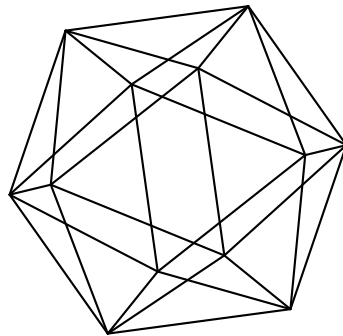# Max-Planck-Institut für Mathematik Bonn

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

by

Fedor Pakovich

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

Fedor Pakovich

Max-Planck-Institut für Mathematik
Vivatsgasse 7
53111 Bonn
Germany

Department of Mathematics
Ben-Gurion University of the Negev
P.O.B. 653
Beer-Sheva
Israel

ON ALGEBRAIC CURVES $A(x) - B(y) = 0$ OF GENUS ZERO

F. PAKOVICH

ABSTRACT. Using a geometric approach involving two-dimensional 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. Our main result states 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 there exist a compact Riemann surface R of genus 0 or 1 and a Galois covering $f : R \to \mathbb{CP}^1$ such that $f = A \circ p$ for some $p : R \to \mathbb{CP}^1$.

1. INTRODUCTION

The problem of classification of irreducible algebraic curves of genus zero having the form

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

where A and B are complex polynomials, has several motivations. First, curves of genus zero have special Diophantine properties. Namely, 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 general, 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 are polynomials with rational coefficients, the problem of description of curves $\mathcal{E}_{A,B}$ of genus zero is important for the number theory (see e.g. [5], [3], [10]).

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

$$(2) \qquad A \circ C = B \circ D.$$

Since equation (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 equation (2) where C and D are allowed to be *entire* functions reduces to the case $C, D \in \mathbb{C}(z)$ (see [2], [15]). Thus, the problem of description of curves $\mathcal{E}_{A,B}$ of genus zero naturally appears also in the complex analysis (see e. g. [5], [14], [15], [17]).

Having in mind possible applications to equation (2) in rational functions, in this paper we will allow A and B to be arbitrary *rational* functions meaning by the curve $\mathcal{E}_{A,B}$ 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. [8]), 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" ([22]) about polynomial solutions of (2). Namely, any such a curve has either the form

$$(3) \qquad\qquad x^n - y^s R^n(y) = 0,$$

where R is an arbitrary polynomial and $\mathrm{GCD}(s, n) = 1$, or the form

$$(4) \qquad\qquad T_n(x) - T_m(y) = 0,$$

where T_n, T_m are Chebyshev polynomials and $\mathrm{GCD}(n, m) = 1$. 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 [5], [6], [7]). In this case, in addition to the above curves we have the following possibilities:

$$(5) \qquad\qquad x^2 - (1 - y^2)S^2(y) = 0,$$

where S is an arbitrary polynomial,

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

where $\mathrm{GCD}(n, m) = 1$, and

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

Finally, the classification obtained in [3] can be extended to the case where A and B are allowed to be Laurent polynomials (see [14]). 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

$$(8) \qquad\qquad T_n(x) - \frac{1}{2}\left(y^m + \frac{1}{y^m}\right) = 0,$$

where $\mathrm{GCD}(n, m) = 1$. 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 in [1]. The above results essentially exhaust the list of general results concerning the problem of description of 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. Our main result is the following statement.

Theorem 1.1. *A rational function A is a basis of series of curves of genus zero if and only if there exist a compact Riemann surface R of genus 0 or 1 and a Galois covering $f : R \to \mathbb{CP}^1$ such that $f = A \circ p$ for some $p : R \to \mathbb{CP}^1$.*

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 ([9]). 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

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

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 Section 5 below). Typical representatives of the second class, consisting of rational compositional left factors of Galois coverings of $\mathbb{CP}^1$ by $\mathbb{T}$, are Lattès functions (see e.g. [12]), but other possibilities also exist.

The approach of the papers [1], [3], [14] to the calculation of $g(\mathcal{E}_{A,B})$ is based on the formula, given in [7], 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:

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

However, the direct analysis of this formula is quite difficult already in the above cases, and the further progress requires even more cumbersome considerations. Furthermore, although (10) provides restrictions on possible ramifications of A and B, it does not ensure that rational functions with such ramifications actually exist. Notice that the problem of existence of a rational function with a prescribed ramification is a part of the so-called Hurwitz existence problem and is widely open (see e. g. the recent papers [19], [13], [20], [21]).

In this paper we propose a new approach to the problem, based on techniques introduced in the recent paper [18] concerning rational solutions of the functional equation $A \circ X = X \circ B$. This approach permits to obtain restrictions on a possible ramification of a basis of series A in geometric terms, and to show that for any A obeying these restrictions a sequence of B_i as above actually exists. The paper is organized as follows. In the second section we recall basic facts about two-dimensional orbifolds and some results from the papers [14], [18]. In the third section we provide low bounds for the genus of $\mathcal{E}_{A,B}$. In the fourth section we prove Theorem 1.1. Finally, in the fifth section we consider an example illustrating methods and results of the article.

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 an orbifold. The Euler characteristic of an orbifold $\mathcal{O} = (R, \nu)$ is defined by the formula

$$(11) \qquad\qquad \chi(\mathcal{O}) = \chi(R) + \sum_{z \in R}\left(\frac{1}{\nu(z)} - 1\right),$$

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

$$(12) \qquad\qquad \nu_2(f(z)) = \nu_1(z)\deg_z f$$

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 (12) a weaker condition

$$(13) \qquad\qquad \nu_2(f(z)) \mid \nu_1(z)\deg_z f$$

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 $\nu(z_1) \neq \nu(z_2)$. 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 [18], Proposition 3.1).

Proposition 2.1. *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* $\varphi : \Gamma_{\mathcal{O}_1} \to \Gamma_{\mathcal{O}_2}$ *such that diagram*

$$(14) \qquad \begin{array}{ccc} \widetilde{\mathcal{O}_1} & \xrightarrow{\;F\;} & \widetilde{\mathcal{O}_2} \\ \Big\downarrow{\scriptstyle\theta_{\mathcal{O}_1}} & & \Big\downarrow{\scriptstyle\theta_{\mathcal{O}_2}} \\ \mathcal{O}_1 & \xrightarrow{\;f\;} & \mathcal{O}_2 \end{array}$$

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

$$(15) \qquad\qquad F \circ \sigma = \varphi(\sigma) \circ F$$

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 other direction, for any holomorphic map* $F : \widetilde{\mathcal{O}_1} \to \widetilde{\mathcal{O}_2}$ *which satisfies (15) for some homomorphism* $\varphi : \Gamma_{\mathcal{O}_1} \to \Gamma_{\mathcal{O}_2}$ *there exists a uniquely defined holomorphic map between orbifolds* $f : \mathcal{O}_1 \to \mathcal{O}_2$ *such that diagram (14) is commutative. The holomorphic map* F *is an isomorphism if and only if* f *is a covering map between orbifolds.* $\square$

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

$$(16) \qquad\qquad \chi(\mathcal{O}_1) = d\chi(\mathcal{O}_2),$$

where $d = \deg f$. For holomorphic maps the following statement is true (see [18], Proposition 3.2).

Proposition 2.2. *Let $f : \mathcal{O}_1 \to \mathcal{O}_2$ be a holomorphic map between orbifolds with compact support. Then*

$$\chi(\mathcal{O}_1) \leq \chi(\mathcal{O}_2) \deg f \tag{17}$$

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

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 (13), 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

$$\nu_2(f(z)) = \nu_1(z)\mathrm{GCD}(\deg_z f, \nu_2(f(z))). \tag{18}$$

In case if (18) 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* $\mathcal{O}_2 = (R_2, \nu_2)$.

With each 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

$$\theta_{\mathcal{O}_2^f} = f \circ \theta_{\mathcal{O}_1^f}. \tag{19}$$

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

$$A \circ p = B \circ q, \tag{20}$$

and

$$\deg A = \deg q, \quad \deg B = \deg p \tag{21}$$

(see [14], 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 [18], Theorem 4.2 and Lemma 2.1).

Theorem 2.1. *Let A, B be rational functions such that the curve $\mathcal{E}(A, B)$ is irreducible, and p, q holomorphic functions such that equalities (20) and (21) hold. Then the commutative diagram*

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

consists of minimal holomorphic maps between orbifolds.

Of coarse, vertical arrows in the above diagram are covering 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 2.1 applied to the functional equation

$$A \circ X = X \circ B,$$

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 [18]). For a rational function A the condition $\chi(\mathcal{O}_2^A) \geq 0$ is quite restrictive, and in fact is equivalent to the condition from Theorem 1.1. We discuss it in the rest of the section.

If $\mathcal{O} = (\mathbb{CP}^1, \nu)$ is an orbifold such that $\chi(\mathcal{O}) = 0$, then (11) 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 $\theta_{\mathcal{O}}$ are Galois coverings of $\mathbb{CP}^1$ by $\mathbb{C}$ and may be written in terms of the corresponding Weierstrass functions as $\wp^2(z)$, $\wp'(z)$, and $\wp'^2(z)$.

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 (11) also allows $\mathcal{O}$ to be a non-ramified sphere or one of two orbifolds without universal covering. However, for any rational function A both orbifolds $\mathcal{O}_1^A$, $\mathcal{O}_2^A$ have a universal covering (see [18], Lemma 4.2), and $\mathcal{O}_2^A$ cannot be non-ramified. Thus, if $\mathcal{O} = \mathcal{O}_2^A$ for some rational function A, then the collection of ramification indices of $\mathcal{O}$ belongs to the above list. For such collections, $\widetilde{\mathcal{O}} = \mathbb{CP}^1$, 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 e.g. [9]).

Rational functions A with $\chi(\mathcal{O}_2^A) \geq 0$ and Galois coverings of the sphere are related as follows.

Lemma 2.1. *Let A be a rational function. Then $\chi(\mathcal{O}_2^A) > 0$ if and only if there exists a Galois covering $f : \mathbb{CP}^1 \to \mathbb{CP}^1$ such that $\mathcal{O}_2^f = \mathcal{O}_2^A$ and $f = A \circ p$ for some $p : \mathbb{CP}^1 \to \mathbb{CP}^1$. Similarly, $\chi(\mathcal{O}_2^A) = 0$ if and only if there exist a complex torus $\mathbb{T}$ and a Galois covering $f : \mathbb{T} \to \mathbb{CP}^1$ such that $\mathcal{O}_2^f = \mathcal{O}_2^A$ and $f = A \circ p$ for some $p : \mathbb{T} \to \mathbb{CP}^1$.*

Proof. In order to prove "if" part we only must show that if R is a compact Riemann surface of genus 0 or 1 and $f : R \to \mathbb{CP}^1$ is a Galois covering, then $\chi(\mathcal{O}_2^f) > 0$ or $\chi(\mathcal{O}_2^f) = 0$, correspondingly. Let Γ be an automorphism group of R such that f coincides with the quotient map $R \to R/\Gamma$. 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 exactly $|G|/d_i$ points, and at each of these points the multiplicity of f equals d_i. Applying the Riemann-Hurwitz

formula, we see that

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

and hence

$$(22) \qquad \chi(\mathcal{O}_2^f) = 2 + \sum_{i=1}^{r}\left(\frac{1}{d_i} - 1\right) = \frac{2 - 2g(R)}{|G|},$$

implying the statement.

Assume now that $\chi(\mathcal{O}_2^A) \geq 0$, and consider the normalization of A, that is a Galois covering $f : R \to \mathbb{CP}^1$ of the lowest possible degree such that $f = A \circ p$ for some $p : R \to \mathbb{CP}^1$. It is known that for such a covering $\mathcal{O}_2^f = \mathcal{O}_2^A$. Therefore, keeping the above notation and using formula (22), we see that if $\chi(\mathcal{O}_2^A) > 0$ (resp. $\chi(\mathcal{O}_2^A) = 0$), then $g(R) = 0$ (resp. $g(R) = 1$). $\qquad \square$

Notice that if $\chi(\mathcal{O}_2^A) = 0$, then, since $\mathbb{CP}^1$ is simply connected, the function f from Lemma 2.1 is a universal covering of $\mathcal{O}_2^A$ and the equality $f = A \circ p$ reduces to equality (19).

3. Lower bound for genus of $\mathcal{E}_{A,B}$

In this section we show that, unless $\chi(\mathcal{O}_2^A) \geq 0$, the genus of $g(\mathcal{E}_{A,B})$ tends to infinity as $\deg B(z)$ tends to infinity. More precisely, the following statement holds.

Theorem 3.1. *Let A be a rational function of degree n such that $\chi(\mathcal{O}_2^A) < 0$. Then for any rational function B of degree m such that the curve $\mathcal{E}_{A,B}$ is irreducible the inequality*

$$(23) \qquad g(\mathcal{E}_{A,B}) > \frac{m - 84n + 168}{168}$$

holds.

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

$$(24) \qquad \chi(\mathcal{O}_2^f) > 4 - 4g - 2n.$$

Indeed, it follows from the definition that

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

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 (24).

Let now $p, q : \widetilde{\mathcal{E}}(A, B) \to \mathbb{CP}^1$ be holomorphic functions such that (20) and (21) hold. Since $B : \mathcal{O}_2^q \to \mathcal{O}_2^A$ is a minimal holomorphic map between orbifolds by Theorem 2.1, it follows from Proposition 2.2 that

$$\tag{25} \chi(\mathcal{O}_2^q) \leq m\chi(\mathcal{O}_2^A).$$

On the other hand, (11) implies that if $\chi(\mathcal{O}) < 0$, then in fact

$$\tag{26} \chi(\mathcal{O}) \leq -\frac{1}{42}$$

(where the equality attains for the collection of ramification indices $(2, 3, 7)$). Therefore, if $\chi(\mathcal{O}_2^A) < 0$, then (26) and (24) imply the inequality

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

which in its turn implies (23). $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

4. Proof of Theorem 1.1

It follows from Theorem 3.1 and Lemma 2.1 that we only must 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 (15) for the homomorphism $\varphi : \Gamma_{\mathcal{O}_2^A} \to \Gamma_{\mathcal{O}_2^A}$ defined on the generators of $\Gamma_{\mathcal{O}_2^A}$ by the equalities

$$\tag{27} \varphi(z + \omega_1) = z + m\omega_1, \quad \varphi(z + \omega_1) = z + m\omega_1, \quad \varphi(\varepsilon z) = \varepsilon z.$$

Therefore, by Proposition 2.1, there exists a rational functions R_m of degree m such that

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

Furthermore, it follows from (16) 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 (27) satisfies the condition

$$\tag{28} \varphi(\Gamma_{\mathcal{O}_1^A}) = \Gamma_{\mathcal{O}_1^A}$$

and hence there exists a rational function S_m of degree m such that

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

Since

$$\tag{29} \theta_{\mathcal{O}_2^A} = A \circ \theta_{\mathcal{O}_1^A},$$

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 [14],

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

$$(30) \qquad\qquad A \circ S = R \circ A$$

and $\mathrm{GCD}(\deg R, \deg A) = 1$. Really, (30) implies that

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

Therefore, since $\mathrm{GCD}(\deg R^{\circ l}, \deg A) = 1$, the sequence $A(x) - R^{\circ l}(y) = 0$ consists of irreducible curves of genus zero. Further, 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 list C_n, D_{2n}, A_4, S_4, A_5 there exists a rational function F of degree corpime with $|\Gamma|$ which is Γ-equivariant, that is satisfies the equality

$$(31) \qquad\qquad F \circ \sigma = \sigma \circ F$$

for any $\sigma \in \Gamma$. Indeed, condition (31) means that the corresponding homomorphism in (15) satisfies $\varphi(\sigma) = \sigma$ for any $\sigma \in \Gamma$, implying that $\varphi(\widetilde{\Gamma}) = \widetilde{\Gamma}$ for any subgroup $\widetilde{\Gamma}$ of Γ. Since, by Lemma 2.1, $\Gamma_{\mathcal{O}_2^A} = \Gamma$ for some group Γ from the list, we conlude as above that

$$(32) \qquad\qquad \theta_{\mathcal{O}_2^A} \circ F = R \circ \theta_{\mathcal{O}_2^A}, \quad \theta_{\mathcal{O}_1^A} \circ F = S \circ \theta_{\mathcal{O}_1^A}$$

for some rational functions S and R such that (30) holds. Moreover, in fact it is enough to consider only the groups A_4, S_4, and A_5, since if $\Gamma_{\mathcal{O}_2^A} = C_n$, then up to the change $f \to \mu_1 \circ f \circ \mu_2$, where μ_1, μ_2 are Möbius transformations, $A = z^m$ for some $m \mid n$, 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 $A = T_m$ or

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

for some $m \mid n$ (see e.g. Appendix of [16]), and hence the statement of the lemma follows from equalities (4) and (8).

Finally, since $A_4 \subset S_4 \subset A_5$, 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

$$(33) \qquad\qquad F = \frac{z^{11} + 66z^6 - 11z}{-11z^{10} - 66z^5 + 1}$$

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,

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

and

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

The Galois covering f from Lemma 2.1 has the group S_4. Fix the generators of S_4 as

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

and write $f=\theta_{\mathcal{O}_2^A}$ in the form

$$f=-\frac{(z^8+14z^4+1)^3}{108z^4(z^4-1)^4}.$$

The critical values of f normalized in such a way are $0,-1,\infty$, and the equality $f=A\circ p$ from Lemma 2.1 holds for the function

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

As an S_4-invariant function of degree corpime with $\deg A=4$ we can take function (33). 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 (32) 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

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

References

1. R. Avanzi, U. Zannier, *Genus one curves defined by separated variable polynomials and a polynomial Pell equation,* Acta Arith. 99 (2001), 227-256.
2. A. Beardon, T. Ng, *Parameterizations of algebraic curves*, Ann. Acad. Sci. Fenn., Math. 31, No. 2, 541-554 (2006)
3. Y. Bilu, R. Tichy, *The Diophantine equation $f(x) = g(y)$*, Acta Arith. 95, No.3, 261-288 (2000).
4. P. Doyle, C. McMullen, *Solving the quintic by iteration,* Acta Math. 163 (1989), no. 3-4, 151-180.
5. M. Fried, *On a theorem of Ritt and related diophantine problems*, J. Reine Angew. Math. 264, 40-55 (1973).
6. M. Fried, *Fields of definition of function fields and a problem in the reducibility of polynomials in two variables*, Ill. J. Math. 17, 128-146 (1973).
7. M. Fried, *Arithmetical properties of function fields. II. The generalized Schur problem,* Acta Arith. 25, 225-258 (1974)
8. M. Fried, *Variables separated equations: strikingly different roles for the branch cycle lemma and the finite simple group classification*, Sci. China Math. 55 (2012), no. 1, 172.
9. F. Klein, *Lectures on the icosahedron and the solution of equations of the fifth degree*, New York: Dover Publications, (1956).
10. D. Kreso, R. Tichy, *Functional composition of polynomials: indecomposability, Diophantine equations and lacunary polynomials*, preprint, arxiv:1503.05401.
11. J. Milnor, *Dynamics in one complex variable*, Princeton Annals in Mathematics 160. Princeton, NJ: Princeton University Press (2006).
12. J. Milnor, *On Lattès maps,* Dynamics on the Riemann Sphere. Eds. P. Hjorth and C. L. Petersen. A Bodil Branner Festschrift, European Mathematical Society, 2006, pp. 9-43.
13. F. Pakovich, *Solution of the Hurwitz problem for Laurent polynomials,* J. Knot Theory Ramifications, 18, No. 2, 271-302 (2009)
14. F. Pakovich, *Prime and composite Laurent polynomials,* Bull. Sci. Math., 133 (2009), 693-732.
15. F. Pakovich, *On the equation $P(f)=Q(g)$, where P,Q are polynomials and f,g are entire functions, Amer. Journal of Math.,* 132 (2010), no. 6, 1591-1607.
16. M. Muzychuk, F. Pakovich, *Jordan-Holder theorem for imprimitivity systems and maximal decompositions of rational functions*, Proc. Lond. Math. Soc., 102 (2011) , no. 1, 1-24.
17. F. Pakovich, *Algebraic curves $P(x)-Q(y)=0$ and functional equations,* Complex Var. and Elliptic Equ., 56 (2011), no. 1-4, 199-213.
18. F. Pakovich, *On semiconjugate rational functions,* preprint, arXiv:1108:1900.
19. C. Petronio, K. Pervova, *On the existence of branched coverings between surfaces with prescribed branch data, II,* Algebr. Geom. Top. 6 (2006), 1957-1985.
20. M. Pascali, C. Petronio, *Surface branched covers and geometric 2-orbifolds* Trans. Amer. Math. Soc. 361 (2009), 5885-5920.
21. M. Pascali, C. Petronio, *Branched covers of the sphere and the prime-degree conjecture,* Ann. Mat. Pura Appl. 191 (2012) 563-594.
22. J Ritt, *Prime and composite polynomials*, American M. S. Trans. 23, 51-66 (1922).

DEPARTMENT OF MATHEMATICS, BEN-GURION UNIVERSITY OF THE NEGEV, P.O.B. 653, BEER-SHEVA, ISRAEL

E-mail address: `pakovich@math.bgu.ac.il`