Computing the Fixing Group of a Rational Function

(Extended Abstract)

Jaime Gutierrez[1], Rosario Rubio[2], and David Sevilla[1]

[1] Departamento de Matemáticas, Estadística y Computación
Facultad de Ciencias, Universidad de Cantabria
Santander E–39071, SPAIN
{jaime,sevillad}@matesco.unican.es
[2] Departamento de Ingeniería
Universidad Antonio de Nebrija
28040 Madrid, Spain
mrubio@nebrija.es

Abstract. Let $\mathrm{Aut}_{\mathbb{K}}\mathbb{K}(x)$ be the Galois group of the transcendental degree one pure field extension $\mathbb{K} \subseteq \mathbb{K}(x)$. In this paper we describe polynomial time algorithms for computing the field $Fix(H)$ fixed by a subgroup H of $\mathrm{Aut}_{\mathbb{K}}\mathbb{K}(x)$ and for computing the fixing group G_f of a rational function $f \in \mathbb{K}(x)$.

1 Introduction

Let $\mathbb{K}$ be an arbitrary field and $\mathbb{K}(x)$ be the rational function field in the variable x. Let $\mathrm{Aut}_{\mathbb{K}}\mathbb{K}(x)$ be the Galois group of the field extension $\mathbb{K} \subseteq \mathbb{K}(x)$.

In this paper we develop an algorithm for computing the automorphism group of an intermediate field in the extension $\mathbb{K} \subseteq \mathbb{K}(x)$. By the classical Lüroth's theorem any intermediate field $\mathbb{F}$ between $\mathbb{K}$ and $\mathbb{K}(x)$ is of the form $\mathbb{F} = \mathbb{K}(f)$ for some rational function $f \in \mathbb{K}(x)$, see [3, 5] and for a constructive proof [2]. Thus, this computational problem is equivalent to determine the fixing group G_f of a univariate rational function f. We also present an algorithm for computing $Fix(H)$, the fixed field by a subgroup $H < \mathrm{Aut}_{\mathbb{K}}\mathbb{K}(x)$. Again, this is equivalent to find a Lüroth's generator of the field fixed by the given subgroup H. Both algorithms are on polynomial time if the field $\mathbb{K}$ has a polynomial time algorithm for computing the set of roots of a univariate polynomial.

The algorithm for computing the fixing group of a rational function uses several techniques related to the rational function decomposition problem. This problem can be stated as follows: given $f \in \mathbb{K}(x)$, determine whether there exists a decomposition (g, h) of f, $f = g(h)$, with g and h of degree greater than one, and in the affirmative case, compute one. When such a decomposition exists some problems become simpler: for instance, the evaluation of a rational function f can be done with fewer arithmetic operations, the equation $f(x) = 0$ can be solved more efficiently, improperly parametrized algebraic curves can be reparametrized properly, etc., see [8], [1] and [6]. In fact, a motivation for this paper is to obtain results on rational functional decomposition. As a consequence of our study of G_f we provide new and interesting conditions of decomposability of rational functions. Another application of this paper is to study the number m of indecomposable components of a rational function $f = f_1 \circ \cdots \circ f_m$ which is strongly related to subgroup chains of G_f, see [7].

The algorithm presented for computing the field $Fix(H)$ is based on Galois theory results and the constructive proof of Lüroth's theorem.

The paper is divided in four sections. In Section 2, we introduce our notations and the background of the rational function decomposition. Section 3 studies the Galois group of $\mathbb{K}(x)$ over $\mathbb{K}$, the fixing group G_f and the field $Fix(H)$, including general theoretical results, and their relation with the functional decomposition problem. Section 4 presents algorithms for computing the fixing group and fixed field. We also give, in this section, examples illustrating our algorithms.

2 Background on Rational Function Decomposition

The set of all non–constant rational functions is a semigroup with identity x, under the element-wise composition of rational functions (symbol $\circ$ for composition): i.e., given non-constant rational functions

$g, h \in \mathbb{K}(x)$, $g \circ h = g(h)$. The units of this semigroup are of the form $\frac{ax+b}{cx+d}$. We will identify these units which the elements of the Galois group of $\mathbb{K}(x)$ over $\mathbb{K}$ and we denote this group by $\Gamma(\mathbb{K}) = \mathrm{Aut}_{\mathbb{K}}\mathbb{K}(x)$.

Given a $f \in \mathbb{K}(x)$, we will denote as f_N, f_D the numerator and denominator of f respectively, assuming that f_N and f_D are relatively prime. We define the degree of f as $\deg f = \max\{\deg f_N, \deg f_D\}$.

If $g, h \in \mathbb{K}(x)$ are rational functions of degree greater than one, $f = g \circ h = g(h)$ is their (functional) composition, (g, h) is a (functional) decomposition of f, and f is a decomposable rational function, otherwise f is indecomposable.

The following lemma describes some basic properties of rational function decomposition, see [1] for a proof.

Theorem 1. *With the above notations and definitions, we have the following:*

- $[\mathbb{K}(x) : \mathbb{K}(f)] = \deg f$.
- $\deg g \circ h = \deg g \cdot \deg h$.
- *The units with respect to the compositions are precisely the rational functions of degree one.*
- *Given $f, h \in \mathbb{K}(x) \setminus \mathbb{K}$, if there exists g such that $f = g(h)$, it is unique. Furthermore, it can be computed from f and h by solving a linear system of equations.* □

If $f, h \in \mathbb{K}(x)$ satisfy $\mathbb{K}(f) \subset \mathbb{K}(h) \subset \mathbb{K}(x)$, then $f = g(h)$ for some $g \in \mathbb{K}(x)$. From this fact the following natural concept arises:

Definition 1. *Let $f = g \circ h = g' \circ h'$. (g, h) and (g', h') are called* ***equivalent decompositions*** *if there is a unit u such that $h' = u \circ h$ (then also $g' = g \circ u^{-1}$).* □

The next result is an immediate consequence of the Lüroth's theorem.

Corollary 1. *Let $f \in \mathbb{K}(x)$ be a non–constant rational function. Then the equivalence classes of the decompositions of f correspond bijectively to intermediate fields $\mathbb{F}$, $\mathbb{K}(f) \subseteq \mathbb{F} \subset \mathbb{K}(x)$.* □

3 The Galois Correspondences in the Extension $\mathbb{K} \subseteq \mathbb{K}(x)$.

We start defining our main notions and tools.

Definition 2. *Let $\mathbb{K}$ be any field.*

- *Let $f \in \mathbb{K}(x)$. The* ***fixing group*** *of f is*

$$G_f = \{u \in \Gamma(\mathbb{K}) : f \circ u = f\}.$$

- *Let H be a subgroup of $\Gamma(\mathbb{K})$. The* ***field fixed*** *by H is*

$$\mathrm{Fix}(H) = \{f \in \mathbb{K}(x) : f \circ u = f \ \forall u \in H\}.$$

□

Before we discuss the computational aspects of these concepts, we will need some properties based on general facts from Galois theory and Theorem 1.

Theorem 2.

- *Let H be a subgroup of $\Gamma(\mathbb{K})$.*
  - *H is infinite $\Rightarrow \mathrm{Fix}(H) = \mathbb{K}$.*
  - *H is finite $\Rightarrow \mathbb{K} \subsetneq \mathrm{Fix}(H)$, $\mathrm{Fix}(H) \subset \mathbb{K}(x)$ is a normal extension, and in particular $\mathrm{Fix}(H) = \mathbb{K}(f)$ with $\deg f = |H|$.*
- *Given a finite subgroup H of $\Gamma(\mathbb{K})$, there is a bijection between the subgroups of H and intermediate fields in $\mathrm{Fix}(H) \subset \mathbb{K}(x)$. Also, if $\mathrm{Fix}(H) = \mathbb{K}(f)$, there is a bijection between components of f (up to equivalence by units) and the subgroups of H.*
- *Given $f \in \mathbb{K}(x) \setminus \mathbb{K}$, the order of G_f divides $\deg f$. Moreover, for every $\mathbb{K}$ there is an $f \in \mathbb{K}(x)$ such that $1 < |G_f| < \deg f$. For example if $f = x^2\,(x-1)^2$ then G_f={x,1-x}.*
- *If $|G_f| = \deg f$ then the extension $\mathbb{K}(f) \subset \mathbb{K}(x)$ is normal. Moreover, if the extension $\mathbb{K}(f) \subset \mathbb{K}(x)$ is also separable, then $\mathbb{K}(f) \subset \mathbb{K}(x)$ is normal implies $|G_f| = \deg f$.*

- *G_f depends on the field $\mathbb{K}$: let $f = x^4$, then for $\mathbb{K} = \mathbb{Q}, G_f = \{x, -x\}$ but for $\mathbb{K} = \mathbb{Q}(i), G_f = \{x, -x, ix, -ix\}$.*
- *If $\mathbb{K}$ is infinite, then $f \in \mathbb{K} \Leftrightarrow G_f$ is infinite.*
- *Let $f \in \mathbb{K}(x)$ and u, v be two units and $H < \Gamma(\mathbb{K})$.*
  - *If $f' = u \circ f \circ v$, then $G_f = v \cdot G_{f'} \cdot v^{-1}$.*
  - *If $\mathrm{Fix}(H) = \mathbb{K}(f)$ then for any u, $\mathrm{Fix}(uHu^{-1}) = \mathbb{K}(f \circ u^{-1})$.*
- *It is possible that f is decomposable but G_f is trivial. For $\mathbb{K} = \mathbb{C}, f = x^2(x-1)^2(x-3)^2$; for $\mathbb{K} = \mathbb{Q}, f = x^9$.*
- *It is possible that f has a non–trivial decomposition $f = g(h)$ and G_f is not trivial but G_h is not a proper subgroup of G_f. For $\mathbb{K} = \mathbb{C}, f = (x^2-1)(x^2-3) \Rightarrow G_f = \{x, -x\}$; for $\mathbb{K} = \mathbb{Q}, f = x^4 \Rightarrow G_f = \{x, -x\}$.* □

Unfortunately, it is not true that $[\mathbb{K}(x) : \mathbb{K}(f)] = |G_f|$. However, some interesting results about decomposability can be given.

Theorem 3. *Let f be indecomposable.*

- *If $\deg f = p$ is prime, then either $G_f \cong C_p$ or G_f is trivial.*
- *If $\deg f$ is not prime, then G_f is trivial.* □

In order to calculate $Fix(H)$, we can distinguish if H is infinite or finite. According to the above theorem if H is infinite then $Fix(H)$ is $\mathbb{K}$. So, only rests when H is finite. Some times it is interesting to see the elements of $\Gamma(\mathbb{K})$ as matrices.

Proposition 1. *The group $\Gamma(\mathbb{K})$ is isomorphic to $PGL_2(\mathbb{K}) = GL_2(\mathbb{K})/D_2(\mathbb{K})$ where $D_2(\mathbb{K}) = \{\lambda I_2 : \lambda \in \mathbb{K}^*\}$. Moreover, if $\mathbb{K}$ is algebraically closed, then it is also isomorphic to $PSL_2(\mathbb{K}) = SL_2(\mathbb{K})/\{\pm I_2\}$.* □

The study of the finite subgroups of $\Gamma(\mathbb{C})$ has a long history. Any element of $\Gamma(\mathbb{K})$ corresponds to a rotation or reflection of the Riemann sphere, so the finite subgroups correspond to the regular solids in three dimensions. Klein [4] gave the first geometric proof of the following classification of the finite subgroups of $\Gamma(\mathbb{C})$.

Theorem 4. *[Klein] Every finite subgroup of $\Gamma(\mathbb{C})$ is isomorphic to one of the following groups:*

- *C_n, the cyclic group of order n;*
- *D_n, the dihedral group of order n;*
- *A_4, the alternating group on four letters or tetrahedral group;*
- *S_4, the symmetric group on four letters or octahedral group;*
- *A_5, the alternating group on five letters or icosahedral group.* □

In the case $\mathbb{K} = \mathbb{Q}$, the correspondence between functions and groups is not so good as in the complex case, see Theorem 2. On the other hand, it is not difficult (personal communication of Prof. Walter Feit) to obtain from Theorem 4 a classification of all finite subgroups of $\Gamma(\mathbb{Q})$.

Suppose that $\mathbb{K}$ is finite, that is, $\mathbb{K} = \mathbb{F}_q$ where q is a power of a prime p. We denote the set of all linear polynomials with coefficients in $\mathbb{F}_q$ as $\Gamma_0(\mathbb{F}_q) = \{ax + b : a \in \mathbb{F}_q^*, b \in \mathbb{F}_q\}$.

Theorem 5. *With the above notation, we have the following:*

- *$|\Gamma_0(\mathbb{F}_q)| = q^2 - q$, $|\Gamma(\mathbb{F}_q)| = q^3 - q$.*
- *$\Gamma_0(\mathbb{F}_q)$ is a non-normal subgroup of $\Gamma(\mathbb{F}_q)$.*
- *The group $\Gamma(\mathbb{F}_q)$ is generated by $\Gamma_0(\mathbb{F}_q)$ and the linear rational function $1/x$, $\Gamma(\mathbb{K}) =< \Gamma_0, 1/x >$.*
- *$Fix(\Gamma_0(\mathbb{F}_q)) = \mathbb{F}_q(f_0)$, where $f_0 = (x^q - x)^{q-1}$.*
- *$Fix(\Gamma(\mathbb{F}_q)) = \mathbb{F}_q(h(f_0))$, where $h = \frac{x^{q+1}+x+1}{x^q}$.* □

As a consequence of Theorem 5 we have the following theoretical result:

Theorem 6. *The extension $\mathbb{K} \subset \mathbb{K}(x)$ is Galois if and only if $\mathbb{K}$ is infinite.* □

4 Algorithms

Now, we have all ingredients to give a computational solution to both problems.

4.1 Algorithm for Computing the Fixed Field

As the next theorem shows, it is easy to compute a generator for the fixed field of an explicitly given group (suggested by Dr. Peter Müller).

Theorem 7. *Let $H = \{g_1, \dots, g_m\} < \Gamma(\mathbb{K})$ be a finite group. Let*

$$P(t) = \prod_1^m (t - g_i) \in \mathbb{K}(x)[t].$$

Then any non–constant coefficient of $P(t)$ generates $Fix(H)$. □

The following example illustrates the algorithm over the field $\mathbb{C}$.

Example 1. Let

$$H = \{\pm\frac{t-i}{t+i}, \pm\frac{t+i}{t-i}, \pm\frac{1}{t}, \pm t, \pm\frac{i(t-1)}{t+1}, \pm\frac{i(t+1)}{t-1}\} < \Gamma(\mathbb{C})$$

which is isomorphic to A_4. All the symmetric functions in the elements of H are in $\mathrm{Fix}(H)$, and any non–constant symmetric function generates it. We compute those functions:

- $\sigma_1 = \sigma_3 = \sigma_5 = \sigma_7 = \sigma_9 = \sigma_{11} = 0$ by symmetry in the group.
- $\sigma_2 = \sigma_{10} = \dfrac{-1 + 33t^4 + 33t^8 - t^{12}}{t^{10} - 2t^6 + t^2}$.
- $\sigma_4 = \sigma_8 = \dfrac{-33t^4 - 66t^2 - 33}{t^4 + 2t^2 + 1}$.
- $\sigma_6 = \dfrac{2 - 66t^4 - 66t^8 + 2t^{12}}{t^2 - 2t^6 + t^{10}}$.
- $\sigma_{12} = 1$.

So,

$$Fix(H) = \mathbb{K}(\sigma_2) = \mathbb{K}(\sigma_4) = \mathbb{K}(\sigma_6).$$

□

Obviously the complexity of this method is dominated by computing the polynomial $P(t)$, that is, the number of arithmetic operations required to multiply m linear rational functions, where m is the order of the group. A bound for this is $O(m^2)$.

4.2 Algorithm for Computing the Fixing Group

The most straightforward method of computing the fixing group of a rational functions is solving a polynomial system of equations. Given

$$f = \frac{a_n x^n + \cdots + a_0}{b_m x^m + \cdots + b_0}$$

we have the system given by equating to 0 the coefficients of the numerator of

$$f \circ \left(\frac{ax+b}{cx+d}\right) - f(x).$$

We can alternatively solve the two systems given by

$$f \circ (ax+b) - f(x) = 0, \quad f \circ \left(\frac{ax+b}{x+d}\right) - f(x) = 0.$$

This method is simple but inefficient; we will present another method that is faster and will allow us to extract useful information even if the group is not computed completely.

We will assume that $\mathbb{K}$ has sufficiently many elements; if it is not the case, we can work in an extension and check later which elements are in $\Gamma(\mathbb{K})$.

Definition 3. *Let $f \in \mathbb{K}(x)$. We say that f is in* ***normal form*** *if $\deg f_N > \deg f_D$ and $f_N(0) = 0$.* □

Theorem 8. *Let $f \in \mathbb{K}(x)$. If $\mathbb{K}$ has sufficiently many elements, there exist units u and v such that $u \circ f \circ v$ is in normal form.* □

The complexity of the computation in Theorem 8 is that of the evaluation of a polynomial.

Theorem 9. *Let $f \in \mathbb{K}(x)$ be in normal form and $u = \frac{ax+b}{cx+d}$ such that $f \circ u = f$.*

- $a \neq 0$ *and* $d \neq 0$.
- $f_N(b/d) = 0$.
- *If* $c = 0$ *then* $a^n = 1$ *where* $n = \deg f$.
- *If* $c \neq 0$ *then* $f_D(a/c) = 0$. □

In order to compute G_f, we use the previous theorem to compute the polynomial and rational units separately.

Thus, if we can compute the roots of any polynomial in $\mathbb{K}[x]$, we have the following algorithm:

Input: $f \in \mathbb{K}(x)$.
Output: $G_f = \{u \in \mathbb{K}(x) : f \circ u = f\}$.
A. Compute units u, v such that $f' = u \circ f \circ v$ is in normal form. Let $n = \deg f$. Let L be an empty set.
B. Compute $A = \{\alpha \in \mathbb{K} : \alpha^n = 1\}$, $B = \{\beta \in \mathbb{K} : f'_N(\beta) = 0\}$ and $C = \{\gamma \in \mathbb{K} : f'_N(\gamma) = 0\}$..
C. For each $(\alpha, \beta) \in A \times B$, check if $f' \circ (ax + b) = f'$. In the affirmative case, add $ax + b$ to L.
D. For each $(\beta, \gamma) \in B \times C$, let $w = \frac{c\gamma x+\beta}{cx+1}$ and compute all values of c for which $f' \circ w = f'$. For each solution, add the resulting unit to L.
E. Let $L = \{w_1, \ldots, w_k\}$. Then, RETURN $\{v \circ w_i \circ v^{-1} : i = 1, \ldots, k\}$. □

The above algorithm briefly described requires to compute roots of a univariate polynomial. The complexity of this algorithm is dominated by step **B**. So, if we suppose that in the field $\mathbb{K}$ there is a polynomial time method for computing the roots, then the algorithm is polynomial in the degree of the rational function. This the case when $\mathbb{K} = \mathbb{Q}$, the rational number field or when $\mathbb{K} = \mathbb{F}_q$, the finite field with q elements. However, in the Maple implementation, it seems that the most of the time is spent in step **C** checking if the corresponding linear rational functions are good candidates or not.

Example 2. Let

$$f = \frac{\left(-3\,x + 1 + x^3\right)^2}{x\left(-2\,x - x^2 + 1 + x^3\right)\left(-1 + x\right)} \in \mathbb{Q}(x).$$

First we normalize f: let $u = 1/(x - 9/2)$ and $v = 1/x - 1$, then

$$f' = u \circ f \circ v = \frac{-4x^6 - 6x^5 + 32x^4 - 34x^3 + 14x^2 - 2x}{27x^5 - 108x^4 + 141x^3 - 81x^2 + 21x - 2}$$

is in normal form.

The roots of the numerator and denominator of f' in $\mathbb{Q}$ are $\{0, 1, 1/2\}$ and $\{1/3, 2/3\}$ respectively. The only sixth roots of unity in $\mathbb{Q}$ are 1 and -1; as char $\mathbb{Q} = 0$ there are no elements of the form $x + b$ in $G_{f'}$. Therefore, there are two polynomial candidates to test: $-x + 1/3$ and $-x + 2/3$. It is easy to check that none of them leaves f' fixed.

Let

$$w = \frac{c\beta x + \alpha}{cx + 1}.$$

- $\alpha = 0, \beta = 1/3$: the unit $\frac{cx/3}{cx+1}$ does not leave f fixed for any value of c.
- $\alpha = 1, \beta = 1/3$: the unit $\frac{cx/3+1}{cx+1}$ does not leave f fixed for any value of c.
- $\alpha = 1/2, \beta = 1/3$: the unit $\frac{cx/3+1/2}{cx+1}$ leaves f fixed for $c = -3/2$.
- $\alpha = 0, \beta = 2/3$: the unit $\frac{2cx/3}{cx+1}$ does not leave f fixed for any value of c.
- $\alpha = 1, \beta = 2/3$: the unit $\frac{2cx/3+1}{cx+1}$ leaves f fixed for $c = -3$.
- $\alpha = 1/2, \beta = 2/3$: the unit $\frac{2cx/3+1/2}{cx+1}$ does not leave f fixed for any value of c.

Therefore,

$$G_{f'} = \{x, \frac{-x+1}{-3x+2}, \frac{-2x+1}{-3x+1}\}$$

and

$$G_f = v \cdot G_{f'} \cdot v^{-1} = \{x, \frac{1}{1-x}, \frac{x-1}{x}\}.$$

From this group we can compute a proper component of f using Theorem 7, and we obtain

$$h = \frac{-3\,x + 1 + x^3}{(-1+x)\,x}$$

which is indeed a component for f, since $f = g \circ h$ with

$$g = \frac{x^2}{x-1}.$$

□

Now we present an example illustrating the algorithm over a finite field.

Example 3. Let $\mathbb{K} = \mathbb{F}_2$ and

$$f = \frac{(x^2+1)(x^6+x^4+x^2+1+x^3)}{x^8+x^4+1+x^5+x^3}.$$

First we normalize f: let $u = \frac{x+1}{x}$ and $v = \frac{1}{x} + 1$. Then

$$f' = u \circ f \circ v = \frac{(x+1)^4 x^4}{(x^2+x+1)(x^4+x+1)}.$$

Since $B = \{0, 1\}$ and $C = \emptyset$, we only have to check the unit $x+1$. As it leaves f' fixed, we have that $G_{f'} = \{x, x+1\}$ and

$$G_f = v \cdot G_{f'} \cdot v^{-1} = \{x, \frac{1}{x}\}.$$

Therefore, a generator of $\mathrm{Fix}(G_f)$ is

$$h = x + \frac{1}{x}$$

which is also a component of f: indeed $f = g \circ h$ with

$$g = \frac{x^4+x}{x^4+x+1}.$$

□

Acknowledgments
This research is partially supported by the National Spanish project BFM2001-1294 and Movilidad del Personal Investigador (MECD) grant PR2002-0009.

References

1. C. Alonso, J. Gutierrez, T. Recio: *A Rational Function Decomposition Algorithm by Near–separated Polynomials*. J. Symbolic Comput. **19**, 1995, pp. 527–544.
2. J. Gutierrez, R. Rubio, D. Sevilla: *Unirational Fields of Transcendence Degree One and Functional Decomposition*. Proc. of ISSAC–01. ACM Press, 2001, pp. 167–174.
3. P. Lüroth: *Beweis eines Satzes über rationale Curven*. Mathematische Annalen, 9, 1876, pp. 163– 165.
4. F. Klein: *Lectures on the Icosahedron and the Solution of Equations of the Fifth Degree*. Dover, New York, 1956.
5. A. Schinzel: *Selected Topics on Polynomials*. Ann Arbor, University Michigan Press, 1982.
6. T.W. Sederberg: *Improperly Parametrized Rational Curves*. Computed Aided Geometric Design, **3**, 1986, pp. 67–75.
7. D. Sevilla: *Ritt's Theorems for Rational Functions*. Dept. of Mathematics, University of Cantabria, Spain, preprint, 2002.
8. R. Zippel: *Rational Function Decomposition*. Proc. of ISSAC-91. ACM press, 1991, 1–6.