ON ITERATES OF RATIONAL FUNCTIONS WITH MAXIMAL NUMBER OF CRITICAL VALUES

By

FEDOR PAKOVICH*

Abstract. Let F be a rational function of one complex variable of degree $m \geq 2$. The function F is called simple if for every $z \in \mathbb{CP}^1$ the preimage $F^{-1}\{z\}$ contains at least $m-1$ points. We show that if F is a simple rational function of degree $m \geq 4$ and $F^{\circ l} = G_r \circ G_{r-1} \circ \cdots \circ G_1$, $l \geq 1$, is a decomposition of an iterate of F into a composition of indecomposable rational functions, then $r = l$ and there exist Möbius transformations μ_i, $1 \leq i \leq r-1$, such that $G_r = F \circ \mu_{r-1}$, $G_i = \mu_i^{-1} \circ F \circ \mu_{i-1}$, $1 < i < r$, and $G_1 = \mu_1^{-1} \circ F$. As applications, we solve a number of problems in complex and arithmetic dynamics for "general" rational functions.

1 Introduction

Let F be a rational function of one complex variable of degree $m \geq 2$. The function F is called **indecomposable** if the equality $F = F_2 \circ F_1$, where F_1, F_2 are rational functions, implies that at least one of the functions F_1, F_2 is of degree one. Any representation of F in the form $F = F_r \circ F_{r-1} \circ \cdots \circ F_1$, where $F_1, F_2, \ldots, F_r$ are rational functions of degree at least two, is called a **decomposition** of F. Two decompositions

$$F = F_r \circ F_{r-1} \circ \cdots \circ F_1 \quad \text{and} \quad F = G_l \circ G_{l-1} \circ \cdots \circ G_1 \tag{1}$$

are called **equivalent** if $l = r$ and either $r = 1$ and $F_1 = G_1$, or $r \geq 2$ and there exist Möbius transformations μ_i, $1 \leq i \leq r-1$, such that

$$F_r = G_r \circ \mu_{r-1}, \quad F_i = \mu_i^{-1} \circ G_i \circ \mu_{i-1}, \quad 1 < i < r, \quad \text{and} \quad F_1 = \mu_1^{-1} \circ G_1.$$

It is obvious that any rational function F of degree $m \geq 2$ can be decomposed into a composition of indecomposable rational functions, although in general not in a unique way. The problem of describing all such decompositions is quite delicate,

*This research was supported by ISF Grant No. 1092/22.

JOURNAL D'ANALYSE MATHÉMATIQUE, Vol. 156 (2025)
DOI 10.1007/s11854-025-0386-z

and the general theory exists only if F is a polynomial or a Laurent polynomial (see [47], [31]).

In dynamical applications, one needs to have a description of decompositions of the whole totality of iterates of a given rational function F (see, e.g., [5], [18], [19], [27], [34], [43], [44]), and the main result of this paper states roughly speaking that for a general rational function of degree $m \geq 4$ all such decompositions are trivial. As applications, we solve a number of problems in complex and arithmetic dynamics for general rational functions. Here and below, saying that some statement holds for **general** rational functions of degree m, we mean the following: if we identify the set of rational functions of degree m with an algebraic variety Rat_m obtained from $\mathbb{CP}^{2m+1}$ by removing the resultant hypersurface, then this statement holds for all $F \in \mathrm{Rat}_m$ with the exception of some proper Zariski closed subset.

In more detail, we prove a number of results, which hold for **simple** rational functions, that is, for rational functions F of degree $m \geq 2$ such that for every $z \in \mathbb{CP}^1$ the preimage $F^{-1}\{z\}$ contains at least $m-1$ points.

Our main result is the following statement.

Theorem 1.1. *Let F be a simple rational function of degree $m \geq 4$. Then any decomposition of $F^{\circ l}$, $l \geq 1$, into a composition of indecomposable rational functions is equivalent to $F^{\circ l}$.*

We apply Theorem 1.1 to describing a variety of objects associated with a rational function F of degree at least two, using the following notation.

$\langle F \rangle$	is the semigroup of rational functions generated by F.
$C(F)$	is the semigroup of all rational functions commuting with F.
$\mathrm{Aut}(F)$	is the group of all Möbius transformations belonging to $C(F)$.
$C_\infty(F)$	is the semigroup of all rational functions commuting with some iterate of F.
$\mathrm{Aut}_\infty(F)$	is the group of all Möbius transformations belonging to $C_\infty(F)$.
$\langle \mathrm{Aut}_\infty(F), F \rangle$	is the semigroup of rational functions generated by F and $\mathrm{Aut}_\infty(F)$.
μ_F	is the measure of maximal entropy of F.
$E_0(F)$	is the group of all Möbius transformations preserving μ_F.
$E(F)$	is the semigroup consisting of all rational functions G of degree at least two with $\mu_G = \mu_F$, completed by the group $E_0(F)$.
$G_0(F)$	is the maximal subgroup of $\mathrm{Aut}(\mathbb{CP}^1)$ such that for every $\sigma \in G_0(F)$ there exists $\nu \in G_0(F)$ satisfying $F \circ \sigma = \nu \circ F$.

Using Theorem 1.1, we show that for simple rational functions the above objects are related in a very simple way.

Theorem 1.2. *Let F be a simple rational function of degree $m \geq 4$. Then*

$$E_0(F) = \mathrm{Aut}_\infty(F) = G_0(F) \quad \textit{and} \quad E(F) = C_\infty(F) = \langle \mathrm{Aut}_\infty(F), F \rangle.$$

The link between Theorem 1.1 and Theorem 1.2 is based on the results of Ritt ([48]) and Levin and Przytycki ([24], [25]). Namely, the theorem of Ritt about commuting rational functions implies that for a fixed non-special rational function F of degree at least two, a rational function G of degree at least two belongs to $C_\infty(F)$ if and only if the equality

$$F^{\circ k} = G^{\circ l} \tag{2}$$

holds for some $k, l \geq 1$. On the other hand, the results of Levin and Przytycki yield that G belongs to $E(F)$ if and only if the equality

$$F^{\circ k_1} = F^{\circ k_2} \circ G^{\circ l} \tag{3}$$

holds for some $k_1, l \geq 1$, $k_2 \geq 0$ (see Section 3.1 for more detail).

As an application of Theorem 1.2, we prove the following result.

Theorem 1.3. *For a general rational function F of degree $m \geq 4$, the equalities*

$$E_0(F) = \mathrm{Aut}_\infty(F) = G_0(F) = \mathrm{id} \quad \textit{and} \quad E(F) = C_\infty(F) = \langle F \rangle$$

hold.

Notice that Theorem 1.3 provides an affirmative answer to the question of Ye, who proved that the equality $E(F) = \langle F \rangle$ holds after removing from Rat_m countably many algebraic sets, and asked whether it remains true if to remove from Rat_m only finitely many such sets ([57]).

Further applications of Theorem 1.1 concern problems that can be reformulated in terms of semiconjugacies between rational functions (see the papers [4], [9], [11], [22], [27], [36], [43] for examples of such problems). We recall that a rational function B of degree at least two is called **semiconjugate** to a rational function A if there exists a non-constant rational function X such that the diagram

$$\begin{array}{ccc} \mathbb{CP}^1 & \xrightarrow{B} & \mathbb{CP}^1 \\ {\scriptstyle X}\downarrow & & \downarrow{\scriptstyle X} \\ \mathbb{CP}^1 & \xrightarrow{A} & \mathbb{CP}^1 \end{array} \tag{4}$$

commutes. A comprehensive description of triples A, B, X such that (4) commutes was obtained in the series of papers [33], [35], [37], [38]. For simple A, Theorem 1.1 permits to reduce this description to the following uncomplicated form suitable for applications.

Theorem 1.4. *Let F be a simple rational function of degree $m \geq 4$, and G, X non-constant rational functions such that the diagram*

$$\begin{array}{ccc} \mathbb{CP}^1 & \xrightarrow{G} & \mathbb{CP}^1 \\ {\scriptstyle X}\downarrow & & \downarrow{\scriptstyle X} \\ \mathbb{CP}^1 & \xrightarrow{F^{\circ r}} & \mathbb{CP}^1 \end{array} \tag{5}$$

commutes for an integer $r \geq 1$. Then there exist a Möbius transformation ν and an integer $l \geq 0$ such that the equalities

$$X = F^{\circ l} \circ \mu, \quad G = \mu^{-1} \circ F^{\circ r} \circ \mu$$

hold.

As an example of an application of Theorem 1.4, we consider the problem of describing periodic algebraic curves for endomorphisms of $(\mathbb{CP}^1)^2$ of the form

$$(F_1, F_2) : (z_1, z_2) \to (F_1(z_1), F_2(z_2)),$$

where F_1, F_2 are rational functions, which reduces to describing solutions of a system of semiconjugacies. A description of periodic curves in the case where F_1, F_2 are polynomials was obtained by Medvedev and Scanlon ([27]) and has numerous applications in complex and arithmetic dynamics (see, e.g., [3], [11], [15], [16], [17], [20], [30]). A description of periodic curves in the general case was obtained in the recent paper [43]. Notice that the problem of describing periodic curves is closely related to a variant of a conjecture of Zhang ([58]) on the existence of Zariski dense orbits for endomorphisms (F_1, F_2) defined over a field K of characteristic zero (see [27], [43], [56]).

Theorem 1.4 permits to shorten considerably the results of [43] in case F_1 and F_2 are simple, leading to the following result, which can be easily used for applications.

Theorem 1.5. *Let F_1 and F_2 be simple rational functions of degree $m \geq 4$, and C an irreducible algebraic curve in $(\mathbb{P}^1(\mathbb{C}))^2$ that is not a vertical or horizontal line. Then $(F_1, F_2)^{\circ d}(C) = C$ for an integer $d \geq 1$ if and only if*

$$F_2^{\circ d} = \alpha \circ F_1^{\circ d} \circ \alpha^{-1}$$

for some Möbius transformation α, and C is one of the graphs

$$y = (\alpha \circ \mu \circ F_1^{\circ s})(x), \quad x = (\mu \circ F_1^{\circ s} \circ \alpha^{-1})(y),$$

where $\mu \in \mathrm{Aut}(F_1^{\circ d})$ and $s \geq 0$.

Using Theorem 1.5, we prove the following result about invariant and periodic curves for general rational functions.

Theorem 1.6. *For every $m \geq 4$ there exists a Zariski open set U in Rat_m such that the following holds. For any $F_1, F_2 \in U$, an irreducible algebraic curve C in $(\mathbb{P}^1(\mathbb{C}))^2$ that is not a vertical or horizontal line is (F_1, F_2)-periodic if and only if*

$$F_2 = \alpha \circ F_1 \circ \alpha^{-1}$$

for some Möbius transformation α, and C is one of the graphs

$$y = (\alpha \circ F_1^{\circ s})(x), \quad x = (F_1^{\circ s} \circ \alpha^{-1})(y),$$

where $s \geq 0$. In particular, any (F_1, F_2)-periodic curve is (F_1, F_2)-invariant.

For proving Theorem 1.1, we use the following strategy. First, we show that if F is a simple rational function of degree $m \geq 4$ and H is an indecomposable rational function of degree at least two such that the algebraic curve

$$H(y) - F(x) = 0 \tag{6}$$

is irreducible, then the genus of this curve is greater than zero. Second, we show that if (6) is reducible, then either $H = F \circ \mu$, where μ is a Möbius transformation, or $\deg H$ is equal to the binomial coefficient $\binom{m}{k}$ for some k, $1 < k < m-1$. Third, using the theorem of Sylvester [53] and Schur [50] about prime divisors of binomial coefficients, we show that there exists a prime number p such that $p \mid \binom{m}{k}$ but $p \nmid m$. The above statements yield that if $F^{\circ l} = H \circ R$ for some rational function R, then H necessarily has the form $H = F \circ \mu$ for some Möbius transformation μ, and this fact allows us to prove the theorem.

The paper is organized as follows. In the second section, using the above approach we prove Theorem 1.1. In the third section, we deduce from Theorem 1.1, Theorem 1.2 and Theorem 1.3. In the fourth section, basing on results about semiconjugate rational functions and invariant curves from [33], [38], [43], we prove Theorem 1.4, Theorem 1.5, and Theorem 1.6.

Finally, in the fifth section, we give a number of conditions implying that some iterate $F^{\circ k}$, $k > 1$, of an indecomposable rational function F has a decomposition not equivalent to $F^{\circ k}$ itself. We also construct explicit examples of simple rational functions of degree 2 and 3 for which Theorems 1.1–1.2 and Theorems 1.4–1.5 are not true. As for Theorem 1.3 and Theorem 1.6, we believe that they have some analogues for $m = 2$ and $m = 3$. However, the methods of this paper do not apply to this situation.

2 Decompositions of iterates of rational functions

2.1 The monodromy group and decompositions. Let G be a group which acts transitively on a finite set S. We recall that a subset T of S is called a block of G, if for each $g \in G$ either $g(T) = T$ or $g(T) \cap T = \emptyset$. Clearly, if T is a block, then $\mathcal{T} = \{\sigma(T), \sigma \in G\}$ is a partition of S, which is called an imprimitvity system of G. The group G is called primitive if its blocks are only singletons and the whole S. Otherwise, G is called imprimitive.

Let F be a rational function, and $c(F) = \{z_1, z_2, \dots, z_r\}$ the set of all critical values of F. Let us fix a point $z_0 \in \mathbb{CP}^1 \setminus c(F)$ and some loops γ_i around z_i, $1 \leq i \leq r$, such that $\gamma_1\gamma_2 \cdots \gamma_r = 1$ in $\pi_1(\mathbb{CP}^1 \setminus c(F), z_0)$. Further, let us denote by δ_i, $1 \leq i \leq r$, a permutation of points of $F^{-1}\{z_0\}$ induced by the lifting of γ_i, $1 \leq i \leq r$. In this notation, the monodromy group of F is defined as the permutation group generated by δ_i, $1 \leq i \leq r$. We will denote this group by $\mathrm{Mon}(F)$.

The imprimitivity systems of the group $\mathrm{Mon}(F)$ correspond to decompositions of F. Namely, if $F = A \circ B$ is a decomposition of F into a composition of rational functions A and B, where $\deg A = d$, then $\mathrm{Mon}(F)$ has an imprimitivity system consisting of d blocks $B^{-1}\{t_i\}$, $1 \leq i \leq d$, where $\{t_1, t_2, \dots, t_d\} = A^{-1}\{z_0\}$. Furthermore, any imprimitivity system of $\mathrm{Mon}(F)$ arises from a decomposition of F, and to decompositions $F = A \circ B$ and $F = C \circ D$ corresponds the same imprimitivity system if and only if there exists a Möbius transformation μ such that

$$A = C \circ \mu^{-1}, \quad B = \mu \circ D.$$

In particular, F is indecomposable if and only if $\mathrm{Mon}(F)$ is primitive.

2.2 A calculation of the genus of $H(x) - F(y) = 0$. Let F be a rational function of degree $m \geq 2$. We denote by $\deg_z F$ the multiplicity of F at a point $z \in \mathbb{CP}^1$. The following two results are known. We include the proofs for the reader's convenience.

Lemma 2.1. *Let F be a rational function of degree $m \geq 2$. Then the following conditions are equivalent:*

(i) *The function is simple.*

(ii) *The number of critical points of F is equal to the number of critical values, and the multiplicity of F at every critical point is equal to two.*

(iii) *The number of critical values of F is equal to $2m-2$.*

Proof. The equivalence (i)⇔(ii) follows from the definition. Furthermore, it follows from the Riemann–Hurwitz formula

$$2m-2 = \sum_{z\in\mathbb{CP}^1} (\deg_z F - 1)$$

that the number of critical points of F does not exceed $2m-2$, and the equality is attained if and only if the multiplicity of F at every critical point is equal to two. Since the number of critical values of F does not exceed the number of critical points, this implies easily the equivalence (ii)⇔(iii). □

Theorem 2.2. *Let F be a simple rational function of degree $m \geq 2$. Then F is indecomposable, and* $\mathrm{Mon}(F) \cong S_m$.

Proof. Assume that

$$F = F_1 \circ F_2, \tag{7}$$

where F_1 and F_2 are rational functions of degrees m_1 and m_2. Since F is simple, the number of critical values of F is $2m_1m_2-2$ by Lemma 2.1. On the other hand, it follows from (7) by the chain rule that the number of critical values of F does not exceed $(2m_1-2)+(2m_2-2)$. Thus,

$$2m_1m_2-2 \leq (2m_1-2)+(2m_2-2),$$

implying that

$$2m_1m_2-2-(2m_1-2)-(2m_2-2) = 2(m_1-1)(m_2-1) \leq 0.$$

Therefore, at least one of the functions F_1 and F_2 has degree one.

Since F is indecomposable, the monodromy group $\mathrm{Mon}(F)$ of F is primitive. Furthermore, for any critical value c of F, the permutation in $\mathrm{Mon}(P)$ corresponding to c is a transposition. Since a primitive permutation group containing a transposition is a full symmetric group (see [55, Theorem 13.3]), we conclude that $\mathrm{Mon}(F) = S_m$. □

Let F and H be rational functions of degrees n and m, and H_1, H_2 and F_1, F_2 pairs of polynomials without common roots such that $H = H_1/H_2$ and $F = F_1/F_2$. Let us define algebraic curves $h_{F,H}(x, y)$ and $h_F(x, y)$ by the formulas

$$h_{H,F}: \ H_1(x)F_2(y) - H_2(x)F_1(y) = 0,$$

and

$$h_F: \ \frac{F_1(x)F_2(y) - F_2(x)F_1(y)}{x - y} = 0.$$

In case these curves are irreducible, their genera can be calculated explicitly in terms of ramification of H and F as follows. Let $S = \{z_1, z_2, \dots, z_r\}$ be the union of all critical values of H and F. For i, $1 \le i \le r$, we denote by

$$(a_{i,1}, a_{i,2}, \dots, a_{i,p_i})$$

the collection of multiplicities of H at the points of $H^{-1}\{z_i\}$, and by

$$(b_{i,1}, b_{i,2}, \dots, b_{i,q_i})$$

the collection of multiplicities of F at the points of $F^{-1}\{z_i\}$. In this notation, the following formulas hold (see [13] or [32]):

$$2 - 2g(h_{H,F}) = \sum_{i=1}^{r} \sum_{j_2=1}^{q_i} \sum_{j_1=1}^{p_i} \mathrm{GCD}(a_{i,j_1} b_{i,j_2}) - mn(r-2), \tag{8}$$

$$4 - 2g(h_F) = \sum_{i=1}^{r} \sum_{j_2=1}^{p_i} \sum_{j_1=1}^{p_i} \mathrm{GCD}(b_{i,j_1} b_{i,j_2}) - (r-2)m^2. \tag{9}$$

Theorem 2.3. *Let F be a simple rational function of degree $m \ge 4$, and H a rational function of degree $n \ge 2$ such that the curve $h_{H,F}$ is irreducible. Then $g(h_{H,F}) > 0$. In particular, the functional equation $F \circ X = H \circ Y$ has no solutions in non-constant rational functions X, Y.*

Proof. Keeping the above notation, let us observe that if z_i, $1 \le i \le r$, is not a critical value of F, then obviously

$$\sum_{j_1=1}^{p_i} \mathrm{GCD}(a_{i,j_1} b_{i,j_2}) = p_i, \quad 1 \le j_2 \le q_i, \tag{10}$$

and

$$\sum_{j_2=1}^{q_i} \sum_{j_1=1}^{p_i} \mathrm{GCD}(a_{i,j_1} b_{i,j_2}) = mp_i. \tag{11}$$

Assume now that z_i, $1 \le i \le r$, is a critical value of F. Then (10) still holds if $b_{i,j_2} = 1$, while if $b_{i,j_2} = 2$, $1 \le j_2 \le q_i$, we have

$$\sum_{j_1=1}^{p_i} \mathrm{GCD}(a_{i,j_1} b_{i,j_2}) = p_i + l_i,$$

where l_i is the number of even numbers among the numbers a_{i,j_1}, $1 \le j_1 \le p_i$. Since among the numbers b_{i,j_2}, $1 \le j_2 \le q_i$, one number is equal to two and $m-2$ other numbers are equal to one, we conclude that

$$\sum_{j_2=1}^{q_i} \sum_{j_1=1}^{p_i} \mathrm{GCD}(a_{i,j_1} b_{i,j_2}) = (m-2)p_i + p_i + l_i = mp_i + (l_i - p_i). \tag{12}$$

As

$$2n - 2 = \sum_{z \in \mathbb{CP}^1} (\deg_z H - 1) = \sum_{i=1}^{r} \sum_{j_1=1}^{p_i} (a_{i,j_1} - 1) = rn - \sum_{i=1}^{r} p_i,$$

the equality

$$\sum_{i=1}^{r} p_i = (r-2)n + 2 \tag{13}$$

holds, implying by (11) and (12) that

$$\begin{aligned} \sum_{i=1}^{r} \sum_{j_2=1}^{q_i} \sum_{j_1=1}^{p_i} \mathrm{GCD}(a_{i,j_1} b_{i,j_2}) &= \sum_{i=1}^{r} mp_i + {\sum}' (l_i - p_i) \\ &= m((r-2)n + 2) + {\sum}' (l_i - p_i), \end{aligned} \tag{14}$$

where the sum $\sum'$ runs only over indices corresponding to critical values of F. It follows now from (8) that $g(h_{H,F}) = 0$ if and only if

$$2m - 2 + {\sum}' (l_i - p_i) = 0.$$

Stated differently, $g(h_{H,F}) = 0$ if and only if the preimage $H^{-1}\{c_1, c_2, \ldots, c_{2m-2}\}$, where $c_1, c_2, \ldots, c_{2m-2}$ are critical values of F, contains exactly $2m-2$ points where the multiplicity of H is odd.

Let us observe now that for any finite subset S of $\mathbb{CP}^1$ it follows from

$$2n - 2 = \sum_{z \in \mathbb{CP}^1} (\deg_z H - 1) \ge \sum_{z \in H^{-1}(S)} (\deg_z H - 1)$$

that the preimage $H^{-1}(S)$ contains at least $n(|S| - 2) + 2$ points and the equality is attained if and only if S contains the set of critical values of H. Therefore,

$$H^{-1}\{c_1, c_2, \ldots, c_{2m-2}\} \ge (2m-4)n + 2,$$

and the equality is attained if and only if any critical value of H is a critical value of F. On the other hand, the condition that $H^{-1}\{c_1, c_2, \dots, c_{2m-2}\}$ contains $2m-2$ points where the multiplicity of H is odd implies that

$$H^{-1}\{c_1, c_2, \dots, c_{2m-2}\} \leq (2m-2) + \frac{n(2m-2) - (2m-2)}{2} = (n+1)(m-1),$$

and the equality is attained if and only if all $2m-2$ points with odd multiplicity in $H^{-1}\{c_1, c_2, \dots, c_{2m-2}\}$ have multiplicity one, while all points with even multiplicity have multiplicity two. Thus, if $g(h_{H,F}) = 0$, then

$$(2m-4)n + 2 \leq (n+1)(m-1),$$

implying that

$$(n-1)(m-3) \leq 0.$$

Since the last inequality is satisfied only for $n = 1$ or for $m = 2, 3$, we conclude that $g(h_{H,F}) > 0$. □

Theorem 2.4. *Let F be a simple rational function of degree $m \geq 3$. Then the curve h_F is irreducible and $g(h_F) > 0$. In particular, the equality $F \circ X = F \circ Y$, where X and Y are non-constant rational functions, implies that $X = Y$.*

Proof. It is well-known (see, e.g., [32, Corollary 2.3]) that the curve $h_F(x, y)$ is irreducible if and only if the monodromy group $\mathrm{Mon}(F)$ is doubly transitive. Therefore, since a symmetric group is doubly transitive, the irreducibility of $h_F(x, y)$ follows from Theorem 2.2.

Further, applying (14) and (13) for $H = F$ we see that

$$\sum_{i=1}^{r} \sum_{j_2=1}^{p_i} \sum_{j_1=1}^{p_i} \mathrm{GCD}(b_{i,j_1} b_{i,j_2}) = \sum_{i=1}^{2m-2} m p_i + \sum_{i=1}^{2m-2} (1 - p_i) = \sum_{i=1}^{2m-2} (m-1)p_i + 2m - 2$$
$$= (m-1)((2m-4)m + 2) + 2m - 2$$
$$= m^2(2m-4) - 2m^2 + 8m - 4.$$

Therefore, by formula (9), we have:

$$g(h_F) = (m-2)^2, \tag{15}$$

and hence $g(h_F) > 0$ whenever $m \geq 3$. □

2.3 Conditions for reducibility of $H(x) - F(y) = 0$. The problem of finding conditions under which the algebraic curve $h_{H,F}$ is reducible, the so-called Davenport–Lewis–Schinzel problem, has a long story and is not solved yet in its full generality (see [14] for an introduction to the topic). In this section, we consider a very particular case of this problem (Theorem 2.7 below), which is related to the subject of this paper and can be handled without using serious group theoretic methods. The reader interested in these methods is referred to the recent paper [23], where significant progress has been made in the polynomial case, and the bibliography therein.

Let F be a rational function of degree $m \geq 2$, and $U \subset \mathbb{CP}^1$ a simply connected domain containing no critical values of F. Then in U there exist $m = \deg F$ different branches of the algebraic function $F^{-1}(z)$. We will denote these branches by small letters $f_1, f_2, \ldots, f_m$.

Lemma 2.5. *Let F be a rational function of degree $m \geq 2$ such that*

$$\mathrm{Mon}(F) = S_m,$$

$f_1, f_2, \ldots, f_m$ different branches of $F^{-1}(z)$ defined in some simply connected domain U containing no critical values of F, and C_i, $0 \leq i \leq m$, rational functions. Then the equality

$$C_1 f_1 + C_2 f_2 + \cdots + C_m f_m = C_0 \tag{16}$$

implies that $C_1 = C_2 = \cdots = C_m$.

Proof. Assume, say, that $C_1 \neq C_2$. Since $\mathrm{Mon}(F) = S_m$, the transposition $\sigma = (1, 2)$ is contained in $\mathrm{Mon}(F)$, and considering the analytical continuation of equality (16) along a loop corresponding to σ we obtain the equality

$$C_1 f_2 + C_2 f_1 + \cdots + C_m f_m = C_0. \tag{17}$$

It follows now from (16) and (17) that

$$(C_1 - C_2)(f_1 - f_2) = 0,$$

whence $f_1 = f_2$ in contradiction with the assumption that $f_1, f_2, \ldots, f_m$ are different. □

Lemma 2.6. *Let H be an indecomposable rational function of degree $n \geq 2$, $h_1, h_2, \ldots, h_m$ different branches of $H^{-1}(z)$ defined in some simply connected domain V containing no critical values of H, and R another rational function. Then either $R(h_i) \neq R(h_j)$ for $i \neq j$, $1 \leq i, j \leq n$, or $R(h_1) = R(h_2) = \cdots = R(h_n)$. In the last case, $R(h_1)$ is a rational function.*

Proof. It is easy to see that for fixed j, $1 \le j \le n$, the set of all i, $1 \le i \le n$, such that $R(h_i) = R(h_j)$ is a block of $\mathrm{Mon}(H)$. Since H is indecomposable, this implies the first statement of the lemma. Finally, if the functions $R(h_i)$, $1 \le i \le n$, are equal, then the algebraic function obtained by a full analytical continuation of $R(h_1)$ is single-valued in $\mathbb{CP}^1$ and therefore it is a rational function. □

Theorem 2.7. *Let H and F be rational functions of degrees $n \ge 2$ and $m \ge 2$ such that H is indecomposable, $\mathrm{Mon}(F) = S_m$, and the curve $h_{H,F}$ is reducible. Then either $H = F \circ \mu$, where μ is a Möbius transformation, or $n = \binom{m}{k}$ for some k, $1 < k < m - 1$.*

Proof. Suppose that

$$h_{H,F}(x, y) = M(x, y)N(x, y)$$

for some non-constant polynomials $M(x, y)$, $N(x, y)$. Notice that since H and F are non-constant, for such polynomials the degrees $\deg_x M$, $\deg_y M$, $\deg_x N$, $\deg_y N$ are distinct from zero.

Let $h_1, h_2, \dots, h_n$ be different branches of $H^{-1}(z)$ and $f_1, f_2, \dots, f_m$ different branches of $F^{-1}(z)$ defined in a simply connected domain $U \subset \mathbb{CP}^1$ containing no critical values of F or H. Since

$$h_{H,F}(h_1, f_i) = 0, \quad 1 \le i \le m,$$

among the indices i, $1 \le i \le m$, there are $k = \deg_y M > 0$ indices for which the equality

$$M(h_1, f_i) = 0 \tag{18}$$

holds. Moreover, $k < m$, since otherwise the equality $\deg_y M + \deg_y N = m$ implies that $\deg_y N = 0$. Let $i_1, i_2, \dots, i_k$ be indices for which (18) holds. Writing $M(x, y)$ in the form

$$M(x, y) = P_k(x)y^k + P_{k-1}(x)y^{k-1} + \cdots + P_1(x)y + P_0(x),$$

where P_i, $0 \le i \le k$, are polynomials, we see that (18) implies that

$$f_{i_1} + f_{i_2} + \cdots + f_{i_k} = Q(h_1), \tag{19}$$

where $Q = P_{k-1}/P_k$ is a rational function. Furthermore, since the set $\{i_1, i_2, \dots, i_k\}$ is a proper subset of $\{1, 2, \dots, m\}$, the function $Q(h_1)$ is not a rational function by Lemma 2.5. Therefore, by Lemma 2.6, the functions $Q(h_i)$, $1 \le i \le n$, are pairwise different.

Continuing equality (19) analytically along an arbitrary closed curve γ in $\mathbb{CP}^1$, we obtain an equality where on the left side is a sum of branches of $F^{-1}(z)$ over a subset of $\{1, 2, \ldots, m\}$ containing k elements, while on the right side is a branch $Q(h_i)$, $1 \leq i \leq n$, of the function $Q(h_1)$. Furthermore, to different subsets of $\{1, 2, \ldots, m\}$ correspond different branches of $Q(h_1)$, for otherwise subtracting we obtain a contradiction with Lemma 2.5. Since the equality $\mathrm{Mon}(F) = S_m$ implies that for an appropriately chosen γ we can obtain on the left side a sum of branches of $F^{-1}(z)$ over any k-element subset of $\{1, 2, \ldots, m\}$, while the transitivity of $\mathrm{Mon}(H)$ implies that for an appropriately chosen γ we can obtain on the right side any branch of $Q(h_i)$, $1 \leq i \leq n$, we conclude that n is equal to the number of k-element subsets of $\{1, 2, \ldots, m\}$, for some k, $1 \leq k \leq n$, that is, $n = \binom{m}{k}$.

To finish the proof, let us observe that if $k = 1$, then $n = \binom{m}{k}$ implies that $n = m$. Furthermore, equality (19) implies the equality

$$z = F(f_{i_1}) = (F \circ Q)(h_1).$$

Thus, the function $F \circ Q$ is inverse to h_1, that is, $H = F \circ Q$. Finally, Q is a Möbius transformation since $n = m$. The same conclusion is true if $k = m - 1$, since we can switch between $M(x, y)$ and $N(x, y)$. □

2.4 Prime divisors of $\binom{m}{k}$. The classical theorem of Sylvester [53] and Schur [50] states that in the set of integers $a, a+1, \ldots, a+b-1$, where $a > b$, there is a number divisible by a prime greater than b. For a natural number x, let us denote by $\mathcal{P}(x)$ the greatest prime factor of x. Then the theorem of Sylvester and Schur may be reformulated as follows ([7]): for any $m \geq 2k$ the inequality $\mathcal{P}(\binom{m}{k}) > k$ holds. Furthermore, the last inequality may be sharpened to the inequality

$$\mathcal{P}\left(\binom{m}{k}\right) \geq \frac{7}{5}k \tag{20}$$

(see [10], [21]). We will prove that this implies the following corollary.

Theorem 2.8. *Let $m \geq 4$ be a natural number, and k a natural number such that $1 < k < m-1$. Then there exists a prime number p such that $p \mid \binom{m}{k}$ but $p \nmid m$.*

Proof. Since $\binom{m}{k} = \binom{m}{m-k}$, it is enough to prove the theorem under the assumption that $m \geq 2k$. Applying the Sylvester–Schur theorem, we conclude that there is a number s, $m - k + 1 \leq s \leq m$, such that $\mathcal{P}(\binom{m}{k}) = \mathcal{P}(s) = p > k$. Moreover, if s is strictly less than m, then p cannot be a divisor of m for otherwise

$$p|(m - s), \tag{21}$$

where $m - s \leq k - 1$ in contradiction with

$$p > k. \tag{22}$$

Since however s can be equal to m, we modify slightly this argument. Namely, we apply the Sylvester–Schur theorem in its strong form (20) to the binomial coefficient $\binom{m-1}{k-1}$ related with $\binom{m}{k}$ by the equality

$$\binom{m}{k} = \frac{m(m-1)\cdots(m-k+1)}{k(k-1)\cdots 1} = \frac{m}{k}\binom{m-1}{k-1}. \tag{23}$$

Notice that (23) implies that every prime factor p of $\binom{m-1}{k-1}$ satisfying (22) remains a prime factor of $\binom{m}{k}$.

Since $m \geq 2k$ implies $m - 1 \geq 2(k-1)$, applying (20) to $\binom{m-1}{k-1}$ we conclude that there is a number s, $m - k + 1 \leq s \leq m - 1$, such that

$$\mathcal{P}\left(\binom{m-1}{k-1}\right) = \mathcal{P}(s) = p \geq \frac{7}{5}(k-1).$$

Furthermore, if $k > 3$ then

$$p \geq \frac{7}{5}(k-1) > k,$$

implying that $p \mid \binom{m}{k}$. On the other hand, $p \nmid m$ since otherwise (21) holds in contradiction with (22).

For $k \leq 3$, the theorem can be proved by an elementary argument. If $k = 2$, then

$$\binom{m}{k} = \frac{m(m-1)}{2}.$$

Therefore, since $\mathrm{GCD}(m, m-1) = 1$, the statement of the theorem is true, whenever $(m-1) \nmid 2$, and the last condition is always satisfied if $m > 3$. Similarly, if $k = 3$, then

$$\binom{m}{k} = \frac{m(m-1)(m-2)}{2 \cdot 3},$$

and the statement of the theorem is true whenever $(m-1) \nmid 6$. The last condition fails to be true for $m > 3$ only if m is equal to 4 or 7. However, the pair $m = 4$, $k = 3$ does not satisfy the condition $1 < k < m - 1$. On the other hand, for the pair $m = 7$, $k = 3$, we have $\binom{m}{k} = \binom{7}{3} = 5 \cdot 7$, and the statement of the theorem is satisfied for $p = 5$. □

Proof of Theorem 1.1. The proof is by induction on l. Let

$$F^{\circ l} = F_r \circ F_{r-1} \circ \cdots \circ F_1 \tag{24}$$

be a decomposition of $F^{\circ l}$, $l \geq 1$, into a composition of indecomposable rational functions. Since F is indecomposable by Theorem 2.2, for $l = 1$ the theorem is true. On the other hand, since by Theorem 2.4 the equality $F \circ X = F \circ Y$ implies that $X = Y$, to prove the inductive step it is enough to show that equality (24) implies that

$$F_r = F \circ \mu \tag{25}$$

for some Möbius transformation μ.

Clearly, equality (24) implies that the algebraic curve

$$F(x) - F_r(y) = 0 \tag{26}$$

has a factor of genus zero. Therefore, (26) is reducible by Theorem 2.3. Since $\mathrm{Mon}(F) = S_m$ by Theorem 2.2, it follows now from Theorem 2.7 that either (25) holds, or $\deg F_r = \binom{m}{k}$ for some k, $1 < k < m - 1$. However, the last case is impossible since (24) implies that any prime divisor of $\deg F_r$ is a prime divisor of $\deg F$ in contradiction with Theorem 2.8. □

Corollary 2.9. *Let F be a simple rational function of degree $m \geq 4$, and G_i, $1 \leq i \leq r$, rational functions of degree at least two such that*

$$F^{\circ l} = G_r \circ G_{r-1} \circ \cdots \circ G_1$$

for some $l \geq 1$. Then there exist Möbius transformations v_i, $1 \leq i < r$, and integers $s_i \geq 1$, $1 \leq i \leq r$, such that

$$G_r = F^{\circ s_r} \circ v_{r-1}, \quad G_i = v_i^{-1} \circ F^{\circ s_i} \circ v_{i-1}, \quad 1 < i < r,$$

and

$$G_1 = v_1^{-1} \circ F^{\circ s_1}.$$

Proof. To prove the corollary, it is enough to decompose each G_i, $1 \leq i \leq r$, into a composition of indecomposable rational functions and to apply Theorem 1.1. □

3 Groups and semigroups related to rational functions

3.1 Groups and semigroups related to simple rational functions. We start this section by recalling some basic facts concerning the groups and semigroups defined in the introduction. We will say that a rational function F of degree at least two is **special** if F is either a Lattès map, or it is conjugate to a power $z^{\pm n}$ or to a Chebyshev polynomial $\pm T_n$ (we will recall the definition of Lattès maps below, in Section 4.1, in a more general context).

It is obvious that $C(F)$ is a semigroup, and it follows from the inclusions

$$C(F^{\circ k}),\ C(F^{\circ l}) \subseteq C(F^{\circ \mathrm{LCM}(k,l)})$$

that $C_\infty(F)$ is also a semigroup. We use the following characterization of $C_\infty(F)$.

Theorem 3.1. *Let F be a non-special rational function of degree at least two. Then a rational function G of degree at least two belongs to $C_\infty(F)$ if and only if equality* (2) *holds for some $k, l \geq 1$.*

Proof. By the Ritt theorem (see [48], and also [8], [40]), commuting rational functions of degree at least two are either special or have a common iterate. Thus, if G belongs to $C_\infty(F) \setminus \mathrm{Aut}_\infty(F)$, then (2) holds for some $k, l \geq 1$. On the other hand, if (2) holds, then G commutes with $F^{\circ k}$, and thus G belongs to $C_\infty(F)$. □

Notice that a practical method for describing $C(F)$ for an arbitrary non-special rational function F was given in the recent paper [40], but a satisfactory description of $C_\infty(F)$ is still not known (see [42] for some particular results). Thus, condition (2) remains the only characterization of $C_\infty(F)$.

Let us recall that by the results of Freire, Lopes, Mañé ([12]) and Lyubich ([26]), for every rational function F of degree $n \geq 2$, there exists a unique probability measure μ_F on $\mathbb{CP}^1$, which is invariant under F, has support equal to the Julia set J_F, and achieves maximal entropy $\log n$ among all F-invariant probability measures. The measure μ_F can be characterized as follows. For $a \in \mathbb{CP}^1$, let $z_i^k(a)$, $i = 1, \dots, n^k$, be the roots of the equation $F^{\circ k}(z) = a$ counted with multiplicity, and $\mu_{F,k}(a)$ be the measure defined by

$$\mu_{F,k}(a) = \frac{1}{n^k} \sum_{i=1}^{n^k} \delta_{z_i^k(a)}. \tag{27}$$

Then for every $a \in \mathbb{CP}^1$ with two possible exceptions, the sequence $\mu_{F,k}(a)$, $k \geq 1$, converges in the weak topology to μ_F. It follows from the characterization of μ_F as a limit of (27) that any G sharing an iterate with F belongs to $E(F)$. Thus,

$$C_\infty(F) \subseteq E(F). \tag{28}$$

Moreover, since the equality

$$F^{\circ n} = \alpha^{-1} \circ F^{\circ n} \circ \alpha,$$

where $\alpha \in \mathrm{Aut}(\mathbb{CP}^1)$ and $n \geq 1$, implies that

$$|S \cap F^{-nk}(a)| = |\alpha(S) \cap F^{-nk}(\alpha(a))|, \quad k \geq 1,$$

for any set $S \subset \mathbb{CP}^1$ and $a \in \mathbb{CP}^1$, this characterization yields that

$$\mathrm{Aut}_\infty(F) \subseteq E_0(F). \tag{29}$$

The fact that $E(F)$ is a semigroup can be established using the Lyubich operator or the balancedness property of μ_F (see [6], [42]), and the analogue of Theorem 3.1 is the following statement.

Theorem 3.2. *Let F be a non-special rational function of degree at least two. Then a rational function G of degree at least two belongs to $E(F)$ if and only if equality* (3) *holds for some $k_1, l \geq 1$, $k_2 \geq 0$.*

Proof. It is known and can be easily shown using the Lyubich operator that equality (3) implies the equality $\mu_F = \mu_G$ ([24]). On the other hand, it is shown in [57] that the characterization of non-special rational functions sharing the measure of maximal entropy obtained in the papers [24], [25] implies that for such functions F and G equality (3) holds. □

A complete description of $E(F)$ is known only if F is a polynomial, in which case $E(F) \setminus E_0(F)$ coincides with the set of polynomials sharing a Julia set with F (see [1], [2], [49] and also [41], [42]). Some partial results in the rational case can be found in [39], [57].

The group $G_0(F)$ obviously is a subgroup of the larger group $G(F)$ consisting of all $\sigma \in \mathrm{Aut}(\mathbb{CP}^1)$ such that

$$F \circ \sigma = \nu \circ F \tag{30}$$

for some $\nu \in \mathrm{Aut}(\mathbb{CP}^1)$. It is easy to see that $G(F)$ is indeed a group and that the map

$$\gamma : \sigma \to \nu_\sigma$$

is a homomorphism from $G(F)$ to the group $\mathrm{Aut}(\mathbb{CP}^1)$. The group $G(F)$ is finite and its order is bounded in terms of $m = \deg F$, unless

$$\alpha \circ F \circ \beta = z^m \tag{31}$$

for some Möbius transformations α, β (see [37, Section 4] or [45, Section 2]). Thus, the group $G_0(F)$ is also finite, unless (31) holds.

Lemma 3.3. *Let F be a simple rational function of degree $m \geq 3$. Then the group $G_0(F)$ is finite, and the restriction of γ to $G_0(F)$ is an automorphism of $G_0(F)$.*

Proof. Since equality (31) is impossible for simple F of degree $m \geq 3$, the group $G_0(F)$ is finite. Furthermore, since the equality $F = F \circ \sigma$, where $\sigma \in G_0(F)$, implies by Theorem 2.4 that σ is the identity element, the restriction of γ on $G_0(F)$ is a monomorphism. Since $\gamma(G_0(F)) \subseteq G_0(F)$ by the definition, this implies that the restriction of γ to $G_0(F)$ is an automorphism of $G_0(F)$. □

Corollary 3.4. *Let F be a simple rational function of degree $m \geq 3$. Then $G_0(F) \subseteq \mathrm{Aut}(F^{\circ s})$, where $s = |\mathrm{Aut}(G_0(F))|$.*

Proof. For $s = |\mathrm{Aut}(G_0(F))|$, the iterate $\gamma^{\circ s}$ is the identity automorphism of $G_0(F)$. Therefore, since for every $\sigma \in G_0(F)$ the equality

$$F^{\circ l} \circ \sigma = \gamma^{\circ l}(\sigma) \circ F^{\circ l}, \quad l \geq 1,$$

holds, every $\sigma \in G_0(F)$ commutes with $F^{\circ s}$. □

Lemma 3.5. *Let F be a rational function, and σ a Möbius transformation such that*

$$(\sigma \circ F)^{\circ l} = F^{\circ l} \tag{32}$$

for some $l \geq 1$. Then $\sigma \in \mathrm{Aut}(F^{\circ l})$.

Proof. Clearly, equality (32) implies the equality

$$(\sigma \circ F)^{\circ (l-1)} \circ \sigma = F^{\circ (l-1)}. \tag{33}$$

Composing now F with both parts of equality (33), we obtain the equality

$$(F \circ \sigma)^{\circ l} = F^{\circ l}. \tag{34}$$

It follows now from (32) and (34) that

$$F^{\circ l} \circ \sigma = (\sigma \circ F)^{\circ l} \circ \sigma = \sigma \circ (F \circ \sigma)^{\circ l} = \sigma \circ F^{\circ l}.$$

□

Lemma 3.6. *Let F be a simple rational function of degree $m \geq 4$. Then F is not a special function.*

Proof. The proof follows easily from the analysis of ramifications of special functions. Since below we prove a more general result (Lemma 4.3), we omit it. □

Theorem 3.7. *Let F be a simple rational function of degree $m \geq 4$. Then*

$$E_0(F) = G_0(F) = \mathrm{Aut}_\infty(F) = \mathrm{Aut}(F^{\circ s}),$$

where $s = |\mathrm{Aut}(G_0(F))|$.

Proof. By Corollary 3.4 and (29), we have

$$G_0(F) \subseteq \mathrm{Aut}(F^{\circ s}) \subseteq \mathrm{Aut}_\infty(F) \subseteq E_0(F).$$

Thus, to prove the theorem we only must prove that $E_0(F) \subseteq G_0(F)$. For this, it is enough to show that for every $\sigma \in E_0(F)$ there exists $\nu \in E_0(F)$ such that (30) holds. Let σ be an element of $E_0(F)$. Then $F \circ \sigma$ is a simple rational function which belongs to $E(F)$, implying by Lemma 3.6 and Theorem 3.2 that

$$F^{\circ k_1} = F^{\circ k_2} \circ (F \circ \sigma)^{\circ l}$$

for some $k_1, l \geq 1$, $k_2 \geq 0$. Applying to the last equality recursively Theorem 2.4, we see that

$$F^{\circ(k_1 - k_2)} = (F \circ \sigma)^{\circ l}. \tag{35}$$

Therefore, by Theorem 1.1, there exist Möbius transformations μ_i, $1 \leq i \leq l-1$, such that

$$F \circ \sigma = F \circ \mu_{r-1}, \quad F \circ \sigma = \mu_i^{-1} \circ F \circ \mu_{i-1}, \quad 1 < i < l, \quad \text{and} \quad F \circ \sigma = \mu_1^{-1} \circ F.$$

Thus, equality (30) holds for $\nu = \mu_1^{-1}$. Furthermore, since equality (35) implies that $k_1 - k_2 = l$, we have

$$F^{\circ l} = (F \circ \sigma)^{\circ l} = (\mu_1^{-1} \circ F)^{\circ l},$$

implying by Lemma 3.5 that

$$\mu_1^{-1} \in \mathrm{Aut}(F^{\circ l}) \subseteq \mathrm{Aut}_\infty(F) \subseteq E_0(F).$$

□

Corollary 3.8. *Let F be a simple rational function of degree $m \geq 4$. Then every element of the semigroup $\langle \mathrm{Aut}_\infty(F), F \rangle$ can be represented in a unique way in the form $\alpha \circ F^{\circ s}$, where $\alpha \in \mathrm{Aut}_\infty(F)$ and $s \geq 0$. Moreover, for every $k \geq 1$, every element of the semigroup $\langle \mathrm{Aut}(F^{\circ k}), F \rangle$ can be represented in a unique way in the form $\alpha \circ F^{\circ s}$, where $\alpha \in \mathrm{Aut}(F^{\circ k})$ and $s \geq 0$.*

Proof. The first part of the corollary follows from the equality

$$\mathrm{Aut}_\infty(F) = G_0(F).$$

To prove the second, it is enough to observe that for every $\nu \in \mathrm{Aut}(F^{\circ k})$ the element $\nu' \in \mathrm{Aut}_\infty(F)$ such that

$$F \circ \nu = \nu' \circ F \tag{36}$$

belongs to $\mathrm{Aut}(F^{\circ k})$. Indeed, (36) implies that

$$F^{\circ k} \circ \nu' \circ F = F^{\circ k} \circ F \circ \nu = F \circ F^{\circ k} \circ \nu = F \circ \nu \circ F^{\circ k} = \nu' \circ F \circ F^{\circ k} = \nu' \circ F^{\circ k} \circ F,$$

whence $\nu' \in \mathrm{Aut}(F^{\circ k})$. □

Proof of Theorem 1.2. In view of Theorem 3.7, we only must show that

$$C_\infty(F) = E(F) = \langle \mathrm{Aut}_\infty(F), F \rangle.$$

By (28), the first equality follows from Theorem 3.2 and Theorem 2.4, since the latter implies that any G satisfying (3) satisfies (2) for $k = k_1 - k_2$. Since the semigroup $\langle \mathrm{Aut}_\infty(F), F \rangle$ is obviously a subsemigroup of $C_\infty(F)$, to finish the proof we only must show that if a rational function G satisfies (2), then it belongs to $\langle \mathrm{Aut}_\infty(F), F \rangle$.

Applying Corollary 2.9 to equality (2), we see that there exist Möbius transformations μ_i, $1 \leq i \leq l-1$, such that

$$G = F^{\circ s} \circ \mu_{l-1}, \quad G = \mu_i^{-1} \circ F^{\circ s} \circ \mu_{i-1}, \quad 1 < i < l,$$

and

$$G = \mu_1^{-1} \circ F^{\circ s},$$

where $s = k/l$. Moreover, since

$$F^{\circ sl} = G^{\circ l} = (\mu_1^{-1} \circ F^{\circ s})^{\circ l},$$

Lemma 3.5 implies that

$$\mu_1^{-1} \in \mathrm{Aut}(F^{\circ sl}) \subseteq \mathrm{Aut}_\infty(F).$$

Thus,

$$G = \mu_1^{-1} \circ F^{\circ s} \in \langle \mathrm{Aut}_\infty(F), F \rangle.$$

□

3.2 Groups and semigroups related to general rational functions. Let us recall that writing a rational function $F = F(z)$ of degree m as $F = P/Q$, where

$$P(z) = a_m z^m + a_{m-1} z^{m-1} + \cdots + a_1 z + a_0, \quad Q(z) = b_m z^m + b_{m-1} z^{m-1} + \cdots + b_1 z + b_0$$

are polynomials of degree m without common roots, we can identify the space of rational functions of degree m with the algebraic variety

$$\mathrm{Rat}_m = \mathbb{CP}^{2m+1} \setminus \{\mathrm{Res}_{m,m,z}(P, Q) = 0\},$$

where $\mathrm{Res}_{m,m,z}(P, Q)$ denotes the resultant of P and Q. We recall that we say that some statement holds for general rational functions of degree m, if it holds for all $F \in \mathrm{Rat}_m$ with the exception of some proper Zariski closed subset.

Lemma 3.9. *A general rational function F of degree $m \geq 2$ is simple.*

Proof. We recall that for $F \in \mathrm{Rat}_m$ the set of finite critical points of F coincides with the set of zeroes of its Wronskian

$$W(z) = P'(z)Q(z) - P(z)Q'(z).$$

Obviously, $\deg W \leq 2m - 2$. Moreover, $\deg W = 2m - 2$, unless F belongs to the projective hypersurface U in $\mathbb{CP}^{2m+1}$ defined by

$$U: \ a_m b_{m-1} - b_m a_{m-1} = 0.$$

Let us define now a polynomial $R(t)$ by the formula

$$R(t) = \mathrm{Res}_{2m-2,m,z}(W(z), P(z) - Q(z)t).$$

By the well-known property of the resultant, for $F \in \mathrm{Rat}_m \setminus U$ the equality

$$R(t) = c \prod_{\zeta, W(\zeta)=0} (P(\zeta) - Q(\zeta)t)$$

holds for some $c \in \mathbb{C}^*$, and thus the set of zeroes of $R(t)$ coincides with the set of finite critical values of F.

Finally, let us define a projective hypersurface Z in $\mathbb{CP}^{2m+1}$ by

$$Z: \ \mathrm{Res}_{2m-2,2m-3,t}(R(t), R'(t)) = 0.$$

By the resultant properties, $F \in \mathrm{Rat}_m \setminus U$ belongs to Z if and only if either some finite critical values of F coincide, or $\deg R(t) < 2m - 2$ meaning that infinity is a critical value of F. Thus, every rational function $F \in \mathrm{Rat}_m \setminus Z \cup U$ has $2m - 2$ distinct finite critical values, and hence is simple. □

Lemma 3.10. *For a general rational function F of degree $m \geq 3$ the group $G(F)$ is trivial.*

Proof. Let

$$\alpha = \frac{\alpha_{1,1}z + \alpha_{0,1}}{\alpha_{1,2}z + \alpha_{0,2}}, \quad \beta = \frac{\beta_{1,1}z + \beta_{0,1}}{\beta_{1,2}z + \beta_{0,2}}$$

be elements of Rat_1, and

$$F = \frac{f_{m,1}z^m + f_{m-1,1}z^{m-1} + \cdots + f_{1,1}z + f_{0,1}}{f_{m,2}z^m + f_{m-1,2}z^{m-1} + \cdots + f_{1,2}z + f_{0,2}}$$

an element of Rat_m. It is easy to see that the coefficients of the numerator of the rational function $\alpha \circ F \circ \beta - F$ are polynomials in α_i^j, β_i^j, f_i^j homogenous of degree one in α_i^j, homogenous of degree two in f_i^j, and homogenous of degree m in β_i^j. Thus, the equality

$$\alpha \circ F \circ \beta = F$$

implies that the coefficients of α, β, and F belong to some projective algebraic variety

$$W \subseteq \mathbb{CP}^3 \times \mathbb{CP}^{2m+1} \times \mathbb{CP}^3.$$

Since the projection

$$p_k : (\mathbb{CP}^1)^l \times (\mathbb{CP}^1)^k \to (\mathbb{CP}^1)^k, \quad k, l \geq 1,$$

is a closed map (see, e.g., [29]), this implies that the set of $F \in \mathrm{Rat}_m$ with non-trivial group $G(F)$ is contained in some Zariski closed subset of $\mathbb{CP}^{2m+1}$.

To finish the proof, we only must show that Z does not contain the whole variety Rat_m for $m \geq 3$. For this, it is enough to show that for every $m \geq 3$ there exists a polynomial F of degree m such that the group $G(F)$ is trivial. Let us recall that for any polynomial F of degree $m \geq 2$ the group $G(F)$ is a finite cyclic group generated by a polynomial, unless (31) holds (see, e.g., [45, Section 2]). On the other hand, it is easy to see that if F has the form

$$F = z^m + a_{m-2}z^{m-2} + a_{m-3}z^{m-3} + \cdots + a_0, \tag{37}$$

then equality (30) may hold for polynomials $\sigma = az + b$, $\mu = cz + d$ only if $b = 0$ and a is a root of unity. This implies easily that for any polynomial of the form (37) with $a_{m-2} \neq 0$, $a_{m-3} \neq 0$ the group $G(F)$ is trivial. □

Notice that Lemma 3.10 is not true for $m = 2$. Indeed, for every rational function F of degree two there exist Möbius transformations α, β such that equality (31) holds, implying that the group $G(P)$ is non-trivial, and even infinite.

Proof of Theorem 1.3. Since $G_0(F)$ is a subgroup of $G(F)$, the theorem follows from Theorem 1.2 combined with Lemma 3.9 and Lemma 3.10. □

4 Semiconjugate rational functions and invariant curves

4.1 Generalized Lattès maps, semiconjugate rational functions, and invariant curves. In this section, we recall some definitions and results related to the functional equation

$$A \circ X = X \circ B \tag{38}$$

in rational functions, and to invariant curves for endomorphisms of $(\mathbb{CP}^1)^2$ of the form

$$(A_1, A_2) : (z_1, z_2) \to (A_1(z_1), A_2(z_2)),$$

where A_1, A_2 are rational functions.

Let us recall that an **orbifold** $\mathcal{O}$ on $\mathbb{CP}^1$ is a ramification function $\nu : \mathbb{CP}^1 \to \mathbb{N}$, which takes the value $\nu(z) = 1$ except at a finite set of points. For an orbifold $\mathcal{O}$, the set of **singular points** of $\mathcal{O}$ is the set

$$c(\mathcal{O}) = \{z_1, z_2, \dots, z_s, \dots\} = \{z \in \mathbb{CP}^1 \mid \nu(z) > 1\},$$

and the **Euler characteristic** of $\mathcal{O}$ is the number

$$\chi(\mathcal{O}) = 2 + \sum_{z \in R} \Big(\frac{1}{\nu(z)} - 1\Big).$$

Let A be a rational function, and $\mathcal{O}_1, \mathcal{O}_2$ orbifolds with ramification functions ν_1 and ν_2. We say that $A : \mathcal{O}_1 \to \mathcal{O}_2$ is a **covering map** between orbifolds if for any $z \in \mathbb{CP}^1$ the equality

$$\nu_2(A(z)) = \nu_1(z) \deg_z A$$

holds. In case the weaker condition

$$\nu_2(A(z)) = \nu_1(z) \mathrm{GCD}(\deg_z A, \nu_2(A(z))$$

is satisfied, we say that $A : \mathcal{O}_1 \to \mathcal{O}_2$ is a **minimal holomorphic map** between orbifolds.

In the above terms, a **Lattès map** can be defined as a rational function A such that $A : \mathcal{O} \to \mathcal{O}$ is a covering map for some orbifold $\mathcal{O}$ (see [28], [38]). Following [38], we say that a rational function A of degree at least two is a **generalized Lattès map** if there exists an orbifold $\mathcal{O}$, distinct from the non-ramified sphere, such that $A : \mathcal{O} \to \mathcal{O}$ is a minimal holomorphic map. Thus, A is a Lattès map if there exists an orbifold $\mathcal{O}$ such that

$$\nu(A(z)) = \nu(z) \deg_z A, \quad z \in \mathbb{CP}^1, \tag{39}$$

and A is a generalized Lattès map if there exists an orbifold $\mathcal{O}$ such that

$$\nu(A(z)) = \nu(z)\mathrm{GCD}(\deg_z A, \nu(A(z))), \quad z \in \mathbb{CP}^1. \tag{40}$$

Since (39) implies (40), any Lattès map is a generalized Lattès map. More generally, any special function is a generalized Lattès map (see [38]). Notice that if (39) holds for some rational function A and orbifold $\mathcal{O}$, then $\mathcal{O}$ has zero Euler characteristic, while (40) implies that the Euler characteristic of $\mathcal{O}$ is non-negative (see, e.g., [38] for more detail).

Lattès maps and generalized Lattès maps can be characterized also in different terms (see [28], [38]). However, the definition using orbifolds is most convenient for our purposes since it permits to show easily that a simple rational function of degree at least four is not a generalized Lattès map. In turn, this fact is crucial for our proof of Theorem 1.4 and Theorem 1.5 since for rational functions A and A_1, A_2 that are not generalized Lattès maps describing solutions of (38) and (A_1, A_2)-invariant curves reduces to describing decompositions of iterates of A and A_1, A_2.

Specifically, our proof of Theorem 1.4 relies on the following corollary of the classification of semiconjugate rational functions (see [43, Proposition 3.3]).

Theorem 4.1. *Let A, B be rational functions of degree at least two and X a rational function of degree at least one such that equality* (38) *holds and A is not a generalized Lattès map. Then there exists a rational function Y such that $X \circ Y = A^{\circ d}$ for some $d \geq 0$.* □

In turn, our proof of Theorem 1.5 uses the following corollary of the description of invariant curves for endomorphisms (A_1, A_2) of $(\mathbb{CP}^1)^2$ (see [43, Theorem 1.1]).

Theorem 4.2. *Let A_1, A_2 be rational functions of degree at least two that are not generalized Lattès maps, and C an irreducible algebraic (A_1, A_2)-invariant curve in $(\mathbb{CP}^1)^2$ that is not a vertical or horizontal line. Then there exist rational functions X_1, X_2, Y_1, Y_2, B such that:*

(1) *The diagram*

$$\begin{array}{ccc} (\mathbb{CP}^1)^2 & \xrightarrow{(B,B)} & (\mathbb{CP}^1)^2 \\ {\scriptstyle (X_1,X_2)}\downarrow & & \downarrow{\scriptstyle (X_1,X_2)} \\ (\mathbb{CP}^1)^2 & \xrightarrow{(A_1,A_2)} & (\mathbb{CP}^1)^2 \end{array} \tag{41}$$

commutes,

(2) *the equalities*

$$X_1 \circ Y_1 = A_1^{\circ d}, \quad X_2 \circ Y_2 = A_2^{\circ d},$$

hold for some $d \geq 0$,

(3) *the map* $t \to (X_1(t), X_2(t))$ *is a parametrization of* C. □

Notice that if diagram (41) commutes, then this condition alone obviously is sufficient for (A_1, A_2)-invariance of the curve C parametrized by $t \to (X_1(t), X_2(t))$.

4.2 Proof of Theorem 1.4, Theorem 1.5, and Theorem 1.6. We start by proving the following lemma.

Lemma 4.3. *Let* F *be a simple rational function of degree* $m \geq 4$. *Then* F *is not a generalized Lattès map.*

Proof. If F is a simple rational function of degree $m \geq 4$, then the preimage of any k distinct points of $\mathbb{CP}^1$ under F contains at least $k(m-2) \geq 2k$ distinct points z such that $\deg_z F = 1$. Thus, if the equality

$$\nu(F(z)) = \nu(z)\mathrm{GCD}(\deg_z F, \nu(F(z))), \quad z \in \mathbb{CP}^1$$

holds for some orbifold $\mathcal{O}$ distinct from the non-ramified sphere, then the preimage $F^{-1}\{c(\mathcal{O})\}$ must contain at least $2|c(\mathcal{O})|$ points where $\nu(z) > 1$. However, this is impossible since any such a point belongs to $c(\mathcal{O})$. □

Proof of Theorem 1.4. By Lemma 4.3, F is not a generalized Lattès map. Since a rational function F is a generalized Lattès map if and only if some iterate $F^{\circ d}$, $d \geq 1$, is a generalized Lattès map (see [43, Section 2.3]), this implies that $F^{\circ r}$ also is not a generalized Lattès map. Hence, by Theorem 4.1, there exists a rational function Y such that the equality

$$X \circ Y = F^{\circ rd}$$

holds for some $d \geq 0$. By Corollary 2.9, this implies that

$$X = F^{\circ l} \circ \mu$$

for some Möbius transformation μ and $l \geq 0$. Thus, diagram (5) reduces to the equality

$$F^{\circ r} \circ F^{\circ l} \circ \mu = F^{\circ l} \circ \mu \circ G,$$

and applying to this equality Theorem 2.4, we conclude that

$$G = \mu^{-1} \circ F^{\circ r} \circ \mu.$$ □

Proof of Theorem 1.5. Assume that

$$(F_1, F_2)^{\circ d}(C) = C, \quad d \geq 1. \tag{42}$$

Then Theorem 4.2 and Theorem 1.4 imply that C is parametrized by

$$t \to ((F_1^{\circ d_1} \circ \beta)(t),\ (F_2^{\circ d_2} \circ \alpha)(t)) \tag{43}$$

for some $d_1, d_2 \geq 0$ and Möbius transformations α, β such that

$$\beta^{-1} \circ F_1^{\circ d} \circ \beta = \alpha^{-1} \circ F_2^{\circ d} \circ \alpha.$$

It is clear that without loss of generality we may assume that β is the identity map implying that

$$F_1^{\circ d} = \alpha^{-1} \circ F_2^{\circ d} \circ \alpha = (\alpha^{-1} \circ F_2 \circ \alpha)^{\circ d}. \tag{44}$$

This yields that

$$\alpha^{-1} \circ F_2 \circ \alpha \in C(F_1^{\circ d}) \subseteq C_\infty(F_1),$$

and hence

$$\alpha^{-1} \circ F_2 \circ \alpha = \mu \circ F_1 \tag{45}$$

for some $\mu \in \mathrm{Aut}_\infty(F_1)$ by Theorem 1.2 and Corollary 3.8. Further, equalities (44) and (45) imply by Lemma 3.5 that $\mu \in \mathrm{Aut}(F_1^{\circ d})$. Therefore,

$$F_2 = \alpha \circ \mu \circ F_1 \circ \alpha^{-1} \tag{46}$$

for some $\mu \in \mathrm{Aut}(F_1^{\circ d})$, and parametrization (43) takes the form

$$t \to (F_1^{\circ d_1}(t),\ \alpha \circ (\mu \circ F_1)^{\circ d_2}(t)). \tag{47}$$

Moreover, it follows from (47) by Corollary 3.8 that there exists $\mu' \in \mathrm{Aut}(F_1^{\circ d})$ such that this parametrization can be written in the form

$$t \to (F_1^{\circ d_1}(t),\ (\alpha \circ \mu' \circ F_1^{\circ d_2})(t)). \tag{48}$$

If $d_1 \leq d_2$, then (48) implies that C is parametrized by

$$t \to (t, (\alpha \circ \mu' \circ F_1^{\circ (d_2 - d_1)})(t))$$

for some $\mu' \in \mathrm{Aut}(F_1^{\circ d})$. On the other hand, if $d_1 > d_2$, then C is parametrized by

$$t \to (F_1^{\circ (d_1 - d_2)}(t),\ (\alpha \circ \mu')(t)).$$

Since Corollary 3.8 implies that

$$F_1^{\circ(d_1-d_2)} \circ \mu'^{-1} \circ \alpha^{-1} = \mu'' \circ F_1^{\circ(d_1-d_2)} \circ \alpha^{-1}$$

for some $\mu'' \in \mathrm{Aut}(F_1^{\circ d})$, we see that in this case C is also parametrized by

$$t \to ((\mu'' \circ F_1^{\circ(d_1-d_2)} \circ \alpha^{-1})(t),\ t)$$

for some $\mu'' \in \mathrm{Aut}(F_1^{\circ d})$. This proves the "only if" part of the theorem.

In the other direction, let us assume that (44) holds and C is a curve parametrized by

$$t \to (t,\ (\alpha \circ \mu \circ F_1^{\circ s})(t))$$

for some $\mu \in \mathrm{Aut}(F_1^{\circ d})$, Möbius transformation α, and $s \geq 0$. Since

$$F_2^{\circ d} \circ (\alpha \circ \mu \circ F_1^{\circ s}) = \alpha \circ F_1^{\circ d} \circ \mu \circ F_1^{\circ s} = \alpha \circ \mu \circ F_1^{\circ d} \circ F_1^{\circ s} = (\alpha \circ \mu \circ F_1^{\circ s}) \circ F_1^{\circ d},$$

in this case the diagram

$$\begin{array}{ccc} (\mathbb{CP}^1)^2 & \xrightarrow{(B,B)} & (\mathbb{CP}^1)^2 \\ {\scriptstyle (X_1,X_2)}\downarrow & & \downarrow{\scriptstyle (X_1,X_2)} \\ (\mathbb{CP}^1)^2 & \xrightarrow{(F_1^{\circ d},F_2^{\circ d})} & (\mathbb{CP}^1)^2 \end{array} \tag{49}$$

commutes for

$$B = F_1^{\circ d}, \quad X_1 = z, \quad X_2 = \alpha \circ \mu \circ F_1^{\circ s},$$

implying that (42) holds. Similarly, if C is parametrized by

$$t \to ((\mu \circ F_1^{\circ s} \circ \alpha^{-1})(t),\ t),$$

then it follows from

$$\begin{aligned} F_1^{\circ d} \circ (\mu \circ F_1^{\circ s} \circ \alpha^{-1}) &= \mu \circ F_1^{\circ d} \circ F_1^{\circ s} \circ \alpha^{-1} = \mu \circ F_1^{\circ s} \circ \alpha^{-1} \circ \alpha \circ F_1^{\circ d} \circ \alpha^{-1} \\ &= (\mu \circ F_1^{\circ s} \circ \alpha^{-1}) \circ F_2^{\circ d} \end{aligned}$$

that diagram (49) commutes for

$$B = F_2^{\circ d}, \quad X_1 = \mu \circ F_1^{\circ s} \circ \alpha^{-1}, \quad X_2 = z.$$

□

Proof of Theorem 1.6. By Lemma 3.9 and Lemma 3.10, there exists a Zariski open set U in Rat_m such that every $F \in U$ is simple and the group $G(F)$ is trivial. By Theorem 1.2, this implies that for every $F \in U$ the group $\mathrm{Aut}_\infty(F)$ is

also trivial. Since for simple F_1, F_2 equality (44) yields equality (46), it follows now from Theorem 1.5 that if $F_1, F_2 \in U$, then (F_1, F_2)-periodic curves exist if and only if

$$F_2 = \alpha \circ F_1 \circ \alpha^{-1}$$

for some Möbius transformation α. Furthermore, these periodic curves have the form

$$y = (\alpha \circ F_1^{\circ s})(x), \quad x = (F_1^{\circ s} \circ \alpha^{-1})(y),$$

and it is easy to check arguing as above that these curves are (F_1, F_2)-invariant. □

5 Indecomposable functions with non-trivial decompositions of iterates

Let F be an indecomposable rational function. In this section, we give a number of conditions implying that some iterate $F^{\circ k}$, $k > 1$, of F has a decomposition into a composition of indecomposable rational functions that is not equivalent to $F^{\circ k}$. For brevity, in this case we will say that $F^{\circ k}$ has a **non-trivial decomposition**. We also give explicit examples of simple rational functions of degrees 2 and 3 for which Theorems 1.1–1.2 and Theorems 1.4–1.5 do not hold.

Let us recall that for a rational function F the group $G(F)$ is defined as the group of all Möbius transformations σ such that

$$F \circ \sigma = \nu \circ F$$

for some Möbius transformations ν. Along with the group $G(F)$ we will consider its subgroup $\Sigma(A)$ consisting of all Möbius transformations σ such that $A \circ \sigma = A$. We recall that for a finite subgroup G of $\mathrm{Aut}(\mathbb{CP}^1)$ an **invariant function** for G is a rational function θ_G such that the equality

$$\theta_G(x) = \theta_G(y), \quad x, y \in \mathbb{CP}^1,$$

holds if and only if there exists $\sigma \in G$ such that $\sigma(x) = y$. Such a function always exists and is defined in a unique way up to the transformation $\theta \to \mu \circ \theta$, where μ is a Möbius transformation. Obviously, the degree of θ_G is equal to the order of G, and it follows easily from the Lüroth theorem that a rational function F is a rational function in θ_G if and only if $G \subseteq \Sigma(F)$.

Theorem 5.1. *Let F be an indecomposable rational function such that the group $G(F^{\circ k_0})$ for some $k_0 > 1$ contains an element that does not belong to the group $G(F)$. Then the iterate $F^{\circ k_0}$ has a non-trivial decomposition.*

Proof. Let α be a Möbius transformation such that $\alpha \in G(F^{\circ k_0})$ but $\alpha \notin G(F)$. Then

$$F^{\circ k_0} \circ \alpha = \nu \circ F^{\circ k_0}$$

for some Möbius transformation ν, implying that

$$F^{\circ k_0} = (\nu^{-1} \circ F) \circ F \circ \cdots \circ F \circ (F \circ \alpha).$$

Moreover, the decomposition on the right side of this equality is non-trivial since otherwise $F = \mu \circ (F \circ \alpha)$ for some Möbius transformation μ, in contradiction with the assumption $\alpha \notin G(F)$. □

Theorem 5.2. *Let F be an indecomposable rational function of degree $n \geq 2$ that is not conjugate to $z^{\pm n}$ such that the group $\Sigma(F^{\circ k_0})$ for some $k_0 > 1$ contains an element that does not belong to the groups $\Sigma(F^{\circ k})$, $1 \leq k < k_0$. Then the iterate $F^{\circ k_0}$ has a non-trivial decomposition.*

Proof. Let σ be such an element. Since $\langle\sigma\rangle$ is a subgroup of $\Sigma(F^{\circ k_0})$, there exists a rational function R such that $F^{\circ k_0} = R \circ \theta_{\langle\sigma\rangle}$. Assume for a moment that

$$|\langle\sigma\rangle| < (\deg F)^{k_0}.$$

Since $\deg \theta_{\langle\sigma\rangle} = |\langle\sigma\rangle|$, in this case $\deg R \geq 2$. Let now

$$R = G_1 \circ G_2 \circ \cdots \circ G_l \quad \text{and} \quad \theta_{\langle\sigma\rangle} = H_1 \circ H_2 \circ \cdots \circ H_t$$

be any decompositions into compositions of indecomposable rational functions. Concatenating them we obtain a decomposition

$$F^{\circ k_0} = G_1 \circ G_2 \circ \cdots \circ G_l \circ H_1 \circ H_2 \circ \cdots \circ H_t \tag{50}$$

of $F^{\circ k_0}$. If this decomposition is equivalent to $F^{\circ k_0}$, then

$$F^{\circ k} = \mu \circ H_1 \circ H_2 \circ \cdots \circ H_t = \mu \circ \theta_{\langle\sigma\rangle},$$

for some Möbius transformation μ and $k \geq 1$. Moreover, $k < k_0$ since $\deg R \geq 2$. Thus, $\sigma \in \Sigma(F^{\circ k})$, where $k < k_0$, in contradiction with the condition. Hence, decomposition (50) is non-trivial.

To finish the proof, we only must show that the equality

$$|\langle\sigma\rangle| = (\deg F)^{k_0}$$

for $\sigma \in \mathrm{Aut}(\mathbb{CP}^1)$ with $|\langle\sigma\rangle| < \infty$ implies that F is conjugate to $z^{\pm n}$. Since

$$\theta_{\langle\sigma\rangle} = \alpha \circ z^{|\langle\sigma\rangle|} \circ \beta$$

for some Möbius transformations α and β, this reduces to showing that if

$$F^{\circ k_0} = z^{n^{k_0}} \circ \beta \tag{51}$$

for some $k_0 > 1$ and Möbius transformations β, then F is conjugate to $z^{\pm n}$.

Clearly, if (51) holds, then the preimage $(F^{\circ k_0})^{-1}\{0, \infty\}$ contains only two points, implying that all the preimages $(F^{\circ k})^{-1}\{0, \infty\}$, $1 \leq k < k_0$, also contain only two points. Set $\{a, b\} = F^{-1}\{0, \infty\}$. Then it follows from (51) that

$$|(F^{\circ(k_0-1)})^{-1}\{0, \infty\}| = |(F^{\circ(k_0-1)})^{-1}\{a, b\}| = 2, \tag{52}$$

implying that

$$|(F^{\circ(k_0-1)})^{-1}\{0, \infty, a, b\}| \leq 4. \tag{53}$$

Let us recall now that the Riemann-Hurwitz formula implies that the preimage of a finite set S under a rational function H of degree $d \geq 2$ contains at least $d(|S| - 2) + 2$ points, and the equality is attained if and only if the set of critical values $c(H)$ of H belongs to S. In particular, if S contains at least three points, then

$$|H^{-1}\{S\}| \geq d + 2.$$

Thus, if $n > 2$ or $k_0 > 2$, then (53) is possible only if $\{0, \infty\} = \{a, b\}$, implying that F is conjugate to $z^{\pm n}$. On the other hand, if $n = k_0 = 2$, then it follows from (52) that $c(F) = \{0, \infty\}$ and $c(F) = \{a, b\}$, implying again that $\{0, \infty\} = \{a, b\}$. □

As an example illustrating the above theorems, let us consider the function

$$F = \frac{z^2 - 1}{z^2 + 1}. \tag{54}$$

Since $F = \frac{z-1}{z+1} \circ z^2$, the group $G(F)$ consists of the transformations $cz^{\pm 1}$, $c \in \mathbb{C} \setminus \{0\}$ (see, e.g., [45, Section 2]). On the other hand, for

$$F^{\circ 2} = -\frac{2z^2}{z^4 + 1},$$

the corresponding group $G(F^{\circ 2})$ contains the transformation $\mu = \frac{z+i}{z-i}$ satisfying

$$F^{\circ 2} \circ \mu = \nu \circ F^{\circ 2}$$

for $\nu = \frac{-z+1}{-3z-1}$. Hence,

$$\frac{z^2 - 1}{z^2 + 1} \circ \frac{z^2 - 1}{z^2 + 1} = \left(\nu^{-1} \circ \frac{z^2 - 1}{z^2 + 1}\right) \circ \left(\frac{z^2 - 1}{z^2 + 1} \circ \mu\right) = -\frac{z^2}{z^2 - 2} \circ \frac{2iz}{z^2 - 1}, \tag{55}$$

where the decomposition on the right side is non-trivial by Theorem 5.1.

Furthermore, the transformation $\delta : z \to \frac{1}{z}$ obviously satisfies

$$F \circ \delta = -F, \quad F^{\circ 2} \circ \delta = F.$$

Thus, $\delta \in \Sigma(F^{\circ 2})$ but $\delta \notin \Sigma(F)$, and therefore $F^{\circ 2}$ is a rational function in

$$\theta_{\langle \delta \rangle} = z + \frac{1}{z}.$$

The corresponding non-trivial decomposition provided by Theorem 5.2 is given by the formula

$$\frac{z^2-1}{z^2+1} \circ \frac{z^2-1}{z^2+1} = -\frac{2}{z^2-2} \circ \left(z + \frac{1}{z}\right). \tag{56}$$

Notice that although δ does not belong to $\Sigma(F)$, it belongs to $G(F)$. Thus, we cannot apply to δ previous Theorem 5.1.

Let us remark that decompositions of $F^{\circ 2}$ on the right sides of (55) and (56) are not equivalent to each other. Indeed, for equivalent decompositions (1) the sets of critical points of F_1 and G_1 are equal. On the other hand, the sets of critical points of the functions $\frac{2iz}{z^2-1}$ and $z + \frac{1}{z}$ are $\{-i, i\}$ and $\{-1, 1\}$. Notice that since the set of critical points of F is $\{0, \infty\}$, this also gives another proof of the fact that decompositions (55) and (56) are non-trivial. Finally, let us mention that $F^{\circ 2}$ has no other non-trivial decompositions. To see this, let us observe that the function $F^{\circ 2}$ is an invariant function for the Klein four group $V \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ generated by the transformations $z \to \frac{1}{z}$ and $z \to -z$. Since $\mathrm{Mon}(\theta_G) \cong G$ for any finite subgroup G of $\mathrm{Aut}(\mathbb{CP}^1)$, this implies that $\mathrm{Mon}(F^{\circ 2}) \cong V$. Therefore, as the group V has three proper imprimitivity systems, $F^{\circ 2}$ has three non-equivalent decompositions (one of which corresponds to the decomposition $F^{\circ 2}$ itself).

In relation with Theorem 5.1 and Theorem 5.2, let us mention that according to the recent results of [45] for any rational function A of degree $n \geq 2$ that is not conjugate to z^n, the orders of the groups $G(A^{\circ k})$, $k \geq 2$, are finite and uniformly bounded in terms of n only.

To construct further examples of rational functions whose iterates admit non-trivial decompositions, we will use Lattès maps. More precisely, we will use those Lattès maps that can be obtained as projections on the x-coordinate of self-isogenies of elliptic curves. We emphasize that this class of Lattès maps does not exhaust the entire class of Lattès maps as it was defined in Section 4.1. However, for brevity, in the rest of the article we will call by Lattès maps only these particular Lattès maps, which are defined in detail below. Notice that this time we use another, more common definition of Lattès maps.

Let $\mathcal{C}$ and $\widetilde{\mathcal{C}}$ be elliptic curves over $\mathbb{C}$ defined in the short Weierstrass form. We recall that an **isogeny** between $\mathcal{C}$ and $\widetilde{\mathcal{C}}$ is a morphism $\psi : \mathcal{C} \to \widetilde{\mathcal{C}}$ that sends the identity element of the group $\mathcal{C}$ to the identity element of the group $\widetilde{\mathcal{C}}$. Such a morphism is necessarily a homomorphism of groups (see, e.g., [51]). Thus, $\psi(-x) = -\psi(x)$, implying that there exists a rational function F such that the diagram

$$\begin{array}{ccc} \mathcal{C} & \xrightarrow{\psi} & \widetilde{\mathcal{C}} \\ \downarrow{\scriptstyle x} & & \downarrow{\scriptstyle x} \\ \mathbb{CP}^1 & \xrightarrow{F} & \mathbb{CP}^1 \end{array} \tag{57}$$

commutes. If $\mathcal{C} = \widetilde{\mathcal{C}}$ and ψ is an endomorphism, we will call the corresponding rational function F a Lattès map. For example, for any elliptic curve $\mathcal{C}$, the multiplication by n on $\mathbb{C}$ induces an endomorphism $[n] : \mathcal{C} \to \mathcal{C}$ of degree n^2. We will denote by $F_{\mathcal{C},n}$ the corresponding Lattès map of degree n^2, which makes the diagram

$$\begin{array}{ccc} \mathcal{C} & \xrightarrow{[n]} & \mathcal{C} \\ \downarrow{\scriptstyle x} & & \downarrow{\scriptstyle x} \\ \mathbb{CP}^1 & \xrightarrow{F_{\mathcal{C},n}} & \mathbb{CP}^1 \end{array}$$

commutative.

Below, we will use the following results about isogenies (see, e.g., [51, Ch. III]). Let $\psi : \mathcal{C} \to \widetilde{\mathcal{C}}$ be a non-zero isogeny of degree n. Then its kernel Γ is a subgroup of order n in $\mathcal{C}$. Moreover, for any subgroup of $\mathcal{C}$ there exists an isogeny $\psi : \mathcal{C} \to \widetilde{\mathcal{C}}$ such that $\ker \psi = \Gamma$, and this isogeny is defined in a unique way up to an isomorphism of $\widetilde{\mathcal{C}}$. Finally, for any isogeny $\psi : \mathcal{C} \to \widetilde{\mathcal{C}}$ of degree n there exists a unique **dual** isogeny $\widehat{\psi} : \widetilde{\mathcal{C}} \to \mathcal{C}$ such that $\widehat{\psi} \circ \psi = [n]$ on $\mathcal{C}$ and $\psi \circ \widehat{\psi} = [n]$ on $\widetilde{\mathcal{C}}$.

Theorem 5.3. *Let p be a prime number, and $\mathcal{C}$ an elliptic curve such that the multiplication by $i\sqrt{p}$ on $\mathbb{C}$ induces an endomorphism of $\mathcal{C}$. Then the corresponding Lattès map F is indecomposable, and the iterate $F^{\circ 2}$ has a non-trivial decomposition.*

Proof. Clearly, $F^{\circ 2}$ makes the diagram

$$\begin{array}{ccc} \mathcal{C} & \xrightarrow{-[p]} & \mathcal{C} \\ \downarrow{\scriptstyle x} & & \downarrow{\scriptstyle x} \\ \mathbb{CP}^1 & \xrightarrow{F^{\circ 2}} & \mathbb{CP}^1 \end{array}$$

commutative. Since the change of the sign of ψ in (57) obviously does not affect the corresponding Lattès map, this implies that $F^{\circ 2} = F_{\mathcal{C},p}$. Therefore, as any rational function of prime degree is clearly indecomposable, to prove the theorem it is enough to show that the function $F_{\mathcal{C},p}$ has more than one equivalence class of decompositions into compositions of indecomposable rational functions.

Let us show that starting from any finite subgroup Γ of $\mathcal{C}$ of order p one can construct a decomposition of $F_{\mathcal{C},p}$ into a composition of rational functions of degree p. Let $\psi_\Gamma : \mathcal{C} \to \mathcal{C}_\Gamma$ be an isogeny such that $\ker \psi_\Gamma = \Gamma$. Then there exists a rational function V_Γ such that the diagram

$$\begin{array}{ccc} \mathcal{C} & \xrightarrow{\psi_\Gamma} & \mathcal{C}_\Gamma \\ \downarrow x & & \downarrow x \\ \mathbb{CP}^1 & \xrightarrow{V_\Gamma} & \mathbb{CP}^1 \end{array}$$

commutes. Similarly, for the dual isogeny $\widehat{\psi}_\Gamma : \mathcal{C}_\Gamma \to \mathcal{C}$ there exists a rational function U_Γ such that the diagram

$$\begin{array}{ccc} \mathcal{C}_\Gamma & \xrightarrow{\widehat{\psi}_\Gamma} & \mathcal{C} \\ \downarrow x & & \downarrow x \\ \mathbb{CP}^1 & \xrightarrow{U_\Gamma} & \mathbb{CP}^1 \end{array}$$

commutes. Gluing these diagrams we obtain a decomposition

$$F_{\mathcal{C},p} = U_\Gamma \circ V_\Gamma.$$

Let us prove now that if $\Gamma_1 \neq \Gamma_2$, then the decompositions $U_{\Gamma_1} \circ V_{\Gamma_1}$ and $U_{\Gamma_2} \circ V_{\Gamma_2}$ are not equivalent. Let us consider the maps $V_{\Gamma_1} \circ U_{\Gamma_1}$ and $V_{\Gamma_2} \circ U_{\Gamma_2}$, which make the diagrams

$$\begin{array}{ccc} \mathcal{C}_{\Gamma_1} & \xrightarrow{\psi_{\Gamma_1} \circ \widehat{\psi}_{\Gamma_1}} & \mathcal{C}_{\Gamma_1} \\ \downarrow x & & \downarrow x \\ \mathbb{CP}^1 & \xrightarrow{V_{\Gamma_1} \circ U_{\Gamma_1}} & \mathbb{CP}^1 \end{array}, \qquad \begin{array}{ccc} \mathcal{C}_{\Gamma 2} & \xrightarrow{\psi_{\Gamma_2} \circ \widehat{\psi}_{\Gamma_2}} & \mathcal{C}_{\Gamma_2} \\ \downarrow x & & \downarrow x \\ \mathbb{CP}^1 & \xrightarrow{V_{\Gamma_2} \circ U_{\Gamma_2}} & \mathbb{CP}^1 \end{array}$$

commutative. Clearly, $V_{\Gamma_1} \circ U_{\Gamma_1}$ and $V_{\Gamma_2} \circ U_{\Gamma_2}$ are Lattès maps. Moreover, if the decompositions $U_{\Gamma_1} \circ V_{\Gamma_1}$ and $U_{\Gamma_2} \circ V_{\Gamma_2}$ are equivalent, then these Lattès maps are conjugate. However, for conjugate Lattès maps the corresponding elliptic curves are isomorphic (see, e.g., [52, Theorem 6.46]). Thus, if the above decompositions are equivalent, then $\mathcal{C}_{\Gamma_1} \cong \mathcal{C}_{\Gamma_2}$, implying that $\Gamma_1 = \Gamma_2$.

To finish the proof, we only must show that there exist at least two different subgroups of order p in $\mathcal{C}$. In fact, it is easy to see that there exist exactly $p+1$ such subgroups. Indeed, any subgroup of order p is cyclic and is contained in the subgroup of points of $\mathcal{C}$ whose order divides p, that is, in the kernel of $[p]$. Thus, the number of subgroups of order p is equal to the number of cyclic subgroups of order p in $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. In turn, this number is equal to the number of elements of order p in $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, which is equal to p^2-1, divided by the number of elements generating the same subgroup, which is equal to $p-1$. □

Notice that Lattès maps satisfying conditions of Theorem 5.3 exist for every prime p. To see this, it is enough to observe that $i\sqrt{p}$ is an endomorphism of an elliptic curve corresponding to the lattice generated by 1 and $i\sqrt{p}$.

Examples illustrating Theorem 5.3 for $p=2$ and $p=3$ are given by the functions

$$L = \frac{2\sqrt{2}x - x^2 - 1}{2x} \quad \text{and} \quad P = \frac{6x}{x^3-2} \tag{58}$$

(see [28]). Using Vélu's formulas for isogenies ([54]) or a brute force calculation, one can find the following non-trivial decompositions of their second iterates:

$$L^{\circ 2} = U \circ V, \tag{59}$$

where

$$U = \frac{x^2}{4(x - \frac{1}{\sqrt{2}-1})}, \quad V = \frac{x^2-1}{x-\sqrt{2}+1},$$

and

$$P^{\circ 2} = Q \circ R, \tag{60}$$

where

$$Q = -\frac{23328x}{x^3 + 216\sqrt[3]{2}x^2 + 3888\,2^{2/3}x - 93312}, \quad R = \frac{36x(2^{2/3}x^2 - 4x + 2\sqrt[3]{2})}{2^{2/3}x^2 + 2x + 2\sqrt[3]{2}}.$$

As above, to see directly that these decompositions are indeed non-trivial it is enough to compare the sets of critical points of L and V for (59) and the sets of critical points of P and R for (60). In the first case, one can check that the corresponding sets are

$$\{-1, 1\} \quad \text{and} \quad \{\sqrt{2}-1+i\sqrt{-2+2\sqrt{2}}, \sqrt{2}-1-i\sqrt{-2+2\sqrt{2}}\}.$$

In the second case, it is enough to observe that ∞ is a critical point of P, but is not a critical point of R.

It is clear that any rational function of degree 2 is simple. Moreover, one can check that the function P in (58) has four critical values and hence is simple by Lemma 2.1. Thus, the functions given by (54) and (58) provide us with counterexamples to Theorem 1.1 for m equal 2 and 3. Moreover, for these values of m, functions given by (58) give counterexamples also to Theorem 1.2. Indeed, for a Lattès map F the semigroups $E(F)$ and $C_\infty(F)$ are not finitely generated (see [28]). On the other hand, the group $\mathrm{Aut}_\infty(F)$ is finite for any rational function F (see [45]).

A simple counterexample to Theorem 1.4 for $m = 2$ is obtained from the semiconjugacy

$$\begin{array}{ccc} \mathbb{CP}^1 & \xrightarrow{z^m} & \mathbb{CP}^1 \\ {\scriptstyle \frac{1}{2}(z+\frac{1}{z})}\downarrow & & \downarrow{\scriptstyle \frac{1}{2}(z+\frac{1}{z})} \\ \mathbb{CP}^1 & \xrightarrow{T_m} & \mathbb{CP}^1 \end{array}$$

for $m = 2$. Indeed, it is clear that z^m and T_m are not conjugate. On the other hand, T_2 is simple. Furthermore, the commutative diagram

$$\begin{array}{ccc} (\mathbb{CP}^1)^2 & \xrightarrow{(z^2,z^2)} & (\mathbb{CP}^1)^2 \\ {\scriptstyle (z,\frac{1}{2}(z+\frac{1}{z}))}\downarrow & & \downarrow{\scriptstyle (z,\frac{1}{2}(z+\frac{1}{z}))} \\ (\mathbb{CP}^1)^2 & \xrightarrow{(z^2,T_2)} & (\mathbb{CP}^1)^2 \end{array}$$

defines for non-conjugate simple rational functions z^2 and T_2 an irreducible (z^2, T_2)-invariant curve parametrized by $z \to (z, \frac{1}{2}(z + \frac{1}{z}))$, providing a counterexample to Theorem 1.5.

Counterexamples to Theorem 1.4 and Theorem 1.5 for $m = 3$ can be obtained from the semiconjugacy

$$\begin{array}{ccc} \mathbb{CP}^1 & \xrightarrow{z(\frac{z^2-a}{z^2-b})} & \mathbb{CP}^1 \\ \downarrow{\scriptstyle z^2} & & \downarrow{\scriptstyle z^2} \\ \mathbb{CP}^1 & \xrightarrow{z(\frac{z-a}{z-b})^2} & \mathbb{CP}^1, \end{array}$$

where $a, b \in \mathbb{C}$, which is a particular case of the semiconjugacy

$$\begin{array}{ccc} \mathbb{CP}^1 & \xrightarrow{z^r R(z^n)} & \mathbb{CP}^1 \\ \downarrow{\scriptstyle z^n} & & \downarrow{\scriptstyle z^n} \\ \mathbb{CP}^1 & \xrightarrow{z^r R^n(z)} & \mathbb{CP}^1, \end{array}$$

where R is an arbitrary rational function and r, n are integer positive numbers.

Setting, for example, $a = 2$, $b = 3$ and observing that

$$A = z\Big(\frac{z-2}{z-3}\Big)^2$$

has three fixed points $0, \infty, 5/2$, while

$$B = z\Big(\frac{z^2-2}{z^2-3}\Big)$$

has only two fixed points 0 and ∞, we see that A and B are not conjugate. On the other hand, since A has four critical values $0, \infty, 32/3, 1/4$, it is a simple rational function. Thus, we obtain a counterexample to Theorem 1.4. A counterexample to Theorem 1.5 is obtained from the diagram

$$\begin{array}{ccc} (\mathbb{CP}^1)^2 & \xrightarrow{(B,B)} & (\mathbb{CP}^1)^2 \\ {\scriptstyle (z,z^2)}\downarrow & & \downarrow{\scriptstyle (z,z^2)} \\ (\mathbb{CP}^1)^2 & \xrightarrow{(B,A)} & (\mathbb{CP}^1)^2 \end{array}$$

in the same way as above, taking into account that B is also simple since it has four critical values $\pm\frac{1}{2}$, $\pm\frac{4\sqrt{6}}{3}$.

In conclusion, we mention that if F is decomposable, then the problem of describing the whole totality of its iterates seems to be even more complicated than in the indecomposable case, and a "qualitative" description comes to the fore. An example of such a description is the result of [59], which states that if F is a polynomial of degree $n \geq 2$ not conjugate to z^n or to $\pm T_n$, then decompositions of its iterates can be obtained from decompositions of a single iterate $F^{\circ N}$ for N big enough in the following sense: there exists an integer $N \geq 1$ such that any decomposition of $F^{\circ d}$ with $d \geq N$ has the form

$$X = F^{\circ k_1} \circ X', \quad Y = Y' \circ F^{\circ k_2},$$

where $F^{\circ N} = X' \circ Y'$ and $k_1, k_2 \geq 0$ (see [59] and also [34], [44] for different proofs of this fact).

Conjecturally, the result of [59] remains true for any non-special rational function F. To date, this conjecture is proved for "tame" rational functions, that is, for the functions F satisfying the following condition: the algebraic curve

$$F(x) - F(y) = 0$$

has no factors of genus zero or one distinct from the diagonal ([44]). Since any simple rational function F of degree $m \geq 4$ is tame by Theorem 2.4 and formula (15), this also shows that the conjecture is true for simple and general rational functions of degree at least four. On the other hand, Theorem 1.1 shows that for such functions it is true already for $N = 1$.

Open access funding provided by Ben-Gurion University.

REFERENCES

[1] P. Atela and J. Hu, *Commuting polynomials and polynomials with same Julia set*, Internat. J. Bifur. Chaos Appl. Sci. Engrg. **6** (1996), 2427–2432

[2] I. Baker and A. Eremenko, *A problem on Julia sets*, Ann. Acad. Sci. Fenn. Ser. A I Math. **12** (1987), 229–236.

[3] M. Baker and L. De Marco, *Special curves and postcritically finite polynomials*, Forum Math. Pi **1** (2013), Article no. e3.

[4] X. Buff and A. Epstein, *From local to global analytic conjugacies*, Ergodic Theory Dynam. Systems **27** (2007), 1073–1094.

[5] C. Cabrera and P. Makienko, *On decomposable rational maps*, Conform. Geom. Dyn. **15** (2011), 210–218.

[6] C. Cabrera and P. Makienko, *Amenability and measure of maximal entropy for semigroups of rational map*, Groups Geom. Dyn. **15** (2021), 1139–1174.

[7] P. Erdős, *On a theorem of Sylvester and Schur*, J. London Math. Soc. **9** (1934), 282–288.

[8] A. Eremenko, *Some functional equations connected with the iteration of rational functions*, Leningrad Math. J. **1** (1990), 905–919.

[9] A. Eremenko, *Invariant curves and semiconjugacies of rational functions*, Fundamenta Math. **219** (2012), 263–270.

[10] M. Faulkner, *On a theorem of Sylvester and Schur*, J. London Math. Soc. **41** (1966), 107–110.

[11] C. Favre and T. Gauthier, *The Arithmetic of Polynomial Dynamical Pairs*, Princeton University Press, Princeton, NJ, 2022.

[12] A. Freire, A. Lopes and R. Mañé, *An invariant measure for rational maps*, Bol. Soc. Brasil. Mat. **14** (1983), 45–62.

[13] M. Fried, *Arithmetical properties of function fields. II. The generalized Schur problem*, Acta Arith. **25** (1974), 225–258.

[14] M. Fried, *Variables separated equations: strikingly different roles for the branch cycle lemma and the finite simple group classification*, Sci. China Math. **55** (2012), 1–72.

[15] D. Ghioca and K. D. Nguyen, *Dynamical anomalous subvarieties: structure and bounded height theorems*, Adv. Math. **288** (2016), 1433–1462.

[16] D. Ghioca and K. Nguyen, *Dynamics of split polynomial maps: uniform bounds for periods and applications*, Int. Math. Res. Not. IMRN **2017** (2017), 213–231.

[17] D. Ghioca and K. D. Nguyen, *A dynamical variant of the Pink–Zilber conjecture*, Algebra Number Theory **12** (2018), 1749–1771.

[18] D. Ghioca, T. Tucker and M. Zieve, *Intersections of polynomial orbits, and a dynamical Mordell–Lang conjecture*, Invent. Math. **171** (2008), 463–483.

[19] D. Ghioca, T. Tucker and M. Zieve, *Linear relations between polynomial orbits*, Duke Math. J. **161** (2012), 1379–1410.

[20] D. Ghioca and H. Ye, *A dynamical variant of the André–Oort conjecture*, Int. Math. Res. Not. IMRN **2018** (2018), 2447–2480.

[21] D. Hanson, *On a theorem of Sylvester and Schur*, Canad. Math. Bull. **16** (1973), 195–199.

[22] H. Inou, *Extending local analytic conjugacies*, Trans. Amer. Math. Soc. **363** (2011), 331–343.

[23] J. König and D. Neftin, *Reducible fibers of polynomial maps*, Int. Math. Res. Not. IMRN **2014** (2024), 5373–5402.

[24] G. Levin, *Symmetries on Julia sets*, Math. Notes **48** (1990), 1126–1131.

[25] G. Levin and F. Przytycki, *When do two rational functions have the same Julia set?*, Proc. Amer. Math. Soc. **125** (1997), 2179–2190.

[26] M. Ljubich, *Entropy properties of rational endomorphisms of the Riemann sphere*, Ergodic Theory Dynam. Systems **3** (1983), 351–385.

[27] A. Medvedev, T. Scanlon, *Invariant varieties for polynomial dynamical systems*, Ann. of Math. (2) **179** (2014), 81–177.

[28] J. Milnor, *On Lattès maps*, in *Dynamics on the Riemann Sphere*, European Mathematical Society, Zürich, 2006, pp. 9–43.

[29] D. Mumford, *Algebraic Geometry I. Complex Projective Varieties*, Springer, Berlin–New York, 1976.

[30] K. D. Nguyen, *Some arithmetic dynamics of diagonally split polynomial maps*, Int. Math. Res. Not. IMRN **2015** (2015), 1159–1199.

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

[32] F. Pakovich, *The algebraic curve $P(x)-Q(y)=0$ and functional equations*, Complex Var. Elliptic Equ. **56** (2011), 199–213.

[33] F. Pakovich, *On semiconjugate rational functions*, Geom. Funct. Anal. **26** (2016), 1217–1243.

[34] F. Pakovich, *Polynomial semiconjugacies, decompositions of iterations, and invariant curves*, Ann. Sc. Norm. Super. Pisa Cl. Sci. (5), **17** (2017), 1417–1446.

[35] F. Pakovich, *Recomposing rational functions*, Int. Math. Res. Not. IMRN **2019** (2019), 1921–1935.

[36] F. Pakovich, *Algebraic curves $A^{\circ l}(x)-U(y)=0$ and arithmetic of orbits of rational functions*, Mosc. Math. J. **20** (2020), 153–183.

[37] F. Pakovich, *Finiteness theorems for commuting and semiconjugate rational functions*, Conform. Geom. Dyn. **24** (2020), 202–229.

[38] F. Pakovich, *On generalized Lattès maps*, J. Anal. Math. **142** (2020), 1–39.

[39] F. Pakovich, *On rational functions sharing the measure of maximal entropy*, Arnold Math. J. **6** (2020), 387–396.

[40] F. Pakovich, *Commuting rational functions revisited*, Ergodic Theory Dynam. Systems **41** (2021), 295–320.

[41] F. Pakovich, *Sharing a measure of maximal entropy in polynomial semigroups*, Int. Math. Res. Not. IMRN **2022** (2022), 13829–13840.

[42] F. Pakovich, *On amenable semigroups of rational functions*, Trans. Amer. Math. Soc. **375** (2022), 7945–7979.

[43] F. Pakovich, *Invariant curves for endomorphisms of $\mathbb{P}^1\times\mathbb{P}^1$*, Math. Ann. **385** (2023), 259–307.

[44] F. Pakovich, *Tame rational functions: Decompositions of iterates and orbit intersections*, J. Eur. Math. Soc. (JEMS) **25** (2023), 3953–3978.

[45] F. Pakovich, *On symmetries of iterates of rational functions*, Ann. Sc. Norm. Super. Pisa., to appear.

[46] J. F. Ritt, *On the iteration of rational functions*, Trans. Amer. Math. Soc. **21** (1920), 348–356.

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

[48] J. F. Ritt, *Permutable rational functions*, Trans. Amer. Math. Soc. **25** (1923), 399–448.

[49] W. Schmidt and N. Steinmetz, *The polynomials associated with a Julia set*, Bull. London Math. Soc. **27** (1995), 239–241.

[50] I. Schur, *Einige Satze uber Primzahlen mit wendung auf Irreduzibilitatsfragen*, Sitzungberichte der preussichen Akedemie der Wissenschaften, Phys. Math. Klasse, **23** (1929), 1–24.

[51] J. Silverman, *The Arithmetic of Elliptic Curves*, Springer, New York, 1986.

[52] J. Silverman, *The Arithmetic of Dynamical Systems*, Springer, New York, 2007.

[53] J. Sylvester, *On arithmetical series*, Messenger of Math. **21** (1892), 87–120.

[54] J. Vélu, *Isogénies entre courbes elliptiques*, C. R. Acad. Sci. Paris Sér. A-B **273** (1971), A238–A241.

[55] H. Wielandt, *Finite Permutation Groups*, Academic Press, New York–London, 1964.

[56] J. Xie, *The existence of Zariski dense orbits for endomorphisms of projective surfaces*, J. Amer. Math. Soc. **38** (2025), 1–62.

[57] H. Ye, *Rational functions with identical measure of maximal entropy*, Adv. Math. **268** (2015), 373–395.

[58] S.-W. Zhang, *Distributions in algebraic dynamics*, in *Surveys in Differential Geometry. Vol. X*, International Press, Somerville, MA, 2006, pp. 381–430.

[59] M.Zieve and P. Müller, *On Ritt's polynomial decomposition theorem*, preprint, arXiv:0807.3578 [math.AG].

Fedor Pakovich
DEPARTMENT OF MATHEMATICS
BEN GURION UNIVERSITY OF THE NEGEV
POB 653, BE'ER SHEVA 8410501, ISRAEL
email: pakovich@math.bgu.ac.il

(Received May 15, 2023 and in revised form October 19, 2023)