Journal of Algebra 423 (2015) 1161–1190

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Computing conjugating sets and automorphism groups of rational functions ☆

Xander Faber [a,*], Michelle Manes [a], Bianca Viray [b]

[a] Department of Mathematics, University of Hawaii at Manoa, Honolulu, HI, United States
[b] Department of Mathematics, University of Washington, Seattle, WA, United States

ARTICLE INFO

Article history:
Received 13 June 2013
Available online 7 October 2014
Communicated by Jon Carlson

MSC:
primary 37P05
secondary 11Y16

Keywords:
Arithmetic dynamics
Rational function
Automorphism group
Conjugating set

ABSTRACT

Let ϕ and ψ be endomorphisms of the projective line of degree at least 2, defined over a field F. From a dynamical perspective, a significant question is to determine whether ϕ and ψ are conjugate (or to answer the related question of whether a given rational function ϕ has a nontrivial automorphism). We construct efficient algorithms for computing the set of conjugating maps (resp., the group of automorphisms), with an emphasis on the case where F is a finite field or a number field. Each of our algorithms takes advantage of different dynamical structures, so context (e.g., field of definition and degree of the map) determines the preferred algorithm.

1. Introduction

Let F be a field, and let $\phi = f/g \in F(z)$ be a rational function, where f, g are relatively prime polynomials. Unless otherwise specified, we assume throughout that

☆ The first and second authors were partially supported by NSF grants DMS-0902532 and DMS-1102858, respectively. The third author was partially supported by NSF grant DMS-1002933 and by the Institute for Computational and Experimental Research in Mathematics.

* Corresponding author.
E-mail addresses: xander@math.hawaii.edu (X. Faber), mmanes@math.hawaii.edu (M. Manes), bviray@math.washington.edu (B. Viray).

http://dx.doi.org/10.1016/j.jalgebra.2014.08.048
0021-8693/

$$d = \deg(\phi) := \max\{\deg(f), \deg(g)\} \geq 2.$$

When viewed as an endomorphism of the projective line $\mathbb{P}^1_F \xrightarrow{\phi} \mathbb{P}^1_F$, a dynamical theory of ϕ arises from iteration. That is, for $x \in \mathbb{P}^1(F)$, we may consider its orbit

$$x \mapsto \phi(x) \mapsto \phi^2(x) \mapsto \phi^3(x) \mapsto \cdots$$

(Here we write $\phi^1 = \phi$ and $\phi^n = \phi \circ \phi^{n-1}$ for each $n > 1$.)

Two rational functions $\phi, \psi \in F(z)$ are *conjugate* if there is some rational function f of degree 1 (an automorphism of $\mathbb{P}^1$) defined over $\overline{F}$, an algebraic closure of F, such that $f \circ \phi = \psi \circ f$. In this case, the two functions exhibit the same *geometric* dynamical behavior. Indeed, if $f \in \overline{F}(z)$ conjugates ϕ to ψ, then f maps the ϕ-orbit of a point $x \in \mathbb{P}^1(\overline{F})$ to the ψ-orbit of $f(x)$. We say that ϕ and ψ are conjugate over a field extension E/F if they satisfy the relation $f \circ \phi = \psi \circ f$ for some rational function $f \in E(z)$ of degree 1. In this case, they have the same *arithmetic* dynamical behavior over E; e.g., f maps ϕ-orbits of E-rational points to ψ-orbits of E-rational points, and the field extension of E generated by the period-n points of ϕ and ψ must agree for every $n \geq 1$.

Conversely, given two functions that seemingly exhibit the same dynamical behavior, one wants to know if they are conjugate, or if there is some deeper structure that should be investigated. This natural question sparked the current work, in which we study the following pair of algorithmic problems:

(1) For two rational functions ϕ and ψ, determine the set of rational functions f of degree 1 (automorphisms of $\mathbb{P}^1$) that conjugate ϕ to ψ, i.e., such that $f \circ \phi \circ f^{-1} = \psi$.
(2) For a given rational function ϕ, determine the **automorphism group of** ϕ; i.e., determine the set of rational functions f of degree 1 such that $f \circ \phi \circ f^{-1} = \phi$.

These two questions are intimately connected. In Section 2 we show that the set of automorphisms can be viewed as the points of a finite group scheme, denoted Aut_ϕ. In Section 3 we show that the set of maps conjugating ϕ to ψ is also a scheme, denoted $\mathrm{Conj}_{\phi,\psi}$, which is a principal homogeneous space for Aut_ϕ. In particular, conjugacy over F and conjugacy over an algebraic closure $\overline{F}$ are equivalent notions whenever ϕ (and ψ) has trivial automorphism group. More generally, one can show that the size of the automorphism group of ϕ (or ψ) bounds the degree of the field extension generated by the coefficients of any conjugating map [9].

The symmetry locus of rational functions — the space of rational functions with nontrivial automorphism group — can be thought of as an analogue of the locus of abelian varieties that have extra automorphisms. Indeed, just as the presence of elliptic curves with extra automorphisms obstructs the existence of a universal elliptic curve, so does the symmetry locus obstruct the existence of a fine moduli space of conjugacy classes