right) = 2, \quad \nu_1^A\left(\frac{4}{3}\right) = 3.$$

Finally,

$$\chi(\mathcal{O}_2^A) = \frac{1}{12}, \quad \chi(\mathcal{O}_1^A) = \frac{1}{3},$$

and $\Gamma_{\mathcal{O}_2^A} = S_4$.

Fix the generators of S_4 as

$$z \to iz, \quad z \to \frac{z+i}{z-i}.$$

Then

$$\theta_{\mathcal{O}_2^A} = -\frac{(z^8 + 14z^4 + 1)^3}{108z^4(z^4 - 1)^4}.$$

The critical values of $\theta_{\mathcal{O}_2^A}$ normalized in such a way are $0, -1, \infty$, and $\theta_{\mathcal{O}_2^A} = A \circ \theta_{\mathcal{O}_1^A}$, where

$$\theta_{\mathcal{O}_1^A} = \frac{\left(\frac{1}{6}(1+i)z^2 - \frac{i}{3}z + \frac{1}{6}(1-i)\right)\left(z^4 + 2\,z^3 + 2\,z^2 - 2\,z + 1\right)}{\left(z^2+1\right)(z+1)(z-1)\,z}.$$

As an S_4-invariant function of degree corpime with $\deg A = 4$ we can take function (36). However, we also can take the function of lesser degree

$$F = \frac{-z^5 + 5z}{5z^4 - 1}$$

obtained from the invariant form

$$x^5y - xy^5$$

by the method of [4]. For such F the functions R and S from equalities (35) are

$$R = \frac{z^2\left(z^3 - 240\,z^2 + 19200\,z - 512000\right)}{1048576 + 625\,z^4 + 16000\,z^3 + 153600\,z^2 + 655360\,z}$$

and

$$S = -\frac{z^2\left(3\,z^3 - 10\,z^2 + 20\,z - 40\right)}{32 - 20\,z^3 + 15\,z^4}.$$

Thus, we obtain a family of irreducible curves of genus zero

$$(3x^4 - 4x^3) - \left(\frac{y^2\left(y^3 - 240\,y^2 + 19200\,y - 512000\right)}{1048576 + 625\,y^4 + 16000\,y^3 + 153600\,y^2 + 655360\,y}\right)^{\circ k} = 0,$$

having the parametrizations

$$x = \left(-\frac{t^2\left(3\,t^3 - 10\,t^2 + 20\,t - 40\right)}{32 - 20\,t^3 + 15\,t^4}\right)^{\circ k}, \qquad y = 3t^4 - 4t^3.$$

Acknowledgements The author is grateful to M. Fried for discussions, and to the Max-Planck-Institut fuer Mathematik for the hospitality and the support.

References

1. Avanzi, R., Zannier, U.: Genus one curves defined by separated variable polynomials and a polynomial Pell equation. Acta Arith. **99**, 227–256 (2001)
2. Beardon, A., Ng, T.: Parameterizations of algebraic curves. Ann. Acad. Sci. Fenn. Math. **31**(2), 541–554 (2006)
3. Bilu, Y., Tichy, R.: The Diophantine equation $f(x) = g(y)$. Acta Arith. **95**(3), 261–288 (2000)
4. Doyle, P., McMullen, C.: Solving the quintic by iteration. Acta Math. **163**(3–4), 151–180 (1989)
5. Eremenko, A.: Some functional equations connected with the iteration of rational functions (Russian). Algebra i Analiz **1**, 102–116 (1989). (translation in Leningrad Math. J. 1, 905–919 (1990))
6. Farkas, H., Kra, I.: Riemann Surfaces, Graduate Texts in Mathematics, vol. 71. Springer, New York (1992)
7. Fried, M.: On a theorem of Ritt and related diophantine problems. J. Reine Angew. Math. **264**, 40–55 (1973)
8. Fried, M.: Fields of definition of function fields and a problem in the reducibility of polynomials in two variables. Ill. J. Math. **17**, 128–146 (1973)
9. Fried, M.: Arithmetical properties of function fields. II. The generalized Schur problem. Acta Arith. **25**, 225–258 (1974)

10. Fried, M.: Variables separated equations: strikingly different roles for the branch cycle lemma and the finite simple group classification. Sci. China Math **55**(1), 172 (2012)
11. Fried, M.: Introduction to modular towers: generalizing dihedral group-modular curve connections, recent developments in the inverse Galois problem. In: Fried, M.D., et al. (eds.) Contemporary Mathematics, vol 186, pp. 111–171. American Mathematical Society, Providence (1995)
12. Klein, F.: Lectures on the Icosahedron and the Solution of Equations of the Fifth Degree. Dover Publications, New York (1956)
13. Kreso, D., Tichy, R.: Functional Composition of Polynomials: Indecomposability, Diophantine Equations and Lacunary Polynomials. Preprint arxiv:1503.05401
14. Milnor, J.: Dynamics in One Complex Variable, Princeton Annals in Mathematics, vol. 160. Princeton University Press, Princeton, NJ (2006)
15. Milnor, J.: On Lattès maps, dynamics on the Riemann sphere. In: Hjorth, P., Petersen, C.L. (eds.) A Bodil Branner Festschrift, pp. 9–43. European Mathematical Society, Providence (2006)
16. Muzychuk, M., Pakovich, F.: Jordan–Holder theorem for imprimitivity systems and maximal decompositions of rational functions. Proc. Lond. Math. Soc. **102**(1), 1–24 (2011)
17. Pakovich, F.: Prime and composite Laurent polynomials. Bull. Sci. Math. **133**, 693–732 (2009)
18. Pakovich, F.: On the equation $P(f) = Q(g)$, where P, Q are polynomials and f, g are entire functions. Am. J. Math. **132**(6), 1591–1607 (2010)
19. Pakovich, F.: Algebraic curves $P(x) - Q(y) = 0$ and functional equations. Complex Var. Elliptic Equ. **56**(1–4), 199–213 (2011)
20. Pakovich, F.: On semiconjugate rational functions. Geom. Funct. Anal. **26**, 1217–1243 (2016)
21. Ritt, J.: Prime and composite polynomials. Trans. Am. Math. Soc. **23**, 51–66 (1922)