Article Submitted to Journal of Symbolic Computation

On Multivariate Rational Function Decomposition

Jaime Gutierrez[+], Rosario Rubio[*] and David Sevilla[+]

[+] *Dpto. de Matemáticas, Estadística y Computación*
Universidad de Cantabria
39071 Santander, Spain

[*] *Departamento de Ingeniería*
Universidad Antonio de Nebrija
28040 Madrid, Spain

Abstract

In this paper we discuss several notions of decomposition for multivariate rational functions, and we present algorithms for decomposing multivariate rational functions over an arbitrary field. We also provide a very efficient method to decide if a unirational field has transcendence degree one, and in the affirmative case to compute the generator.

1. Introduction

If $\mathbb{K}$ is a field, and $g, h \in \mathbb{K}(x)$ are rational functions of degree greater than one, then $f = g \circ h = g(h)$ is their (functional) composition, (g, h) is a (functional) decomposition of f, and f is a decomposable rational function. The univariate rational functional decomposition problem can be stated as follows: given $f \in \mathbb{K}(x)$, determine whether there exists a decomposition (g, h) of f 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 more efficiently solved, improperly parametrized algebraic curves can be reparametrized properly, etc. Zippel (1991) presented a polynomial time algorithm to decompose a univariate rational function over any field with efficient polynomial factorization. Alonso, Gutierrez & Recio (1995) presented two exponential–time algorithms to decompose univariate rational functions, which are quite efficient in practice. Klüners (2000) presented an exponential–time algorithm to decompose univariate rational functions over the rational numbers field $\mathbb{Q}$.

If $f, h \in \mathbb{K}(x)$ are such that $\mathbb{K}(f) \subset \mathbb{K}(h) \subset \mathbb{K}(x)$, then $f = g(h)$ for some

$g \in \mathbb{K}(x)$. By the classical Lüroth's theorem (see Lüroth (1876)) this problem can be translated into field theory: given $f \in \mathbb{K}(x)$ compute, if it exists a proper intermediate field $\mathbb{F}$ such that $\mathbb{K}(f) \subset \mathbb{F} \subset \mathbb{K}(x)$. The following extended version of Lüroth's theorem is a central result, as it allows to generalize this problem to multivariate rational functions.

THEOREM 1.1: *Let $\mathbb{K}(\mathbf{x}) = \mathbb{K}(x_1, \ldots, x_n)$ be the field of rational functions in the variable $\mathbf{x} = (x_1, \ldots, x_n)$ over an arbitrary field $\mathbb{K}$. If $\mathbb{F}$ is a field of transcendence degree 1 over $\mathbb{K}$ with $\mathbb{K} \subset \mathbb{F} \subset \mathbb{K}(\mathbf{x})$, then there exists $f \in \mathbb{K}(\mathbf{x})$ such that $\mathbb{F} = \mathbb{K}(f)$. Moreover, if $\mathbb{F}$ contains a non–constant polynomial over $\mathbb{K}$, then there exists a polynomial $f \in \mathbb{K}[\mathbf{x}] = \mathbb{K}[x_1, \ldots, x_n]$ such that $\mathbb{F} = \mathbb{K}(f)$.*

For a proof, we refer to Schinzel (1982), Theorems 3 and 4, and Nagata (1993).

We will use the above theorem to show that the number of certain types of multivariate decompositions is finite. In particular, a univariate rational function $f \in \mathbb{K}(x)$ is indecomposable if and only if $\mathbb{K}(f) \subset \mathbb{K}(x)$ is an algebraic extension without proper subfields, thus by the primitive element theorem (see Lang (1967)) there exist only a finite number of intermediate subfields; moreover, if f is a polynomial then f is indecomposable as a rational function if and only if it is an indecomposable polynomial.

A unirational field over $\mathbb{K}$ is an intermediate field $\mathbb{F}$ between $\mathbb{K}$ and $\mathbb{K}(\mathbf{x})$. We know that any unirational field is finitely generated over $\mathbb{K}$ (see Nagata (1993)). In the following, whenever we talk about computing an intermediate field we mean that such finite set of generators is to be calculated. Thus, the constructive version of the Theorem 1.1 result can be stated as follows:

PROBLEM 1: *Given rational functions $f_1, \ldots, f_m \in \mathbb{K}(\mathbf{x})$ decide if the field $\mathbb{F} = \mathbb{K}(f_1, \ldots, f_m)$ has transcendence degree 1 over $\mathbb{K}$ and in the affirmative case, compute $f \in \mathbb{K}(\mathbf{x})$ such that $\mathbb{F} = \mathbb{K}(f)$.*

Moreover we wish to know if $\mathbb{F}$ contains a non–constant polynomial and in the affirmative case, compute a polynomial $f \in \mathbb{K}[\mathbf{x}]$ so that $\mathbb{F} = \mathbb{K}(f)$.

For algorithms related to this problem, we can mention the recent work of Müller–Quade & Steinwandt (1999). They have presented a method which requires the computation of a Gröbner bases using tag variables. In this paper we present a polynomial time algorithm which only requires the computation of a greatest common divisor of m multivariate polynomials. We prove that the algorithm presented in ISSAC'01 conference (see Gutierrez, Rubio & Sevilla (2001)) only requires a step. As a consequence we provide a new and interesting characterization of unirational fields of transcendence degree one.

Another motivation of this paper is, on one hand, to generalize the notions of decomposable multivariate polynomials introduced by von zur Gathen, Gutierrez & Rubio (1999) to rational functions; and, on the other hand, to give algorithms for decomposing multivariate rational functions and to analyze these decompositions from the field theory point of view. In the ISSAC'01 work we presented

some preliminary results for only one kind of multivariate rational function decomposition, the so called uni–multivariate one.

The paper is organized as follows. In Section 2, we define and study three notions of decomposition for multivariate rational functions. We state some finiteness results related to these decompositions and we also present algorithms to find such decompositions. Section 3 is devoted to solve Problem 1. We provide a polynomial time algorithm that works over any field. As a consequence of the results in Section 2 and this algorithm, we provide a method to compute all unirational fields of transcendence degree one containing a given finite set of multivariate rational functions.

2. Multivariate rational decomposition

The univariate rational function decomposition problem suggests the following natural decomposition problem.

PROBLEM 2: *Given rational functions* $f_1, \ldots, f_m \in \mathbb{K}(\mathbf{x})$ *find, if there exists, a proper intermediate subfield* $\mathbb{F}$ *such that*

$$\mathbb{K}(f_1, \ldots, f_m) \subset \mathbb{F} \subset \mathbb{K}(\mathbf{x}).$$

This problem is equivalent to find rational functions $h_1, \ldots, h_s \in \mathbb{K}(\mathbf{x})$, and $g_1, \ldots, g_m \in \mathbb{K}(y_1, \ldots, y_s)$ such that $\mathbb{K}(f_1, \ldots, f_m) \subset \mathbb{F} \subset \mathbb{K}(\mathbf{x})$ and

$$f_i(\mathbf{x}) = g_i(h_1, \ldots, h_s),$$

where $\mathbb{F} = \mathbb{K}(h_1, \ldots, h_s)$. This leads to the following concept.

Definition: Let $f \in \mathbb{K}(\mathbf{x})$, $h_1, \ldots, h_m \in \mathbb{K}(\mathbf{x})$ and $g \in \mathbb{K}(y_1, \ldots, y_s)$ such that $f = g(h_1, \ldots, h_s)$. Then we say that $(g, h_1, \ldots, h_s)$ is a **decomposition** of f.

Regarding algorithms to solve this general problem we can mention the recent works of Müller–Quade & Steinwandt (1999), which requires to compute primary ideal decomposition on polynomial rings; and the method presented in Rubio (2001), it needs factorization over algebraic extensions.

Both algorithms lacks of effectiveness and does not inherit some good properties of the univariate case. For instance, there is no relation between the degrees of the components, and there is not a good behaviour with polynomials, that is, even if the given rational functions are all polynomials, an intermediate field may not have polynomial generators. On the other hand, for every rational function f, in at least two variables, there are infinitely many proper intermediate fields $\mathbb{F}$ containing $\mathbb{K}(f)$.

Thus, it is natural to impose some restrictions on $\mathbb{F}$ that make the problem amenable to computation. Of particular interest are restrictions that make decompositions finite in an appropriate sense. In fact, this is, overall, one of the main goals of this section. With this restrictions we define and analyze different definitions of decomposable multivariate rational functions, generalizing the ones formulated for polynomials in von zur Gathen, Gutierrez & Rubio (1999).

2.1. Uni–multivariate rational decomposition

In this subsection we define and analyze the uni–multivariate decomposition of a rational function. An extended abstract of these results can be found in Gutierrez, Rubio & Sevilla (2001).

Given a multivariate rational function $f \in \mathbb{K}(\mathbf{x})$ we will denote as f_N, f_D the numerator and denominator of f, respectively and we will suppose that $\gcd(f_N, f_D) = 1$. We define the **degree** of the rational function f as $\deg\ f = \deg\ (f) = \max\ \{\deg\ f_N, \deg\ f_D\}$. A rational function of degree one is called a linear rational function.

Definition: Let $f, h \in \mathbb{K}(\mathbf{x})$ and $g \in \mathbb{K}(y)$ such that $f = g(h)$. Then we say that (g, h) is a **uni–multivariate decomposition** of f. It is **non–trivial** if $1 < \deg h < \deg f$. The rational function f is **uni–multivariate decomposable** if there exists a non–trivial decomposition.

The uni–multivariate decomposition problem is to decide if the multivariate rational function f is uni–multivariate decomposable; and in the affirmative case, to compute the rational functions g, h.

It is well known that the degree is multiplicative with respect to the composition of univariate rational functions, see Alonso, Gutierrez & Recio (1995). In particular a univariate rational function $f \in \mathbb{K}(x)$ is a composition unit if there exists $g \in \mathbb{K}(x)$ such that $f(g) = g(f) = x$. This happens if and only if f is a linear rational function. Linear rational functions are also called (composition) units.

One of the most important properties of the uni–multivariate decomposition is also the good behavior of the degree with respect to this composition.

PROPOSITION 2.1: *Let $f \in \mathbb{K}(\mathbf{x})$ be a rational function. If (g, h) is a uni–multivariate decomposition of f, then*

$$\deg\ (f) = \deg\ (g) \cdot \deg\ (h).$$

Proof: Let $\widehat{\mathbb{K}}$ be the algebraic clousure of $\mathbb{K}$. There exist $(\alpha_2, \ldots, \alpha_n) \in \widehat{\mathbb{K}}^{n-1}$ and $(\beta_2, \ldots, \beta_n) \in \widehat{\mathbb{K}}^{n-1}$ such that $r = \deg(f) = \deg(\hat{f})$ and $s = \deg(h) = \deg(\hat{h})$ where

$$\hat{f} = f(x_1, \beta_2 + \alpha_2 x_1, \ldots, \beta_n + \alpha_n x_1)$$

and

$$\hat{h} = h(x_1, \beta_2 + \alpha_2 x_1, \ldots, \beta_n + \alpha_n x_1).$$

From the equality $f = g(h)$ we obtain $\hat{f} = g(\hat{h})$ and since the degree of the univariate rational function is multiplicative with respect to the composition, we have $r = s \deg(g)$. □

A consequence of this proposition is the uniqueness of the left component g, given the rational functions f, h.

COROLLARY 2.1: *Given f, h non-constant rational functions in $\mathbb{K}(\mathbf{x})$, if there exists g such that $f = g(h)$ is unique. Furthermore, it can be computed from f and h by solving a linear system of equations.*

Proof: If $f = g_1(h) = g_2(h)$, then $(g_1 - g_2)(h) = 0$, and by Proposition 2.1, $\deg(g_1 - g_2) = 0$, thus $g_1 - g_2$ is constant. Clearly it must be 0, that is, $g_1 = g_2$. Again by Proposition 2.1, the degree of g is determined by those of f and h. We can write g as a function with the corresponding degree and undetermined coefficients. The equation $f - g(h) = 0$ provides a linear homogenous system of equations in the coefficients of g. □

The relation between the decomposition and the subfield computation allows to formulate the problem of the uni–multivariate decomposition in terms of field theory. First we will define the following equivalence relation.

Definition: Let $f \in \mathbb{K}(\mathbf{x})$ be rational function. Two uni–multivariate decompositions (g, h) and (g', h') of f are **equivalent** if there exists $l \in \mathbb{K}(y)$ composition unit such that $h = l(h')$.

PROPOSITION 2.2: *Let $f \in \mathbb{K}(\mathbf{x})$ be a non–constant rational function. Then the equivalence classes of the uni–multivariate decompositions of f correspond bijectively to intermediate fields $\mathbb{F}$, $\mathbb{K}(f) \subset \mathbb{F} \subset \mathbb{K}(\mathbf{x})$, with transcendence degree 1 over $\mathbb{K}$.*

Proof: The bijection is

$$\begin{array}{ccc} \{[(g,h)],\ f = g(h)\} & \longrightarrow & \{\mathbb{K}(f) \subset \mathbb{F}, \mathrm{tr.deg}(\mathbb{F}/\mathbb{K}) = 1\}. \\ [(g,h)] & \longmapsto & \mathbb{F} = \mathbb{K}(h) \end{array}$$

Suppose we have a uni–multivariate decomposition (g, h) of f. Since $f = g(h)$, $\mathbb{F} = \mathbb{K}(h)$ is an intermediate field of $\mathbb{K}(f) \subset \mathbb{K}(\mathbf{x})$ with transcendence degree 1 over $\mathbb{K}$. On the other hand, if (g', h') is equivalent to (g, h) then $h = l \circ h'$ for some unit $l \in \mathbb{K}(y)$. Consequently $h' = l^{-1} \circ h$ and $\mathbb{K}(h) = \mathbb{K}(h')$.

If (g, h) and (g', h') are two uni–multivariate decompositions of f such that $\mathbb{K}(h) = \mathbb{K}(h')$, then there exist $l, l' \in \mathbb{K}(y)$ rational functions such that $h = l \circ h'$ and $h' = l' \circ h$. By Proposition 2.1, $\deg(l \circ l') = 1$ and $\deg l = \deg l' = 1$. By the uniqueness of the left component,(see Corollary 2.1), $y = l \circ l'$. So, $l \in \mathbb{K}(y)$ is a composition unit and (g, h), (g', h') are equivalent.

Finally, by Theorem 1.1, given the intermediate field $\mathbb{F}$ there exist $h \in \mathbb{K}(\mathbf{x})$ and $g \in \mathbb{K}(y)$ such that $\mathbb{F} = \mathbb{K}(h)$ and $f = g(h)$. □

Because of this result the uni–multivariate decomposition problem is a particular case of Problem 2.

2.1.1. An algorithm

We describe a method to know if a rational function is uni–multivariate decomposable and compute a decomposition in the affirmative case.

The main idea of the present method generalizes one of the univariate rational function decomposition methods presented in Alonso, Gutierrez & Recio (1995) and is based on the near–separated polynomial concept. This notion was defined only for bivariate polynomials, see also Alonso, Gutierrez & Recio (1997). We will consider near–separated polynomials with $2n$ variables:

Definition: Let $p \in \mathbb{K}[\mathbf{x},\mathbf{y}] = \mathbb{K}[x_1,\ldots,x_n,y_1,\ldots,x_n]$ be a non–constant polynomial in the variables $(\mathbf{x},\mathbf{y}) = (x_1,\ldots,x_n,y_1,\ldots,y_n)$ We say that p is **near–separated** if there exist non–constant polynomials $r_1, s_1 \in \mathbb{K}[\mathbf{x}]$ and $r_2, s_2 \in \mathbb{K}[\mathbf{y}]$, such that neither r_1, s_1 are associated, nor r_2, s_2 are associated and $p = r_1 s_2 - r_2 s_1$.

In the particular case $p = r(\mathbf{x})s(\mathbf{y}) - s(\mathbf{x})r(\mathbf{y})$, we say that p is a **symmetric near–separated** polynomial and (r,s) is a **symmetric near–separated representation** of p.

Given a polynomial $q \in \mathbb{K}[\mathbf{x},\mathbf{y}]$ we will denote by $\deg_{\mathbf{x}}(p)$ the total degree with respect to the variables $\mathbf{x}$ and by $\deg_{\mathbf{y}}(p)$ the total degree with respect to the variables $\mathbf{y}$ of p.

In the following proposition we give some basic properties of near–separated polynomials, for later use.

PROPOSITION 2.3: *Let $p \in \mathbb{K}[\mathbf{x},\mathbf{y}]$ be a near–separated polynomial and r_1, s_1, r_2, s_2 as in the above definition. Then*

(i) *If* $\gcd(r_1,s_1) = 1$ *and* $\gcd(r_2,s_2) = 1$, *p has no factors in* $\mathbb{K}[\mathbf{x}]$ *or* $\mathbb{K}[\mathbf{y}]$.

(ii) $\deg_{\mathbf{x}} p = \max\{\deg\ r_1, \deg\ s_1\}$ *and* $\deg_{\mathbf{y}} p = \max\{\deg\ r_2, \deg\ s_2\}$.

(iii) *If p is symmetric and $(\alpha_1,\ldots,\alpha_n) \in \mathbb{K}^n$ satifies $p(\mathbf{x},\alpha_1,\ldots,\alpha_n) \neq 0$, then there exists a symmetric near–separated representation (r,s) of p, such that $r(\alpha_1,\ldots,\alpha_n) = 0$ and $s(\alpha_1,\cdots,\alpha_n) = 1$.*

(iv) *If p is symmetric, the coefficient of $x_k^i y_k^j$ in p is the near–separated polynomial*

$$a_i(x_1,\ldots,x_{k-1},x_{k+1},\ldots,x_n)b_j(y_1,\ldots,y_{k-1},y_{k+1},\ldots,y_n) - b_i(x_1,\ldots,x_{k-1},x_{k+1},\ldots,x_n)a_j(y_1,\ldots,y_{k-1},y_{k+1},\ldots,y_n),$$

where a_i is the coefficient of x_k^i in r and b_i is the coefficient of x_k^i in s.

Proof: **(i)** Suppose $v \in \mathbb{K}[\mathbf{x}]$ is a non–constant factor of p. Then there exists i such that $\deg_{x_i} v \geq 1$. Without loss of generality we will suppose that $i = 1$. Let α be a root of v, considering p as a univariate polynomial in the variable x_1, in a suitable extension of $\mathbb{K}[x_2,\ldots,x_n]$. If α is a root of any of the polynomials

r_1 or s_1, then it is also a root of the other. This is a contradiction, because $\gcd(r_1, s_1) = 1$. Therefore α is neither a root of r_1 nor of s_1. Then,

$$\frac{r_1(\alpha, x_2, \ldots, x_n)}{s_1(\alpha, x_2, \ldots, x_n)} = \frac{r_2(\mathbf{y})}{s_2(\mathbf{y})} \in \mathbb{K}.$$

A contradiction again, since r_2, s_2 are not associated in $\mathbb{K}$.

(ii) If $\deg\ r_1 \neq \deg\ s_1$, the equality is trivial. Otherwise, if $\deg\ r_1 = \deg\ s_1 > \deg_{\mathbf{x}} p$, the terms with greatest degree with respect to $\mathbf{x}$ must vanish. This is a contradiction, because r_2, s_2 are not associated. The proof is similar for r_2, s_2.

(iii) Let (r, s) be a representation of p.

- If $r(\alpha_1, \ldots, \alpha_n) = 0$, since $p(\mathbf{x}, \alpha_1, \ldots, \alpha_n) \neq 0$, we have $s(\alpha_1, \ldots, \alpha_n) \neq 0$. Then we have a new near–separated representation:

$$\left(r\, s(\alpha_1, \ldots, \alpha_n), \frac{s}{s(\alpha_1, \ldots, \alpha_n)} \right).$$

- If $s(\alpha_1, \ldots, \alpha_n) = 0$, then the representation $(-s, r)$ we are in the previous case.
- If $r(\alpha_1, \ldots, \alpha_n), s(\alpha_1, \ldots, \alpha_n) \neq 0$, then we consider the representation

$$\left(r\, s(\alpha_1, \ldots, \alpha_n) - s\, r(\alpha_1, \ldots, \alpha_n), \frac{s}{s(\alpha_1, \ldots, \alpha_n)} \right).$$

(iv) This is a simple routine confirmation. □

Note: By Proposition 2.3, we can decide if p is symmetric and near–separated polynomial; and in the affirmative case, find a near–separated representation of p, that is, compute $r, s \in \mathbb{K}[\mathbf{x}]$ such that $p = r(\mathbf{x})s(\mathbf{y}) - r(\mathbf{y})s(\mathbf{x})$.

Firstly, we would consider $(\alpha_1, \ldots, \alpha_n) \in \mathbb{K}^n$ with $p(\mathbf{x}, \alpha_1, \ldots, \alpha_n) \neq 0$ and we get the polynomial $r(\mathbf{x}) = p(\mathbf{x}, \alpha_1, \ldots, \alpha_n)$. If the ground field $\mathbb{K}$ is sufficiently "big", the existence of such n–tuple is guaranteed. Secondly, $s(\mathbf{x})$ is computed by means of the linear systems which provides item **iv)** of Proposition 2.3. □

LEMMA 2.1: *In the above conditions, any other solution s' gives the same field, that is, $\mathbb{K}(r/s) = \mathbb{K}(r/s')$.*

Proof: If $s' \in \mathbb{K}[\mathbf{x}]$ is another solution, we have: $p = r(\mathbf{x})s(\mathbf{y}) - r(\mathbf{y})s(\mathbf{x}) = r(\mathbf{x})s'(\mathbf{y}) - r(\mathbf{y})s'(\mathbf{x})$, that is, $r(\mathbf{x})(s(\mathbf{y}) - s'(\mathbf{y})) = r(\mathbf{y})(s'(\mathbf{x}) - s'(\mathbf{x}))$. Then there exists $0 \neq \alpha \in \mathbb{K}$, such that $\alpha r(\mathbf{y}) = s(\mathbf{y}) - s'(\mathbf{y})$. Let $u(x) = x/(-\alpha x + 1)$, which is a unit in $\mathbb{K}(x)$. We have $r/s' = u(r/s)$. □

We have just seen how we can know if a symmetric polynomial is near–separated. Now, we state an important theorem that relates uni–multivariate decompositions to near–separated polynomials, which was proved in Schicho (1995):

THEOREM 2.1: *Let $A = \mathbb{K}(\mathbf{x})$ and $B = \mathbb{K}(\mathbf{y})$ be rational function fields over $\mathbb{K}$. Let $f, h \in A$ and $f', h' \in B$ be non–constant rational functions. Then the following statements are equivalent:*

A) *There exists a rational function $g \in \mathbb{K}(t)$ satisfying $f = g(h)$ and $f' = g(h')$.*

B) *$h - h'$ divides $f - f'$ in $A \otimes_{\mathbb{K}} B$.*

An immediate consequence of the above important theorem is the following useful result.

COROLLARY 2.2: *Let $f, h \in \mathbb{K}(\mathbf{x}), f', h' \in \mathbb{K}(\mathbf{y})$, be non–constant rational functions. Then the following statements are equivalent:*

A) *$f \in \mathbb{K}(h)$ and $f' \in \mathbb{K}(h')$.*

B) *$h_N(\mathbf{x})h'_D(\mathbf{y}) - h_D(\mathbf{x})h'_N(\mathbf{y})$ divides $f_N(\mathbf{x})f'_D(\mathbf{y}) - f_D(\mathbf{x})f'_N(\mathbf{y})$ in $\mathbb{K}[\mathbf{x}, \mathbf{y}]$.*

So, in order to find a uni–multivariate decomposition of a rational function f we should look for symmetric near–separated factors of the polynomial $f_N(\mathbf{x})f_D(\mathbf{y}) - f_D(\mathbf{x})f_N(\mathbf{y})$. Let us describe formally this algorithm.

ALGORITHM 2.1: **Input:** $f \in \mathbb{K}(\mathbf{x})$.

Output: *(g, h) uni–multivariate decomposition of f, if it exists, and "no decomposition" otherwise.*

A *Factor the symmetric polynomial*

$$p = f_N(\mathbf{x})f_D(\mathbf{y}) - f_D(\mathbf{x})f_N(\mathbf{y}).$$

B *Let H be a divisor of p.*

C *Check if H is a symmetric near–separated polynomial using Algorithm* **??**.

- *If $H = r(\mathbf{x})s(\mathbf{y}) - r(\mathbf{y})s(\mathbf{x})$, then $h = \frac{r}{s}$. Compute the left component g by solving a linear system of equations (see Corollary 2.1) and RETURN (g, h).*
- *If there is no factor to take, then RETURN "no decomposition".*
- *Take H another factor and repeat* **C**. □

A detailed analysis of this algorithm is rather difficult, especially if the analysis is to match experience. In the worst case, this algorithm is exponential in $\deg f$, since p may split into linear factors, yet f may be indecomposable. This would require step **B** to examine an exponential number of possible candidates, none of which is a symmetric near–separated polynomial. Each of the other steps requires only random polynomial time. However, in practice it seems that most of the time is spent in step **A**, factoring the multivariate polynomial p in $2n$ variables. An exponential algorithm is presented in Gutierrez, Rubio & Sevilla (2001) which requires factoring polynomials in only n variables.

COROLLARY 2.3: *Given a rational function $f \in \mathbb{K}(\mathbf{x})$ we can compute all the equivalence classes of the uni–multivariate decompositions of f.*

Proof: It is immediate from Algorithm 2.1 and Lemma 2.1. □

To conclude this subsection, we will illustrate the algorithm by an example.

EXAMPLE 2.1: *Let*

$$f = \frac{y^2x^2 + 2\,x^2yz^2 - 2\,y^6x + z^4x^2 - 2\,z^2xy^5 + y^{10} - 81\,x^2 - 450\,xyz - 625\,y^2z^2}{y^2x^2 + 2\,x^2yz^2 - 2\,y^6x + z^4x^2 - 2\,z^2xy^5 + y^{10} - 162\,x^2 - 900\,xyz - 1250\,y^2z^2}.$$

We look for all the intermediate fields of $\mathbb{Q}(f) \subset \mathbb{Q}(x,y,z)$ with transcendence degree 1 over $\mathbb{Q}$.

First, we factor the polynomial,

$$f_N(x,y,z)f_D(s,t,u) - f_N(s,t,u)f_D(x,y,z) = -625 f_1 f_2,$$

where

$$\begin{aligned} f_1 = \;& -xtz^2u + \tfrac{9}{25}\,xt^5 - zsty - zu^2sy + zt^5y - \tfrac{9}{25}\,xz^2s - \tfrac{9}{25}\,xu^2s - \tfrac{9}{25}\,xys - xyut \\ & -\tfrac{9}{25}\,xts + \tfrac{9}{25}\,sy^5 + uty^5, \\ f_2 = \;& -xtz^2u - \tfrac{9}{25}\,xt^5 + zsty + zu^2sy - zt^5y - \tfrac{9}{25}\,xz^2s + \tfrac{9}{25}\,xu^2s - \tfrac{9}{25}\,xys - xyut \\ & +\tfrac{9}{25}\,xts + \tfrac{9}{25}\,sy^5 + uty^5. \end{aligned}$$

We have $f_1(x,y,z,x,y,z) \neq 0$, then f_1 is not symmetric near–separated. On the other hand, $f_2(x,y,z,x,y,z) = 0$ and moreover,

$$\begin{aligned} f_2 = \;& -zt^5y + uty^5 + \left(-\frac{9}{25}\,t^5 - tz^2u - yut\right)x + \left(zty + \frac{9}{25}\,y^5 + zu^2y\right)s + \\ & \left(-\frac{9}{25}\,z^2 + \frac{9}{25}\,t + \frac{9}{25}\,u^2 - \frac{9}{25}\,y\right)sx. \end{aligned}$$

Now, we check that f_2 is a symmetric near–separated polynomial and (r,s) is a symmetric near–separated representation of f_2:

$$\begin{aligned} r &= -\frac{9}{25}xz^2 - \frac{9}{25}xy + \frac{9}{25}y^5, \\ s &= x + \frac{25}{9}zy. \end{aligned}$$

Finally, we compute g which is a univariate function of degree 2. By solving the linear system of equations $f = g(h)$ where $h = r/s$, we obtain

$$g = \frac{625\,t^2 - 6561}{625\,t^2 - 13122}.$$

□

2.2. Multi–univariate rational decomposition

Gröbner bases computation can be simplify by means of a polynomial decomposition, see Gutierrez & Rubio (1998). The behavior of the reduced Gröbner bases under the composition suggests a new notion of decomposable polynomial and consequently of rational function.

In this subsection, we will define the multi–univariate decomposition and an analysis will be made over this kind of decomposition. We will prove similar properties to the uni–multivariate case, Subsection 2.1.

Definition: Let $f, g \in \mathbb{K}(\mathbf{x})$ and $h_i \in \mathbb{K}(x_i)$, for $1 \leq i \leq n$, such that $f = g(h_1(x_1), \ldots, h_n(x_n))$. Then we say that $(g, h_1, \ldots, h_n)$ is a **multi–univariate decomposition** of f. It is **non–trivial** if $\deg h_i \geq 1$ for any i, and if there exists j satisfying $1 < \deg h_j < \deg_{x_j} f$. The rational function f is **multi–univariate decomposable** if there exists a non–trivial decomposition.

The multi–univariate decomposition problem is to decide if the multivariate rational function f is multi–univariate decomposable; and in the affirmative case, compute the rational functions $g, h_1, \ldots, h_n$.

Immediately from the definition we get the following result about the behavior of the degrees with respect to the multi-univariate decomposition.

Proposition 2.4: *Let $f \in \mathbb{K}(\mathbf{x})$ be a rational function. If $(g, h_1, \ldots, h_n)$ is a multi–univariate decomposition of f, then for every $1 \leq i \leq n$*

$$\deg_{x_i} f = \deg_{x_i} g \cdot \deg h_i.$$

This result allows to affirm that given $f, h_1, \ldots, h_n$, the left component g is unique.

Now, we will see how can formulate the multi–univariate decomposition problem in terms of field theory. Firstly, we will define the equivalence classes for multi–univariate decompositions.

Definition: Let $f \in \mathbb{K}(\mathbf{x})$ be a rational function. Two multi–univariate decompositions $(g, h_1, \ldots, h_n)$ and $(g', h'_1, \ldots, h'_n)$ of f are **equivalent** if for each $1 \leq i \leq n$ there exists $l_i \in \mathbb{K}(y)$ composition unit, such that $h_i = l_i(h'_i)$.

The following result relates the multi–univariate decomposition to fields with transcendence degree n and generated by univariate rational functions.

Proposition 2.5: *Let $f \in \mathbb{K}(\mathbf{x})$ be a rational function with $\deg_{x_i} f \geq 1$ for any i. Then the equivalence classes of the multi–univariate decompositions of f correspond bijectively with the intermediate fields $\mathbb{F}$, $\mathbb{K}(f) \subset \mathbb{F} \subset \mathbb{K}(\mathbf{x})$, with transcendence degree n over $\mathbb{K}$ and generated by univariate rational functions.*

Proof: The bijection is

$$\begin{array}{ccc} \{[(g,h_1,\ldots,h_n)] \mid f = g(h_1,\ldots,h_n)\} & \longrightarrow & \left\{ \begin{array}{c} \mathbb{K}(f) \subset \mathbb{F} \subset \mathbb{K}(\mathbf{x}) \\ \text{tr.deg}(\mathbb{F}/\mathbb{K}) = n \\ h_i \in \mathbb{K}(x_i) \end{array} \right\}. \\ [(g,h_1,\ldots,h_n)] & \longmapsto & \mathbb{F} = \mathbb{K}(h_1,\ldots,h_n) \end{array}$$

Suppose we have a multi–univariate decomposition $(g,h_1,\ldots,h_n)$ of f. Since $f = g(h_1,\ldots,h_n)$, $\mathbb{K}(f) \subset \mathbb{K}(h_1,\ldots,h_n) \subset \mathbb{K}(\mathbf{x})$. Moreover, $\deg(h_i) \geq 1$ for every i, then $\mathbb{K}(h_1,\ldots,h_n)$ has transcendence degree n.

On the other hand, if $(g',h'_1,\ldots,h'_n)$ is equivalent to $(g,h_1,\ldots,h_n)$, then $h_i = l_i \circ h'_i$ for some $l_i \in \mathbb{K}(y)$ composition unit. So, $h'_i = l_i^{-1} \circ h_i$, in other words, $\mathbb{K}(h_1,\ldots,h_n) = \mathbb{K}(h'_1,\ldots,h'_n)$.

Let $(g,h_1,\ldots,h_n)$ and $(g',h'_1,\ldots,h'_n)$ be two multi–univariate decompositions of f such that $\mathbb{K}(h_1,\ldots,h_n) = \mathbb{K}(h'_1,\ldots,h'_n)$. For each $i \in \{1,\ldots,n\}$ there exists $l_i \in \mathbb{K}(\mathbf{y})$, such that $h_i = l_i(h'_1(x_1),\ldots,h'_n(x_n))$. By Proposition 2.4, $l_i \in \mathbb{K}(y)$ and $h_i = l_i \circ h'_i$.

Analogously, for each i there exists $l'_i \in \mathbb{K}(y)$ such that $h'_i = l'_i \circ h$. Therefore, $\deg l_i = \deg l'_i = 1$ and $(g,h_1,\ldots,h_n)$ and $(g',h'_1,\ldots,h'_n)$ are equivalent. So the injectivity of the correspondence is done.

Applying Theorem 1.1 to each variable, there exists $h_i \in \mathbb{K}(x_i)\backslash\mathbb{K}$ such that $\mathbb{F} = \mathbb{K}(h_1,\ldots,h_n)$. There also exists $g \in \mathbb{K}(\mathbf{y})$ such that $f = g(h_1,\ldots,h_n)$. □

2.2.1. An algorithm

Now, we show an algorithm to compute multi–univariate decompositions of rational functions. Again, for this algorithm, we suppose that $\mathbb{K}$ has sufficiently many elements. So, we can assume –without loss of generality– that if we write $f_i(x_i) = f(0,\ldots,0,x_i,0,\ldots,0)$ then $f_i(x_i)$ is a non–constant univariate rational function. Otherwise, we will take another point $(\alpha_1,\ldots,\alpha_n) \in \mathbb{K}^n$ such that $f_i(x_i)$ is a non–constant rational function, where $f_i(x_i) = f(\alpha_1,\ldots,\alpha_{i-1},x_i,\alpha_{i+1},\ldots,\alpha_n)$.

On the other hand, if we suppose that f has a multi–univariate decomposition $f = g(h_1(x_1),\ldots,h_n(x_n))$, then

$$f_i(x_i) = g(0,\ldots,0,h_i(x_i),0,\ldots,0).$$

So, the univariate rational function $f_i(x_i)$ has a decomposition $f_i(x_i) = g_i(h_i(x_i))$ where $g_i = g(0,\ldots,0,x_i,0,\ldots,0)$. This observation is the key to the following algorithm.

ALGORITHM 2.2: **Input:** $f \in \mathbb{K}(\mathbf{x})$ *and* $\underline{d} = (d_1,\ldots,d_n)$ *a lists of positive integers, such that* $d_i \mid \deg_{x_i} f$.

Output: $(g,h_1(x_1),\ldots,h_n(x_n))$ *multi–univariate decomposition of* f *such that* $d_i = \deg h_i$, *if it exists and "no decomposition" otherwise.*

A *Compute all non equivalence univariate decomposition classes* $(g_i, h_i(x_i))$ *of* $f_i(x_i)$ *such that* $d_i = \deg h_i$ *for* $1 \leq i \leq n$. *(Using an algorithm for univariate decomposition). If there is no decomposition, RETURN "no decomposition".*

B *For a list* $L = (h_1(x_1), \ldots, h_n(x_n))$ *consider* g *a rational function with unknown coefficients in the variables* $\mathbf{y}$, *and such that* $\deg_{y_i} g = \dfrac{\deg_{x_i} f}{\deg h_i}$. *Solve the linear system of equations:*

$$f(x_1, \ldots, x_n) = g(h_1(x_1), \ldots, h_n(x_n)).$$

If the system has solution, then RETURN $(g, h_1(x_1), \ldots, h_n(x_n))$. *Otherwise take another list* L *and repeat step* **B**. *If the corresponding linear system has no solution for every list, then RETURN "no decomposition" .* □

Proposition 2.5 implies that the algorithm determines correctly whether f has a multi–univariate decomposition with the required degrees, and if so, computes a decomposition whenever decompositions over a rational function field $\mathbb{K}(x)$ could be computed. Since the numbers of divisors of $\deg(f)$ is finite, we obtain an algorithm to compute all non-equivalence multi–univariate decompositions classes of a rational function f. The complexity is dominated in step **A** by decomposing univariate rational functions.

The following example illustrates Algorithm 2.2.

EXAMPLE 2.2: *Let*

$$f = -\frac{(x^2 + 2\,x - 10)\,(-5\,xy^2 + 15\,y^2 + x^2y^4 - 2\,x^2y^2 + x^2 + 2\,xy^4 + 2\,x - 10\,y^4 - 10)}{(x^2y^2 - x^2 + 2\,xy^2 - 2\,x - 10\,y^2 + 10 + yx + 5\,y)\,(x + 5)\,(y^2 - 1)}.$$

We are looking for all non-equivalence multi–univariate decomposition classes of f *over the rational function field* $\mathbb{Q}(x, y)$. *We consider the non–constant univariate rational functions* $f(x, 0)$ *and* $f(y, 0)$:

$$f(x,0) = -\frac{x^2 + 2\,x - 10}{x + 5}, \quad f(0,y) = \frac{4 - 6\,y^2 + 4\,y^4}{-4\,y^2 + 2 + 2\,y^4 - y^3 + y}.$$

Using univariate rational function decomposition algorithms, we obtain that $f(x, 0)$ *is indecomposable and* $f(0, y)$ *has one non–trivial decomposition, with right component* $\dfrac{1 - y^2}{y}$. *So, we have five lists of univariate rational functions* $(h_1(x), h_2(y))$:

$$[(f(x,0),\ f(0,y)),\ (f(x,0),\ \frac{1-y^2}{y}),\ (x,\ \frac{1-y^2}{y}),\ (f(x,0),\ y),\ (x, f(0,y))].$$

Now, for every list (h_1, h_2) *we consider* g *a rational function with undetermined coefficients of degree at most* 4. *Solving the linear system of equations* $f =$

$g(h_1, h_2)$ we have three multi–univariate decompositions $(g(x, y), h_1(x), h_2(y))$ of f:

$$\left(\frac{x - x^2y^2}{-y + x}, -\frac{x^2 + 2\,x - 10}{x + 5}, \frac{1 - y^2}{y}\right),$$

$$\left(\frac{7\,x^2 - y^2x^4 + x^3 - 4\,x^3y^2 - 50 - 100\,y^2 + 40\,xy^2 + 16\,x^2y^2}{-25\,y - x^2y + 7\,x^2y^2 - 10\,yx - 50\,y^2 + x^3y^2}, x, \frac{1 - y^2}{y}\right)$$

$$\left(\frac{-x^2 + xy^2 - x^2y^4 + 2\,x^2y^2}{xy^4 - 2\,xy^2 + x + y^3 - y}, -\frac{x^2 + 2\,x - 10}{x + 5}, y\right).$$

□

Remark: The rational function of the Example 2.1 is multi–univariate indecomposable and the rational function of the above Example 2.2 is uni–multivariate indecomposable. So, we have two independent decompositions. □

2.3. Single–variable decomposition

This subsection will introduce the last notion of multivariate rational function decomposable. We will show that this includes as special cases the two concepts of uni–multivariate and multi–univariate decomposition discussed in Subsection 2.1 and Subsection 2.2. The underlying idea of this new decomposition arises when we consider the multivariate rational functions as functions in one variable.

Definition: Let i be an integer with $1 \leq i \leq n$, $\mathbb{L} = \mathbb{K}(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n)$ and $f, g, h \in \mathbb{L}(x_i)$, such that $f = g(h)$. Then we say that (i, g, h) is a **single–variable decomposition** of f. It is **non–trivial** if $1 < \deg_{x_i} h < \deg_{x_i} f$. The rational function f is **s**ingle–variable decomposable if there exists a non–trivial decomposition.

The single–variable decomposition problem is to decide if the multivariate rational function $f \in \mathbb{K}(\mathbf{x})$ is single–variable decomposable; and in the affirmative case, compute the integer i and the rational functions g, h.

It is important to stand out the existence of the integer i. We need to know with respect to which variable we are decomposing. For example, $f \in \mathbb{K}(\mathbf{x})$ can be decomposable with respect to x_i, but be indecomposable with respect to the rest of the variables.

Directly from the definition we obtain that the degree is multiplicative with respect the single–variable decomposition in an appropriate sense.

Proposition 2.6: *Let $f \in \mathbb{K}(\mathbf{x})$ be a rational function. If (i, g, h) is a single–variable decomposition of f, then*

$$\deg_{x_i} f = \deg_{x_i} g \cdot \deg_{x_i} h.$$

Next comes the corresponding equivalence relation.

Definition: Let $f \in \mathbb{K}(\mathbf{x})$ be rational function. Two single–variable decompositions (i, g, h) and (j, g', h') of f are **equivalent** if $i = j$ and there exists a unit $l \in \mathbb{L}(y)$ such that $h = l(h')$, where $\mathbb{L} = \mathbb{K}(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n)$.

The following proposition states that single–variable decomposition simultaneously generalizes the two previous ones, uni–multivariate and multi–univariate decompositions. We have seen in Remark 2.1 these two are independent of each other.

PROPOSITION 2.7: *Let $f \in \mathbb{K}(\mathbf{x})$ be a non–constant rational function. Then,*

i) *A non–trivial equivalence class of of uni–multivariate decompositions of f is contained in an equivalence class of single–variable decompositions.*

ii) *A non–trivial equivalence class of multi–univariate decompositions of f is contained in non–trivial equivalence class of single–variable decompositions.*

Proof: **i)** Suppose (g, h) is a non–trivial uni–multivariate decomposition of f. Then $f = g(h(\mathbf{x}))$ and $1 < \deg h < \deg f$. Therefore, there exists i such that $\deg_{x_i} h \geq 1$ and (i, g, h) is a uni–multivariate decomposition of f.

Let (g', h') be a uni–multivariate decomposition equivalent to (g, h). Then, there exists $l \in \mathbb{K}(y)$ composition unit such that $h = l \circ h'$. And therefore, $\deg_{x_i} h' = \deg_{x_i} h$ and (i, g', h') is a single–variable decomposition of f. Hence, (i, g, h) and (i, g', h') are equivalent single–variable decompositions.

ii) Suppose $(g, h_1, \ldots, h_n)$ is a non–trivial multi–univariate decomposition of f. Then $f = g(h_1(x_1), \ldots, h_n(x_n))$ and there exists $i \in \{1, \ldots, n\}$ such that $1 < \deg h_i < \deg_{x_i} f$.

We have $h'(\mathbf{x}) = h_i(x_i)$ and $g'(\mathbf{x}) = g(h_1, \ldots, h_{i-1}, x_i, h_{i+1}, \ldots, h_n)$, (i, g', h') is a non–trivial single–variable decomposition.

On the other hand, if $(\widetilde{g}, \widetilde{h}_1, \ldots, \widetilde{h}_n)$ is a multi–univariate decomposition equivalent to $(g, h_1, \ldots, h_n)$, then there exists $l_j \in \mathbb{K}(y)$ such that $h_j = l_j \circ \widetilde{h}_j$ for any j. Thus, $\deg h_j = \deg \widetilde{h}_j$, and we can take the integer i. If $\widetilde{g}' = \widetilde{g}(\widetilde{h}_1, \ldots, \widetilde{h}_{i-1}, x_i, \widetilde{h}_{i+1}, \ldots, \widetilde{h}_n)$ and $\widetilde{h}' = \widetilde{h}_i$, then $(i, \widetilde{g}', \widetilde{h}')$ is a single–variable decomposition of f equivalent to (i, g', h'). □

Next comes an example of a rational function which is uni–multivariate and multi–univariate indecomposable, but does have nontrivial single–variable decomposition.

EXAMPLE 2.3: *The rational function*

$$f = \frac{x^5 - x^4 - 2\,x^3 y + 2\,x^2 y - 3\,y^2 x - y^2 + y^4 x^3 - 2\,x^2 y^2 + x + 2\,y^4 x^2 + 2}{\left(y^2 x - 1\right)^2 (x - 1)}$$

has the non trivial single–variable decomposition $(2, g, h)$*, where*

$$g = y^2 + \frac{x+2}{x-1}, \quad h = \frac{x^2 - y}{y^2 x - 1},$$

that is, $f = g(x, h)$*. But* f *is uni–multivariate and multi–univariate rational function indecomposable.* □

The following example illustrates a decomposition of a rational function which is single–variable indecomposable.

EXAMPLE 2.4: *The rational function*

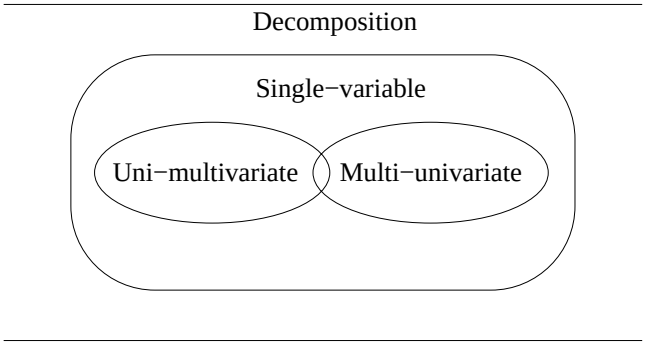
$$f = -\frac{-x^2 y + y^2 + x^5 - x^3 y - 2\,yx + 2}{x^2 - y - yx + 1}$$

can be decomposed as $g(h_1, h_2)$*, where*

$$g(y_1, y_2) = \frac{yx + 2}{x - 1}, \quad h_1 = \frac{x^2 - y}{yx - 1}, \quad h_2 = y - x^3.$$

But it is single–variable indecomposable. □

As in the polynomial case (see von zur Gathen, Gutierrez & Rubio (1999)), the situation on multivariate rational function can be also illustrated in the following diagram of decompositions.



The single–variable decomposition problem also admits its version in field theory terms.

PROPOSITION 2.8: *Let* $f \in \mathbb{K}(\mathbf{x})$ *be a non–constant rational function and* $1 \leq i \leq n$*. Then the equivalence classes of the single–variable decompositions of* f*,* (i, g, h)*, correspond bijectively to intermediate fields* $\mathbb{F}$*, such that*

$$\mathbb{L}(f) \subset \mathbb{F} \subset \mathbb{L}(x_i).$$

Proof: The bijection is

$$\begin{array}{ccc} \{(i,g,h)\} & \longrightarrow & \{\mathbb{L}(f) \subset \mathbb{F} \subset \mathbb{L}(x_i)\}. \\ [(i,g,h)] & \longmapsto & \mathbb{L}(h) \end{array}$$

Suppose we have a single–variable decomposition (i,g,h) of f. If we consider f,g,h as rational functions in $\mathbb{L}(x_i)$, $f = g(h)$, therefore it is well–defined.

On the other hand, if (i,g',h') is equivalent to (i,g,h), then $h = l(h')$ for some composition unit $l \in \mathbb{L}(y)$, then $h' = l^{-1}(h_i)$ and $\mathbb{L}(h) = \mathbb{L}(h')$, and therefore it is an application.

Let (i,g,h) and (i,g',h') be two single–variable decompositions of f such that $\mathbb{L}(h) = \mathbb{L}(h')$. Then, there exists $l \in \mathbb{L}(y)$ composition unit satisfying $h = l(h')$.

Finally, if $\mathbb{F}$ is an intermediate field between $\mathbb{L}(f)$ and $\mathbb{L}(x_i)$, then by Theorem 1.1 there exists $h \in \mathbb{L}(x_i)$ such that $\mathbb{F} = \mathbb{L}(h)$. Besides, there exists $g \in \mathbb{L}(y)$ such that $f = g(h)$. □

One of our goals was to find a reasonable definition for decomposing multivariate rational functions that makes the problem amenable to computation. Of particular interest is finiteness.

COROLLARY 2.4: *Let $f \in \mathbb{K}(\mathbf{x})$ be a rational function such that $0 < \deg_{x_i} f$ for $1 \leq i \leq n$. Then there exists a finite number of equivalence classes of uni–multivariate, multi–univariate and single–variable decompositions of f.*

Proof: If $0 < \deg_{x_i} f$ then the primitive element theorem (see Lang (1967)) asserts that there exists a finite number of intermediate subfields in the extension $\mathbb{L}(f) \subset \mathbb{L}(x)$. As consequence of Proposition 2.8 we have a finite number of single–variable decompositions of f.

On the other hand, it is straightforward to check that the number of trivial equivalence classes of uni–multivariate, multi–univariate and single–variable decomposition of f is finite, see Rubio (2001) for details. And the claim follows of Proposition 2.7. □

Then, we have single–variable decomposition of a rational function is essentially univariate decomposition over a field $\mathbb{L} = \mathbb{K}(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n)$. We simply need to know with respect to which variable we are decomposing. In the worst case, this algorithm has to compute n different decompositions. Then the complexity is n multiply by the cost of the computation of a univariate decomposition over the field $\mathbb{L} = K(x_1, \ldots, x_{n-1})$.

3. Unirational fields of tanscendence degree one

In this last section we will solve Problem 1. Our method only requires compute a gcd of m multivariate polynomials, so it is more effective than the algorithm

presented in the recent work of Müller–Quade & Steinwandt (1999), which requires the computation of a Gröbner bases using tag variables in a polynomial ring in n variables with coefficients in a unirational field. As a consequence we provide a method to compute all unirational fields of transcendence degree one contained in a field, given a finite set of generators. We also obtain some improvements results with respect to previous work Gutierrez, Rubio & Sevilla (2001) and Rubio (2001) concerning the Theorem 1.1 and we state a characterization of unirational fields of transcendence degree one.

NOTATION 1: *In this section we use the following notation:*

- *Let* $\mathbb{F} = \mathbb{K}(f_1, \ldots, f_m)$ *be a rational field,* $\mathbb{K} \subset \mathbb{F} \subset \mathbb{K}(\mathbf{x})$. *We denote by* $\text{Ideal}(H_1, \ldots, H_m)$ *the ideal generated by the polynomials* $H_1, \ldots, H_m \in \mathbb{F}[\mathbf{y}]$.
- *If* $M \in \mathbb{F}[\mathbf{y}]$, *we denote by* $\text{Ideal}(H_1, \ldots, H_m) : (M)^\infty$ *the saturation ideal of* $\text{Ideal}(H_1, \ldots, H_m)$ *with respect to the polynomial* M, *namely the set*

$$\{G \in \mathbb{F}[\mathbf{y}] \mid \exists p \in \mathbb{N} : M^p G \in \text{Ideal}(H_1, \ldots, H_m)\}.$$

- *We consider the map* $\phi_{\mathbb{F}} : \mathbb{F}[\mathbf{y}] \to \mathbb{K}(\mathbf{x})$ *defined by* $\phi_{\mathbb{F}}(y_i) = x_i \;\; (i = 1, \ldots, n)$ *is the ring homomorphism leaving* $\mathbb{F}$ *fixed, the kernel of* $\phi_{\mathbb{F}}$ *is an ideal in the polynomial ring* $\mathbb{F}[\mathbf{y}]$ *and it denoted by* $\mathcal{B}_{\mathbb{F}/\mathbb{K}}$. *It was introduced in the classical book of Weil (1964).*
- *Given an admissible monomial ordering* $>$ *in a polynomial ring and a nonzero polynomial* G *in that ring, we denote by* $\text{lm}\ G$ *the leading monomial of* G *with respect to* $>$ *and* $\text{lc}\ G$ *its leading coefficient.*
- *Finally, we associate to* $f = f_N/f_D \in \mathbb{K}(\mathbf{x})$ *the multivariate rational function* $F = f_N(\mathbf{y}) - f(\mathbf{x}) f_D(\mathbf{y})$ *as an element in the polynomial ring* $\mathbb{K}(f)[\mathbf{y}]$. □

We will use the following result which was proved in Müller–Quade & Steinwandt (1999).

LEMMA 3.1: *With the above notation,* $\mathcal{B}_{\mathbb{F}/\mathbb{K}} = \text{Ideal}(F_1, \ldots, F_m) : (d_f(\mathbf{y}))^\infty$, *where* $d_f = \prod_{j=1}^{m} f_{j\,D}$.

In the following we obtain an interesting property of unirational fields, for later use.

PROPOSITION 3.1: *Let* $g_1, \ldots, g_r$ *be multivariate rational function in* $\mathbb{K}(\mathbf{x})$ *such that* $\mathbb{F} = \mathbb{K}(g_1, \ldots, g_r)$. *We have* $H = \gcd(F_1, \ldots, F_m) = \gcd(G_1, \ldots, G_r)$.

Proof: Let $d_f = \prod_{j=1}^{m} f_{j\,D}$ and $d_g = \prod_{j=1}^{r} g_{j\,D}$. By Lemma 3.1, the ideal $\mathcal{B}_{\mathbb{F}/\mathbb{K}}$ does not depend on the generators; in other terms, $\text{Ideal}(F_1,\ldots,F_m) : (d_f(\mathbf{y}))^\infty = \text{Ideal}(G_1,\ldots,G_r) : (d_g(\mathbf{y}))^\infty$. Therefore, there exists $p \in \mathbb{N}$ such that $G_i \cdot d_f(\mathbf{y})^p \in \text{Ideal}(F_1,\ldots,F_m)$. This implies H divides $G_i \cdot d_f(\mathbf{y})^p$. Since H divides the near–separated polynomials associated to the f_i's, it has no factors in $\mathbb{K}[\mathbf{y}]$ (see Proposition 2.3). Hence $H \mid G_i$, for all $i \leq r$.

On the other hand, there exists $p \in \mathbb{N}$ such that $F_j \cdot d_g(\mathbf{y})^p \in \text{Ideal}(G_1,\ldots,G_r)$. Let d be a polynomial in $\mathbb{F}[\mathbf{y}]$, if $d \mid G_i$ for all i then d also divides $F_j d_g$. Again, we have that d has no factors in $\mathbb{F}[\mathbf{y}]$ and $d \mid F_j$. As consequence, $d \mid H$ and $H = \gcd(G_1,\ldots,G_r)$. □

Now, we have all ingredients to solve Problem 1.

ALGORITHM 3.1: **Input:** $f_1,\ldots,f_m \in \mathbb{K}(\mathbf{x})$.

Output: $f \in \mathbb{K}(\mathbf{x})$ *such that* $\mathbb{K}(f) = \mathbb{F} = \mathbb{K}(f_1,\ldots,f_m)$, *if it exists, and "no Lüroth's generator" otherwise.*

A *Let* $>$ *be a graded lexicographical ordering for* $\mathbf{y} = (y_1,\ldots,y_n)$.

B *Let*

- $F_k = f_{k\,N}(\mathbf{y}) - f_k(\mathbf{x}) f_{k\,D}(\mathbf{y})$ *for* $k = 1,\ldots,m$.
- $i \in \{1,\ldots,m\}$ *such that* $\text{lm}\, F_i \leq \text{lm}\, F_j$

C *Compute* $H = \gcd(\{F_k,\ k = 1,\ldots,m\})$ *with* $\text{lc}\, H = 1$.

- *If* $H = 1$, *RETURN "no Lüroth's generator" (*$\mathbb{F}$ *does not have transcendence degree* 1 *over* $\mathbb{K}$*).*
- *Otherwise,* $H = f_N(\mathbf{y}) - f(\mathbf{x}) f_D(\mathbf{y})$ *for some* $f(\mathbf{x}) \in \mathbb{F}$, *RETURN* f.

Correctness proof. If $\mathbb{F}$ has transcendence degree 1 over $\mathbb{K}$; we can write $\mathbb{F} = \mathbb{K}(f)$. By Corollary 2.2, $f_N(\mathbf{y}) - f(\mathbf{x}) f_D(\mathbf{y})$ divides H. Therefore H cannot be constant if a Lüroth's generator exists.

If $\text{lm}\, H = \text{lm}\, F_i$, then F_i is a greater common divisor of $\{F_j, j = 1,\ldots,m\}$. Then for any i, F_i divides F_j.

Let $q = \overline{f_{j\,N}(\mathbf{y})}^{\{F_i\}}$, $s = \overline{f_{j\,D}(\mathbf{y})}^{\{F_i\}}$ be the normal form with respect to the monomial ordering $>$, that is, there exist $p, q, r, s \in \mathbb{F}[\mathbf{y}]$ such that

$$\begin{aligned} f_{j\,N}(\mathbf{y}) &= p(\mathbf{y}) F_i - q(\mathbf{y}) \\ f_{j\,D}(\mathbf{y}) &= r(\mathbf{y}) F_i - s(\mathbf{y}), \end{aligned}$$

and $\text{lm}\, F_i$ doesn't divide any monomial of q neither of s. By Proposition 2.3, $q, s \neq 0$ and moreover,

$$F_j = F_i(p - f_j(\mathbf{x}) r) + (q - f_j(\mathbf{x}) s).$$

Hence F_i divides $q - f_j(\mathbf{x})s$ and we conclude that $q - f_j(\mathbf{x})s = 0$, since otherwise we would get $\operatorname{lm} F_i$ divides $\operatorname{lm}(q - f_j(\mathbf{x})s)$, which contradicts the choice of the polynomials q, s. Thus $f_j(\mathbf{x}) = \dfrac{q}{s} \in \mathbb{F} = \mathbb{K}(f_i)$.

If $\operatorname{lm} H < \operatorname{lm} F_i$, there exists $C \in \mathbb{F}[\mathbf{y}]$ non–constant such that $F_i = HC$. Let d, α be the lowest common multiples of the denominators of the coefficients of H and C, respectively. Then $D = Hd, C' = \alpha C \in \mathbb{K}[\mathbf{x}, \mathbf{y}]$. Since H is monic, the polynomial D is primitive. Then,

$$f_{iN}(\mathbf{y}) f_{iD}(\mathbf{x}) - f_{iN}(\mathbf{x}) f_{iD}(\mathbf{y}) = \frac{D}{d}\frac{C'}{\alpha} f_{iD}.$$

By Proposition 2.3 there exists $\widehat{C} \in \mathbb{K}[\mathbf{x}, \mathbf{y}]$ such that

$$f_{iN}(\mathbf{y}) f_{iD}(\mathbf{x}) - f_{iN}(\mathbf{x}) f_{iD}(\mathbf{y}) = D\widehat{C}.$$

On one hand, $D \notin \mathbb{K}[\mathbf{y}]$, then D and H have a non–constant coefficient. On the other hand, $\widehat{C} \notin \mathbb{K}[\mathbf{y}]$, then the non–constant coefficients of D in the ring $\mathbb{K}(\mathbf{x})[\mathbf{y}]$ have smaller degree than deg $(f_i(\mathbf{x}))$. The choice of d assures that the coefficients of H have smaller degree than f_i.

Summarizing, every non–constant coefficient $f \in \mathbb{F}$ of H has smaller degree than the generators, and there is at least one non–constant coefficient. We choose f a non–constant coefficient of H with smallest degree. By Proposition 3.1, $H = \gcd(F_1, \ldots, F_m, F)$, and therefore $\operatorname{lm}(F) = \operatorname{lm}(H)$: Otherwise, as above, there would exist a non–constant coefficient of H with degree less then $\deg(f)$ which is a contradiction.

As we showed before, since $\operatorname{lm}(F) = \operatorname{lm}(H)$, f is a Lüroth's generator and $H = f_N(\mathbf{y}) - f(\mathbf{x}) f_D(\mathbf{y})$. □

The complexity of this algorithm is dominated in the step **C** by computing gcd's of multivariate polynomials, so the algorithm is polynomial in the degree of the rational functions and in n (see von zur Gathen & Gerhard (1999)).

On the other hand, it is interesting to remark that the Lüroth's generator is independent in the field that we are working on, i.e., from the fact that the Lüroth generator can be found with only a gcd computation, we obtain that if f is a Lüroth generator of $\mathbb{K}(f_1, \ldots, f_m)$ then it is also a Lüroth generator of $\mathbb{K}'(f_1, \ldots, f_m)$ for any field extension $\mathbb{K}'$ of $\mathbb{K}$, $\mathbb{K} \subset \mathbb{K}'$.

EXAMPLE 3.1: *Let* $\mathbb{Q}(f_1, f_2) \subset \mathbb{Q}(x, y, z)$ *where*

$$f_1 = \frac{y^2x^4 - 2y^2x^2z + y^2z^2 + x^2 - 2xz + z^2}{yx^3 - yxz - yzx^2 + z^2y}$$

$$f_2 = \frac{y^2x^4 - 2y^2x^2z + y^2z^2}{x^2 - 2xz + yx^3 - yxz + z^2 - yzx^2 + z^2y}.$$

Let

$$F_i = f_{iN}(s, t, u) - f_i(x, y, z) f_{iD}(s, t, u), \quad i = 1, 2.$$

Compute

$$H = \gcd(F_1, F_2) = -tu + s^2 t + \frac{x^2 y - zy}{x - z} u + \frac{-x^2 y + zy}{x - z} s.$$

Then, we can take $f = \dfrac{x^2 y - zy}{x - z}$ *as a Lüroth generator of* $\mathbb{Q}(f_1, f_2)$.

Next comes an interesting characterization of unirational fields with tanscendence degree one over $\mathbb{K}$.

THEOREM 3.1: *Let* $\mathbb{F} = \mathbb{K}(f_1, \ldots, f_m)$ *be a rational field in* $\mathbb{K}(\mathbf{x})$. *Then* $\mathbb{F}$ *has transcendence degree one if and only if* $H = \gcd(F_1, \ldots, F_m) \neq 1$.

Proof: $\boxed{\Longrightarrow}$ If tr.deg.$(\mathbb{F}/\mathbb{K}) = 1$ then there exists $f \in \mathbb{F}$ such that $\mathbb{F} = \mathbb{K}(f)$. By Corollary 2.2 we have $F(\mathbf{y}) = f_N(\mathbf{y}) - f(\mathbf{x}) f_D(\mathbf{y})$ divides F_j, $\forall j$. Thus F divides H, and the greatest common divisor is not a constant.
$\boxed{\Longleftarrow}$ Suppose $H \neq 1$, the above algorithm computes a Lüroth's generator and we are done. □

It is important to highlight that when the field $\mathbb{F}$ contains a non–constant polynomial you can compute a polynomial as a generator, and this generator neither depends on the ground field $\mathbb{K}$.

COROLLARY 3.1: *If the unirational field* $\mathbb{F}$ *contains a non–constant polynomial over* $\mathbb{K}$ *and* tr.deg$(\mathbb{F}/\mathbb{K}) = 1$, *then the algorithm returns a polynomial.*

Proof: By Theorem 1.1 there exists $p \in \mathbb{K}[\mathbf{x}]$ such that $\mathbb{F} = \mathbb{K}(p)$. By Proposition 3.1, $H = p(\mathbf{y}) - p(\mathbf{x})$, (lc$(H) = 1$). □

We have just solved Problem 1. Finally, as consequence of Algorithms 2.1, 3.1 and Corollary 2.3 we are able to solve the following computational problem.

PROBLEM 3: *Given* $f_1, \ldots, f_m \in \mathbb{K}(\mathbf{x})$ *rational functions; compute all rational fields* $\mathbb{E}$ *with* tr.deg$(\mathbb{E}/\mathbb{K}) = 1$ *such that*

$$\mathbb{K}(f_1, \ldots, f_m) \subseteq \mathbb{E} \subseteq \mathbb{K}(\mathbf{x}).$$

There are finite number of them, because the number of non equivalence classes of uni–multivariate rational function are finite.

Acknowledgments

This research is partially supported by Spain Ministerio Ciencia y Tecgnologia Grant Project BFM2001-1294.

References

C. Alonso, J. Gutierrez, T. Recio, A Rational Function decomposition Algorithm by Near–separated Polynomials, *J. Symbolic Comput.*, **19**, 527–544. (1995).

C. Alonso, J. Gutierrez, T. Recio, A note on separated factors of separated polynomials, *J. of Pure and Applied Algebra*, **121**, 217–222. (1997).

J. von zur Gathen, J. Gerhard, *Modern Computer Algebra*, Cambridge University Press, (1999).

J. von zur Gathen, J. Gutierrez, R. Rubio, On multivariate polynomial decomposition, *Computer algebra in scientific computing—CASC'99*, Springer–Verlag, Berlin, 463–478. (1999).

J. Gutierrez, R. Rubio, Reduced Gröbner Basis Under Composition, *J. Symbolic Comput.*, **26**, 433–444. (1998).

J. Gutierrez, R. Rubio, D. Sevilla, Unirational fields of tanscendence degree one and functional decomposition, *Proc. of ISAAC–01. ACM Press*, 167–174. (2001).

J. Klüners, Algorithms for function fields, *(preprint)*, , 1–15. (2000).

S. Lang, *Algebra*, Addison–Wesley, Reading, Mass, (1967).

P. Lüroth, Beweis eines Satzes über rationale Curven, *Mathematische Annalen*, **9**, 163–165. (1876).

J. Müller–Quade, R. Steinwandt, Basic Algorithms for Rational Function Fields, *J. Symbolic Comput.*, **27**, 143–170. (1999).

J. Müller–Quade, R. Steinwandt, Recognizing simple subextensions of pure transcendental field extensions, *AAECC*, **11**, 35–41. (2000).

M. Nagata, Theory of commutative fields, *Translations of Mathematical Monographs*, **125**, American Mathematical Society (1993).

R. Rubio, *Unirational fields. Theorems, algorithms and applications*, PhD. Thesis. Dep. of Mathematics, University of Cantabria, Spain, (2001).

J. Schicho, A note on a theorem of Fried and MacRae, *Arch. Math. (Basel)*, **65**, 3, 239–243. (1995).

A. Schinzel, *Selected topics on polynomials*, Ann Arbor, University of Michigan Press, (1982).

A. Weil, *Foundations of Algebraic Geometry*, AMS, Colloquium Publications, V 29, (1964).

R. Zippel, Rational Function Decomposition, Proc. of ISSAC–91. ACM press, 1–6. (1991).