Journal of Algebra 406 (2014) 1–19

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Effective differential Lüroth's theorem ☆

Lisi D'Alfonso [a], Gabriela Jeronimo [b,*], Pablo Solernó [b]

[a] Departamento de Ciencias Exactas, Ciclo Básico Común, Universidad de Buenos Aires, Ciudad Universitaria, 1428, Buenos Aires, Argentina

[b] Departamento de Matemática and IMAS, UBA-CONICET, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires, Ciudad Universitaria, 1428, Buenos Aires, Argentina

ARTICLE INFO

Article history:
Received 27 September 2012
Available online xxxx
Communicated by Bruno Salvy

MSC:
12Y05
12H05

Keywords:
Differential algebra
Lüroth's theorem
Differentiation index

ABSTRACT

This paper focuses on effectivity aspects of the Lüroth's theorem in differential fields. Let $\mathcal{F}$ be an ordinary differential field of characteristic 0 and $\mathcal{F}\langle u\rangle$ be the field of differential rational functions generated by a single indeterminate u. Let be given non-constant rational functions $v_1,\ldots,v_n \in \mathcal{F}\langle u\rangle$ generating a differential subfield $\mathcal{G} \subseteq \mathcal{F}\langle u\rangle$. The differential Lüroth's theorem proved by Ritt in 1932 states that there exists $v \in \mathcal{G}$ such that $\mathcal{G} = \mathcal{F}\langle v\rangle$. Here we prove that the total order and degree of a generator v are bounded by $\min_j \operatorname{ord}(v_j)$ and $(nd(e+1)+1)^{2e+1}$, respectively, where $e := \max_j \operatorname{ord}(v_j)$ and $d := \max_j \deg(v_j)$. As a byproduct, our techniques enable us to compute a Lüroth generator by dealing with a polynomial ideal in a polynomial ring in finitely many variables.

☆ Partially supported by the following Argentinian grants: ANPCyT PICT 2007/816, UBACYT 20020100100418 01 (2011–2014) and UBACYT 20020090100069 (2010–2012).

* Corresponding author.
E-mail addresses: lisi@cbc.uba.ar (L. D'Alfonso), jeronimo@dm.uba.ar (G. Jeronimo), psolerno@dm.uba.ar (P. Solernó).

http://dx.doi.org/10.1016/j.jalgebra.2014.02.022
0021-8693/

1. Introduction

In 1876, J. Lüroth in [17] presented his famous result, currently known as Lüroth's theorem: if $k \subset L \subset k(u)$ is an extension of fields, where $k(u)$ is the field of rational functions in one variable u, then $L = k(v)$ for a suitable $v \in L$ (see [24, §10.2] for a modern proof). In 1893 G. Castelnuovo solved the same problem for rational function fields in two variables over an algebraically closed ground field. For three variables, Lüroth's problem has been solved negatively.

In 1932 J.F. Ritt [20] addressed the differential version of this result: *Let $\mathcal{F}$ be an ordinary differential field of characteristic 0, u an indeterminate over $\mathcal{F}$ and $\mathcal{F}\langle u\rangle$ the smallest field containing $\mathcal{F}$, u and all its derivatives. Then, if $\mathcal{G}$ is a differential field such that $\mathcal{F} \subset \mathcal{G} \subset \mathcal{F}\langle u\rangle$, there is an element $v \in \mathcal{G}$ such that $\mathcal{G} = \mathcal{F}\langle v\rangle$.* Such an element will be called a Lüroth generator of the extension $\mathcal{F} \subset \mathcal{G}$.

In fact, Ritt considered the case of a differential field $\mathcal{F}$ of meromorphic functions in an open set of the complex plane and $\mathcal{G}$ a finitely generated extension of $\mathcal{F}$. Later, E. Kolchin in [15] and [16] gave a new proof of this theorem for any differential field of characteristic 0 and without the hypothesis of finiteness on $\mathcal{G}$. Contrary to the classical setting, the differential Lüroth problem fails in the case of two variables (see [19]). A possible weak generalization of the differential Lüroth's theorem to dimension greater than one is the conjecture in control theory which states that every system linearizable by dynamic feedback is linearizable by endogenous feedback, or in algebraic terms, that a subextension of a differentially flat extension is differentially flat [6], [7, Section 4.2].

The present paper deals with quantitative aspects of the differential Lüroth's theorem. Our main result is the following theorem, which follows from Propositions 5 and 19.

Theorem 1. *Let $\mathcal{F}$ be an ordinary differential field of characteristic 0, u differentially transcendental over $\mathcal{F}$ and $\mathcal{G} := \mathcal{F}\langle P_1(u)/Q_1(u), \ldots, P_n(u)/Q_n(u)\rangle$, where $P_j, Q_j \in \mathcal{F}\{u\}$ are relatively prime differential polynomials of order at most $e \geqslant 1$ (i.e. at least one derivative of u occurs in P_j or Q_j for some j) and total degree bounded by d such that $P_j/Q_j \notin \mathcal{F}$ for every $1 \leqslant j \leqslant n$. Then, any Lüroth generator v of the differential extension $\mathcal{G}/\mathcal{F}$ can be written as the quotient of two relatively prime differential polynomials $P(u), Q(u) \in \mathcal{F}\{u\}$ with order bounded by $\min\{\mathrm{ord}(P_j/Q_j);\ 1 \leqslant j \leqslant n\}$ and total degree bounded by $\min\{(d+1)^{(e+1)n}, (nd(e+1)+1)^{2e+1}\}$.*

Our approach combines elements of Ritt's and Kolchin's proofs (mainly the introduction of the differential polynomial ideal related to the graph of the rational map $u \mapsto (P_j/Q_j)_{1 \leqslant j \leqslant n}$) with estimations concerning the order and the differentiation index of differential ideals developed in [22,3,5]. These estimations allow us to reduce the problem of computing a Lüroth generator to a Gröbner basis computation in a polynomial ring in finitely many variables (see Remark 17).

An algorithmic version of Ritt's proof of the differential Lüroth's theorem is given in [8]. The authors propose a deterministic algorithm that relies on the computation of ascending chains by means of the Wu–Ritt's zero decomposition algorithm; however, no quantitative questions on the order or the degree of the Lüroth generator are addressed. For effectiveness considerations of the classical not differential version, we refer the interested reader to [18,23,1,11,12,2].

This paper is organized as follows. In Section 2 we introduce the notations, definitions and previous results from differential algebra (mainly concerning the notions of order and differentiation index) needed in the rest of the paper. In Section 4, by estimating the differentiation index and the order of an associated DAE system, we provide a characterization of a Lüroth generator by means of an ideal of a polynomial ring in finitely many variables. This enables us to obtain degree upper bounds for its numerator and denominator by considering an elimination problem in effective classical algebraic geometry. As a byproduct, we give a Gröbner basis based procedure for the computation of a Lüroth generator. Finally, in Section 5 we show two simple examples illustrating our constructions.

2. Preliminaries

In this section we introduce the notation used throughout the paper and recall some definitions and results from differential algebra.

2.1. Basic definitions and notation

A *differential field* $(\mathcal{F}, \Delta)$ is a field $\mathcal{F}$ with a set of derivations $\Delta = \{\delta_i\}_{i\in I}$, $\delta_i : \mathcal{F} \to \mathcal{F}$. In this paper, all differential fields are *ordinary* differential fields; that is to say, they are equipped with only *one* derivation δ; for instance, $\mathcal{F} = \mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$ with $\delta = 0$, or $\mathcal{F} = \mathbb{Q}(t)$ with the usual derivation $\delta(t) = 1$. For this reason, we will simply write *differential field* (instead of ordinary differential field).

Let $(\mathcal{F}, \delta)$ be a differential field of characteristic 0.

The ring of differential polynomials in α indeterminates $z := z_1, \dots, z_\alpha$, which is denoted by $\mathcal{F}\{z_1, \dots, z_\alpha\}$ or simply $\mathcal{F}\{z\}$, is defined as the commutative polynomial ring $\mathcal{F}[z_j^{(p)}, 1 \leqslant j \leqslant \alpha,\ p \in \mathbb{N}_0]$ (in infinitely many indeterminates), extending the derivation of $\mathcal{F}$ by letting $\delta(z_j^{(i)}) = z_j^{(i+1)}$, that is, $z_j^{(i)}$ stands for the ith derivative of z_j (as customarily, the first derivatives are also denoted by $\dot{z}_j$). We write $z^{(p)} := z_1^{(p)}, \dots, z_\alpha^{(p)}$ and $z^{[p]} := z, z^{(1)}, \dots, z^{(p)}$ for every $p \in \mathbb{N}_0$.

The fraction field of $\mathcal{F}\{z\}$ is a differential field, denoted by $\mathcal{F}\langle z\rangle$, with the derivation obtained by extending the derivation δ to the quotients in the usual way. For $g \in \mathcal{F}\{z\}$, the *order of g with respect to z_j* is $\operatorname{ord}(g, z_j) := \max\{i \in \mathbb{N}_0\colon\ z_j^{(i)} \text{ appears in } g\}$, and the *order of g* is $\operatorname{ord}(g) := \max\{\operatorname{ord}(g, z_j)\colon\ 1 \leqslant j \leqslant \alpha\}$; this notion of order extends naturally to $\mathcal{F}\langle z\rangle$ by taking the maximum of the orders of the numerator and the denominator in a reduced representation of the rational fraction.

Given differential polynomials $H := h_1, \dots, h_\beta \in \mathcal{F}\{z\}$, we write $[H]$ to denote the smallest *differential* ideal of $\mathcal{F}\{z\}$ containing H (i.e. the smallest ideal containing the polynomials H and all their derivatives of arbitrary order). The minimum *radical* differential ideal of $\mathcal{F}\{z\}$ containing H is denoted by $\{H\}$. For every $i \in \mathbb{N}$, we write $H^{(i)} := h_1^{(i)}, \dots, h_\beta^{(i)}$ and $H^{[i]} := H, H^{(1)}, \dots, H^{(i)}$.

A *differential field extension* $\mathcal{G}/\mathcal{F}$ consists of two differential fields $(\mathcal{F}, \delta_\mathcal{F})$ and $(\mathcal{G}, \delta_\mathcal{G})$ such that $\mathcal{F} \subseteq \mathcal{G}$ and $\delta_\mathcal{F}$ is the restriction to $\mathcal{F}$ of $\delta_\mathcal{G}$. Given a subset $\Sigma \subset \mathcal{G}$, $\mathcal{F}\langle\Sigma\rangle$ denotes the minimal differential subfield of $\mathcal{G}$ containing $\mathcal{F}$ and Σ.

An element $\xi \in \mathcal{G}$ is said to be *differentially transcendental* over $\mathcal{F}$ if the family of its derivatives $\{\xi^{(p)}\colon\ p \in \mathbb{N}_0\}$ is algebraically independent over $\mathcal{F}$; otherwise, it is said to be *differentially algebraic* over $\mathcal{F}$. A *differential transcendence basis* of $\mathcal{G}/\mathcal{F}$ is a minimal subset $\Sigma \subset \mathcal{G}$ such that the differential field extension $\mathcal{G}/\mathcal{F}\langle\Sigma\rangle$ is differentially algebraic. All the differential transcendence bases of a differential field extension have the same cardinality (see [14, Ch. II, Sec. 9, Theorem 4]), which is called its *differential transcendence degree*.

2.2. Differential polynomials, ideals and manifolds

Here we recall some definitions and properties concerning differential polynomials and their solutions.

Let $g \in \mathcal{F}\{z\} = \mathcal{F}\{z_1, \dots, z_\alpha\}$. The *class* of g for the order $z_1 < z_2 < \cdots < z_\alpha$ of the variables is defined to be the greatest j such that $z_j^{(i)}$ appears in g for some $i \geqslant 0$ if $g \notin \mathcal{F}$, and 0 if $g \in \mathcal{F}$. If g is of class $j > 0$ and of order p in z_j, the *separant* of g, which will be denoted by S_g, is $\partial g/\partial z_j^{(p)}$ and the *initial* of g, denoted by I_g, is the coefficient of the highest power of $z_j^{(p)}$ in g.

Given g_1 and g_2 in $\mathcal{F}\{z\}$, g_2 is said to be of *higher rank in z_j than* g_1 if either $\operatorname{ord}(g_2, z_j) > \operatorname{ord}(g_1, z_j)$ or $\operatorname{ord}(g_2, z_j) = \operatorname{ord}(g_1, z_j) = p$ and the degree of g_2 in $z_j^{(p)}$ is greater than the degree of g_1 in $z_j^{(p)}$. Finally, g_2 is said to be of *higher rank than* g_1 if g_2 is of higher class than g_1 or they are of the same class $j > 0$ and g_2 is of higher rank in z_j than g_1.

We will use some elementary facts of the well-known theory of *characteristic sets*. For the definitions and basic properties of rankings and characteristic sets, we refer the reader to [14, Ch. I, §8–10].

Let H be a (not necessarily finite) system of differential polynomials in $\mathcal{F}\{z\}$. The *manifold of* H is the set of all the zeros $\eta \in \mathcal{G}^\alpha$ of H for all possible differential extensions $\mathcal{G}/\mathcal{F}$.

Every radical differential ideal $\{H\}$ of $\mathcal{F}\{z\}$ has a unique representation as a finite irredundant intersection of prime differential ideals, which are called the *essential prime divisors* of $\{H\}$ (see [21, Ch. II, §16–17]).

For a differential polynomial g in $\mathcal{F}\{z\}$ of positive class and algebraically irreducible, there is only one essential prime divisor of $\{g\}$ which does not contain S_g; the manifold of this prime differential ideal is called the *general solution of* g (see [21, Ch. II, §12–16]).

2.3. Hilbert–Kolchin function and differentiation index

Let $\mathfrak{P}$ be a prime differential ideal of $\mathcal{F}\{z\}$. The *differential dimension* of $\mathfrak{P}$, denoted by $\operatorname{diffdim}(\mathfrak{P})$, is the differential transcendence degree of the extension $\mathcal{F} \hookrightarrow \operatorname{Frac}(\mathcal{F}\{z\}/\mathfrak{P})$ (where Frac denotes the fraction field). The *differential Hilbert–Kolchin function* of $\mathfrak{P}$ with respect to $\mathcal{F}$ is the function $H_{\mathfrak{P},\mathcal{F}} : \mathbb{N}_0 \to \mathbb{N}_0$ defined as:

$$H_{\mathfrak{P},\mathcal{F}}(i) := \text{the (algebraic) transcendence degree of } \operatorname{Frac}\bigl(\mathcal{F}\bigl[z^{[i]}\bigr]/\bigl(\mathfrak{P} \cap \mathcal{F}\bigl[z^{[i]}\bigr]\bigr)\bigr) \text{ over } \mathcal{F}.$$

For $i \gg 0$, this function equals the linear function $\operatorname{diffdim}(\mathfrak{P})(i+1) + \operatorname{ord}(\mathfrak{P})$, where $\operatorname{ord}(\mathfrak{P}) \in \mathbb{N}_0$ is an invariant called the *order* of $\mathfrak{P}$ [14, Ch. II, Sec. 12, Theorem 6]. The minimum i from which this equality holds is the Hilbert–Kolchin *regularity* of $\mathfrak{P}$.

Let F be a finite set of differential polynomials contained in $\mathfrak{P}$ of order bounded by a non-negative integer e. Throughout the paper we assume that $e \geqslant 1$, in other words, all the systems we consider are actually differential but not purely algebraic.

Definition 2. The set F is *quasi-regular* at $\mathfrak{P}$ if, for every $k \in \mathbb{N}_0$, the Jacobian matrix of the polynomials $F, \dot{F}, \ldots, F^{(k)}$ with respect to the variables $z^{[e+k]}$ has full row rank over the fraction field of $\mathcal{F}\{z\}/\mathfrak{P}$.

A fundamental invariant associated to ordinary differential algebraic equation systems is the *differentiation index*. There are several definitions of this notion (see [3] and the references given there), but in every case it represents a measure of the implicitness of the given system. Here we will use the following definition, introduced in [3, Section 3], in the context of quasi-regular differential polynomial systems with respect to a fixed prime differential ideal $\mathfrak{P}$:

Definition 3. The $\mathfrak{P}$-*differentiation index* σ of a quasi-regular system F of polynomials in $\mathcal{F}\{z\}$ of order at most e is

$$\sigma := \min\bigl\{k \in \mathbb{N}_0\colon\ \bigl(F, \dot{F}, \ldots, F^{(k)}\bigr)_{\mathfrak{P}_{e+k}} \cap \mathcal{F}\bigl[z^{[e]}\bigr]_{\mathfrak{P}_e} = [F]_{\mathfrak{P}} \cap \mathcal{F}\bigl[z^{[e]}\bigr]_{\mathfrak{P}_e}\bigr\},$$

where, for every $k \in \mathbb{N}_0$, $\mathfrak{P}_{e+k} := \mathfrak{P} \cap \mathcal{F}[z^{[e+k]}]$ (i.e. the contraction of the prime ideal $\mathfrak{P}$), $\mathcal{F}[z^{[e+k]}]_{\mathfrak{P}_{e+k}}$ denotes the localized ring at the prime ideal $\mathfrak{P}_{e+k}$ and $(F, \dot{F}, \ldots, F^{(k)})_{\mathfrak{P}_{e+k}}$ is the algebraic ideal generated by $F, \dot{F}, \ldots, F^{(k)}$ in $\mathcal{F}[z^{[e+k]}]_{\mathfrak{P}_{e+k}}$.

Roughly speaking, the differentiation index of the system F is the minimum number of derivatives of the polynomials F needed to write all the relations given by the differential ideal $\mathfrak{P}$ up to order e.

3. Differential Lüroth's theorem

In [20, Ch. VIII] (see also [21] and [14]), the classical Lüroth's theorem for transcendental field extensions is generalized to the differential algebra framework:

Theorem 4 *(Differential Lüroth's theorem). Let $\mathcal{F}$ be an ordinary differential field of characteristic* 0 *and let u be differentially transcendental over $\mathcal{F}$. Let $\mathcal{G}$ be a differential field such that $\mathcal{F} \subset \mathcal{G} \subset \mathcal{F}\langle u\rangle$. Then, there is an element $v \in \mathcal{G}$ such that $\mathcal{G} = \mathcal{F}\langle v\rangle$.*

Our goal is the following: for $n > 1$, let be given differential polynomials $P_1, \dots, P_n$, $Q_1, \dots, Q_n \in \mathcal{F}\{u\}$, with $P_j/Q_j \notin \mathcal{F}$ and P_j, Q_j relatively prime polynomials for every $1 \leqslant j \leqslant n$, and denote

$$\mathcal{G} := \mathcal{F}\big\langle P_1(u)/Q_1(u), \dots, P_n(u)/Q_n(u)\big\rangle,$$

which is a subfield of $\mathcal{F}\langle u\rangle$. We are interested in *a priori* upper bounds for the orders and degrees of a Lüroth generator of $\mathcal{G}/\mathcal{F}$, that is, for a pair of differential polynomials $P, Q \in \mathcal{F}\{u\}$ such that $Q \not\equiv 0$ and $\mathcal{G} = \mathcal{F}\langle P(u)/Q(u)\rangle$. These bounds will also allow us to reduce the problem of computing a Lüroth generator to standard computer algebra computations in a polynomial ideal in finitely many variables.

An optimal estimate for the order of the polynomials P and Q can be obtained by elementary computations (see Section 3.1). However, the problem of estimating their degrees seems to be a more delicate question which requires a more careful analysis that we will do in the subsequent sections of the paper.

3.1. Bound for the order

We start by proving an upper bound for the order of a Lüroth generator. The following proposition will prove the first part of Theorem 1.

Proposition 5. *Under the previous assumptions and notation, any element $v \in \mathcal{G}$ such that $\mathcal{G} = \mathcal{F}\langle v\rangle$ satisfies* $\operatorname{ord}(v) \leqslant \min\{\operatorname{ord}(P_j/Q_j)\colon\ 1 \leqslant j \leqslant n\}$.

Proof. Let $v \in \mathcal{G}$ be such that $\mathcal{G} = \mathcal{F}\langle v\rangle$ and $\varepsilon := \operatorname{ord}(v)$.

For $j = 1, \dots, n$, let $v_j = P_j(u)/Q_j(u)$. By assumption, $v_j \notin \mathcal{F}$. Let T be a new differential indeterminate over $\mathcal{F}$. Since $v_j \in \mathcal{G} = \mathcal{F}\langle v\rangle$, there exists $\Theta_j \in \mathcal{F}\langle T\rangle$ such that $v_j = \Theta_j(v)$. Let $N_j = \operatorname{ord}(\Theta_j)$. Then, $\operatorname{ord}(v_j) \leqslant N_j + \varepsilon$. In addition,

$$\frac{\partial v_j}{\partial u^{(N_j+\varepsilon)}} = \frac{\partial(\Theta_j(v))}{\partial u^{(N_j+\varepsilon)}} = \sum_{i\geqslant 0} \frac{\partial \Theta_j}{\partial T^{(i)}}(v)\frac{\partial v^{(i)}}{\partial u^{(N_j+\varepsilon)}} = \frac{\partial \Theta_j}{\partial T^{(N_j)}}(v)\frac{\partial v^{(N_j)}}{\partial u^{(N_j+\varepsilon)}}.$$

Since N_j is the order of Θ_j, it follows that $\frac{\partial \Theta_j}{\partial T^{(N_j)}} \neq 0$, and as v is differentially transcendental over $\mathcal{F}$, we have that $\frac{\partial \Theta_j}{\partial T^{(N_j)}}(v) \neq 0$. Furthermore, $\frac{\partial v^{(N_j)}}{\partial u^{(N_j+\varepsilon)}} = \frac{\partial v}{\partial u^{(\varepsilon)}} \neq 0$, since $\varepsilon = \operatorname{ord}(v)$. We conclude that $\frac{\partial v_j}{\partial u^{(N_j+\varepsilon)}} \neq 0$ and, therefore, $\operatorname{ord}(v_j) = N_j + \varepsilon$.

The proposition follows. □

Note that the above proposition shows that all possible Lüroth generators v have the same order. In fact, two arbitrary generators are related by a homographic map with coefficients in $\mathcal{F}$ (see for instance [15, §1], [21, Ch. II, §44]).

3.2. *Ritt's approach*

Here we discuss some ingredients which appear in the classical proofs of Theorem 4 (see [21,15]) and that we also consider in our approach.

Following [21, II. §39 and §40], let y be a new differential indeterminate over the field $\mathcal{F}\langle u\rangle$ (and, in particular, over $\mathcal{G}$) and consider the differential prime ideal Σ of all differential polynomials in $\mathcal{G}\{y\}$ vanishing at u:

$$\Sigma := \{A \in \mathcal{G}\{y\} \text{ such that } A(u) = 0\}. \tag{1}$$

Lemma 6. *The manifold of Σ is the general solution of an irreducible differential polynomial $B \in \mathcal{G}\{y\}$. More precisely, B is a differential polynomial in Σ with the lowest rank in y.*

Proof. Let $B \in \Sigma$ be a differential polynomial with the lowest rank in y. Note that $B \in \mathcal{G}\{y\}$ is algebraically irreducible, since Σ is prime. We denote the order of B by k and the separant of B by $S_B = \partial B/\partial y^{(k)}$. Consider the differential ideal

$$\Sigma_1(B) := \{A \in \mathcal{G}\{y\} \mid S_B A \equiv 0 \bmod \{B\}\}.$$

As shown in [21, II. §12], the ideal $\Sigma_1(B)$ is prime; moreover, we have that $A \in \Sigma_1(B)$ if and only if $S_B^a A \equiv 0 \bmod [B]$ for some $a \in \mathbb{N}_0$ and, in particular, if $A \in \Sigma_1(B)$ is of order at most $k = \operatorname{ord}(B)$, then A is a multiple of B (see [21, II. §13]). Furthermore, $\Sigma_1(B)$ is an essential prime divisor of $\{B\}$ and, in the representation of $\{B\}$ as an intersection of its essential prime divisors, it is the only prime which does not contain S_B [21, II. §15]. Therefore, the manifold of $\Sigma_1(B)$ is the general solution of B.

In order to prove the lemma, it suffices to show that $\Sigma = \Sigma_1(B)$.

Let $A \in \Sigma_1(B)$. Then, $S_B A \in \{B\}$. Taking into account that Σ is prime, $\{B\} \subset \Sigma$, and $S_B \notin \Sigma$, it follows that $A \in \Sigma$.

To see the other inclusion, consider a differential polynomial $A \in \Sigma$. By the minimality of B, we have that A is of rank at least the rank of B. Reducing A modulo B, we obtain a relation of the type

$$S_B^b I_B^c A \equiv R \mod [B],$$

where $b, c \in \mathbb{N}_0$, I_B is the initial of B and R is a differential polynomial whose rank is lower than the rank of B. Since A and B lie in the differential ideal Σ, it follows that $R \in \Sigma$, and so, the minimality of B implies that $R = 0$. In particular, $S_B^b I_B^c A \in [B]$ and, therefore, $I_B^c A \in \Sigma_1(B)$. Now, $I_B \notin \Sigma_1(B)$ since, otherwise, it would be a differential polynomial in Σ with a rank lower than the rank of B (recall that $\Sigma_1(B) \subset \Sigma$); it follows that $A \in \Sigma_1(B)$. □

Multiplying the polynomial $B \in \mathcal{G}\{y\}$ given by Lemma 6 by a suitable denominator, we obtain a differential polynomial $C \in \mathcal{F}\{u, y\}$ with no factor in $\mathcal{F}\{u\}$. The following result is proved in [21, II. §42 and §43]:

Proposition 7. *If $P_0(u)$ and $Q_0(u)$ are two non-zero coefficients of C (regarded as a polynomial in $\mathcal{F}\{u\}\{y\}$) such that $P_0(u)/Q_0(u) \notin \mathcal{F}$, the polynomial*

$$D(u, y) := Q_0(u)P_0(y) - P_0(u)Q_0(y)$$

is a multiple of C by a factor in $\mathcal{F}$, and $\mathcal{G} = \mathcal{F}\langle P_0(u)/Q_0(u)\rangle$. □

Note that, by the definition of C, the ratio between two coefficients of C coincides with the ratio of the corresponding coefficients of B.

3.3. An alternative characterization of a Lüroth generator

Under the previous assumptions, consider the map of differential algebras defined by

$$\begin{aligned} \psi : \mathcal{F}\{x_1, \dots, x_n, u\} &\to \mathcal{F}\bigl\{P_1(u)/Q_1(u), \dots, P_n(u)/Q_n(u), u\bigr\} \\ x_i &\mapsto P_i(u)/Q_i(u) \\ u &\mapsto u \end{aligned}$$

Let $\mathfrak{P} \subset \mathcal{F}\{x, u\}$ be the kernel of the morphism ψ; then, we have an isomorphism

$$\mathcal{F}\bigl\{P_1(u)/Q_1(u), \dots, P_n(u)/Q_n(u), u\bigr\} \simeq \mathcal{F}\{x_1, \dots, x_n, u\}/\mathfrak{P}.$$

This implies that $\mathfrak{P}$ is a *prime* differential ideal and, moreover, that the fraction field of $\mathcal{F}\{x_1, \dots, x_n, u\}/\mathfrak{P}$ is isomorphic to $\mathcal{F}\langle u\rangle$. In addition, the previous isomorphism gives an inclusion

$$\mathcal{F}\bigl\{P_1(u)/Q_1(u), \dots, P_n(u)/Q_n(u)\bigr\} \hookrightarrow \mathcal{F}\{x_1, \dots, x_n, u\}/\mathfrak{P},$$

and the inclusion induced from this map in the fraction fields leads to the original extension $\mathcal{G} = \mathcal{F}\langle P_1(u)/Q_1(u), \dots, P_n(u)/Q_n(u)\rangle \hookrightarrow \mathcal{F}\langle u\rangle$.

As above, let y be a new differential indeterminate over $\mathcal{F}\langle u\rangle$ and Σ the ideal of $\mathcal{G}\{y\}$ introduced in (1). If $A \in \mathcal{G}\{y\}$ is a non-zero differential polynomial in Σ, multiplying it by an adequate element in $\mathcal{F}\{P_1(u)/Q_1(u), \ldots, P_n(u)/Q_n(u)\}$, we obtain a differential polynomial in $\mathcal{F}\{P_1(u)/Q_1(u), \ldots, P_n(u)/Q_n(u)\}\{y\}$, with the same rank in y as A. Taking a representative (with respect to ψ) in $\mathcal{F}\{x_1, \ldots, x_n\}$ for each of its coefficients, we get a differential polynomial $\widehat{A} \in \mathcal{F}\{x_1, \ldots, x_n, y\}$, with the same rank in y as A, such that $\widehat{A}(x_1, \ldots, x_n, u) \in \mathfrak{P}$.

Conversely, given a differential polynomial $M \in \mathcal{F}\{x_1, \ldots, x_n, u\}$ such that $M \in \mathfrak{P}$ and not every coefficient of M as a polynomial in $\mathcal{F}\{x_1, \ldots, x_n\}\{u\}$ lies in $\mathfrak{P} \cap \mathcal{F}\{x_1, \ldots, x_n\}$, the differential polynomial

$$\widetilde{M}(y) := M\big(P_1(u)/Q_1(u), \ldots, P_n(u)/Q_n(u), y\big) \in \mathcal{G}\{y\} \tag{2}$$

is not the zero polynomial, vanishes at u and has a rank in y no higher than that of M.

We conclude that if $M \in \mathcal{F}\{x_1, \ldots, x_n, u\}$ is a differential polynomial with the lowest rank in u among all the differential polynomials as above, the associated differential polynomial $\widetilde{M}(y)$ is a multiple by a factor in $\mathcal{G}$ of the minimal polynomial B of u over $\mathcal{G}$ introduced in Lemma 6. Therefore, by Proposition 7, a Lüroth generator of $\mathcal{G}/\mathcal{F}$ can be obtained as the ratio of any pair of coefficients of $\widetilde{M} \in \mathcal{G}\{y\}$ provided that this ratio does not lie in $\mathcal{F}$. Moreover:

Proposition 8. *Let $M \in \mathcal{F}\{x_1, \ldots, x_n, u\}$ be a differential polynomial in $\mathfrak{P} \setminus (\mathfrak{P} \cap \mathcal{F}\{x_1, \ldots, x_n\})\{u\}$ with the lowest rank in u and let $\widetilde{M}(y) \in \mathcal{G}\{y\}$ be as in (2). Assume that $\widetilde{M} \in \mathcal{F}(u^{[\epsilon]})\{y\}$ for a suitable non-negative integer ϵ. Consider two generic points $\upsilon_1, \upsilon_2 \in \mathbb{Q}^{\epsilon+1}$. Let $P(y)$ and $Q(y)$ be the differential polynomials obtained from $\widetilde{M}(y)$ by substituting $u^{[\epsilon]} = \upsilon_1$ and $u^{[\epsilon]} = \upsilon_2$ respectively. Then $P(u)/Q(u)$ is a Lüroth generator of $\mathcal{G}/\mathcal{F}$.*

Proof. By Proposition 7, we have that

$$\widetilde{M}(y) = M\big(P_1(u)/Q_1(u), \ldots, P_n(u)/Q_n(u), y\big) = \gamma\big(Q_0(u)P_0(y) - P_0(u)Q_0(y)\big)$$

for some $\gamma \in \mathcal{G}$, and P_0, Q_0 are such that $\mathcal{G} = \mathcal{F}\langle P_0(u)/Q_0(u)\rangle$. Then, by means of two specializations υ_1, υ_2 of the variables $u^{[\epsilon]}$ so that $Q_0, Q_1, \ldots, Q_n$ and γ do not vanish and $P_0(\upsilon_1)/Q_0(\upsilon_1) \neq P_0(\upsilon_2)/Q_0(\upsilon_2)$, we obtain polynomials of the form

$$P(y) = \alpha_1 P_0(y) - \beta_1 Q_0(y) \quad \text{and} \quad Q(y) = \alpha_2 P_0(y) - \beta_2 Q_0(y),$$

where $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathcal{F}$ and $\alpha_1\beta_2 - \alpha_2\beta_1 \neq 0$. The proposition follows since $\mathcal{F}\langle P(u)/Q(u)\rangle = \mathcal{F}\langle P_0(u)/Q_0(u)\rangle = \mathcal{G}$. $\square$

4. Reduction to a polynomial ring and degree bound

In this section, we will obtain upper bounds for the order and the degree of the differential polynomial $M \in \mathcal{F}\{x_1, \ldots, x_n, u\}$ involved in our characterization of a Lüroth generator of $\mathcal{G}/\mathcal{F}$ (see Proposition 8). These bounds imply, in particular, an upper bound for the degrees of the numerator and the denominator of the generator (see Section 4.3).

4.1. Bounding the order of a minimal polynomial M

Here we estimate the order in the variables $x = x_1, \dots, x_n$ and u of a differential polynomial $M(x,u) \in \mathfrak{P} \setminus (\mathfrak{P} \cap \mathcal{F}\{x_1, \dots, x_n\})\{u\}$ of minimal rank in u, where $\mathfrak{P}$ is the prime differential ideal introduced in Section 3.3.

Remark 9. The differential dimension of $\mathfrak{P}$ equals 1, since the fraction field of $\mathcal{F}\{x_1, \dots, x_n, u\}/\mathfrak{P}$ is isomorphic to $\mathcal{F}\langle u\rangle$.

Let $e := \max\{\operatorname{ord}(P_j/Q_j)\colon 1 \leqslant j \leqslant n\}$. Without loss of generality, we may assume that $\operatorname{ord}(P_1(u)/Q_1(u)) \geqslant \cdots \geqslant \operatorname{ord}(P_n(u)/Q_n(u))$. Consider the elimination order in $\mathcal{F}\{x_1, \dots, x_n, u\}$ with $x_1 < \cdots < x_n < u$.

Since $P_1(u)/Q_1(u) \notin \mathcal{F}$, it is transcendental over $\mathcal{F}$. Now, as the variable $u^{(e+1)}$ appears in the derivative $(P_1(u)/Q_1(u))'$ but it does not appear in $P_1(u)/Q_1(u)$, it follows that $(P_1(u)/Q_1(u))'$ is (algebraically) transcendental over $\mathcal{F}(P_1(u)/Q_1(u))$. Continuing in the same way with the successive derivatives, we conclude that $P_1(u)/Q_1(u)$ is differentially transcendental over $\mathcal{F}$. This implies that the differential ideal $\mathfrak{P}$ contains no differential polynomial involving only the variable x_1.

Thus, a characteristic set of $\mathfrak{P}$ for the considered elimination order is of the form

$$R_1(x_1, x_2), R_2(x_1, x_2, x_3), \dots, R_{n-1}(x_1, \dots, x_n), R_n(x_1, \dots, x_n, u).$$

Furthermore, $R_n(x_1, \dots, x_n, u)$ is a differential polynomial in $\mathfrak{P} \setminus (\mathfrak{P} \cap \mathcal{F}\{x_1, \dots, x_n\})\{u\}$ with a minimal rank in u, that is, we can take $M(x,u) = R_n(x,u)$. Following [22, Lemma 19], we may assume this characteristic set to be irreducible. Then, by [22, Theorem 24], we have that $\operatorname{ord}(R_i) \leqslant \operatorname{ord}(\mathfrak{P})$ for every $1 \leqslant i \leqslant n$; in particular,

$$\operatorname{ord}(M) \leqslant \operatorname{ord}(\mathfrak{P}). \tag{3}$$

The order of the differential prime ideal $\mathfrak{P}$ can be computed exactly. In order to do this, we introduce a system of differential polynomials that provides us with an alternative characterization of the ideal $\mathfrak{P}$ which enables us to compute its order.

For every j, $1 \leqslant j \leqslant n$, denote $F_j := Q_j(u)x_j - P_j(u) \in \mathcal{F}\{x,u\}$, and let $F := F_1, \dots, F_n$. Then we have:

Lemma 10. *The ideal $\mathfrak{P}$ is the (unique) minimal differential prime ideal of $[F]$ which does not contain the product $Q_1 \dots Q_n$. Moreover, $\mathfrak{P} = [F] : (Q_1 \dots Q_n)^\infty$.*

Proof. From the definitions of $\mathfrak{P}$ and F it is clear that $[F] \subset \mathfrak{P}$ and $Q_1(u) \dots Q_n(u) \notin \mathfrak{P}$. Moreover, since F is a characteristic set for the order in $\mathcal{F}\{x,u\}$ given by $u < x_1 < \cdots <$

x_n and $\mathfrak{P} \cap \mathcal{F}\{u\} = (0)$, we conclude that for any polynomial $H \in \mathfrak{P}$ there exists $N \in \mathbb{N}_0$ such that $(Q_1(u) \dots Q_n(u))^N H \in [F]$ (observe that Q_j is the initial and the separant of the polynomial F_j for every j). The proposition follows. □

The system F we have introduced has the following property that we will use in the sequel (recall Definition 2):

Lemma 11. *The system F is quasi-regular at $\mathfrak{P}$.*

Proof. Let e be the maximum of the orders of the differential polynomials F_j, $1 \leqslant j \leqslant n$. For every $i \in \mathbb{N}$, let J_i be the Jacobian matrix of the polynomials $F^{[i-1]}$ with respect to the variables $(x, u)^{[i-1+e]}$. We have that

$$\frac{\partial F_j^{(k)}}{\partial x_h^{(l)}} = \begin{cases} 0 & \text{if } h \neq j \text{ or } h = j,\ k < l \\ \binom{k}{l} Q_j^{(k-l)} & \text{if } h = j,\ k \geqslant l \end{cases}$$

and so, for every $i \in \mathbb{N}$, the minor of J_i corresponding to partial derivatives with respect to the variables $x^{[i-1]}$ is a scalar multiple of $(Q_1(u) \dots Q_n(u))^i$, which is not zero modulo $\mathfrak{P}$. □

Now, we apply results from [3] in order to compute the order of $\mathfrak{P}$.

Proposition 12. *The order of the differential ideal $\mathfrak{P}$ equals $e = \max\{\operatorname{ord}(P_j(u)/Q_j(u)) \colon 1 \leqslant j \leqslant n\}$.*

Proof. Lemma 10 states that the ideal $\mathfrak{P}$ is an essential prime divisor of $[F]$, where $F := F_1, \dots, F_n$ with $F_j(x, u) := Q_j(u)x_j - P_j(u)$, $1 \leqslant j \leqslant n$, and, as shown in Lemma 11, the system F is quasi-regular at $\mathfrak{P}$. Therefore, taking into account that e is the maximum of the orders of the polynomials in F, by [3, Theorem 12], the regularity of the Hilbert–Kolchin function of $\mathfrak{P}$ is at most $e - 1$. This implies that the order of $\mathfrak{P}$ can be obtained from the value of this function at $e - 1$; more precisely, since the differential dimension of $\mathfrak{P}$ equals 1, we have that

$$\operatorname{ord}(\mathfrak{P}) = \operatorname{trdeg}_{\mathcal{F}}\big(\mathcal{F}\big[x^{[e-1]}, u^{[e-1]}\big] / \big(\mathfrak{P} \cap \mathcal{F}\big[x^{[e-1]}, u^{[e-1]}\big]\big)\big) - e.$$

In order to compute the transcendence degree involved in the above formula, we observe first that

$$\mathcal{F}\big[x^{[e-1]}, u^{[e-1]}\big] / \big(\mathfrak{P} \cap \mathcal{F}\big[x^{[e-1]}, u^{[e-1]}\big]\big) \simeq \mathcal{F}\big[(P_j/Q_j)^{[e-1]}, u^{[e-1]}\big].$$

It is clear that the variables $u^{[e-1]}$ are algebraically independent in this ring. Then, if $L = \mathcal{F}(u^{[e-1]})$, the order of the ideal $\mathfrak{P}$ coincides with the transcendence degree of $L((P_j/Q_j)^{[e-1]},\ j = 1, \dots, n)$ over L. Without loss of generality, we may assume that $\operatorname{ord}(P_1/Q_1) = e$. Since the variable $u^{(e)}$ appears in P_1/Q_1, we have that $L(u^{(e)})/L(P_1/Q_1)$ is algebraic. Similarly, since $u^{(e+1)}$ appears in $(P_1/Q_1)'$, it follows that the extension $L(u^{(e)}, u^{(e+1)})/L((P_1/Q_1), (P_1/Q_1)')$ is algebraic. Proceeding in the same way with the successive derivatives of P_1/Q_1, we conclude that $L(u^{(e)}, u^{(e+1)}, \ldots, u^{(2e-1)})$ is algebraic over $L((P_1/Q_1)^{[e-1]})$.

Since $\operatorname{ord}(P_j/Q_j) \leqslant e$ for $j = 1, \ldots, n$, we have that $L((P_j/Q_j)^{[e-1]}, j = 1, \ldots, n) \subset L(u^{(e)}, u^{(e+1)}, \ldots, u^{(2e-1)})$ and, by the arguments in the previous paragraph, this extension is algebraic. Therefore,

$$\operatorname{trdeg}_L L\big((P_j/Q_j)^{[e-1]},\ j = 1, \ldots, n\big) = \operatorname{trdeg}_L L\big(u^{(e)}, u^{(e+1)}, \ldots, u^{(2e-1)}\big) = e. \qquad \square$$

Then, by inequality (3) we conclude:

Proposition 13. *There is a differential polynomial* $M \in \mathfrak{P} \setminus (\mathfrak{P} \cap \mathcal{F}\{x_1, \ldots, x_n\})\{u\}$ *with the lowest rank in* u *such that* $\operatorname{ord}(M) \leqslant e$. $\square$

4.2. Reduction to algebraic polynomial ideals

As stated in Proposition 8, the Lüroth generator of $\mathcal{G}/\mathcal{F}$ is closely related with a polynomial $M(x_1, \ldots, x_n, u) \in \mathfrak{P} \setminus (\mathfrak{P} \cap \mathcal{F}\{x_1, \ldots, x_n\})\{u\}$ with the lowest rank in u.

By Proposition 13, such a polynomial M can be found in the algebraic ideal $\mathfrak{P} \cap \mathcal{F}[x^{[e]}, u^{[e]}]$ of the polynomial ring $\mathcal{F}[x^{[e]}, u^{[e]}]$. The following result will enable us to work with a finitely generated ideal given by known generators; the key point is the estimation of the $\mathfrak{P}$-differentiation index of the system $F := F_1, \ldots, F_n$ (see Definition 3):

Lemma 14. *The* $\mathfrak{P}$*-differentiation index of* F *equals* e. *In particular, we have that*

$$[F]_{\mathfrak{P}} \cap \mathcal{F}\big[x^{[e]}, u^{[e]}\big]_{\mathfrak{P}_e} = \big(F, \dot{F}, \ldots, F^{(e)}\big)_{\mathfrak{P}_{2e}} \cap \mathcal{F}\big[x^{[e]}, u^{[e]}\big]_{\mathfrak{P}_e},$$

where $\mathfrak{P}_e := \mathfrak{P} \cap \mathcal{F}[x^{[e]}, u^{[e]}]$ *and* $\mathfrak{P}_{2e} := \mathfrak{P} \cap \mathcal{F}[x^{[2e]}, u^{[2e]}]$.

Proof. For every $k \in \mathbb{N}$, let $\mathfrak{J}_k$ be the Jacobian submatrix of the polynomials $F, \ldots, F^{(k-1)}$ with respect to the variables $(x,u)^{(e)}, \ldots, (x,u)^{(e+k-1)}$. The $\mathfrak{P}$-differentiation index of F can be obtained as the minimum k such that $\operatorname{rank}(\mathfrak{J}_{k+1}) - \operatorname{rank}(\mathfrak{J}_k) = n$ holds, where the ranks are computed over the fraction field of $\mathcal{F}\{x,u\}/\mathfrak{P}$ (see [3, Section 3.1]).

Now, since the order of the polynomials F in the variables x is zero, no derivative $x^{(l)}$ with $l \geqslant e$ appears in $F, \dot{F}, \ldots, F^{(e-1)}$. This implies that the columns of the Jacobian submatrices $\mathfrak{J}_k$ of these systems corresponding to partial derivatives with respect to $x^{(l)}$, $l = e, \ldots, e+k-1$, are null. On the other hand, as e is the order of the system F, we may suppose that the variable $u^{(e)}$ appears in the polynomial F_1 and so, $\partial F_1/\partial u^{(e)} \neq 0$. Thus, $\partial F_1^{(i)}/\partial u^{(h)} \neq 0$ for $h - i = e$ and $\partial F_j^{(i)}/\partial u^{(h)} = 0$ for $h - i > e$; that is, the matrices $\mathfrak{J}_k$, $k = 1, \ldots, e$, are block, lower triangular matrices of the form

$$\mathfrak{J}_k = \begin{pmatrix} 0 & \cdots & 0 & * & & & & & & & & & \\ 0 & \cdots & 0 & \star & 0 & \cdots & 0 & * & & & & & \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \cdots & & & & \\ 0 & \cdots & 0 & \star & 0 & \cdots & 0 & \star & \cdots & 0 & \cdots & 0 & * \end{pmatrix}$$

where 0 denotes a zero column vector and $*$ a non-zero column vector. Then, $\operatorname{rank}(\mathfrak{J}_k) = k$ for $k = 1, \ldots, e$. Moreover,

$$\mathfrak{J}_{e+1} = \begin{pmatrix} & \mathfrak{J}_e & & & & \\ \frac{\partial F^{(e)}}{\partial x^{(e)}} & \cdots & \cdots & 0 & \cdots & 0 \ * \end{pmatrix}$$

and, by the diagonal structure of

$$\frac{\partial F^{(e)}}{\partial x^{(e)}} = \begin{pmatrix} Q_1(u) & 0 & \cdots & 0 \\ 0 & Q_2(u) & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & Q_n(u) \end{pmatrix},$$

we see that $\operatorname{rank}(\mathfrak{J}_{e+1}) = \operatorname{rank}(\mathfrak{J}_e) + n$.

It follows that the $\mathfrak{P}$-differentiation index of the system equals e. □

Notation 15. We denote by $\mathbb{V} \subset \mathbb{A}^{(e+1)n} \times \mathbb{A}^{2e+1}$ the affine variety defined as the Zariski closure of the solution set of the polynomial system

$$F = 0, \qquad \dot{F} = 0, \ldots, F^{(e)} = 0, \qquad \prod_{1 \leqslant j \leqslant n} Q_j \neq 0,$$

where $F = F_1, \ldots, F_n$ and $F_j(x, u^{[e]}) = Q_j(u^{[e]})x_j - P_j(u^{[e]})$ for every $1 \leqslant j \leqslant n$.

The algebraic ideal corresponding to the variety $\mathbb{V}$ is $(F, \dot{F}, \ldots, F^{(e)}) : q^\infty$, where $q := \prod_{1 \leqslant j \leqslant n} Q_j$. This ideal is prime, since it is the kernel of the map

$$\begin{aligned} \mathcal{F}\left[x^{[e]}, u^{[2e]}\right] &\to \mathcal{F}\left[(P_j/Q_j)^{[e]}_{1 \leqslant j \leqslant n}, u^{[2e]}\right] \\ x_j^{(k)} &\mapsto (P_j/Q_j)^{(k)} \\ u^{(i)} &\mapsto u^{(i)} \end{aligned}$$

Then, $\mathbb{V}$ is an irreducible variety. Moreover, $F, \dot{F}, \ldots, F^{(e)}$ is a reduced complete intersection in $\{q \neq 0\}$ and so, the dimension of $\mathbb{V}$ is $2e + 1$.

Now, the ideal of the variety $\mathbb{V}$ enables us to re-interpret the ideal $\mathfrak{P} \cap \mathcal{F}[x^{[e]}, u^{[e]}]$ where the minimal polynomial M lies:

Proposition 16. *The following equality of ideals holds:*

$$\left(F, \dot{F}, \ldots, F^{(e)}\right) : q^\infty \cap \mathcal{F}\left[x^{[e]}, u^{[e]}\right] = \mathfrak{P} \cap \mathcal{F}\left[x^{[e]}, u^{[e]}\right].$$

Proof. We start showing that

$$\big(F, \dot{F}, \ldots, F^{(e)}\big) : q^{\infty} \cap \mathcal{F}\big[x^{[e]}, u^{[e]}\big] = \big(F, \dot{F}, \ldots, F^{(e)}\big)_{\mathfrak{P}_{2e}} \cap \mathcal{F}\big[x^{[e]}, u^{[e]}\big].$$

First note that $(F, \dot{F}, \ldots, F^{(e)}) : q^{\infty} \subset (F, \dot{F}, \ldots, F^{(e)})_{\mathfrak{P}_{2e}}$ since $q \notin \mathfrak{P}$. Conversely, if $h \in (F, \dot{F}, \ldots, F^{(e)})_{\mathfrak{P}_{2e}} \cap \mathcal{F}[x^{[e]}, u^{[e]}]$, there is a polynomial $g \in \mathcal{F}[x^{[2e]}, u^{[2e]}]$ such that $g \notin \mathfrak{P}$ and $gh \in (F, \dot{F}, \ldots, F^{(e)})$; but $g \notin (F, \dot{F}, \ldots, F^{(e)}) : q^{\infty}$, since otherwise, $q^N g \in (F, \dot{F}, \ldots, F^{(e)}) \subset \mathfrak{P}$ for some $N \in \mathbb{N}$ contradicting the fact that $q \notin \mathfrak{P}$ and $g \notin \mathfrak{P}$. Since $(F, \dot{F}, \ldots, F^{(e)}) : q^{\infty}$ is a prime ideal, it follows that $h \in (F, \dot{F}, \ldots, F^{(e)}) : q^{\infty}$.

Now, Lemma 14 implies that

$$\big(F, \dot{F}, \ldots, F^{(e)}\big)_{\mathfrak{P}_{2e}} \cap \mathcal{F}\big[x^{[e]}, u^{[e]}\big] = [F]_{\mathfrak{P}} \cap \mathcal{F}\big[x^{[e]}, u^{[e]}\big].$$

Finally, since $[F]_{\mathfrak{P}}\mathcal{F}\{x, u\}_{\mathfrak{P}} = \mathfrak{P}_{\mathfrak{P}}\mathcal{F}\{x, u\}_{\mathfrak{P}}$ (see [3, Proposition 3]), we conclude that

$$[F]_{\mathfrak{P}} \cap \mathcal{F}\big[x^{[e]}, u^{[e]}\big] = \mathfrak{P}_{\mathfrak{P}} \cap \mathcal{F}\big[x^{[e]}, u^{[e]}\big] = \mathfrak{P} \cap \mathcal{F}\big[x^{[e]}, u^{[e]}\big];$$

therefore,

$$\big(F, \dot{F}, \ldots, F^{(e)}\big) : q^{\infty} \cap \mathcal{F}\big[x^{[e]}, u^{[e]}\big] = \mathfrak{P} \cap \mathcal{F}\big[x^{[e]}, u^{[e]}\big]. \qquad \square$$

The previous proposition can be applied in order to effectively compute the polynomial $M(x_1, \ldots, x_n, u) \in \mathfrak{P} \backslash (\mathfrak{P} \cap \mathcal{F}\{x_1, \ldots, x_n\})\{u\}$ with minimal rank in u, and consequently a Lüroth generator of the extension $\mathcal{G}/\mathcal{F}$, working over a polynomial ring in finitely many variables (see Proposition 8):

Remark 17. Consider the polynomial ideal $(F, \dot{F}, \ldots, F^{(e)}) : q^{\infty} \subset \mathcal{F}[x^{[e]}, u^{[2e]}]$. Compute a Gröbner basis G of this ideal for a pure lexicographic order with the variables $x^{[e]}$ smaller than the variables $u^{[2e]}$ and $u < \dot{u} < \cdots < u^{(2e)}$. Then, the polynomial M is the smallest polynomial in G which contains at least one variable in $u^{[2e]}$. A Lüroth generator of $\mathcal{G}/\mathcal{F}$ can be obtained from the polynomial M following Proposition 8.

4.3. Degree bounds

In order to estimate the degree of a minimal polynomial $M(x_1, \ldots, x_n, u)$ as in the previous section and, therefore, by Proposition 8, also the degree of a Lüroth generator of $\mathcal{G}/\mathcal{F}$, we will relate M to an eliminating polynomial for the algebraic variety $\mathbb{V}$ under a suitable linear projection.

Let $k_0 \in \mathbb{N}_0$ be the order of u in M. By Proposition 13, we have that $k_0 \leqslant e$ and so, $M \in \mathcal{F}[x^{[e]}, u^{[k_0]}]$. Consider the field extension

$$K := \operatorname{Frac}\big(\mathcal{F}\big[x^{[e]}\big]/\big(\mathfrak{P} \cap \mathcal{F}\big[x^{[e]}\big]\big)\big) \hookrightarrow \operatorname{Frac}\big(\mathcal{F}\big[x^{[e]}, u^{[e]}\big]/\big(\mathfrak{P} \cap \mathcal{F}\big[x^{[e]}, u^{[e]}\big]\big)\big) =: L.$$

The minimality of the rank in u of M is equivalent to the fact that $\{u^{[k_0-1]}\} \subset L$ is algebraically independent over K and M is the minimal polynomial of $u^{(k_0)} \in L$ over $K(u^{[k_0-1]})$.

Then, if $Z \subset \{x^{[e]}\}$ is a transcendence basis of K over $\mathcal{F}$ and we denote $U := \{u^{[k_0-1]}\} \subset L$, we have that $\{Z, U\} \subset L$ is algebraically independent over $\mathcal{F}$ and $\{Z, U, u^{(k_0)}\} \subset L$ is algebraically dependent over $\mathcal{F}$ and, since $L \subset \mathcal{F}(\mathbb{V})$, the same holds in $\mathcal{F}(\mathbb{V})$.

Let N be the cardinality of $\{Z, U\}$. Consider the projection

$$\pi : \mathbb{V} \to \mathbb{A}^{N+1}, \quad \pi\left(x^{[e]}, u^{[2e]}\right) = \left(Z, U, u^{(k_0)}\right). \tag{4}$$

From the construction of Z, U, the dimension of $\pi(\mathbb{V})$ equals N and so, the Zariski closure of $\pi(\mathbb{V})$ is a hypersurface in $\mathbb{A}^{N+1}$. Let $M_0 \in \mathcal{F}[Z, U, u^{(k_0)}]$ be an irreducible polynomial defining this hypersurface (recall that $\mathbb{V}$ is an irreducible variety). From [13, Lemma 2], we have the inequality

$$\deg M_0 \leqslant \deg \mathbb{V}. \tag{5}$$

Note that $M_0 \in \mathfrak{P} \setminus (\mathfrak{P} \cap \mathcal{F}\{x\})\{u\}$ and $\operatorname{ord}_u(M_0) = k_0 = \operatorname{ord}_u(M)$. However, M_0 may not necessarily have the property of minimal rank in u, as the following simple example shows:

Example 1. Let $\mathcal{G} = \mathcal{F}\langle \dot{u}, (\dot{u})^2 \rangle$. Here:

- $e = 1$, $n = 2$,
- $F_1 = x_1 - \dot{u}$, $F_2 = x_2 - (\dot{u})^2$, $q = 1$.

Following our previous construction,

$$\mathbb{V} = V(F_1, F_2, \dot{F}_1, \dot{F}_2) = V\left(x_1 - \dot{u}, x_2 - (\dot{u})^2, \dot{x}_1 - u^{(2)}, x_2^{(2)} - 2\dot{u}u^{(2)}\right)$$

and we can take $Z = \{x_2, \dot{x}_2\}$ and $U = \{u\}$. Then, $M_0 = (\dot{u})^2 - x_2$, which has not minimal rank in u, since $\dot{u} - x_1$ vanishes over $\mathbb{V}$. In fact, $M = \dot{u} - x_1$.

Even though the polynomial M_0 is not the minimal rank polynomial M we are looking for, the following relation between their degrees will be sufficient to obtain a degree upper bound for a Lüroth generator.

Proposition 18. *With the previous assumptions and notation, we have that* $\deg_{(U,u^{(k_0)})}(M) \leqslant \deg_{(U,u^{(k_0)})}(M_0)$. *In particular,* $\deg_{(U,u^{(k_0)})}(M) \leqslant \deg(\mathbb{V})$.

Proof. By construction, M is the minimal polynomial of $u^{(k_0)}$ over $K(U)$ and M_0 is the minimal polynomial of $u^{(k_0)}$ over $\mathcal{F}(Z, U)$. Without loss of generality, we may assume that M and M_0 are polynomials with coefficients in $\mathcal{F}$ having content 1 in $K[U]$ and $\mathcal{F}[Z,U]$ respectively. Since $\mathcal{F}(Z,U) \subset K(U)$, we infer that M divides M_0 in $K[U][u^{(k_0)}]$. The proposition follows taking into account inequality (5). □

Recalling that a Lüroth generator v of $\mathcal{G}/\mathcal{F}$ can be obtained as the quotient of two specializations of the variables $x_1, \ldots, x_n$ and their derivatives in the polynomial M (see Proposition 8) and that two arbitrary generators are related by a homographic map with coefficients in $\mathcal{F}$ (see [15, §1], [21, Ch. II, §44]), we conclude that the degrees of the numerator and the denominator of any Lüroth generator of $\mathcal{G}/\mathcal{F}$ are bounded by the degree of the variety $\mathbb{V}$.

We can exhibit purely syntactic degree bounds for $\mathbb{V}$ in terms of the number n of given generators for $\mathcal{G}/\mathcal{F}$, their maximum order e, and an upper bound d for the degrees of their numerators and denominators.

First, since the variety $\mathbb{V}$ is an irreducible component of the algebraic set defined by the $(e+1)n$ polynomials $F, \dot{F}, \ldots, F^{(e)}$ of total degrees bounded by $d+1$ (here $F = F_1, \ldots, F_n$ and $F_j(x,u) = Q_j(u)x_j - P_j(u)$), Bézout's theorem (see for instance [13, Theorem 1]) implies that

$$\deg \mathbb{V} \leqslant (d+1)^{(e+1)n}.$$

An analysis of the particular structure of the system leads to a different upper bound for $\deg(\mathbb{V})$, which is not exponential in n: taking into account that $\mathbb{V}$ is an irreducible variety of dimension $2e+1$, its degree is the number of points in its intersection with a generic linear variety of codimension $2e+1$, that is,

$$\deg \mathbb{V} = \#\big(\mathbb{V} \cap V(L_1, \ldots, L_{2e+1})\big),$$

where, for every $1 \leqslant i \leqslant 2e+1$, L_i is a generic affine linear form in the variables $x^{[e]}, u^{[2e]}$,

$$L_i\big(x^{[e]}, u^{[2e]}\big) = \sum_{\substack{1 \leqslant j \leqslant n \\ 0 \leqslant k \leqslant e}} a_{ijk} x_j^{(k)} + \sum_{0 \leqslant k \leqslant 2e} b_{ik} u^{(k)} + c_i. \tag{6}$$

For every $1 \leqslant j \leqslant n$, the equation $F_j(x_j, u) = 0$ implies that, generic points of $\mathbb{V}$ satisfy $x_j = P_j(u)/Q_j(u)$. Proceeding inductively, it follows easily that, generically

$$x_j^{(k)} = \left(\frac{P_j(u)}{Q_j(u)}\right)^{(k)} = \frac{R_{jk}(u^{[e+j]})}{Q_j(u^{[e]})^{k+1}} \quad \text{with } \deg(R_{jk}) \leqslant d(k+1)$$

for every $1 \leqslant j \leqslant n$, $0 \leqslant k \leqslant e$. Substituting these formulae into (6) and clearing denominators, we deduce that the degree of $\mathbb{V}$ equals the number of common solutions of the system defined by the $2e+1$ polynomials

$$\mathbb{L}_i\big(u^{[2e]}\big) := \Big(\prod_{1\leqslant j\leqslant n} Q_j^{e+1}\Big)\, L_i\bigg(\bigg(\frac{P_1}{Q_1},\dots,\frac{P_n}{Q_n}\bigg)^{[e]}, u^{[2e]}\bigg)$$
$$= \sum_{\substack{1\leqslant j\leqslant n\\ 0\leqslant k\leqslant e}} a_{ijk}R_{jk}Q_j^{e-k}\prod_{h\neq j} Q_h^{e+1} + \sum_{0\leqslant k\leqslant 2e} b_{ik}u^{(k)}\prod_{1\leqslant j\leqslant n} Q_j^{e+1} + c_i\prod_{1\leqslant j\leqslant n} Q_j^{e+1}$$

for generic coefficients a_{ijk}, b_{ik}, c_i and the inequality $q \neq 0$. From the upper bounds for the degrees of the polynomials Q_j, R_{jk}, it follows that $\mathbb{L}_i$ is a polynomial of total degree bounded by $nd(e+1)+1$ for every $1 \leqslant i \leqslant 2e+1$. Therefore, Bézout's bound implies that

$$\deg \mathbb{V} \leqslant \big(nd(e+1)+1\big)^{2e+1}.$$

We conclude that:

Proposition 19. *Under the previous assumptions and notation, the degrees of the numerator and the denominator of any Lüroth generator of $\mathcal{G}/\mathcal{F}$ are bounded by* $\min\{(d+1)^{(e+1)n}, (nd(e+1)+1)^{2e+1}\}$. □

This completes the proof of Theorem 1.

5. Examples

As before, let $\mathcal{F}$ be a differential field of characteristic 0 and u a differentially transcendental element over $\mathcal{F}$.

Example 2. Let $\mathcal{G} = \mathcal{F}\langle u/\dot{u}, u+\dot{u}\rangle$. In this case, we have:

- $e = 1$, $n = 2$,
- $F_1 = \dot{u}x_1 - u$, $F_2 = x_2 - u - \dot{u}$, $q = \dot{u}$.

As the ideal $(F_1, F_2, \dot{F}_1, \dot{F}_2) = (\dot{u}x_1 - u, x_2 - u - \dot{u}, u^{(2)}x_1 + \dot{u}\dot{x}_1 - \dot{u}, \dot{x}_2 - \dot{u} - u^{(2)})$ is prime and does not contain $\dot{u}$, we have that $(F_1, F_2, \dot{F}_1, \dot{F}_2) : q^\infty = (F_1, F_2, \dot{F}_1, \dot{F}_2)$ and, therefore,

$$\mathbb{V} = V(F_1, F_2, \dot{F}_1, \dot{F}_2) = V\big(\dot{u}x_1 - u, x_2 - u - \dot{u}, u^{(2)}x_1 + \dot{u}\dot{x}_1 - \dot{u}, \dot{x}_2 - \dot{u} - u^{(2)}\big).$$

The dimension of $\mathbb{V}$ equals 3 and $\{x_1, x_2, \dot{x}_1\}$ is a transcendence basis of $\mathcal{F}(\mathbb{V})$ over $\mathcal{F}$. Then, $k_0 = 0$ and so, we look for a polynomial $M_0(x_1, x_2, \dot{x}_1, u) \in (F_1, F_2, \dot{F}_1, \dot{F}_2)$. It is easy to see that

$$M_0(x_1, x_2, \dot{x}_1, u) = (x_1 + 1)u - x_1x_2.$$

Since $\deg_u(M_0) = 1$ we can take $M = M_0$. Finally, specializing $(u, \dot{u}, u^{(2)})$ into $u_1 = (1, 1, 0)$ and $u_2 = (0, 1, 0)$, we compute specialization points $(1, 2, 1)$ and $(0, 1, 1)$ respectively for $(x_1, x_2, \dot{x}_1)$; hence, we obtain the following Lüroth generator for $\mathcal{G}/\mathcal{F}$:

$$v = \frac{P(u)}{Q(u)} = \frac{2u - 2}{u}.$$

In the previous example, the polynomial M lies in the polynomial ideal (F_1, F_2), that is, no differentiation of the equations is needed in order to compute it and, consequently, a Lüroth generator can be obtained as an algebraic rational function of the given generators. However, this is not always the case, as the following example shows.

Example 3. Let $\mathcal{G} = \mathcal{F}\langle \dot{u}, u + u^{(2)} \rangle$. We have:

- $e = 2$, $n = 2$,
- $F_1 = x_1 - \dot{u}$, $F_2 = x_2 - u - u^{(2)}$, $q = 1$.

Following our previous arguments, we consider the ideal

$$\begin{aligned} &\bigl(F_1, F_2, \dot{F}_1, \dot{F}_2, F_1^{(2)}, F_2^{(2)}\bigr) \\ &\quad = \bigl(x_1 - \dot{u}, x_2 - u - u^{(2)}, \dot{x}_1 - u^{(2)}, \dot{x}_2 - \dot{u} - u^{(3)}, x_1^{(2)} - u^{(3)}, x_2^{(2)} - u^{(2)} - u^{(4)}\bigr). \end{aligned}$$

This is a prime ideal of $\mathcal{F}[x^{[2]}, u^{[4]}]$. The variety $\mathbb{V}$ is the zero-set of this ideal and it has dimension 5. A transcendence basis of $\mathcal{F}(\mathbb{V})$ over $\mathcal{F}$ including a maximal subset of $x^{[2]}$ is $\{x_1, x_2, \dot{x}_1, \dot{x}_2, x_2^{(2)}\}$ and the minimal polynomial of u over $\mathcal{F}(x_1, x_2, \dot{x}_1, \dot{x}_2, x_2^{(2)})$ is

$$M_0 = u - x_2 + \dot{x}_1.$$

Again, since $\deg_u(M_0) = 1$, we can take $M = M_0$. Two specializations of this polynomial lead us to a Lüroth generator of $\mathcal{G}/\mathcal{F}$ of the form $v = \frac{u+a}{u+b}$. We conclude that $\mathcal{G} = \mathcal{F}\langle u \rangle$.

6. Conclusions

We give degree and order upper bounds for a Lüroth generator of a differential field generated by a finite number of differential rational functions in one variable.

These bounds can be applied to effectively compute a Lüroth generator working in a polynomial ring in finitely many variables. Although these computations can be done by means of Gröbner bases techniques, we expect that more specific symbolic algorithms with better complexity bounds could be designed following Kronecker's approach (see [9] and [10]) adapted to the differential setting in the spirit of [4]. This will be the subject of our future work.

Acknowledgments

We thank the anonymous reviewers for their comments and suggestions, especially the one who pointed out a mistake in the original version of this paper. We are also grateful to Teresa Krick and Juan Sabia for very helpful discussions.

References

[1] C. Alonso, J. Gutiérrez, T. Recio, A rational function decomposition algorithm by near-separated polynomials, J. Symbolic Comput. 19 (1995).

[2] G. Chèze, Nearly optimal algorithms for the decomposition of multivariate rational functions and the extended Lüroth's theorem, J. Complexity 26 (4) (2010) 344–363.

[3] L. D'Alfonso, G. Jeronimo, G. Massaccesi, P. Solernó, On the index and the order of quasi-regular implicit systems of differential equations, Linear Algebra Appl. 430 (2009) 2102–2122.

[4] L. D'Alfonso, G. Jeronimo, F. Ollivier, A. Sedoglavic, P. Solernó, A geometric index reduction method for implicit systems of differential algebraic equations, J. Symbolic Comput. 46 (10) (2011) 1114–1138.

[5] L. D'Alfonso, G. Jeronimo, P. Solernó, On the complexity of the resolvent representation of some prime differential ideals, J. Complexity 22 (3) (2006) 396–430.

[6] M. Fliess, J. Lévine, Ph. Martin, P. Rouchon, A Lie–Bäcklund approach to equivalence and flatness of nonlinear systems, IEEE Trans. Automat. Control 44 (5) (1999) 922–937.

[7] M. Fliess, Variations sur la notion de contrôlabilité, in: Quelques aspects de la théorie du contrôle, SMF J. Annu., 2000, Soc. Math. France, Paris, 2000, pp. 47–86.

[8] X. Gao, T. Xu, Lüroth's theorem in differential fields, J. Syst. Sci. Complex. 15 (4) (2002) 376–383.

[9] M. Giusti, J. Heintz, K. Hägele, J.E. Morais, L.M. Pardo, J.L. Montaña, Lower bounds for Diophantine approximations, in: Algorithms for Algebra, Eindhoven, 1996, in: J. Pure Appl. Algebra, vols.117/118, 1997, pp. 277–317.

[10] M. Giusti, J. Heintz, J.E. Morais, J. Morgenstern, L.M. Pardo, Straight-line programs in geometric elimination theory, J. Pure Appl. Algebra 124 (1–3) (1998) 101–146.

[11] J. Gutiérrez, R. Rubio, D. Sevilla, On multivariate rational function decomposition, in: Computer Algebra, London, ON, 2001, J. Symbolic Comput. 33 (5) (2002) 545–562.

[12] J. Gutiérrez, R. Rubio, D. Sevilla, Unirational fields of transcendence degree one and functional decomposition, in: Proc. of the 2001 Int. Symposium on Symb. and Alg. Comput., ISSAC'01, ACM Press, New York, 2001, pp. 167–174.

[13] J. Heintz, Definability and fast quantifier elimination in algebraically closed fields, Theoret. Comput. Sci. 24 (3) (1983) 239–277.

[14] E.R. Kolchin, Differential Algebra and Algebraic Groups, Academic Press, New York, 1973.

[15] E.R. Kolchin, Extensions of differential fields, II, Ann. of Math. (2) 45 (1944) 358–361.

[16] E.R. Kolchin, Extensions of differential fields, III, Bull. Amer. Math. Soc. 53 (1947) 397–401.

[17] J. Lüroth, Beweis eines Satzes über rationale curven, Math. Ann. 9 (1876) 163–165.

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

[19] F. Ollivier, Une réponse négative au problème de Lüroth différentiel en dimension 2, C. R. Math. Acad. Sci. Paris, Ser. I 327 (10) (1998) 881–886.

[20] J.F. Ritt, Differential Equations from the Algebraic Standpoint, Amer. Math. Soc. Colloq. Publ., vol. XIV, Amer. Math. Soc., New York, 1932.

[21] J.F. Ritt, Differential Algebra, Amer. Math. Soc. Colloq. Publ., vol. 33, Amer. Math. Soc., New York, 1950.

[22] B. Sadik, A bound for the order of characteristic set elements of an ordinary prime differential ideal and some applications, Appl. Algebra Engrg. Comm. Comput. 10 (3) (2000) 251–268.

[23] T.W. Sederberg, Improperly parametrized rational curves, Comput. Aided Geom. Design 3 (1986) 67–75.

[24] B.L. van der Waerden, Modern Algebra, vol. I, Springer-Verlag, 1991.