Unirational Fields of Transcendence Degree One and Functional Decomposition

Jaime Gutierrez, Rosario Rubio and David Sevilla *
Dept. of Mathematics, Statistics and Computation
University of Cantabria
39071 Santander, Spain
{jaime,sarito,sevillad}@matesco.unican.es

ABSTRACT

In this paper we present an algorithm to compute all unirational fields of transcendence degree one containing a given finite set of multivariate rational functions. In particular, we provide an algorithm to decompose a multivariate rational function f of the form $f = g(h)$, where g is a univariate rational function and h a multivariate one.

1. INTRODUCTION

Let $\mathbb{K}$ be an arbitrary field and $\mathbb{K}(\mathbf{x}) = \mathbb{K}(x_1, \ldots, x_n)$ be the rational function field in the variables $\mathbf{x} = (x_1, \ldots, x_n)$. 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 [6]). In the following whenever we talk about "computing an intermediate field" we mean that such finite set of generators is to be calculated. The problem of finding unirational fields is a classical one. In this paper we are looking for unirational fields $\mathbb{F}$ over $\mathbb{K}$ of transcendence degree one over $\mathbb{K}$, $\text{tr.deg}(\mathbb{F}/\mathbb{K}) = 1$.

In the univariate case, the problem can be stated as follows: given univariate rational functions $f_1, \ldots, f_m \in \mathbb{K}(y)$, we wish to know if there exists a proper intermediate field $\mathbb{F}$ such that $\mathbb{K}(f_1, \ldots, f_m) \subset \mathbb{F} \subset \mathbb{K}(y)$; and in the affirmative case, to compute it. By the classical Lüroth theorem (see [14]) the problem is divided in two parts: first to compute f such that $\mathbb{K}(f_1, \ldots, f_m) = \mathbb{K}(f)$, and second to decompose the rational function f, i.e., to find $g, h \in \mathbb{K}(y)$ such that, $\mathbb{F} = \mathbb{K}(h)$ with $f = g(h)$. Constructive proofs of Lüroth's theorem can be found in [7], [12] and [1]. Algorithms for decomposition of univariate rational functions can be found in [17] and [1].

In the multivariate case, the problem is: given $f_1, \ldots, f_m$ in $\mathbb{K}(\mathbf{x})$ we wish to know if there exists a proper intermediate field $\mathbb{F}$ such that $\mathbb{K}(f_1, \ldots, f_m) \subset \mathbb{F} \subset \mathbb{K}(\mathbf{x})$ with $\text{tr.deg}(\mathbb{F}/\mathbb{K}) = 1$; and in the affirmative case, to compute it. A central result is the following generalization of Lüroth's theorem:

Theorem 1 (Extended Lüroth's Theorem). *Let $\mathbb{F}$ be a field such that $\mathbb{K} \subset \mathbb{F} \subset \mathbb{K}(\mathbf{x})$. If $\text{tr.deg}(\mathbb{F}/\mathbb{K}) = 1$, then there exists $f \in \mathbb{K}(\mathbf{x})$ such that $\mathbb{F} = \mathbb{K}(f)$.*

Such an f is called a Lüroth's generator of the field $\mathbb{F}$. This theorem was first proved in [2] for characteristic zero and in [4] in general, see also [11] Theorem 3. Using Gröbner basis computation, the paper [5] provides an algorithm to compute a Lüroth's generator, if it exits. See also [9] for another algorithmic proof of this result. In this paper we present a new algorithm, which only requires to compute gcd's, to detect if a unirational field has transcendence degree 1 and, in the affirmative case, to compute a Lüroth's generator. We also present a constructive proof of the above theorem for polynomials (see [8]): if the unirational field contains a non-constant polynomial, then it is generated by a polynomial.

By the Extended Lüroth's theorem, to find an intermediate field of transcendence degree one is equivalent to the following: first to find a Lüroth's generator f, i.e., $\mathbb{K}(f_1, \ldots, f_m) = \mathbb{K}(f)$, if it exists, and second to decompose the multivariate rational function f, i.e., to find $g \in \mathbb{K}(y)$ and $h \in \mathbb{K}(\mathbf{x})$ such that $f = g(h)$ in a nontrivial way. The pair (g, h) is called a uni–multivariate decomposition of f. We present two algorithms to compute a nontrivial uni–multivariate decomposition of a multivariate rational function, if it exits.

This paper is divided in four sections. In section 2 we state the proof of the Extended Lüroth's theorem and its polynomial version. In section 3 we present and analyze two algorithms to compute a uni–multivariate decomposition of a rational function, if it exists. In section 4 we discuss the performance of these algorithms.

2. THE EXTENDED LÜROTH THEOREM

In this section we present an algorithm to the following computational problem: given $f_1, \ldots, f_m \in \mathbb{K}(\mathbf{x})$, to compute a Lüroth generator f for $\mathbb{F} = \mathbb{K}(f_1, \ldots, f_m)$ if it exists, moreover we detect if $\mathbb{F}$ contains a non-constant polynomial, and in the affirmative case we find a generating polynomial. We start with the following definition:

*This work is partially supported by Spanish DGES Grant Project PB97–0346

ISSAC 2001, UWO, Canada
©2001 ACM 1-58113-218-2/ 00/ 0008 $5.00

DEFINITION 1. *Let $p \in \mathbb{K}[x_1,\dots,x_n,y_1,\dots,y_n] = \mathbb{K}[\mathbf{x},\mathbf{y}]$ be a non–constant polynomial. We say that p is* **near–separated** *if there exist non–constant polynomials $r_1, s_1 \in \mathbf{K}[\mathbf{x}] = \mathbb{K}[x_1,\dots,x_n]$ and $r_2, s_2 \in \mathbf{K}[\mathbf{y}] = \mathbb{K}[y_1,\dots,y_n]$, 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 when $p = r(x_1,\dots,x_n)s(y_1,\dots,y_n) - s(x_1,\dots,x_n)r(y_1,\dots,y_n)$, we say that p is a* **symmetric near–separated** *polynomial. We say that (r,s) is a* **symmetric near–separated representation** *of p.*

In this paper, $\deg_{x_1,\dots,x_n}$ will denote the total degree with respect to the variables $x_1,\dots,x_n$ and deg will denote the total degree with respect to all the variables. Also, given a rational function f we will also de note as f_n, f_d the numerator and denominator of f, respectively.

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

THEOREM 2. *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) *$\deg_{x_1,\dots,x_n} p = \max\{\deg r_1, \deg s_1\}$ and $\deg_{y_1,\dots,y_n} p = max\{\deg r_2, \deg s_2\}$.*

(iii) *If p is symmetric and $(\alpha_1,\dots,\alpha_n) \in \mathbb{K}^n$ verifies $p(x_1,\dots,x_n,\alpha_1,\dots,\alpha_n) \neq 0$, then there exists (r,s), a symmetric near–separated representation of p, such that*

$$r(\alpha_1,\dots,\alpha_n) = 0 \quad \text{and} \quad s(\alpha_1,\dots,\alpha_n) = 1.$$

(iv) *If p is symmetric, the coefficient of $x_k^{i_0} y_k^{j_0}$ in p is the near–separated polynomial*

$$a_{i_0}\, b_{j_0} - b_{i_0}\, a_{j_0},$$

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 $v \in \mathbb{K}[x_1,\dots,x_n]$ 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 $\mathbb{K}[x_2,\dots,x_n]$. 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,

$$\frac{r_1(\alpha, x_2,\dots,x_n)}{s_1(\alpha, x_2,\dots,x_n)} = \frac{r_2(y_1,\dots,y_n)}{s_2(y_1,\dots,y_n)} \in \mathbb{K}.$$

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 $\deg r_1 = \deg s_1 > \deg_{x_1,\dots,x_n} p$, the terms with greatest degree with respect to $x_1,\dots,x_n$ vanish. This is a contradiction, because r_2, s_2 are not associated. The proof is the same for r_2, s_2.

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

– If $r(\alpha_1,\dots,\alpha_n) = 0$, since $p(x_1,\dots,x_n,\alpha_1,\dots,\alpha_n) \neq 0$, we have $s(\alpha_1,\dots,\alpha_n) \neq 0$. Then we have a new near–separated representation:

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

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

– If $r(\alpha_1,\dots,\alpha_n), s(\alpha_1,\dots,\alpha_n) \neq 0$, then we consider the representation

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

(iv) This is a simple routine confirmation. □

Now, we state an important theorem that relates uni–multivariate decompositions to near–separated polynomials, that is proved in [10]:

THEOREM 3. *Let $\mathbb{A} = \mathbb{K}(\mathbf{x})$ and $\mathbb{B} = \mathbb{K}(\mathbf{y})$ be rational function fields over $\mathbb{K}$. Let $f, h \in \mathbb{A}$ and $f', h' \in \mathbb{B}$ 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 $\mathbb{A} \otimes_{\mathbb{K}} \mathbb{B}$.*

As a consequence, a rational function $f \in \mathbb{K}(\mathbf{x})$ verifies $f = g(h)$ for some g, h if and only if $h_n(\mathbf{x})\, h_d(\mathbf{y}) - h_d(\mathbf{x})\, h_n(\mathbf{y})$ divides $f_n(\mathbf{x})\, f_d(\mathbf{y}) - f_d(\mathbf{x})\, f_n(\mathbf{y})$.

Given an admissible monomial ordering $>$ in a polynomial ring and a nonzero polynomial G in that ring, we denote by $\operatorname{lm} G$ the leading monomial of G with respect to $>$ and $\operatorname{lc} G$ its leading coefficient.

ALGORITHM 1.

Input: $f_1,\dots,f_m \in \mathbb{K}(\mathbf{x})$.

Output: *$f \in \mathbb{K}(\mathbf{x})$ such that $\mathbb{K}(f) = \mathbb{F} = \mathbb{K}(f_1,\dots,f_m)$, if it exists. Otherwise, returns null.*

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

B *Let $F_k = f_{k_n}(\mathbf{y}) - f_k(\mathbf{x}) f_{k_d}(\mathbf{y})$ for $k = 1,\dots,i$.*

C *Compute $H_i = \gcd(\{F_k,\ k = 1,\dots,i\})$ with $\operatorname{lc} H_i = 1$.*

D – *If $H_i = 1$,* ***RETURN NULL*** *($\mathbb{F}$ does not have transcendence degree 1 over $\mathbb{K}$).*

– *If there exists $j \in \{1,\dots,i\}$ such that $\operatorname{lm} H_i = \operatorname{lm} F_j$, then* ***RETURN*** *$f_j$.*

– *Otherwise, let f_{i+1} be a coefficient of H_i in $\mathbb{F} \setminus \mathbb{K}$. Increase i and go to* ***B****.*

Correctness proof. If $\mathbb{F}$ has transcendence degree 1 over $\mathbb{K}$, we can write $\mathbb{F} = \mathbb{K}(f)$. By Theorem 3,

$$f_n(\mathbf{y}) - f(\mathbf{x})f_d(\mathbf{y})$$

divides H_i for any i. Therefore, H_i is non–constant if a Lüroth generator exists.

If there are i, j such that lm $H_i =$ lm F_j, then F_j is a greatest common divisor of $\{F_k, k = 1, \dots, i\}$. Therefore, F_j divides F_k for every k. Fix such a k. Let $q = \overline{f_{k_n}(\mathbf{y})}^{\{F_j\}}$, $s = \overline{f_{k_d}(\mathbf{y})}^{\{F_j\}}$ the normal form with respect to the monomial ordering $>$; then there exist $p, q, r, s \in \mathbb{F}[\mathbf{y}]$ such that

$$\begin{array}{l} f_{j_n}(\mathbf{y}) = p(\mathbf{y})F_i - q(\mathbf{y}) \\ f_{j_d}(\mathbf{y}) = r(\mathbf{y})F_i - s(\mathbf{y}) \end{array}$$

where lm F_j does not divide any monomial of q or s. By theorem 2(i), $q, s \neq 0$. By the definition in step B,

$$F_k = F_j(p - r\, f_k(\mathbf{x})) - (q - s\, f_k(\mathbf{x})).$$

Hence F_j divides $q - s\, f_k(x_1, \dots, x_n)$ and we conclude that $q - s\, f_k(\mathbf{x}) = 0$, since otherwise we would get that lm F_j divides lm $(q - s\, f_k(x_1, \dots, x_n))$, which contradicts the choice of the polynomials q, s. Thus $f_k(x_1, \dots, x_n) = \frac{q}{s} \in \mathbb{F} = \mathbb{K}(f_j)$.

Now we suppose that lm $H_i <$ lm F_k for all k. Again, fix a value for k. Then there exists a $C \in \mathbb{F}[\mathbf{y}] \setminus \mathbb{F}$ such that $F_k = H_i C$. Let d, α be the lowest common multiples of the denominators of the coefficients of H_i and C, respectively. Then $D = H_i d, C' = \alpha C \in \mathbb{K}[\mathbf{x}, \mathbf{y}]$. Since H_i is monic, the polynomial D is primitive. Then,

$$f_{k_n}(\mathbf{y})\, f_{k_d}(\mathbf{x}) - f_{k_n}(\mathbf{x})\, f_{k_d}(\mathbf{y}) = \frac{D}{d}\,\frac{C'}{\alpha}\, f_{k_d}$$

and by theorem 2,

$$f_{k_n}(\mathbf{y})\, f_{k_d}(\mathbf{x}) - f_{k_n}(\mathbf{x})\, f_{k_d}(\mathbf{y}) = D\widehat{C},$$

$\widehat{C} \in \mathbb{K}[\mathbf{x}, \mathbf{y}]$. On one hand, $D \notin \mathbb{K}[\mathbf{y}]$, thus D (and H_i) 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 that of $f_k(\mathbf{x})$. The choice of d assures that the coefficients of H have smaller degree than f_k. Summarizing, there exists a coefficient $a \in \mathbb{F}$ of H_i that can be added to the list of generators and has smaller degree than them. If tr.deg $(\mathbb{F}/\mathbb{K}) = 1$, H_i is non–constant for all i, and the generator has smaller degree than the others. Therefore, the algorithm ends in a finite number of steps.

Finally, we note that complexity 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 [16]).

From the fact that the Lüroth generator can be found with only some gcd computations, we obtain that if f is a Lüroth generator of $\mathbb{K}(f_1, \dots, f_n)$ then it is also a Lüroth generator of $\mathbb{K}'(f_1, \dots, f_n)$ for any field extension $\mathbb{K}'$ of $\mathbb{K}$, $\mathbb{K} \subset \mathbb{K}'$.

EXAMPLE 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

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

Compute

$$H_2 = \gcd(F_1, F_2) = -tu + s^2t + \frac{x^2y - zy}{x - z}u + \frac{-x^2y + zy}{x - z}s.$$

Since lm $H_2 <$ lm F_i *with respect to the lexicographical ordering* $s > t > u$*, we take a non–constant coefficient of* H_2*:* $f_3 = \frac{x^2y - zy}{x - z}$*. Now*

$$H_3 = -tu + s^2t + \frac{x^2y - zy}{x - z}u + \frac{-x^2y + zy}{x - z}s$$

and $H_3 = F_3$*, since* $H_3 = H_2$*. The algorithm returns* f_3*, a Lüroth generator of* $\mathbb{Q}(f_1, f_2)$*.*

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 $\mathbb{K}$. This result was proved in [8], for zero characteristic. A general proof can be found in [11].

ALGORITHM 2.

Input: $f_1, \dots, f_m \in \mathbb{K}(\mathbf{x})$.

Output: $f \in \mathbb{K}[\mathbf{x}]$ *such that* $\mathbb{K}(f) = \mathbb{F} = \mathbb{K}(f_1, \dots, f_m)$*, if it exists. Otherwise, returns null.*

A *Compute a Lüroth generator* f *of* $\mathbb{K}(f_1, \dots, f_m)$ *using Algorithm 1.*

B *Let* s *be the degree of* f'*.*

- *If* $s >$ deg f'_n *and* f'_n *is not constant, return null. Otherwise, let* $f = 1/f'$*.*
- *If* $s >$ deg f'_d *and* f'_d *is not constant, return null. Otherwise, let* $f = f'$*.*
- *Let* ${f_n^{(s)}}', {f_d^{(s)}}'$ *be the homogeneous components of degree* s *of* f'_n, f'_d*, respectively. Let* $a = \frac{{f_n^{(s)}}'}{{f_d^{(s)}}'}$*. If* a *or* $f'_n - af'_d$ *are not constant, return null. Otherwise, let* $f = \frac{1}{y - a} \circ f'$*.*

Correctness proof. Once a Lüroth's generator has been computed, take a generator f with degree m such that if $f = \frac{f_n}{f_d}$ and

$$\begin{array}{ll} f_n & = f_n^{(s)} + \cdots + f_n^{(0)}, \\ f_d & = f_d^{(s)} + \cdots + f_d^{(0)}, \end{array}$$

the sum in homogeneous polynomials, then either $f_d^{(s)} = 0$ or $\dfrac{f_n^{(s)}}{f_d^{(s)}} \notin \mathbb{K}$.

If $p \in \mathbb{K}(f)$ is a polynomial, then there exists $g \in \mathbb{K}(y)$ with degree r such that $p = g(f)$. If $g = \dfrac{a_r y^r + \cdots + a_0}{b_r y^r + \cdots + b_0}$,

$$\begin{aligned} p &= \frac{a_r f_n^r + \cdots + a_0 f_d^r}{b_r f_n^r + \cdots + b_0 f_d^r} \\ &= \frac{a_r (f_n^{(s)} + \cdots + f_n^{(0)})^r + \cdots + a_0 (f_d^{(s)} + \cdots + f_d^{(0)})^r}{b_r (f_n^{(s)} + \cdots + f_n^{(0)})^r + \cdots + b_0 (f_d^{(s)} + \cdots + f_d^{(0)})^r}. \end{aligned}$$

Since p is a polynomial, the degree of the previous denominator is smaller than the degree of the numerator. Therefore $b_r {f_n^{(s)}}^r + \cdots + b_0 {f_d^{(s)}}^r = 0$.

If $f_d^{(s)} = 0$ then $b_r = 0$ and $p = \dfrac{a_r f_n^r + \cdots + a_0 f_d^r}{f_d (b_{r-1} f_n^{r-1} + \cdots + b_0 f_d^{r-1})}$. Hence f_d divides the numerator of p, and therefore divides f_n. This proves that f is a polynomial.

If, on the contrary, $f_d^{(s)} \neq 0$, $g_d \left(\dfrac{f_n^{(s)}}{f_d^{(s)}} \right) = 0$. Contradiction, since $\dfrac{f_n^{(s)}}{f_d^{(s)}} \notin \mathbb{K}$.

3. TWO UNI–MULTIVARIATE DECOMPOSITION ALGORITHMS

We define the **degree** of a rational function $f = f_n/f_d \in \mathbb{K}(\mathbf{x})$ as deg f = max {deg f_n, deg f_d} if $\gcd(f_n, f_d) = 1$. The following definition was introduced in [15] for polynomials.

DEFINITION 2. *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 is uni-multivariate decomposable if there exits a non-trivial decomposition.*

If f is a polynomial having a nontrivial uni-multivariate decomposition, then by Algorithm 2 we get that there exits a uni-multivariate decomposition (g, h) with g and h polynomials. The paper [15] provides an algorithm to compute a nontrivial uni-multivariate decomposition of a polynomial f of degree m that only requires $O(nm(m+1)^n \log\, m)$ arithmetic operations in the ground field $\mathbb{K}$.

The known techniques for decomposition all divide the problem into two parts. Given f, in order to find a decomposition $f = g(h)$,

1. one first computes candidates h,
2. then computes g given h.

Determining g from f and h is a subfield membership problem. The paper [13] gives a solution to this part. We also present another faster method, that only requires solving a linear system of equations. Usually, the harder step is to find candidates for h. One goal in decomposition is to have components of smaller degree than the composed polynomial. This will be the case here.

3.1 Preliminary results

First, we state some results that will be used in the algorithms presented later. On the properties to highlight out of uni-multivariate decomposition is the good behaviour of the degree with respect to this composition.

THEOREM 4. *Let $g \in \mathbb{K}(y)$ and $h \in \mathbb{K}(\mathbf{x})$, and $f = g(h)$. Then* deg f = deg $g \cdot$ deg h.

PROOF. Let $g = \dfrac{g_n}{g_d}$ and $h = \dfrac{h_n}{h_d}$ with $\gcd(g_n, g_d) = 1$ and $\gcd(h_n, h_d) = 1$. Then there exist polynomials $A, B \in \mathbb{K}[y]$ such that

$$g_n(y)\, A(y) + g_d(y)\, B(y) = 1.$$

Homogenizing the polynomials g_n, g_d, A, B we obtain, respectively, the bivariate polynomials $\widetilde{g}_n(y_1, y_2), \widetilde{g}_d(y_1, y_2), \widetilde{A}(y_1, y_2), \widetilde{B}(y_1, y_2)$ verifying

$$\widetilde{g}_n(y_1, y_2)\, \widetilde{A}(y_1, y_2)\, y_2^u + \widetilde{g}_d(y_1, y_2)\, \widetilde{B}(y_1, y_2)\, y_2^v = y_2^w$$

with either $u = 0$ or $v = 0$ and $w = \max\{u, v\}$. Therefore,

$$\widetilde{g}_n(h_n, h_d)\, \widetilde{A}(h_n, h_d)\, h_d^u + \widetilde{g}_d(h_n, h_d)\, \widetilde{B}(h_n, h_d)\, h_d^v = h_d^w.$$

If d is an irreducible factor of $\gcd(\widetilde{g}_n(h_n, h_d), \widetilde{g}_d(h_n, h_d))$, then d divides h_d. On the other hand, d divides $\widetilde{g}_n(h_n, h_d)$ and $\widetilde{g}_d(h_n, h_d)$; this implies that d divides h_n. As a consequence, $\gcd(\widetilde{g}_n(h_n, h_d), \widetilde{g}_d(h_n, h_d)) = 1$. So,

$$f = \frac{\widetilde{g}_n(h_n, h_d)}{\widetilde{g}_d(h_n, h_d)}\, h_d^a\,,\ |a| = |\text{deg } h_n - \text{deg } h_d|$$

is in reduced form. Without loss of generality, we can take deg $g_n = r_n \geq r_d =$deg g_d with

$$\begin{aligned} g_n(y) &= a_{r_n}\, y^{r_n} + \cdots + a_0 \\ g_d(y) &= b_{r_d}\, y^{r_d} + \cdots + b_0. \end{aligned}$$

Then, deg f = max {deg $\widetilde{g}_n(h_n, h_d)$, deg $\widetilde{g}_d(h_n, h_d)\, h_d^{r_n - r_d}$} and

$$\begin{aligned} \widetilde{g}_n(h_n, h_d) &= a_{r_n} h_n^{r_n} + \cdots + a_0 h_d^{r_n} \\ \widetilde{g}_d(h_n, h_d) &= b_{r_d} h_n^{r_d} + \cdots + b_0 h_d^{r_d}. \end{aligned}$$

If deg $\widetilde{g}_n(h_n, h_d) = r_n$ deg h, we immediately obtain that deg f = deg g deg h. If deg $\widetilde{g}_n(h_n, h_d) < r_n$deg h, then $s =$ deg h_n = deg h_d. Write

$$\begin{aligned} h_n &= h_n^{(s)} + h_n^{(s-1)} + \cdots + h_n^{(0)} \\ h_d &= h_d^{(s)} + h_d^{(s-1)} + \cdots + h_d^{(0)} \end{aligned}$$

where $h_n^{(j)}, h_d^{(j)}$ are the homogeneous components of h_n and h_d with degree j, respectively. Since the degree decreases, deg $\widetilde{g}_n(h_n^{(s)}, h_d^{(s)}) = 0$ and deg $\widetilde{g}_n \left(\dfrac{h_n^{(s)}}{h_d^{(s)}} \right) = 0$. Therefore, $\dfrac{h_n^{(s)}}{h_d^{(s)}} \in \mathbb{K}$. In this case, you can take $h' \in \mathbb{K}(\mathbf{x})$ a rational function with deg h = degh', deg $h'_n \neq$ deg h'_d and such that $f = g'(h')$ for some $g' \in \mathbb{K}(y)$ with deg g = deg g'. Under these hypothesis, we proved before that deg f = deg g' deg h' = deg g deg h. □

COROLLARY 1. *Let $g = g_n/g_d$ with $g_n = a_u y^u + \cdots + a_0$, $g_d = b_v y^v + \cdots + b_0$ and $h = h_n/h_d$ verifying* $\gcd(g_n, g_d) = \gcd(h_n, h_d) = 1$. *If $f = f_n/f_d = g(h)$ with*

$$f_n = (a_u\, h_n^u + \cdots + a_0\, h_d^u)\, h_d^{\max\{v-u,0\}}$$
$$f_d = (b_v\, h_n^v + \cdots + b_0\, h_d^v)\, h_d^{\max\{u-v,0\}}$$

then $\gcd(f_n, f_d) = 1$.

PROOF. It is easy to prove that

$$\deg\, f_n, \deg\, f_d \le \max\{u, v\} \cdot \max\{\deg\, h_n, \deg\, h_d\}.$$

If $\gcd(f_n, f_d) \neq 1$, then $\deg\, f < \deg\, g \deg\, h$, contradicting theorem 4. $\square$

COROLLARY 2. *Given f and h, if there exists g such that $f = g(h)$, then g 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 theorem 4, $\deg\, (g_1 - g_2) = 0$, thus $g_1 - g_2$ is constant. It is then clear that it must be 0, that is, $g_1 = g_2$. Again by theorem 4, 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. Equating to zero the coefficients of the numerator of $f - g(h)$, we obtain a linear homogeneous system of equations in the coefficients of g. If we compute a non–trivial solution to this system, we find g. $\square$

DEFINITION 3. *Let $f \in \mathbb{K}(\mathbf{x})$ be a rational function. Two uni–multivariate decompositions (g, h) and (g', h') of f are* **equivalent** *if there exists a composition unit $l \in \mathbb{K}(y)$, i.e., $\deg\, l = 1$, such that $h = l(h')$.*

COROLLARY 3. *Let $f \in \mathbb{K}(\mathbf{x})$ be a non–constant rational function. Then the equivalence classes of 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

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

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 $\mathbb{K}$. Also, if (g', h') is equivalent to (g, h), $h = l(h')$ for some composition unit $l \in \mathbb{K}(y)$. Consequently, $h' = l^{-1}(h)$ and $\mathbb{K}(h) = \mathbb{K}(h')$. Let (g, h) and (g', h') be two uni–multivariate decompositions of f such that $\mathbb{K}(h) = \mathbb{K}(h')$. Then there exists rational functions $l, l' \in \mathbb{K}(y)$ such that $h = l(h')$ and $h' = l'(h)$. By theorem 4, $\deg\, l(l') = 1$ and $\deg\, l = \deg\, l' = 1$. By the uniqueness (see Corollary 2) of the left component, $y = l(l')$. So, $l \in \mathbb{K}(y)$ is a composition unit and (g, h), (g', h') are equivalent. By Theorem 1, there exist $h \in \mathbb{K}(\mathbf{x})$ and $g \in \mathbb{K}(y)$ such that $\mathbb{F} = \mathbb{K}(h)$ and $f = g(h)$. $\square$

3.2 First algorithm

We now proceed with the first algorithm for computing candidates $h = h_n/h_d$. This algorithm is based on Theorem 3. Since $h_n(\mathbf{x})\, h_d(\mathbf{y}) - h_d(\mathbf{x})\, h_n(\mathbf{y})$ divides $f_n(\mathbf{x})\, f_d(\mathbf{y}) - f_d(\mathbf{x}) f_n(\mathbf{y})$, one can compute candidates for h from f merely looking at the near-separated divisors $H = r(\mathbf{x})\, s(\mathbf{y}) - r(\mathbf{y}) s(\mathbf{x})$. Next, the problem is: given a multivariate polynomial $H = (\mathbf{x}, \mathbf{y})$, how can one determine if it is a symmetric near-separated polynomial? This is a consequence of theorem 2:

COROLLARY 4. *Given a polynomial $p \in \mathbb{K}[\mathbf{x}, \mathbf{y}]$, it is possible to find a near–separated representation $(r, s) \in \mathbb{K}[\mathbf{x}]^2$ of p, if it exists, by solving a linear system of equations with coefficients in $\mathbb{K}$. Moreover, any other solution (r', s') of this linear system of equations gives an equivalent decomposition.*

ALGORITHM 3.

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

Output: *A uni–multivariate decomposition (g, h) of f, if it exists.*

A *Factor the symmetric polynomial*

$$p = f_n(\mathbf{x})\, f_d(\mathbf{y}) - f_d(\mathbf{x})\, f_n(\mathbf{y}).$$

Let $D = \{H_1, \ldots, H_m\}$ the set of factors of p (up to product by constants). Let $i = 1$.

B *Check if H_i is a symmetric near–separated polynomial. If $H = r(\mathbf{x})\, s(\mathbf{y}) - r(\mathbf{y})\, s(\mathbf{x})$, then $h = \dfrac{r}{s}$ is a right–component for f; compute the left component g by solving a linear system (see Corollary 2) and* ***RETURN*** *(g, h).*

C *If $i < m$, then increase i and go to* ***B***. *Otherwise,* ***RETURN NULL*** *(f is uni–multivariate indecomposable).*

EXAMPLE 2. *Let*

$$\begin{aligned} f \;=\; & 4z^4y^2 - 8z^3y^3 + 8z^2yx + 4z^2y^4 - 8zy^2x \\ & +4x^2 - 2z^2y + 2zy^2 - 2x + 10. \end{aligned}$$

The factorization of the polynomial $f(x, y, z) - f(s, t, u)$ is

$$\begin{aligned} & 2\left(2x - 1 + 2s - 2ut^2 + 2u^2t - 2zy^2 + 2z^2y\right) \\ & \left(x - s + z^2y - zy^2 - u^2t + ut^2\right). \end{aligned}$$

The first factor $f_1 = 2x - 1 + 2s - 2ut^2 + 2u^2t - 2zy^2 + 2z^2y$ is not symmetric near–separated because $f_1(x, y, z, x, y, z) \neq 0$. On the other hand, the second factor $f_2 = x - s + z^2y - zy^2 - u^2t + ut^2$ does satisfy $f_2(x, y, z, x, y, z) = 0$. Note that by a previous remark, the components of the decomposition can be considered as polynomials. Then f_2 can be written as $f_2 = h(x, y, z) - h(s, t, u)$. Taking $h(x, y, z) = f_2(x, y, z, 0, 0, 0) = x + z^2y - zy^2$, we check that it satisfies the previous equation (see theorem 2). The left component g is also a polynomial, and by theorem 4, has degree 2. Solving the equation $f = g(h)$ we have the multi–univariate decomposition:

$$(4t^2 - 2t + 10, x + z^2y - zy^2).$$

EXAMPLE 3. *Let $f = \dfrac{f_n}{f_d}$ with*

$$\begin{aligned} f_n \;=\; & y^2x^2 + 2x^2yz^2 - 2y^6x + z^4x^2 - 2z^2xy^5 + y^{10} \\ & -81x^2 - 450xyz - 625y^2z^2, \\ f_d \;=\; & y^2x^2 + 2x^2yz^2 - 2y^6x + z^4x^2 - 2z^2xy^5 + y^{10} \\ & -162x^2 - 900xyz - 1250y^2z^2. \end{aligned}$$

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 will 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

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

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

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

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

We check that f_2 is symmetric near–separated, by solving a linear system of equations. Define

$$\begin{aligned} f_2(x,y,z,1,0,0) = r(x,y,z) &= -\frac{9}{25}xz^2 - \frac{9}{25}xy + \frac{9}{25}y^5 \\ &= \left(-\frac{9}{25}z^2 - \frac{9}{25}y\right)x + \frac{9}{25}y^5 \end{aligned}$$

Next, we compute $s_0(y,z)$ such that

$$\frac{9}{25}y^5 s_0(t,u) - \frac{9}{25}t^5 s_0(y,z) = -zt^5y + uty^5.$$

Let $s_0(y,z) = a_5(z)\,y^5 + \cdots + a_0(z)$. Then $a_1 = \frac{25}{9}z$ and $a_0 = a_2 = a_3 = a_4 = a_5 = 0$. Hence, $s_0 = \frac{25}{9}zy$ and $s_1(y,z) = \dfrac{r_1(y,z)\,s_0(t,u) - c_{10}}{r_0(t,u)} = 1$. Thus $s = x + \frac{25}{9}zy$, $s(1,0,0) = 1$ and (r,s) is a symmetric near–separated representation of p:

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

Now we compute g, which is a univariate function with degree 2. Solving the corresponding linear system of equations we obtain

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

3.3 Second algorithm

For this algorithm, we suppose that $\mathbb{K}$ has sufficiently many elements. If it is not the case, then we can decompose f in an algebraic extension $\mathbb{K}[\omega]$ of $\mathbb{K}$, and then check if it is equivalent to a decomposition with coefficients in $\mathbb{K}$; this last step can be done by solving a system of linear equations in the same fashion as the computation of g. The algorithm is based on Corollary 1; we will need several technical results too.

LEMMA 1. *Let $f \in \mathbb{K}(\mathbf{x})$. Then for any admissible monomial ordering $>$ there are units $u \in \mathbb{K}(y)$, $v_i \in \mathbb{K}(x_i)$, $i = 1,\ldots,n$ such that, if $\overline{f} = \overline{f}_n / \overline{f}_d = u \circ f(v_1,\ldots,v_n)$, then $\text{lm } \overline{f}_n > \text{lm } \overline{f}_d$, $\overline{f}_n(0,\ldots,0) = 0$ and $\overline{f}_d(0,\ldots,0) \neq 0$.*

PROOF. Let $>$ be any admissible monomial ordering. Let $u_1 \in \mathbb{K}(y)$ be a unit such that $f_1 = f_{1n} / f_{1d} = u_1(f)$ verifies $\text{lm } f_{1n} > \text{lm } f_{1d}$. Such a unit always exists:

– If $\text{lm } f_n < \text{lm } f_d$, let $u_1 = 1/y$.

– If $\text{lm } f_n = \text{lm } f_d$, let $u_1 = (1/y) \circ (y - \dfrac{\text{lc } f_n}{\text{lc } f_d})$.

– If $\text{lm } f_n > \text{lm } f_d$, let $u_1 = y$.

Let $\underline{\alpha} = (\alpha_1,\ldots,\alpha_n) \in \mathbb{K}^n$ such that $f_{1d}(\underline{\alpha}) \neq 0$ (such a α exists if $\mathbb{K}$ has sufficiently many elements). Let $v_i = x_i + \alpha_i$, $i = 1,\ldots,n$ and $f_2 = f_{2n}/f_{2d} = f_1(v_1,\ldots,v_n)$. Then $f_{2d}(0,\ldots,0) \neq 0$, and we can take

$$u = y - \frac{f_{2n}(0,\ldots,0)}{f_{2d}(0,\ldots,0)}$$

so that $\overline{f} = u \circ f(v_1,\ldots,v_n)$ verifies all the conditions. □

LEMMA 2. *Let $i,j,k \in \mathbb{N}$ with $i < j \leq k$, $P, Q \in \mathbb{K}[\underline{x}]$ and $>$ an admissible monomial ordering such that $\text{lm } P > \text{lm } Q$. Then $\text{lm } P^jQ^{k-j} > \text{lm } P^iQ^{k-i}$.*

LEMMA 3. *Let $\overline{f} = \overline{f}_n/\overline{f}_d \in \mathbb{K}(\mathbf{x})$ such that $\text{lm } \overline{f}_n > \text{lm } \overline{f}_d$, $\overline{f}_n(0,\ldots,0) = 0$ and $\overline{f}_d(0,\ldots,0) \neq 0$. Then, for every uni–multivariate decomposition $\overline{f} = g(h)$ there exists an equivalent decomposition $\overline{f} = \overline{g}(\overline{h})$ with $\overline{g} = \overline{g}_n/\overline{g}_d, \deg \overline{g}_n > \deg \overline{g}_d$ and $\overline{g}_n(0) = 0$ (thus $\overline{g}_d(0) \neq 0$).*

PROOF. As in the proof of Lemma 1, there exists a unit u_1 such that if $h_1 = u(h) = h_{1n}/h_{1d}$, then $h_{1n}(0,\ldots,0) = 0$. Let $g_1 = g(u^{-1}) = (a_uy^u + \cdots + a_0)/(b_vy^v + \cdots + b_0)$. Then

$$\overline{f} = \frac{a_uh_{1n}^u + \cdots + a_0h_{1d}^u}{b_vh_{1n}^v + \cdots + b_0h_{1d}^v}h_{1d}^{v-u}$$

and by Corollary 1, $\overline{f}_d = (b_vh_{1n}^v + \cdots + b_0h_{1d}^v)h_{1d}^{max\{u-v,0\}}$. As $\overline{f}_d(0,\ldots,0) \neq 0$ and $h_{1n}(0,\ldots,0) = 0$ we must have $h_{1d}(0,\ldots,0) \neq 0$. But $\overline{f}_n(0,\ldots,0) = 0$ and $\overline{f}_n = (a_uh_{1n}^u + \cdots + a_0h_{1d}^u)h_{1d}^{max\{v-u,0\}}$, thus $a_0 = 0$. Next, we will prove that there is an equivalent decomposition verifying the condition on the degrees of the left–component. To that end, we will consider three cases. Let $>$ be any admissible monomial ordering and $w = \deg g_1 = \max\{u,v\}$.

– If $\text{lm } h_{1n} < \text{lm } h_{1d}$ then using repeatedly Lemma 2,

$$\text{lm } \overline{f}_n = \text{lm } h_{1n}h_{1d}^{w-1} < \text{lm } h_{1d}^w = \text{lm } \overline{f}_d$$

which contradicts our hypothesis.

– If $\text{lm } h_{1n} > \text{lm } h_{1d}$, then applying Lemma 2,

$$\begin{aligned} \text{lm } \overline{f}_n &= \text{lm } h_{1n}^uh_{1d}^{max\{v-u,0\}} \\ \text{lm } \overline{f}_d &= \text{lm} h_{1n}^vh_{1d}^{max\{u-v,0\}}. \end{aligned}$$

As $\text{lm } \overline{f}_n > \text{lm } \overline{f}_d$ by hypothesis, by Lemma 2 again we must have $u > v$, that is, $\deg g_{1n} > \deg g_{1d}$.

– If $\text{lm } h_{1n} = \text{lm } h_{1d}$ then, as in Lemma 1, we can cancel the leading monomial of h_{1d} with a unit u_2 on the left, so that $\overline{f} = g_2(h_2)$ with $\text{lm } h_{2n} > \text{lm } h_{2d}$ which is the previous case.

□

Let $f = g(h)$ be a uni–multivariate decomposition of f with $f = f_n/f_d, g = (a_uy^u + \cdots + a_0)/(b_vy^v + \cdots + b_0)$ and

$h = h_n/h_d$. By the previous lemma, we can suppose $u > v$ and $g(0) = 0$, i.e. $a_0 = 0$. Then, as

$$f = \frac{a_u h_n^u + \cdots + a_1 h_n h_d^{u-1}}{(b_v h_n^v + \cdots + b_0 h_d^v) h_d^{u-v}}$$

we have that $h_n \mid f_n$ and $h_d \mid f_d$. This is the key to the following algorithm.

ALGORITHM 4.

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

Output: (g, h) *a uni–multivariate decomposition of f, if it exists.*

A *Compute $u, v_1, \ldots, v_n$ as in Lemma 1. Let*

$$\overline{f} = \overline{f}_n/\overline{f}_d = u \circ f(v_1, \ldots, v_n)$$

B *Factor $\overline{f}_n$ and $\overline{f}_d$. Let $D = \{(A_1, B_1), \ldots, (A_m, B_m)\}$ be the set of pairs (A, B) such that A, B divide $\overline{f}_n, \overline{f}_d$ respectively (up to product by constants). Let $i = 1$.*

C *Check if there exists $g \in \mathbb{K}(y)$ with $\overline{f} = g(A_i/B_i)$; if such a g exists,* ***RETURN*** $\left(u^{-1}(g), h(v_1^{-1}, \ldots, v_n^{-1})\right)$.

D *If $i < m$, increase i and go to* ***C****, otherwise* ***RETURN NULL*** *(f is uni–multivariate indecomposable).*

EXAMPLE 4. *Let*

$$\begin{aligned} f &= 4z^4y^2 - 8z^3y^3 + 8z^2yx + 4z^2y^4 - 8zy^2x \\ &\quad +4x^2 - 2z^2y + 2zy^2 - 2x + 10 \end{aligned}$$

as in Example 2. We take $u = t - 10 \in \mathbb{K}(t)$ and $v_1 = x, v_2 = y, v_3 = z$. Then

$$\begin{aligned} \overline{f} &= 4z^4y^2 - 8z^3y^3 + 8z^2yx + 4z^2y^4 - 8zy^2x \\ &\quad +4x^2 - 2z^2y + 2zy^2 - 2x. \end{aligned}$$

We factor $\overline{f} = 2(x + z^2y - zy^2)(2x - 1 + 2z^2y - 2zy^2)$. We first take the candidate $(x + z^2y - zy^2)$. We have to check if there are values of a_1, a_2 for which $g = a_2t^2 + a_1t$ verifies $\overline{f} = g(x + z^2y - zy^2)$. We find the solution $a_2 = 4, a_1 = -2$. Thus $f = (4t^2 - 2t + 10)(x + z^2y - zy^2)$.

EXAMPLE 5. *Let $f = \dfrac{f_n}{f_d}$ with*

$$\begin{aligned} f_n &= y^2x^2 + 2x^2yz^2 - 2y^6x + z^4x^2 - 2z^2xy^5 \\ &\quad +y^{10} - 81x^2 - 450xyz - 625y^2z^2, \\ f_d &= y^2x^2 + 2x^2yz^2 - 2y^6x + z^4x^2 - 2z^2xy^5 \\ &\quad +y^{10} - 162x^2 - 900xyz - 1250y^2z^2, \end{aligned}$$

as in Example 3. Let $>$ be the pure lexicographical ordering with $y > x > z$. Then $\mathrm{lm}\ f_n = \mathrm{lm}\ f_d = y^{10}$. Following the proof of lemma 1, let $u_1 = 1/(t-1)$, then $u_1(f) = f_{1n}/f_{1d}$ with

$$\begin{aligned} f_{1n} &= y^2x^2 + 2x^2yz^2 - 2y^6x + z^4x^2 - 2z^2xy^5 \\ &\quad +y^{10} - 162x^2 - 900xyz - 1250y^2z^2, \\ f_{1d} &= 81x^2 + 450xyz + 625y^2z^2. \end{aligned}$$

Now, let $\alpha = (1, 0, 0)$, so that the denominator of the previous expression is non–zero at the point α. Then $f_{2n}/f_{2d} = u(f(x+1, y, z))$ with

$$\begin{aligned} f_{2n} &= y^2x^2 + 2y^2x + y^2 + 2x^2yz^2 + 4yz^2x + 2yz^2 \\ &\quad -2y^6x - 2y^6 + z^4x^2 + 2z^4x + z^4 - 2z^2xy^5 \\ &\quad -2z^2y^5 + y^{10} - 162x^2 - 324x - 162 \\ &\quad -900xyz - 900yz - 1250y^2z^2, \\ f_{2d} &= 81x^2 + 162x + 81 + 450xyz + 450yz + 625y^2z^2. \end{aligned}$$

Table 1: Average computing times (in seconds)

n	d	Alg 3	Fact.	Alg 4	Fact.
2	10	32.17	23.15	27.03	22.44
2	25	68.20	46.34	51.10	40.33
2	30	89.40	62.48	91.22	71.06
4	8	54.37	38.56	32.07	25.47
4	25	89.75	65.95	64.41	46.72
4	30	156.87	110.30	134.60	99.87
8	10	234.90	162.89	156.12	116.66
8	25	349.44	235.41	341.11	276.85
8	30	654.72	454.36	678.89	511.01

As $f_{2n}(0,0,0) = -162$ and $f_{2d}(0,0,0) = 81$, if $u_2 = t + 2$, we have that

$$u_2(u_1(f(x+1, y, z))) = \overline{f} = \frac{\overline{f}_n}{\overline{f}_d}$$

verifies the conditions of Lemma 3. We factor $\overline{f}_n$ and $\overline{f}_d$:

$$\begin{aligned} \overline{f}_n &= \left(z^2 + z^2x + y + xy - y^5\right)^2, \\ \overline{f}_d &= (9x + 9 + 25yz)^2. \end{aligned}$$

As the degree is multiplicative and $\deg\ \underline{f} = 10$, and also $\mathrm{lm}\ \overline{h}_n > \mathrm{lm}\ \overline{h}_d$, the possible values of $\overline{h}_n, \overline{h}_d$ are

$$\begin{aligned} \overline{h}_n &= z^2 + z^2x + y + xy - y^5, \\ \overline{h}_d &\in \{1, 9x + 9 + 25yz, (9x + 9 + 25yz)^2\} \end{aligned}$$

To check them, let $\overline{g} = \frac{a_2t^2 + a_1t}{b_1t + b_0}$. We substitute $\overline{h}$ in $\overline{g}$ and solve the homogeneous linear system obtained by comparing the coefficients with those of $\overline{f}$.

– *If $\overline{h}_d = 1$, there is only the trivial solution, thus $\overline{h}$ is not a candidate for $\overline{f}$.*

– *If $\overline{h}_d = 9x + 9 + 25yz$, we get the non–trivial solution $a_2 = b_0 = 1, a_1 = b_1 = 0$, thus f has a uni–multivariate decomposition*

$$\left(u_1^{-1}(u_2^{-1}(\overline{g}))\,,\ \overline{h}(x-1, y, z)\right) = \left(\tfrac{-1+t^2}{t^2-2}, \tfrac{z^2x + yx - y^5}{9x + 25yz}\right).$$

– *If $\overline{h}_d = (9x + 9 + 25yz)^2$, the only solution is the trivial one.*

Therefore, any uni–multivariate decomposition of f is equivalent to the decomposition (g, h) computed before.

4. PERFORMANCE

Both algorithms run in exponential time, since the number of candidates to be tested is, in the worst case, exponential in the degree of the input; the rest of the steps in both algorithms are in polynomial time. However, in practical examples it seems that most of the time is spent in the factorization of the associated symmetric near–separated polynomial, in Algorithm 3, or the numerator and denominator in Algorithm 4. We show in Table 1 the average times obtained by running implementations of these algorithms in Maple VI (see [3]) on a collection of random functions. The parameters are the number of variables n and the degree of the rational function d. We have also included the factorization times for each algorithm.

5. REFERENCES

[1] Alonso, C., Gutierrez, J., and Recio, T. A rational function decomposition algorithm by near-separated polynomials. *J. Symb. Comp. 19* (1995), 527–544.

[2] Gordan, P. Über biquadratische Gleichungen. *Math. Ann. 29* (1887), 318–326.

[3] Gutierrez, J., and Rubio, R. Cadecom: Computer Algebra software for functional DECOMposition. In *Computer Algebra in Scientific Computing CASC'00* (Samarkand, 2000), Springer-Verlag, pp. 233–248.

[4] Igusa, J. On a theorem of Lüroth. *Mem. Coll. Sci. Univ. Kyoto, Ser. A Math. 26* (1951), 251–253.

[5] Muller-Quade, J., and Steinwandt, R. Recognizing simple subextensions of pure transcendental field extensions. *AAECC 11* (2000), 35–41.

[6] Nagata, M. *Theory of commutative fields.* Translations of Mathematical Monographs, vol 125. AMS, 1993.

[7] Netto, E. Über einen Lüroth gordaschen staz. *Math. Ann. 46* (1895), 310–318.

[8] Noether, E. Korper und systeme rationaler funktionen. *Math. Ann. 76* (1915), 161–196.

[9] Rubio, R. *Unirational fields. Theorems, Algorihms and Applications.* Thesis Dissertation, University of Cantabria, Spain, 2000.

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

[11] Schinzel, A. *Selected topics on polynomials.* University of Michigan Press, 1982.

[12] Sedeberg, T. Improperly parametrized rational curves. *Computer Aided Geometric Design 3* (1986), 67–75.

[13] Sweedler, M. Using Groebner bases to determine the algebraic and transcendental nature of field extensions: return of the killer tag variables. In *AAECC-10* (Berlin; Heidelberg, 1993), G. Cohen, T. Mora, and O. Moreno, Eds., vol. 673 of *LNCS*, Springer, pp. 66–75.

[14] van der Waerden, B. L. *Modern Algebra, volumes 1 and 2.* Frederic Unger Publishing Co., 1966.

[15] von zur Gathen, J. Functional decomposition of polynomials: the tame case. *J. Symb. Comput. 9* (1990), 281–299.

[16] von zur Gathen, J., and Gerhard, J. *Modern Computer Algebra.* Cambridge University Press, 1999.

[17] Zippel, R. Rational Function Decomposition. In *Proceedings of ISSAC'91* (Baltimore, 1991), S. M. Watt, Ed., ACM Press, pp. 1–6.