Journal of Algebra ••• (••••) •••–•••

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

# Quantitative aspects of the generalized differential Lüroth's Theorem ☆

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

[a] *Universidad de Buenos Aires, Ciclo Básico Común, Departamento de Ciencias Exactas, Área Matemática, Buenos Aires, Argentina*
[b] *Universidad de Buenos Aires, Facultad de Ciencias Exactas y Naturales, Departamento de Matemática, Buenos Aires, Argentina*
[c] *Universidad de Buenos Aires, Consejo Nacional de Investigaciones Científicas y Técnicas, Instituto de Investigaciones Matemáticas Luis A. Santaló (IMAS), Buenos Aires, Argentina*

ARTICLE INFO

*Article history:*
Received 25 January 2017
Available online xxxx
Communicated by Bruno Salvy

*MSC:*
12Y05
12H05

*Keywords:*
Differential algebra
Lüroth's Theorem
Differentiation index

ABSTRACT

Let $\mathcal{F}$ be a differential field of characteristic 0, $\mathbf{t} = t_1, \ldots, t_m$ a finite set of differential indeterminates over $\mathcal{F}$ and $\mathcal{G} \subset \mathcal{F}\langle \mathbf{t} \rangle$ a differential field extension of $\mathcal{F}$, generated by nonconstant rational functions $\alpha_1, \ldots, \alpha_n$ of total degree and order bounded by $d$ and $e \geq 1$ respectively. The generalized differential Lüroth's Theorem states that if the differential transcendence degree of $\mathcal{G}$ over $\mathcal{F}$ is 1, there exists $v \in \mathcal{G}$ such that $\mathcal{G} = \mathcal{F}\langle v \rangle$. We prove a new explicit upper bound for the degree of $v$ in terms of $n, m, d$ and $e$. Further, we exhibit an effective procedure to compute $v$.



☆ Partially supported by Universidad de Buenos Aires: UBACYT 20020120100133BA (2013–2016) and UBACYT 20020160100039BA (2017).

* Corresponding author at: Universidad de Buenos Aires, Facultad de Ciencias Exactas y Naturales, Departamento de Matemática, Buenos Aires, Argentina.
*E-mail addresses:* lisi@cbc.uba.ar (L. D'Alfonso), jeronimo@dm.uba.ar (G. Jeronimo), psolerno@dm.uba.ar (P. Solernó).

https://doi.org/10.1016/j.jalgebra.2018.01.050
0021-8693/

## 1. Introduction

Let $\mathcal{F}$ be a differential field, $\mathbf{t} = t_1, \ldots, t_m$ a finite set of differential indeterminates over $\mathcal{F}$ and $\mathcal{G} \subset \mathcal{F}\langle \mathbf{t} \rangle$ a differential field extension of $\mathcal{F}$. The *generalized differential Lüroth's Theorem* states that *if the differential transcendence degree of $\mathcal{G}$ over $\mathcal{F}$ is* 1*, then there exists $v \in \mathcal{G}$ such that $\mathcal{G} = \mathcal{F}\langle v \rangle$*. The case $m = 1$ is the classical differential Lüroth's Theorem.

This theorem is a differential generalization of similar results valid in the *algebraic* framework: the classical *algebraic* result (i.e. for $m = 1$) is established by Lüroth in 1876 (see [16]). Its extension for an arbitrary integer $m$ in the case of characteristic 0 is given by Gordan ten years later in [7] and in 1951, Igusa [10] shows the generalization for arbitrary characteristic.

In the differential setting, the first version of the classical *differential* Lüroth's Theorem is given by Ritt in 1932 (see [17]) for the field of complex meromorphic functions and extended by Kolchin in [12] and [13] for any differential base field of characteristic 0. Moreover, in his book [11] Kolchin points out that the arguments given by Ritt and himself could be adapted in order to prove the *generalized* differential Lüroth's Theorem for an arbitrary integer $m$ (see [11, Ch. IV, Section 7, Exercise 2]).

The present paper deals with quantitative aspects of the generalized differential Lüroth's Theorem. More precisely, suppose that the intermediate field $\mathcal{G}$ is finitely generated over $\mathcal{F}$ by differential nonconstant rational functions $\alpha_1, \ldots, \alpha_n \in \mathcal{F}\langle \mathbf{t} \rangle$ whose total degrees are bounded by an integer $d$ (the total degree of a rational function is defined as the maximum of the total degrees of the numerator and the denominator in an irreducible representation). Let $e$ be an upper bound for the order of $\alpha_1, \ldots, \alpha_n$, which for technical reasons we assume to be at least 1. We are interested in the determination of *a priori* bounds for the order and the degree of a *Lüroth generator* $v$ in terms of the parameters $m, n, d, e$ and in the design of an effective method to find $v$.

An elementary calculation shows that the order of any Lüroth generator is bounded by the minimum of the orders of the generators $\alpha_j$ (see for instance [3, Proposition 5]).

Obtaining an upper bound for the degrees of the polynomials describing the Lüroth generator is a more delicate task. The first results for the case $m = 1$ are given in [3] and [4]. In the present paper, we get new bounds for arbitrary $m$ by suitably adapting and extending the main arguments in our previous paper [3]: in Theorem 17 below, we show that any Lüroth generator $v$ of $\mathcal{G}$ over $\mathcal{F}$ has total degree bounded by

$$\min\left\{\big((d+1)\big((n+\mu-1)d+1\big)\big)^{\min\{m,2\}e+1}\ ,\ (d+1)^{n(\min\{m,n\}e+1)}\right\},$$

where $\mu$ is the minimal order of any variable appearing in $\alpha_1, \ldots, \alpha_n$. Moreover, if the ground differential field $\mathcal{F}$ contains a nonconstant element, we obtain the better bound

$$\min\left\{\big((d+1)((n-1)d+1)\big)^{\min\{m,2\}e+1}\ ,\ (d+1)^{n(\min\{m,n\}e+1)}\right\}.$$

Please cite this article in press as: L. D'Alfonso et al., Quantitative aspects of the generalized differential Lüroth's Theorem, J. Algebra (2018), https://doi.org/10.1016/j.jalgebra.2018.01.050

These bounds lead to new bounds also for the case $m = 1$ (see Corollary 18). In this special case our estimations improve those of [3] and [4], except when $d$ is large enough with respect to the other parameters (see Section 4.4 for a more detailed comparison with previous results).

Independently of these degree bounds, our approach also allows us to deduce an effective method to decide if a differential extension $\mathcal{G} \subset \mathcal{F}\langle \mathbf{t} \rangle$, finitely generated over $\mathcal{F}$, has differential transcendence degree 1 and, in the affirmative case, compute a Lüroth generator (see Section 5). Previous algorithms for the computation of a Lüroth generator in the classical differential case can be found in [5] and [3].

The paper is organized as follows: in Section 2 we introduce basic definitions and notations from standard differential algebra. Section 3 is devoted to introducing the differential generalized Lüroth's Theorem and the approach given by Kolchin. The core of the paper is Section 4, where the degree upper bounds for a Lüroth generator are discussed. In Section 5 an effective procedure to compute a Lüroth generator and an example illustrating our results are presented.

## 2. Preliminaries

In this section we introduce the notation we will use 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 $\delta$; 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 $\alpha$ indeterminates $\mathbf{z} := z_1, \ldots, z_\alpha$, which is denoted by $\mathcal{F}\{z_1, \ldots, z_\alpha\}$ or simply $\mathcal{F}\{\mathbf{z}\}$, is defined as the commutative polynomial ring $\mathcal{F}[z_j^{(p)}, 1 \leq j \leq \alpha,\ p \in \mathbb{N}_0]$ (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 $i$th derivative of $z_j$ (as customarily, the first derivatives are also denoted by $\dot{z}_j$). We write $\mathbf{z}^{(p)} := z_1^{(p)}, \ldots, z_\alpha^{(p)}$ and $\mathbf{z}^{[p]} := \mathbf{z}, \mathbf{z}^{(1)}, \ldots, \mathbf{z}^{(p)}$ for every $p \in \mathbb{N}_0$.

The fraction field of $\mathcal{F}\{\mathbf{z}\}$ is a differential field, denoted by $\mathcal{F}\langle \mathbf{z} \rangle$, with the derivation obtained by extending the derivation $\delta$ to the quotients in the usual way. For $g \in \mathcal{F}\{\mathbf{z}\}$, the *order of $g$ with respect to $z_j$* is $\operatorname{ord}(g, z_j) := \max\{i \in \mathbb{N}_0 : z_j^{(i)} \text{ appears in } g\}$. If a variable $z_j$ does not occur in $g$, we set $\operatorname{ord}(g, z_j) := -\infty$. The *order of $g$* is $\operatorname{ord}(g) := \max\{\operatorname{ord}(g, z_j) : 1 \leq j \leq \alpha\}$. This notion of order extends naturally to $\mathcal{F}\langle \mathbf{z} \rangle$ by taking the maximum of the orders of the numerator and the denominator in a reduced representation of the rational fraction.

Please cite this article in press as: L. D'Alfonso et al., Quantitative aspects of the generalized differential Lüroth's Theorem, J. Algebra (2018), https://doi.org/10.1016/j.jalgebra.2018.01.050

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

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 $\Sigma$.

A family of elements $(\xi_i)_{i\in I}$ in $\mathcal{G}$ is said to be *differentially algebraically independent* over $\mathcal{F}$ (or a family of *differential indeterminates* over $\mathcal{F}$) if the family of its derivatives $\{\xi_i^{(p)} : i \in I, p \in \mathbb{N}_0\}$ is algebraically independent over $\mathcal{F}$; otherwise, it is said to be *differentially algebraically dependent* over $\mathcal{F}$. In the special case in which $\Sigma$ consists of a single element $\xi \in \mathcal{G}$, then $\xi$ is said to be, correspondingly, *differentially transcendental* or *differentially algebraic*. If every $\xi \in \mathcal{G}$ is differentially algebraic over $\mathcal{F}$, we say that $\mathcal{G}/\mathcal{F}$ is *differentially algebraic* over $\mathcal{F}$.

A *differential transcendence basis* of a differential field extension $\mathcal{G}/\mathcal{F}$ 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 [11, Ch. II, Sec. 9, Theorem 4]), which is called its *differential transcendence degree*.

### 2.2. Differential polynomials and ideals

Here we recall some definitions and properties concerning differential polynomials and differential ideals.

A *ranking* on a finite family of differential indeterminates $\mathbf{z} := z_1, \ldots, z_\alpha$ is a total order $\prec$ in the set $\Theta(\mathbf{z}) := \{z_i^{(l)} : l \in \mathbb{N}_0\}$ satisfying $u \prec \delta(u)$, for every $u \in \Theta(\mathbf{z})$, and $\delta(u) \prec \delta(v)$ if $u \prec v$, for all $u, v \in \Theta(\mathbf{z})$. A ranking on $\mathbf{z}$ is an *orderly ranking* if $z_i^{(r)} \prec z_j^{(s)}$ whenever $r < s$, and it is an *elimination ranking* with $z_1 \prec z_2 \prec \cdots \prec z_\alpha$ if $z_i^{(r)} \prec z_j^{(s)}$ whenever $i < j$. If $\mathbf{w}$ and $\mathbf{z}$ are two disjoint subsets of a set of differential indeterminates and $\prec_\mathbf{w}$ and $\prec_\mathbf{z}$ are rankings on $\mathbf{w}$ and $\mathbf{z}$ respectively, the induced *block elimination ranking with* $\mathbf{w} \ll \mathbf{z}$ is the ranking on $\mathbf{w}, \mathbf{z}$ defined by the conditions that any element of $\Theta(\mathbf{w})$ is smaller than any element of $\Theta(\mathbf{z})$ and two elements of $\Theta(\mathbf{w})$ (respectively $\Theta(\mathbf{z})$) are ordered according to $\prec_\mathbf{w}$ (respectively $\prec_\mathbf{z}$).

Assume that a ranking on $\mathbf{z}$ is fixed. Let $g \in \mathcal{F}\{\mathbf{z}\} \setminus \mathcal{F}$. The *leader* of $g$, denoted by $\ell(g)$, is the greatest element of $\Theta(\mathbf{z})$ appearing in $g$. If the polynomial $g$ is considered as a polynomial in the variable $\ell(g)$, its leading coefficient, denoted by $I_g$, is called the *initial* of $g$, and $S_g := \partial g/\partial \ell(g)$ is the *separant* of $g$.

From a given ranking on $\mathbf{z}$, a comparative *rank* can be defined in the whole differential polynomial ring $\mathcal{F}\{\mathbf{z}\}$ as follows:

- Every element of $\mathcal{F}$ has lower rank than every element of $\mathcal{F}\{\mathbf{z}\} \setminus \mathcal{F}$.

Please cite this article in press as: L. D'Alfonso et al., Quantitative aspects of the generalized differential Lüroth's Theorem, J. Algebra (2018), https://doi.org/10.1016/j.jalgebra.2018.01.050

- If $A, B \in \mathcal{F}\{\mathbf{z}\} \setminus \mathcal{F}$, and if either $\ell(A) \prec \ell(B)$, or $\ell(A) = \ell(B)$ and $\deg_{\ell(A)}(A) < \deg_{\ell(B)}(B)$, then $A$ has lower rank than $B$.
- Two elements of $\mathcal{F}\{\mathbf{z}\}$ that either are both in $\mathcal{F}$ or have the same leader and the same degree in that leader have the same rank.

We will also use some elementary facts of the well-known theory of *characteristic sets*. For the definitions and basic properties, we refer the reader to [11, Ch. I, §8–10].

Every radical differential ideal $\{H\}$ of $\mathcal{F}\{\mathbf{z}\}$ has a unique representation as a finite irredundant intersection of prime differential ideals, which are called the *essential prime divisors* of $\{H\}$ (see [18, Ch. II, §16–17]). For an algebraically irreducible differential polynomial $g$ in $\mathcal{F}\{\mathbf{z}\}$, there is only one essential prime divisor of $\{g\}$, which will be denoted $\mathfrak{p}_{\mathcal{F}}(g)$, that does not contain any separant of $g$; this prime differential ideal is called the *general component of $g$ in $\mathcal{F}\{\mathbf{z}\}$* (see [11, Ch. IV, Sect. 6]).

Let $\mathfrak{P}$ be a prime differential ideal of $\mathcal{F}\{\mathbf{z}\}$. The *differential dimension* of $\mathfrak{P}$, denoted by $\operatorname{diffdim}(\mathfrak{P})$, is the differential transcendence degree of the extension $\mathcal{F} \hookrightarrow \operatorname{Frac}(\mathcal{F}\{\mathbf{z}\}/\mathfrak{P})$ (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:

$$H_{\mathfrak{P},\mathcal{F}}(i) \quad := \quad \begin{array}{l}\text{the (algebraic) transcendence degree of} \\ \operatorname{Frac}(\mathcal{F}[\mathbf{z}^{[i]}]/(\mathfrak{P} \cap \mathcal{F}[\mathbf{z}^{[i]}])) \text{ over } \mathcal{F}.\end{array}$$

For $i$ sufficiently large, 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 called the *order* of $\mathfrak{P}$ ([11, 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 $\mathfrak{P}$, we say that $F$ is *quasi-regular* at $\mathfrak{P}$ if, for every $k \in \mathbb{N}_0$, and every upper order bound $e$, the Jacobian matrix of the polynomials $F, \dot{F}, \ldots, F^{(k)}$ with respect to the variables $\mathbf{z}^{[e+k]}$ has full row rank over the fraction field of $\mathcal{F}\{\mathbf{z}\}/\mathfrak{P}$. Observe that this condition is independent of the choice of the upper bound $e$ for the order, since for $e > \operatorname{ord}(F)$ the partial derivatives of $F^{(k)}$ with respect to $\mathbf{z}^{[e+k]}$ are zero.

## 3. Differential Lüroth's Theorem

In [17, Chapter VIII] (see also [18] and [11]), the classical Lüroth's Theorem for transcendental field extensions is generalized to the differential algebra framework:

**Theorem 1** *(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 $\mathcal{G} = \mathcal{F}\langle v\rangle$.*

Please cite this article in press as: L. D'Alfonso et al., Quantitative aspects of the generalized differential Lüroth's Theorem, J. Algebra (2018), https://doi.org/10.1016/j.jalgebra.2018.01.050

The following generalization of this result is proposed in [11, Ch. IV, Sect. 7, Exercise 2.b)]:

**Theorem 2** *(Generalized differential Lüroth's Theorem). Let $\mathcal{F}$ be an ordinary differential field of characteristic 0 and let $\mathbf{t} = t_1, \ldots, t_m$ be differentially algebraically independent over $\mathcal{F}$. Let $\mathcal{G}$ be a differential field such that $\mathcal{F} \subset \mathcal{G} \subset \mathcal{F}\langle \mathbf{t} \rangle$ and the differential transcendence degree of $\mathcal{G}/\mathcal{F}$ is 1. Then, there is an element $v \in \mathcal{G}$ such that $\mathcal{G} = \mathcal{F}\langle v \rangle$.*

This paper is concerned with effective aspects of this result. More precisely: for $n > 1$, let be given differential polynomials $P_1, \ldots, P_n$, $Q_1, \ldots, Q_n \in \mathcal{F}\{\mathbf{t}\}$, with $P_j/Q_j \notin \mathcal{F}$ and $P_j, Q_j$ relatively prime polynomials for every $1 \leq j \leq n$, such that

$$\mathcal{G} := \mathcal{F}\langle P_1(\mathbf{t})/Q_1(\mathbf{t}), \ldots, P_n(\mathbf{t})/Q_n(\mathbf{t}) \rangle$$

is a differential subextension of $\mathcal{F}\langle \mathbf{t} \rangle/\mathcal{F}$ with differential transcendence degree over $\mathcal{F}$ equal to 1. We are interested in the study of *a priori* upper bounds for the orders and degrees of a pair of differential polynomials $P, Q \in \mathcal{F}\{\mathbf{t}\}$ such that $Q \not\equiv 0$ and $\mathcal{G} = \mathcal{F}\langle P(\mathbf{t})/Q(\mathbf{t}) \rangle$. In addition, we want to show an effective procedure to determine whether the given differential field extension $\mathcal{G}/\mathcal{F}$ has differential transcendence degree equal to 1 and, if this is the case, to compute a Lüroth generator $v = P(\mathbf{t})/Q(\mathbf{t})$ of $\mathcal{G}/\mathcal{F}$.

As in the univariate case of the Differential Lüroth's Theorem, an optimal estimate for the order of the polynomials $P$ and $Q$ can be obtained straightforwardly (see for instance [3, Proposition 5]):

**Proposition 3.** *Under the previous assumptions and notation, any element $v \in \mathcal{G}$ such that $\mathcal{G} = \mathcal{F}\langle v \rangle$ satisfies* $\operatorname{ord}(v) \leq \min\{\operatorname{ord}(P_j/Q_j) : 1 \leq j \leq n\}$.

The problem of estimating the degrees requires a more careful analysis that we will do in the subsequent sections of the paper.

### *3.1. Kolchin's approach*

We start by sketching a proof of Theorem 2 following the approach suggested in [11, Ch. IV, Sect. 7, Exercise 2].

Let $\mathbf{y} = y_1, \ldots, y_m$ be new differential indeterminates over the field $\mathcal{F}\langle \mathbf{t} \rangle$ and consider the differential ideal $\Xi$ of all differential polynomials in $\mathcal{G}\{\mathbf{y}\}$ vanishing when evaluated at $\mathbf{t} = t_1, \ldots, t_m$:

$$\Xi := \{A \in \mathcal{G}\{\mathbf{y}\} \text{ such that } A(\mathbf{t}) = 0\}, \tag{1}$$

that is, the kernel of the map of differential rings

Please cite this article in press as: L. D'Alfonso et al., Quantitative aspects of the generalized differential Lüroth's Theorem, J. Algebra (2018), https://doi.org/10.1016/j.jalgebra.2018.01.050

$$\begin{array}{ccccl} \phi : \mathcal{G}\{y_1, \ldots, y_m\} & \to & \mathcal{F}\langle t_1, \ldots, t_m\rangle & & \\ y_i & \mapsto & t_i & & \text{for } 1 \leq i \leq m \\ c & \mapsto & c & & \text{for } c \in \mathcal{G}. \end{array}$$

Since the fraction field of the image of this map is $\mathcal{F}\langle \mathbf{t}\rangle$ and the differential transcendence degree of $\mathcal{F}\langle \mathbf{t}\rangle/\mathcal{G}$ equals $m-1$, it follows that $\Xi$ is a prime differential ideal of differential dimension $m-1$. By [11, Ch. IV, Proposition 4], there is an irreducible polynomial $A \in \mathcal{G}\{\mathbf{y}\}$ of order $\epsilon := \mathrm{ord}(\Xi)$ such that $\Xi = \mathfrak{p}_{\mathcal{G}}(A)$, that is, it is the general component of the differential ideal $[A]$. Moreover, if we consider an orderly ranking in the variables $\mathbf{y}$, then $A$ is a polynomial of minimal rank among all the polynomials in $\Xi$.

We may assume that some coefficient of $A$ equals 1. Note that not every coefficient of $A$ lies in $\mathcal{F}$, since $\mathbf{t}$ is differentially algebraically independent over $\mathcal{F}$.

Multiplying $A \in \mathcal{G}\{\mathbf{y}\} \subset \mathcal{F}\langle \mathbf{t}\rangle\{\mathbf{y}\}$ by the lowest common multiple of the denominators of its coefficients, we obtain a differential polynomial $B \in \mathcal{F}\{\mathbf{t}, \mathbf{y}\}$ with no factor in $\mathcal{F}\{\mathbf{t}\}$ and $\mathrm{ord}_{\mathbf{y}}(B) = \mathrm{ord}(A) = \epsilon$. It can be seen that $B$ is a square-free polynomial such that all its irreducible factors have order $\epsilon$ in the variables $\mathbf{y}$ and involve the variables $\mathbf{t}$.

Let $b_1(\mathbf{t}), b_2(\mathbf{t})$ be two non-zero coefficients of $B$ (considered as a polynomial in $\mathcal{F}\langle \mathbf{t}\rangle\{\mathbf{y}\}$) such that $b_1(\mathbf{t})/b_2(\mathbf{t}) \notin \mathcal{F}$. Then, $v := b_1(\mathbf{t})/b_2(\mathbf{t}) \in \mathcal{G}$, since it is the quotient of the corresponding coefficients of $A \in \mathcal{G}\{\mathbf{y}\}$ (recall that $B$ is a multiple of $A$ by a polynomial in $\mathcal{F}\{\mathbf{t}\}$).

**Claim.** *The element $v$ is a Lüroth generator for $\mathcal{G}/\mathcal{F}$.*

Write $v = H(\mathbf{t})/K(\mathbf{t})$, with $H, K \in \mathcal{F}\{\mathbf{t}\}$ relatively prime polynomials. Note that $vK(\mathbf{y}) - H(\mathbf{y}) \in \Xi$, so its order is at least $\epsilon = \mathrm{ord}(A)$. Let $\rho = \mathrm{ord}_{\mathbf{t}}(B)$. Since $\mathrm{ord}(H), \mathrm{ord}(K) \leq \mathrm{ord}_{\mathbf{t}}(B)$, it follows that $\epsilon \leq \rho$.

Consider the differential polynomial

$$\Upsilon(\mathbf{t}, \mathbf{y}) = H(\mathbf{t})K(\mathbf{y}) - K(\mathbf{t})H(\mathbf{y}) \in \mathcal{F}\{\mathbf{t}, \mathbf{y}\}.$$

By looking at the irreducible factors of $B \in \mathcal{F}\{\mathbf{t}, \mathbf{y}\}$ successively by decreasing order in the variables $\mathbf{t}$, it is not difficult to see that each of them divides $\Upsilon$. Taking into account that $\deg_{\mathbf{t}}(B) \geq \deg(H), \deg(K)$, it follows that $\Upsilon$ is a multiple of $B$ by a factor $C(\mathbf{y}) \in \mathcal{F}\{\mathbf{y}\}$. By symmetry, we deduce that $C(\mathbf{t})$ divides $\Upsilon$ and so, it also divides $B(\mathbf{t}, \mathbf{y})$, which implies that $C$ is constant. We conclude that $\rho = \epsilon$ and

$$H(\mathbf{t})K(\mathbf{y}) - K(\mathbf{t})H(\mathbf{y}) = aB(\mathbf{t}, \mathbf{y}), \quad a \in \mathcal{F},$$

and so,

$$vK(\mathbf{y}) - H(\mathbf{y}) = \alpha A(\mathbf{y}), \quad \alpha \in \mathcal{G}. \tag{2}$$

Please cite this article in press as: L. D'Alfonso et al., Quantitative aspects of the generalized differential Lüroth's Theorem, J. Algebra (2018), https://doi.org/10.1016/j.jalgebra.2018.01.050

The claim follows now easily by showing that every $\theta = H_\theta(\mathbf{t})/K_\theta(\mathbf{t}) \in \mathcal{G}$ remains fixed by any isomorphism of $\mathcal{F}\langle\mathbf{t}\rangle$ relative to $\mathcal{F}\langle v\rangle$, which is a consequence of the fact that $\theta K_\theta(\mathbf{y}) - H_\theta(\mathbf{y}) \in \Xi = \mathfrak{p}_{\mathcal{G}}(A)$ and identity (2).

### *3.2. An alternative characterization of a Lüroth generator*

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

$$\begin{array}{rcl} \psi : \mathcal{F}\{x_1, \ldots, x_n, y_1, \ldots, y_m\} & \to & \mathcal{F}\{P_1(\mathbf{t})/Q_1(\mathbf{t}), \ldots, P_n(\mathbf{t})/Q_n(\mathbf{t}), \mathbf{t}\} \\ x_j & \mapsto & P_j(\mathbf{t})/Q_j(\mathbf{t}) \\ y_i & \mapsto & t_i \end{array} \tag{3}$$

If $\mathfrak{P} \subset \mathcal{F}\{\mathbf{x}, \mathbf{y}\}$ is the kernel of the morphism $\psi$, we have an isomorphism

$$\mathcal{F}\{P_1(\mathbf{t})/Q_1(\mathbf{t}), \ldots, P_n(\mathbf{t})/Q_n(\mathbf{t}), \mathbf{t}\} \simeq \mathcal{F}\{\mathbf{x}, \mathbf{y}\}/\mathfrak{P}.$$

This implies that $\mathfrak{P}$ is a prime differential ideal and the fraction field of $\mathcal{F}\{\mathbf{x}, \mathbf{y}\}/\mathfrak{P}$ is isomorphic to $\mathcal{F}\langle\mathbf{t}\rangle$. In addition, the previous isomorphism gives an inclusion

$$\mathcal{F}\{P_1(\mathbf{t})/Q_1(\mathbf{t}), \ldots, P_n(\mathbf{t})/Q_n(\mathbf{t})\} \hookrightarrow \mathcal{F}\{\mathbf{x}, \mathbf{y}\}/\mathfrak{P},$$

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

Let $\Xi$ be the differential ideal of $\mathcal{G}\{\mathbf{y}\}$ introduced in (1) and fix an orderly ranking in the variables $\mathbf{y}$.

If $A \in \mathcal{G}\{\mathbf{y}\}$ is a non-zero differential polynomial in $\Xi$, multiplying it by an adequate element in $\mathcal{F}\{P_1(\mathbf{t})/Q_1(\mathbf{t}), \ldots, P_n(\mathbf{t})/Q_n(\mathbf{t})\}$, we obtain a differential polynomial in $\mathcal{F}\{P_1(\mathbf{t})/Q_1(\mathbf{t}), \ldots, P_n(\mathbf{t})/Q_n(\mathbf{t})\}\{\mathbf{y}\}$, with the same rank in $\mathbf{y}$ as $A$. Taking a representative (with respect to $\psi$) in $\mathcal{F}\{\mathbf{x}\}$ for each of its coefficients yields a differential polynomial $\widehat{A} \in \mathcal{F}\{\mathbf{x}, \mathbf{y}\}$, with the same rank in $\mathbf{y}$ as $A$, such that $\widehat{A}(\mathbf{x}, \mathbf{y}) \in \mathfrak{P}$.

Conversely, given a differential polynomial $M \in \mathcal{F}\{\mathbf{x}, \mathbf{y}\}$ such that $M \in \mathfrak{P}$ and not every coefficient of $M$ as a polynomial in $\mathcal{F}\{\mathbf{x}\}\{\mathbf{y}\}$ lies in $\mathfrak{P} \cap \mathcal{F}\{\mathbf{x}\}$, the differential polynomial

$$\widetilde{M}(\mathbf{y}) := M(P_1(\mathbf{t})/Q_1(\mathbf{t}), \ldots, P_n(\mathbf{t})/Q_n(\mathbf{t}), \mathbf{y}) \in \mathcal{G}\{\mathbf{y}\} \tag{4}$$

is not the zero polynomial, vanishes when evaluating $\mathbf{y} = \mathbf{t}$ and has a rank in $\mathbf{y}$ no higher than that of $M$.

We conclude that if $M \in \mathcal{F}\{\mathbf{x}, \mathbf{y}\}$ is a differential polynomial with the lowest rank in $\mathbf{y}$ among all the differential polynomials as above, the associated differential polynomial $\widetilde{M}(\mathbf{y})$ is a multiple by a factor in $\mathcal{G}$ of a polynomial $A \in \mathcal{G}\{\mathbf{y}\}$ such that $\Xi = \mathfrak{p}_{\mathcal{G}}(A)$. Therefore, as shown in the previous section, a Lüroth generator of $\mathcal{G}/\mathcal{F}$ can be obtained as the ratio of any pair of coefficients of $\widetilde{M} \in \mathcal{G}\{\mathbf{y}\}$ provided that this ratio does not

Please cite this article in press as: L. D'Alfonso et al., Quantitative aspects of the generalized differential Lüroth's Theorem, J. Algebra (2018), https://doi.org/10.1016/j.jalgebra.2018.01.050

lie in $\mathcal{F}$. We have the following result which is essential for our degree estimations and computation of the Lüroth generator:

**Proposition 4.** *Let $M \in \mathcal{F}\{\mathbf{x},\mathbf{y}\}$ be a differential polynomial in $\mathfrak{P}\setminus(\mathfrak{P}\cap\mathcal{F}\{\mathbf{x}\})\{\mathbf{y}\}$ with the lowest rank in $\mathbf{y}$ and let $\widetilde{M}(\mathbf{y}) \in \mathcal{G}\{\mathbf{y}\}$ be defined as in (4). Assume that $\widetilde{M} \in \mathcal{F}(\mathbf{t}^{[\varrho]})\{\mathbf{y}\}$ for a suitable non-negative integer $\varrho$. Consider two generic points $\upsilon_1, \upsilon_2 \in \mathbb{Q}^{m(\varrho+1)}$. Let $P(\mathbf{y})$ and $Q(\mathbf{y})$ be the differential polynomials obtained from $\widetilde{M}(\mathbf{y})$ by substituting $\mathbf{t}^{[\varrho]} = \upsilon_1$ and $\mathbf{t}^{[\varrho]} = \upsilon_2$ respectively. Then $P(\mathbf{t})/Q(\mathbf{t})$ is a Lüroth generator of $\mathcal{G}/\mathcal{F}$.*

**Proof.** It follows in the same way as [3, Proposition 8] simply by changing the single variable $u$ in [3] by the $m$ variables $\mathbf{t}$. □

**Remark 5.** Following the proof in [3, Proposition 8] it follows that, in order for $\upsilon_1$ and $\upsilon_2$ to produce a Lüroth generator, it suffices that $Q_j(\upsilon_i) \neq 0$ for $j = 1,\dots,n$ and $i = 1, 2$, and that $\widetilde{M}(\upsilon_1, \upsilon_2) \neq 0$.

## 4. Degree bounds

The aim of this section is to obtain an upper bound for the degrees of the numerator and the denominator of a Lüroth generator of $\mathcal{G}/\mathcal{F}$ in terms of the syntactic parameters $n, m, d$ and $e$ associated to the given generators of the extension. For technical reasons we assume $e \geq 1$.

### *4.1. Reduction to algebraic polynomial ideals*

We start by estimating the order in the variables $\mathbf{x} = x_1,\dots,x_n$ and $\mathbf{y} = y_1,\dots,y_m$ of a differential polynomial $M(\mathbf{x},\mathbf{y}) \in \mathfrak{P} \setminus (\mathfrak{P} \cap \mathcal{F}\{\mathbf{x}\})\{\mathbf{y}\}$ of minimal rank in $\mathbf{y}$, where $\mathfrak{P}$ is the prime differential ideal introduced in Section 3.2, namely, the kernel of the map in (3). In doing this, we will characterize $\mathfrak{P}$ as a prime component of a finitely generated differential ideal with known generators, which will in term enable us to find such a polynomial $M$ in an associated algebraic polynomial ideal.

First, note that the differential dimension of $\mathfrak{P}$ equals $m$, since the fraction field of $\mathcal{F}\{\mathbf{x},\mathbf{y}\}/\mathfrak{P}$ is isomorphic to $\mathcal{F}\langle\mathbf{t}\rangle$, with $\mathbf{t} = t_1,\dots,t_m$.

Consider the block elimination ranking in $\mathcal{F}\{\mathbf{x},\mathbf{y}\}$ with $x_1 \ll x_2 \ll \cdots \ll x_n \ll \mathbf{y}$, where the block $\mathbf{y}$ is given the orderly ranking with $y_1 < \cdots < y_m$. Since $P_1(\mathbf{t})/Q_1(\mathbf{t})$ is differentially transcendental over $\mathcal{F}$, the differential ideal $\mathfrak{P}$ contains no differential polynomial involving only the variable $x_1$. Then, the assumption that $\mathcal{G}/\mathcal{F}$ has differential transcendence degree equal to 1 and the fact that the differential dimension of $\mathfrak{P}$ is $m$ imply that a characteristic set of $\mathfrak{P}$ for the considered ranking is of the form

$$C_1(x_1,x_2), C_2(x_1,x_2,x_3),\dots,C_{n-1}(x_1,\dots,x_n), C_n(x_1,\dots,x_n,\mathbf{y}).$$

Please cite this article in press as: L. D'Alfonso et al., Quantitative aspects of the generalized differential Lüroth's Theorem, J. Algebra (2018), https://doi.org/10.1016/j.jalgebra.2018.01.050

By [19, Lemma 19], there exists an *irreducible* characteristic set $C_1, C_2, \ldots, C_n$ of $\mathfrak{P}$ for this ranking (see [19, Section 4] for a definition) and, by the proof of [6, Theorem 27], it follows that the involved differential polynomials satisfy

$$\operatorname{ord}(C_i) \leq \operatorname{ord}(\mathfrak{P}) \qquad \text{for } 1 \leq i \leq n.$$

Furthermore, the irreducibility of the characteristic set implies that $C_n$ is a differential polynomial in $\mathfrak{P}\backslash(\mathfrak{P}\cap\mathcal{F}\{\mathbf{x}\})\{\mathbf{y}\}$ with a minimal rank in $\mathbf{y}$, that is, we can take $M(\mathbf{x},\mathbf{y}) = C_n(\mathbf{x},\mathbf{y})$ and so,

$$\operatorname{ord}(M) \leq \operatorname{ord}(\mathfrak{P}). \tag{5}$$

In order to estimate the order of $\mathfrak{P}$, we introduce a system of differential polynomials that provides us with an alternative characterization of this prime differential ideal: denote

$$F_j := Q_j(\mathbf{y})x_j - P_j(\mathbf{y}) \in \mathcal{F}\{\mathbf{x},\mathbf{y}\} \qquad \text{for } 1 \leq j \leq n.$$

Set $F := F_1, \ldots, F_n$ and $q := Q_1 \ldots Q_n$.

The following lemma is a straightforward generalization of [3, Lemmas 10 & 11] for the case $m > 1$; for this reason, we omit its proof.

**Lemma 6.** *With the previous assumptions and notation, we have:*

(a) *The ideal $\mathfrak{P}$ is the (unique) minimal prime differential ideal of $[F]$ which does not contain the product $q$; moreover, $\mathfrak{P} = [F] : q^\infty$.*
(b) *The system $F$ is quasi-regular at $\mathfrak{P}$.*

For technical reasons (see Remark 8 below) we need also the following result:

**Proposition 7.** *Let $p \in \mathbb{N}_0$ be an arbitrary non-negative integer. Then:*

(a) *The algebraic ideal $(F, \dot{F}, \ldots, F^{(p)}) : q^\infty \subset \mathcal{F}[\mathbf{x}^{[p]}, \mathbf{y}^{[p+e]}]$ is prime.*
(b) *The localization of the ring $\mathcal{F}[\mathbf{x}^{[p]}, \mathbf{y}^{[p+e]}]/(F, \dot{F}, \ldots, F^{(p)})$ by the powers of $q$ can be embedded naturally in the fraction field of the differential domain $\mathcal{F}\{\mathbf{x},\mathbf{y}\}/\mathfrak{P}$.*

**Proof.** The statement (a) follows from the fact that the ideal $(F, \dot{F}, \ldots, F^{(p)}) : q^\infty \subset \mathcal{F}[\mathbf{x}^{[p]}, \mathbf{y}^{[p+e]}]$ is the kernel of the map

$$\begin{array}{rccc} \psi_p : & \mathcal{F}[\mathbf{x}^{[p]}, \mathbf{y}^{[p+e]}] & \to & \mathcal{F}[(P_j/Q_j)^{[p]}_{1\leq j\leq n}\ ,\ \mathbf{y}^{[p+e]}] \\ & x_j^{(k)} & \mapsto & (P_j/Q_j)^{(k)} \\ & y_h^{(i)} & \mapsto & y_h^{(i)} \end{array} .$$

Please cite this article in press as: L. D'Alfonso et al., Quantitative aspects of the generalized differential Lüroth's Theorem, J. Algebra (2018), https://doi.org/10.1016/j.jalgebra.2018.01.050

In order to prove (b), let $\mathcal{O}$ be the ring $\mathcal{F}[\mathbf{x}^{[p]}, \mathbf{y}^{[p+e]}]/(F, \dot{F}, \ldots, F^{(p)})$ localized by the powers of the single polynomial $q$. From (a) we infer that $\mathcal{O}$ is a domain. Moreover, by extending $\psi_p$ and localizing in the powers of $q$, which is also a multiplicative set in $\mathcal{F}\{\mathbf{x}, \mathbf{y}\}/\mathfrak{P}$, we obtain a natural ring morphism $\mathcal{O} \to (\mathcal{F}\{\mathbf{x}, \mathbf{y}\}/\mathfrak{P})_q$. It suffices to show that this morphism is injective: let $\mathfrak{Q} \subset \mathcal{O}$ be the kernel of this morphism (which is also a prime ideal). Since the variables $\mathbf{y}$ are differentially independent modulo $\mathfrak{P}$, we conclude that the variables $\mathbf{y}^{[p+e]}$ must be algebraically independent in $\mathcal{O}/\mathfrak{Q}$. Hence, the Krull dimensions of the domains $\mathcal{O}$ and $\mathcal{O}/\mathfrak{Q}$ are equal to $(m+1)(p+e)$ (observe that each variable $x_j^{(k)}$ in $\mathcal{O}$ is algebraic over the variables $\mathbf{y}^{[p+e]}$ for all $j$ and $k \leq p$). Hence $\mathfrak{Q} = 0$ and statement (b) is proved. □

**Remark 8.** Lemma 6(b) and Proposition 7(b) state that the conditions in [1, Definition 1] and [1, Hypothesis in §2.4], respectively, are fulfilled by the system $F$ with respect to the differential prime ideal $\mathfrak{P}$. Then, the definitions, methods and results of [1], based on the properties of the differentiation index, can be applied in our setting.

Now, we are able to estimate the order of the differential ideal $\mathfrak{P}$. In [3, Lemma 6] we have shown in an elementary way that for the case $m = 1$ the order of $\mathfrak{P}$ is exactly the maximum of the orders of the generators $P_j/Q_j$. In the general case $m \geq 1$, with the help of Jacobi's order bound, we are able to prove the following inequality, which will be enough for our purposes:

**Lemma 9.** *Let* $e := \max\{\operatorname{ord}(P_j(\mathbf{y})/Q_j(\mathbf{y})) : 1 \leq j \leq n\}$. *Then,* $\operatorname{ord}(\mathfrak{P}) \leq \min\{m, n\}e$.

**Proof.** The result is a consequence of Jacobi's bound for the order of a prime differential ideal $\mathfrak{P}$ associated to a quasi-regular system $F$ (see [1, Theorem 18] or [14,15]). Let $\mathcal{E} := (\epsilon_{hk})_{1 \leq h \leq n, 1 \leq k \leq n+m}$ be the order matrix of the system $F = F_1, \ldots, F_n$, namely, the matrix where $\epsilon_{hk} := \operatorname{ord}_{x_k}(F_h)$ for $1 \leq k \leq n$ and $\epsilon_{hk} = \operatorname{ord}_{y_{k-n}}(F_h)$ for $n+1 \leq k \leq n+m$, where the order is set to be $-\infty$ if the variable is not present in the polynomial. Then, Jacobi's bound is as follows:

$$\operatorname{ord}(\mathfrak{P}) \leq \max\{\sum_{1 \leq h \leq n} \epsilon_{h\tau(h)} \mid \tau : \{1, \ldots, n\} \to \{1, \ldots, n+m\} \text{ is an injection}\}.$$

Since $\operatorname{ord}_{x_h}(F_h) = 0$, $\operatorname{ord}_{x_i}(F_h) = -\infty$ if $i \neq h$, and $\operatorname{ord}_{y_j}(F_h) \leq e$ for every $1 \leq j \leq m$, we have that, for every $\tau$, $\sum_{1 \leq h \leq n} \epsilon_{h\tau(h)} \leq ne$ and $\sum_{1 \leq h \leq n} \epsilon_{h\tau(h)} \leq me$. □

Combining the previous proposition with inequality (5) we conclude:

**Corollary 10.** *There is a differential polynomial* $M \in \mathfrak{P} \setminus (\mathfrak{P} \cap \mathcal{F}\{\mathbf{x}\})\{\mathbf{y}\}$ *with the lowest rank in* $\mathbf{y}$ *such that* $\operatorname{ord}(M) \leq \min\{m, n\}e$.

Please cite this article in press as: L. D'Alfonso et al., Quantitative aspects of the generalized differential Lüroth's Theorem, J. Algebra (2018), https://doi.org/10.1016/j.jalgebra.2018.01.050

The above proposition implies that a polynomial $M$ providing a Lüroth generator of $\mathcal{G}/\mathcal{F}$ can be found in the algebraic ideal $\mathfrak{P} \cap \mathcal{F}[\mathbf{x}^{[\nu]}, \mathbf{y}^{[\nu]}]$ of the polynomial ring $\mathcal{F}[\mathbf{x}^{[\nu]}, \mathbf{y}^{[\nu]}]$, where

$$\nu := \min\{m, n\}e.$$

The following result, which is an extension of Proposition 7 above, will allow us to work with a finitely generated algebraic ideal given by known generators. It can be viewed also as a suitable generalization of the results shown for the case $m = 1$ in [3, Lemma 14 & Proposition 16]. The main tool to prove it is the estimation of the $\mathfrak{P}$-differentiation index of the system $F := F_1, \ldots, F_n$ (see, for instance, [1, Section 3]). This invariant enables us to determine the number of differentiations of the system $F$ that should be considered in order to obtain all the differential polynomials of pre-fixed order in the differential ideal.

**Proposition 11.** *With the previous assumptions and notations the following equality of ideals holds:*

$$\mathfrak{P} \cap \mathcal{F}[\mathbf{x}^{[\nu]}, \mathbf{y}^{[\nu]}] = (F, \dot{F}, \ldots, F^{(\nu)}) : q^\infty \cap \mathcal{F}[\mathbf{x}^{[\nu]}, \mathbf{y}^{[\nu]}].$$

**Proof.** We start by estimating the $\mathfrak{P}$-differentiation index of the system $F$. For the sake of completeness we recall here the definition given in [1] of this invariant: 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 $(\mathbf{x}, \mathbf{y})^{(e)}, \ldots, (\mathbf{x}, \mathbf{y})^{(e+k-1)}$. The $\mathfrak{P}$-differentiation index of $F$ is 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 $\mathcal{F}\{\mathbf{x}, \mathbf{y}\}/\mathfrak{P}$.

We are going to prove that the $\mathfrak{P}$-differentiation index of the system $F$ is at most $e$. In order to do this, by the previous definition, it suffices to show that $\operatorname{rank}(\mathfrak{J}_{e+1}) - \operatorname{rank}(\mathfrak{J}_e) = n$. To this end, we analyze the structure of the matrices $\mathfrak{J}_e$ and $\mathfrak{J}_{e+1}$.

Since the order of $F$ in the variables $\mathbf{x}$ is zero, no derivative $x_j^{(e)}$ appears effectively in $F, \dot{F}, \ldots, F^{(e-1)}$. This implies that the columns of the Jacobian submatrix $\mathfrak{J}_e$ of this system corresponding to partial derivatives with respect to $\mathbf{x}^{(e)}$ are null, that is,

$$\mathfrak{J}_e = \begin{pmatrix} \mathbf{0} & \widetilde{\mathfrak{J}}_e \end{pmatrix}$$

where $\mathbf{0}$ is the zero matrix of size $ne \times n$. Moreover,

$$\mathfrak{J}_{e+1} = \begin{pmatrix} \mathbf{0} & \widetilde{\mathfrak{J}}_e & 0 \\ \frac{\partial F^{(e)}}{\partial \mathbf{x}^{(e)}} & * & \frac{\partial F^{(e)}}{\partial (\mathbf{x}, \mathbf{y})^{(2e)}} \end{pmatrix}.$$

On the other hand, since

Please cite this article in press as: L. D'Alfonso et al., Quantitative aspects of the generalized differential Lüroth's Theorem, J. Algebra (2018), https://doi.org/10.1016/j.jalgebra.2018.01.050

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

the submatrix $\dfrac{\partial F^{(e)}}{\partial \mathbf{x}^{(e)}}$ has the diagonal structure

$$\begin{pmatrix} Q_1(\mathbf{y}) & 0 & \cdots & 0 \\ 0 & Q_2(\mathbf{y}) & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & Q_n(\mathbf{y}) \end{pmatrix}.$$

So, we deduce that $\operatorname{rank}(\mathfrak{J}_{e+1}) = \operatorname{rank}(\mathfrak{J}_e) + n$, as we wanted to prove.

Then, as a consequence of the main property of the differentiation index established in [1, Theorem 10], since $\nu \geq e$, we have that

$$[F]_{\mathfrak{P}} \cap \mathcal{F}[\mathbf{x}^{[\nu]}, \mathbf{y}^{[\nu]}] = (F, \dot{F}, \ldots, F^{(\nu)})_{\mathfrak{P}_{\nu+e}} \cap \mathcal{F}[\mathbf{x}^{[\nu]}, \mathbf{y}^{[\nu]}], \tag{6}$$

where $\mathfrak{P}_{\nu+e} := \mathfrak{P} \cap \mathcal{F}[\mathbf{x}^{[\nu+e]}, \mathbf{y}^{[\nu+e]}]$ and the subscripts denote the localizations in the complement of the prime ideals $\mathfrak{P}$ and $\mathfrak{P}_{\nu+e}$, respectively.

Moreover, by Lemma 6 and [1, Proposition 3], the equality of ideals $[F]_{\mathfrak{P}}\mathcal{F}\{\mathbf{x}, \mathbf{y}\}_{\mathfrak{P}} = \mathfrak{P}_{\mathfrak{P}}\mathcal{F}\{\mathbf{x}, \mathbf{y}\}_{\mathfrak{P}}$ holds; therefore,

$$[F]_{\mathfrak{P}} \cap \mathcal{F}[\mathbf{x}^{[\nu]}, \mathbf{y}^{[\nu]}] = \mathfrak{P}_{\mathfrak{P}} \cap \mathcal{F}[\mathbf{x}^{[\nu]}, \mathbf{y}^{[\nu]}] = \mathfrak{P} \cap \mathcal{F}[\mathbf{x}^{[\nu]}, \mathbf{y}^{[\nu]}].$$

In order to finish the proof, let us show that

$$(F, \dot{F}, \ldots, F^{(\nu)})_{\mathfrak{P}_{\nu+e}} \cap \mathcal{F}[\mathbf{x}^{[\nu]}, \mathbf{y}^{[\nu]}] = (F, \dot{F}, \ldots, F^{(\nu)}) : q^{\infty} \cap \mathcal{F}[\mathbf{x}^{[\nu]}, \mathbf{y}^{[\nu]}].$$

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

### *4.2. A first degree bound*

To get an upper bound for the degree of a Lüroth generator of $\mathcal{G}/\mathcal{F}$, we will estimate the degree of a polynomial $M(\mathbf{x}, \mathbf{y}) \in \mathfrak{P} \setminus (\mathfrak{P} \cap \mathcal{F}\{\mathbf{x}\})\{\mathbf{y}\}$ with the properties stated in Section 3.2. In order to do this, by means of the results in the previous section, we relate $M$ to an eliminating polynomial for an associated algebraic variety under a suitable linear projection.

Please cite this article in press as: L. D'Alfonso et al., Quantitative aspects of the generalized differential Lüroth's Theorem, J. Algebra (2018), https://doi.org/10.1016/j.jalgebra.2018.01.050

Most of the arguments we use in this subsection are *mutatis mutandis* the same ones applied in [3, Section 4.3] for the case $m = 1$. We repeat them here for the sake of comprehensiveness.

**Notation 12.** *We denote with* $\mathbb{V} \subset \mathbb{A}^{n(\nu+1)} \times \mathbb{A}^{m(\nu+e+1)}$ *the affine variety defined as the Zariski closure of the solution set of the polynomial system*

$$F = 0, \dot{F} = 0, \dots, F^{(\nu)} = 0, q \neq 0,$$

*where* $F = F_1, \dots, F_n$ *with* $F_j(\mathbf{x}, \mathbf{y}^{[e]}) = Q_j(\mathbf{y}^{[e]})x_j - P_j(\mathbf{y}^{[e]})$ *for every* $1 \leq j \leq n$, $q(\mathbf{y}^{[e]}) = \prod_{1 \leq j \leq n} Q_j(\mathbf{y}^{[e]})$ *and* $\nu = \min\{m, n\}e$.

Note that $\mathbb{V}$ is an irreducible variety, since the algebraic ideal corresponding to $\mathbb{V}$ is $(F, \dot{F}, \dots, F^{(\nu)}) : q^\infty \subset \mathcal{F}[\mathbf{x}^{[\nu]}, \mathbf{y}^{[\nu+e]}]$, which is a prime ideal (see Proposition 7(a)). Moreover, since $F, \dot{F}, \dots, F^{(\nu)}$ is a reduced complete intersection in $\{q \neq 0\}$, the dimension of $\mathbb{V}$ is $m(\nu + e + 1)$.

**Proposition 13.** *With the previous assumptions and notation, for a differential polynomial* $M(\mathbf{x}, \mathbf{y}) \in \mathfrak{P} \setminus (\mathfrak{P} \cap \mathcal{F}\{\mathbf{x}\})\{\mathbf{y}\}$ *of minimal rank in* $\mathbf{y}$*, we have that* $\deg_{\mathbf{y}}(M) \leq \deg(\mathbb{V})$.

**Proof.** Let $\nu_0 \in \mathbb{N}_0$ be the order of $M$ in the variables $\mathbf{y}$. By Corollary 10, we have that $\nu_0 \leq \nu = \min\{m, n\}e$. Consider the fields

$$\mathcal{K} := \mathrm{Frac}(\mathcal{F}[\mathbf{x}^{[\nu]}]/(\mathfrak{P} \cap \mathcal{F}[\mathbf{x}^{[\nu]}]))$$

and

$$\mathcal{L} := \mathrm{Frac}(\mathcal{F}[\mathbf{x}^{[\nu]}, \mathbf{y}^{[\nu]}]/(\mathfrak{P} \cap \mathcal{F}[\mathbf{x}^{[\nu]}, \mathbf{y}^{[\nu]}])).$$

The minimality of the rank in $\mathbf{y}$ of $M$ implies that $\{\mathbf{y}^{[\nu_0-1]}\} \subset \mathcal{L}$ is algebraically independent over $\mathcal{K}$. Furthermore, if

$$j_0 := \min\left\{1 \leq j \leq m : \{y_1^{(\nu_0)}, \dots, y_j^{(\nu_0)}\} \text{ is algebraically dependent over } \mathcal{K}(\mathbf{y}^{[\nu_0-1]})\right\},$$

then $M$ is the minimal polynomial of $y_0 := y_{j_0}^{(\nu_0)} \in \mathcal{L}$ over $\mathcal{K}(\mathbf{y}^{[\nu_0-1]}, y_1^{(\nu_0)}, \dots, y_{j_0-1}^{(\nu_0)})$.

Let $X \subset \{\mathbf{x}^{[\nu]}\}$ be a transcendence basis of $\mathcal{K}$ over $\mathcal{F}$. Then, if we denote $Y := \{\mathbf{y}^{[\nu_0-1]}, y_1^{(\nu_0)}, \dots, y_{j_0-1}^{(\nu_0)}\} \subset \mathcal{L}$, we have that $\{X, Y\} \subset \mathcal{L}$ is algebraically independent over $\mathcal{F}$ and $\{X, Y, y_0\} \subset \mathcal{L}$ is algebraically dependent over $\mathcal{F}$. Moreover, if $\mathbb{V}$ is the affine variety introduced in Notation 12, since $\mathcal{L} \subset \mathcal{F}(\mathbb{V})$ (see Proposition 11), the previous facts hold in $\mathcal{F}(\mathbb{V})$.

Consider the projection $\pi : \mathbb{V} \to \mathbb{A}^{N+1}$, $\pi(\mathbf{x}^{[\nu]}, \mathbf{y}^{[\nu+e]}) = (X, Y, y_0)$, where $N$ is the cardinality of $\{X, Y\}$. Since $\mathbb{V}$ is an irreducible variety and $\{X, Y\}$ is algebraically

independent in $\mathcal{F}(\mathbb{V})$, the Zariski closure of $\pi(\mathbb{V})$ is a hypersurface in $\mathbb{A}^{N+1}$; then, it is definable by an irreducible polynomial $M_0 \in \mathcal{F}[X, Y, y_0]$ such that

$$\deg(M_0) \leq \deg(\mathbb{V}) \tag{7}$$

(see [8, Lemma 2]).

We have that $M$ is the minimal polynomial of $y_0$ over $\mathcal{K}(Y)$, whereas $M_0$ is the minimal polynomial of $y_0$ over $\mathcal{F}(X, Y) \subset \mathcal{K}(Y)$, and we may assume that $M$ and $M_0$ are polynomials with coefficients in $\mathcal{F}$ having content 1 in $\mathcal{K}[Y]$ and $\mathcal{F}[X, Y]$ respectively. We infer that $M$ divides $M_0$ in $\mathcal{K}[Y][y_0]$ and, therefore, $\deg_{\mathbf{y}}(M) = \deg_{Y,y_0}(M) \leq \deg_{Y,y_0}(M_0)$. The proposition follows from inequality (7). □

Recalling that a Lüroth generator $v$ of $\mathcal{G}/\mathcal{F}$ can be obtained as the quotient of two specializations of the variables $\mathbf{x}$ and their derivatives in the polynomial $M$ (see Proposition 4) and that two arbitrary generators are related by an homographic map with coefficients in $\mathcal{F}$ (see [12, §1], [18, Chapter II, §44]), we conclude:

**Corollary 14.** *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 $\mathbb{V}$ introduced in Notation 12.*

Now, by applying Bézout's theorem (see for instance [8, Theorem 1]) to obtain an upper bound for $\deg(\mathbb{V})$, we can exhibit an upper bound for the degrees of the numerator and the denominator of a Lüroth generator $v = P(\mathbf{t})/Q(\mathbf{t})$ of $\mathcal{G}/\mathcal{F}$ in terms of the number $m$ of differential indeterminates $\mathbf{t}$, 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.

Recall that $\mathbb{V}$ is an irreducible component of the algebraic set defined by the $(\nu+1)n$ polynomials $F, \dot{F}, \ldots, F^{(\nu)}$, where $F = F_1, \ldots, F_n$ with $F_j(\mathbf{x}, \mathbf{y}) = Q_j(\mathbf{y})x_j - P_j(\mathbf{y}))$ and $\nu = \min\{m, n\}e$. If, for every $1 \leq j \leq n$, $d_j$ is an upper bound for the degrees of $P_j$ and $Q_j$, we have that $\deg(F_j^{(l)}) \leq d_j + 1$ for every $l$, and we obtain the bound:

$$\prod_{1 \leq j \leq n} (d_j + 1)^{(\min\{m,n\}e+1)}.$$

Summarizing:

**Proposition 15.** *Let $\mathcal{F}$ be an ordinary differential field of characteristic 0, $\mathbf{t} = t_1, \ldots, t_m$ differentially transcendental over $\mathcal{F}$, and*

$$\mathcal{G} = \mathcal{F}\langle P_1(\mathbf{t})/Q_1(\mathbf{t}), \ldots, P_n(\mathbf{t})/Q_n(\mathbf{t})\rangle$$

*a differential field extension of $\mathcal{F}$ of differential transcendence degree 1. Assume that $P_j, Q_j \in \mathcal{F}\{\mathbf{t}\}$ are relatively prime differential polynomials of total degrees bounded by $d_j$.*

Please cite this article in press as: L. D'Alfonso et al., Quantitative aspects of the generalized differential Lüroth's Theorem, J. Algebra (2018), https://doi.org/10.1016/j.jalgebra.2018.01.050

*Let* $e := \max\{\operatorname{ord}(P_j/Q_j) : 1 \leq j \leq n\} \geq 1$. *Then, any Lüroth generator of* $\mathcal{G}/\mathcal{F}$ *can be written as the quotient of two relatively prime differential polynomials* $P(\mathbf{t}), Q(\mathbf{t}) \in \mathcal{F}\{\mathbf{t}\}$ *with total degrees bounded by* $\prod_{1\leq j\leq n}(d_j+1)^{(\min\{m,n\}e+1)}$.

### *4.3. Refined degree bounds*

We present here refined degree bounds for the differential Lüroth generator. To obtain these bounds, we follow the approach in [4]. The strategy consists in reducing the problem to the case of a field with two given generators by means of the primitive element theorem for differential field extensions in order to apply the bounds of Proposition 15 in this setting.

For $j = 1, \ldots, n$, let $\alpha_j := P_j(\mathbf{t})/Q_j(\mathbf{t})$ with $P_j, Q_j \in \mathcal{F}\{\mathbf{t}\}$ relatively prime differential polynomials of degrees bounded by $d$.

Let

$$e = \max_j\{\operatorname{ord}(\alpha_j)\} \geq 1$$
$$\mu = \min_{i,j}\{\operatorname{ord}(\alpha_j, t_i) : t_i \text{ appears in } \alpha_j\} \geq 0.$$

Without loss of generality suppose that $\mu = \operatorname{ord}(\alpha_1, t_1)$. We consider the intermediate field $\mathcal{F}_1 := \mathcal{F}\langle\alpha_1\rangle$, so that

$$\mathcal{F} \hookrightarrow \mathcal{F}_1 = \mathcal{F}\langle\alpha_1\rangle \hookrightarrow \mathcal{G} = \mathcal{F}_1\langle\alpha_2, \ldots, \alpha_n\rangle.$$

Since the differential transcendence degree of $\mathcal{G}/\mathcal{F}$ equals 1 and we are assuming that $\alpha_1 \notin \mathcal{F}$, it follows that $\mathcal{G}/\mathcal{F}_1$ is differentially algebraic, and $\mathcal{F}_1$ has nonconstant elements. By the primitive element theorem for differential field extensions (see [20, Theorem 1]), there is an element $\beta \in \mathcal{G}$ such that

$$\beta = \sum_{j=2}^{n} c_j\alpha_j \qquad \text{and} \qquad \mathcal{G} = \mathcal{F}_1\langle\beta\rangle = \mathcal{F}\langle\alpha_1, \beta\rangle,$$

where the coefficients $c_j$ can be taken as *generic* elements of $\mathcal{F}_1 = \mathcal{F}\langle\alpha_1\rangle$ for $j = 2, \ldots, n$.

Note that such an element $\beta$ can be represented as $\beta = \widehat{P}(\mathbf{t})/\widehat{Q}(\mathbf{t})$ for two relatively prime polynomials $\widehat{P}(\mathbf{t})$ and $\widehat{Q}(\mathbf{t})$ in $\mathcal{F}\{\mathbf{t}\}$. In order to apply the results of the previous section, we estimate the degrees of these polynomials for a suitably chosen primitive element $\beta$.

**Proposition 16.** *With the above assumptions and notations,*

(a) *if the field* $\mathcal{F}$ *contains a nonconstant element, then* $\beta$ *can be taken as the ratio of two relatively prime polynomials* $\widehat{P}(\mathbf{t})$ *and* $\widehat{Q}(\mathbf{t})$ *in* $\mathcal{F}\{\mathbf{t}\}$ *with degrees bounded by* $(n-1)d$;

(b) *if $\mathcal{F}$ is a field of constants, then $\beta$ can be taken as the ratio of two relatively prime polynomials $\widehat{P}(\mathbf{t})$ and $\widehat{Q}(\mathbf{t})$ in $\mathcal{F}\{\mathbf{t}\}$ with degrees bounded by $(n+\mu-1)d$.*

**Proof.** From the proof of [20, Theorem 1] (see also [2, Theorem 29]) it follows that, if $\zeta \in \mathcal{F}_1$ is a nonconstant element, the coefficients $c_j \in \mathcal{F}_1$, with $j = 2, \ldots, n$, in the definition of $\beta$ can be taken to be polynomials in $\zeta$ with rational coefficients.

Then, in the case that $\mathcal{F}$ contains a nonconstant element, $c_2, \ldots, c_n$ can actually be taken in $\mathcal{F}$ and so, the bound in (a) is a direct consequence of the fact that $\alpha_j = P_j/Q_j$ and $\deg(P_j), \deg(Q_j) \leq d$, for $j = 2, \ldots, n$.

Suppose now that $\mathcal{F}$ is a field of constants. Since $\alpha_1 \in \mathcal{F}_1$ is a nonconstant element, then $c_2, \ldots, c_n$ can be chosen in the polynomial ring $\mathbb{Q}[\alpha_1]$. Moreover, if $\mathfrak{Q}$ is the prime differential ideal of $\mathcal{F}\langle\alpha_1\rangle\{x_2, \ldots, x_n\}$ such that $\mathcal{F}\langle\alpha_1\rangle\langle\alpha_2, \ldots, \alpha_n\rangle$ is the fraction field of $\mathcal{F}\langle\alpha_1\rangle\{x_2, \ldots, x_n\}/\mathfrak{Q}$, then by [2, Proposition 30] and the arguments in [18, Chapter II, Section 22], $\operatorname{ord}(\mathfrak{Q})$ is the algebraic transcendence degree of the field $\mathcal{G} := \mathcal{F}\langle\alpha_1, \alpha_2, \ldots, \alpha_n\rangle$ over $\mathcal{F}\langle\alpha_1\rangle$ and, for $j = 2, \ldots, n$, the element $c_j$ can be taken to be a polynomial in $\mathbb{Q}[\alpha_1]$ with $\deg_{\alpha_1}(c_j) \leq \operatorname{ord}(\mathfrak{Q})$. Then, if we obtain a bound for the order of $\mathfrak{Q}$, we also have a bound for the degrees of $c_2, \ldots, c_n$ and, therefore, a bound for the degrees of a numerator and a denominator of $\beta$.

Let $v_0 \in \mathcal{G}$ be a Lüroth generator of $\mathcal{G}$ over $\mathcal{F}$. Thus, there exists a univariate reduced rational differential function $\Theta = \Theta_1/\Theta_2$ with $\Theta_1, \Theta_2 \in \mathcal{F}\{T\}$ such that $\alpha_1 = \Theta(v_0)$. Then, $\Theta_2(T)\alpha_1 - \Theta_1(T) \in \mathcal{F}_1\{T\}$ is a non-zero differential polynomial vanishing at $v_0$ and, therefore, the transcendence degree of $\mathcal{G} = \mathcal{F}_1\langle v_0\rangle$ over $\mathcal{F}_1$ is $\operatorname{ord}(\Theta)$. It is easy to see that this order is bounded by $\min\{\operatorname{ord}(\alpha_1, t_i) : t_i \text{ appears in } \alpha_1\}$ and, therefore, by $\mu$ (see for instance the proof of [3, Proposition 5]). So, $\deg_{\alpha_1}(c_j) \leq \operatorname{ord}(\mathfrak{Q}) \leq \mu$.

Thus, for $j = 2, \ldots, n$, regarding $c_j$ as an element of $\mathcal{F}\langle\mathbf{t}\rangle$, we have that it can be written as the ratio of a polynomial of degree bounded by $d\mu$ and $Q_1(\mathbf{t})$ raised to a power bounded by $\mu$. From these bounds we deduce that $\beta = c_2\alpha_2 + \ldots + c_n\alpha_n$ can be represented as $\widehat{P}(\mathbf{t})/\widehat{Q}(\mathbf{t})$ with

$$\deg(\widehat{P}(\mathbf{t})), \deg(\widehat{Q}(\mathbf{t})) \leq d\mu + d(n-1) = d(n+\mu-1).$$

This finishes the proof of the Proposition. □

As a consequence of the previous proposition, we have that

$$\mathcal{G} = \mathcal{F}\langle\alpha_1, \beta\rangle \qquad \text{where} \quad \alpha_1 = P_1(\mathbf{t})/Q_1(\mathbf{t}) \ \text{ and } \ \beta = \widehat{P}(\mathbf{t})/\widehat{Q}(\mathbf{t})$$

with $P_1(\mathbf{t}), Q_1(\mathbf{t})$ and $\widehat{P}(\mathbf{t}), \widehat{Q}(\mathbf{t})$ two pairs of relatively prime polynomials in $\mathcal{F}\{\mathbf{t}\}$ of maximal order $e \geq 1$ and bounded degrees. Applying the bound from Proposition 15 in this setting, we deduce the following result:

**Theorem 17.** *Let $\mathcal{F}$ be an ordinary differential field of characteristic 0, $\mathbf{t} = t_1, \ldots, t_m$ differentially transcendental over $\mathcal{F}$, and*

Please cite this article in press as: L. D'Alfonso et al., Quantitative aspects of the generalized differential Lüroth's Theorem, J. Algebra (2018), https://doi.org/10.1016/j.jalgebra.2018.01.050

$$\mathcal{G} = \mathcal{F}\langle P_1(\mathbf{t})/Q_1(\mathbf{t}), \ldots, P_n(\mathbf{t})/Q_n(\mathbf{t})\rangle$$

*a differential field extension of $\mathcal{F}$ of differential transcendence degree* 1. *Assume that $P_j, Q_j \in \mathcal{F}\{\mathbf{t}\}$ are relatively prime differential polynomials of degrees bounded by $d$. Let $e = \max_j\{ord(\alpha_j)\} \geq 1$ and $\mu = \min_{i,j}\{\mathrm{ord}(\alpha_j, t_i) : t_i$ appears in $\alpha_j\}$. Then, any Lüroth generator of $\mathcal{G}/\mathcal{F}$ can be written as the quotient of two relatively prime differential polynomials $P(\mathbf{t}), Q(\mathbf{t}) \in \mathcal{F}\{\mathbf{t}\}$ with total degrees bounded by*

$$\min\left\{\big((d+1)\big((n+\mu-1)d+1\big)\big)^{\min\{m,2\}e+1}\ ,\ (d+1)^{n(\min\{m,n\}e+1)}\right\}.$$

*Moreover, if $\mathcal{F}$ is a differential field containing a nonconstant element, then the total degrees of $P(\mathbf{t})$ and $Q(\mathbf{t})$ are bounded by*

$$\min\left\{\big((d+1)((n-1)d+1)\big)^{\min\{m,2\}e+1}\ ,\ (d+1)^{n(\min\{m,n\}e+1)}\right\}.$$

For the case $m = 1$ we deduce the following bounds:

**Corollary 18.** *If $m = 1$, an upper bound for the degree of the numerator and the denominator of a Lüroth generator is*

$$\min\left\{\big((d+1)\big((n+\mu-1)d+1\big)\big)^{e+1}\ ,\ (d+1)^{n(e+1)}\right\}.$$

*Moreover, if $\mathcal{F}$ contains a nonconstant element, the bound $((d+1)((n-1)d+1))^{e+1}$ holds.*

**Proof.** It is a direct consequence of Theorem 17. We observe that for the case where the differential field $\mathcal{F}$ contains a nonconstant element (or for the case $\mu = 0$) the inequality $((d+1)((n-1)d+1))^{e+1} \leq (d+1)^{n(e+1)}$ holds. □

*4.4. Comparisons with other degree upper bounds for $m = 1$*

For the case $m = 1$, i.e. when $\mathbf{t}$ is a single variable $t$, two previous works addressed the computation of upper bounds for the degree of a Lüroth generator. In [3, Theorem 1] the upper bound

$$\min\left\{(nd(e+1)+1)^{2e+1}\ ,\ (d+1)^{n(e+1)}\right\} \tag{8}$$

is given (for any ground differential field $\mathcal{F}$ of characteristic 0). Later, in [4] the authors show the degree upper bounds

$$(d(n+e-1)+1)^{2e+2} \tag{9}$$

and

$$(\lceil n/2 \rceil\, d + 1)^{2e+2}, \tag{10}$$

the second one if $\mathcal{F}$ contains a nonconstant element.

It is easy to see that the inequality

$$\big((d+1)\big((n+\mu-1)d+1\big)\big)^{e+1} < (d(n+e-1)+1)^{2e+2}$$

holds. Also, we have that

$$\big((d+1)((n-1)d+1)\big)^{e+1} \leq (\lceil n/2 \rceil\, d+1)^{2e+2}$$

with equality only for $n = 2$. Hence, the bounds stated in Corollary 18 improve (9) and (10).

On the other hand, the expression $\delta_1 = (nd(e+1)+1)^{2e+1}$ in (8) may be smaller than our new bound $\tau_1 = \big((d+1)\big((n+\mu-1)d+1\big)\big)^{e+1}$ when $d$ is sufficiently large with respect to the other parameters, but otherwise $\tau_1$ seems to be more accurate. For instance, taking $d = 100$, $n = 3$ and $e = \mu = 1$, we have $\delta_1 = 217081801$, $\tau_1 = 924220801$ and the ratio $\delta_1/\tau_1 \approx 0.23488$; but if we put $n = 20$ instead of 3, we obtain $\delta_1 = 64048012001$, $\tau_1 = 40844814201$ and $\delta_1/\tau_1 \approx 1.5681$.

Summarizing, our bounds improve the known ones except if the degree $d$ is large with respect to the other parameters. In any case, we have the following improvement of Corollary 18 which includes the bounds given in [3] and [4]:

**Corollary 19.** *With the notations above, in the case $m = 1$, the total degree of a Lüroth generator is bounded by*

$$\min\{\big((d+1)\big((n+\mu-1)d+1\big)\big)^{e+1}\ ,\ (nd(e+1)+1)^{2e+1}\ ,\ (d+1)^{(e+1)n}\}.$$

*Moreover, if the base field $\mathcal{F}$ contains a nonconstant element, this bound can be replaced by* $\min\{\big((d+1)((n-1)d+1)\big)^{e+1}\ ,\ (nd(e+1)+1)^{2e+1}\}$.

## 5. Algorithmic aspects

Complementing the discussion of quantitative aspects on Lüroth generators developed in the previous sections, here we present an algorithmic procedure to solve the following problem:

*Given a differentially finitely generated subextension $\mathcal{G}/\mathcal{F}$ of $\mathcal{F}\langle \mathbf{t}\rangle/\mathcal{F}$, decide if a Lüroth generator for this extension exists and in the affirmative case compute it.*

We start exhibiting an effective method to decide if an arbitrary differentially finitely generated subfield $\mathcal{G}$ of $\mathcal{F}\langle \mathbf{t}\rangle/\mathcal{F}$ has differential transcendence degree 1 over $\mathcal{F}$. Then, we

describe a Gröbner-based algorithm for the computation of a Lüroth generator of such extensions from a given set of differential rational functions generating $\mathcal{G}/\mathcal{F}$.

Even if these procedures are completely independent of the previous estimations for the degree of a Lüroth generator, their correctness is a consequence of the arguments developed in the preceding sections.

### *5.1. Testing differential transcendence degree one*

Let $\mathcal{G} = \mathcal{F}\langle\alpha_1, \ldots, \alpha_n\rangle$ be a differential subextension of $\mathcal{F}\langle\mathbf{t}\rangle/\mathcal{F}$, where $\mathbf{t} := t_1, \ldots, t_m$ are differential indeterminates over $\mathcal{F}$. Assume each $\alpha_j$ is represented as a quotient $P_j/Q_j$ of relatively prime differential polynomials in $\mathcal{F}\{\mathbf{t}\}$ of order at most $e \geq 1$.

In order to avoid new notations we keep those introduced in the previous sections, even if the context is slightly different here, because now the field extension $\mathcal{G}/\mathcal{F}$ is not assumed to be of differential transcendence degree 1.

Without loss of generality suppose that no $\alpha_j$ belongs to the field $\mathcal{F}$. In particular the extension $\mathcal{F}\langle\alpha_1\rangle$ has differential transcendence degree 1 over $\mathcal{F}$. Then, we have that $\mathcal{G}/\mathcal{F}$ has differential transcendence degree 1 over $\mathcal{F}$ if and only if, for every $j = 2, \ldots, n$, $\alpha_j$ is differentially algebraic over $\mathcal{F}\langle\alpha_1\rangle$.

As in Section 3.2, we consider the morphism $\psi : \mathcal{F}\{\mathbf{x}, \mathbf{y}\} \to \mathcal{F}\{\alpha_1, \ldots, \alpha_n, \mathbf{t}\}$ (defined in (3)) and denote its kernel by $\mathfrak{P}$. The differential dimension of $\mathfrak{P}$ is $m$, since the fraction field of the image of $\psi$ is $\mathcal{F}\langle\mathbf{t}\rangle$.

Take an index $j$, $2 \leq j \leq n$, such that $\alpha_j$ is differentially algebraic over $\mathcal{F}\langle\alpha_1\rangle$ and consider the block-elimination ranking in $\mathcal{F}\{\mathbf{x}, \mathbf{y}\}$: $x_1 \ll x_j \ll x_2 \ll \cdots \ll x_n \ll \mathbf{y}$, where in the block $\mathbf{y}$ is given the orderly ranking with $y_1 < \cdots < y_m$. Then, our assumption on $\alpha_j$ implies that any characteristic set of $\mathfrak{P}$ for this ranking must contain a differential polynomial $C(x_1, x_j)$ and by [19, Lemma 19] and the proof of [6, Theorem 27] we may suppose that $C$ is irreducible and its total order is bounded by the order of the ideal $\mathfrak{P}$. Moreover, since Lemmas 6 and 9 are independent of the differential transcendence degree of $\mathcal{G}$ over $\mathcal{F}$, we infer that the inequality $\operatorname{ord}(\mathfrak{P}) \leq \nu = \min\{m, n\}e$ holds.

In this way, we transform a differential problem in an algebraic one. More precisely, we have:

**Proposition 20.** *The fraction $\alpha_j$ is differentially algebraic over $\mathcal{F}\langle\alpha_1\rangle$ if and only if the set $\{\alpha_1^{[\nu]}, \alpha_j^{[\nu]}\}$ is* algebraically *dependent over $\mathcal{F}$ as a subset of the algebraic rational field $\mathcal{F}(\mathbf{t}^{[\nu+e]})$.*

This proposition allows us to apply a classical result from algebraic geometry which states that a finite set in a field of rational functions $L$ with coefficients in a field $K$ is algebraically independent over $K$ if and only if their gradient vectors are linearly independent over $L$ (see for instance [9, Ch. 7, Th. III, p. 135]).

Hence, we have the following effective criterion to decide if the extension $\mathcal{G}/\mathcal{F}$ has differential transcendence degree 1:

Please cite this article in press as: L. D'Alfonso et al., Quantitative aspects of the generalized differential Lüroth's Theorem, J. Algebra (2018), https://doi.org/10.1016/j.jalgebra.2018.01.050

**Theorem 21.** *The differential field extension $\mathcal{G}/\mathcal{F}$ has differential transcendence degree 1 if and only if for all index $j$, with $2 \leq j \leq n$, the rank over $\mathcal{F}(\mathbf{t}^{[\nu+e]})$ of the $2(\nu+1) \times m(\nu+e+1)$ Jacobian matrix*

$$\begin{pmatrix} \dfrac{\partial \alpha_1^{[\nu]}}{\partial \mathbf{t}^{[\nu+e]}} \\ \dfrac{\partial \alpha_j^{[\nu]}}{\partial \mathbf{t}^{[\nu+e]}} \end{pmatrix}$$

*is strictly smaller than $2(\nu+1)$.*

### *5.2. Computation of the Lüroth generator*

Here we describe a probabilistic algorithmic procedure to compute a Lüroth generator of a finitely generated differential subextension $\mathcal{G}/\mathcal{F}$ of $\mathcal{F}\langle \mathbf{t} \rangle/\mathcal{F}$ with differential transcendence degree 1, working over a polynomial ring in finitely many variables.

In order to achieve this, we combine the characterization of a Lüroth generator given in Section 3.2 and the results from Section 4.1 that enable us to translate a problem involving differential ideals into a problem concerning polynomial ideals with finitely many known generators.

Keeping our previous notations, if $\mathcal{G} = \mathcal{F}\langle P_1(\mathbf{t})/Q_1(\mathbf{t}), \ldots, P_n(\mathbf{t})/Q_n(\mathbf{t}) \rangle$, let $F_j = Q_j(\mathbf{y})x_j - P_j(\mathbf{y})$ for $j = 1, \ldots, n$, and $F = F_1, \ldots, F_n$.

First, we compute a polynomial $M(\mathbf{x}, \mathbf{y}) \in \mathfrak{P} \setminus (\mathfrak{P} \cap \mathcal{F}\{\mathbf{x}\})\{\mathbf{y}\}$ with minimal rank in $\mathbf{y}$ for an orderly ranking in the variables $\mathbf{y}$: following Proposition 11, consider the polynomial ideal $(F, \dot{F}, \ldots, F^{(\nu)}) : q^\infty \subset \mathcal{F}[\mathbf{x}^{[\nu]}, \mathbf{y}^{[\nu+e]}]$. Compute a Gröbner basis $G$ of this ideal for a product monomial order in $\mathcal{F}[\mathbf{x}^{[\nu]}, \mathbf{y}^{[\nu+e]}]$ such that

- $\mathbf{x} < \dot{\mathbf{x}} < \cdots < \mathbf{x}^{(\nu)} < \mathbf{y} < \dot{\mathbf{y}} < \cdots < \mathbf{y}^{(\nu+e)}$,
- each group of variables $\mathbf{x}^{(k)}$, for $k = 0, \ldots, \nu$, and $\mathbf{y}^{(l)}$, for $l = 0, \ldots, \nu+e$, is given the graded lexicographic order.

The smallest polynomial in $G$ which contains at least one variable in $\mathbf{y}^{[\nu+e]}$ is a polynomial $M$ satisfying the required conditions.

Then, we choose at random two specialization points $\upsilon_1$ and $\upsilon_2$ in $\mathbb{Q}^{m(\nu+e+1)}$ for the variables $\mathbf{t}^{[\nu+e]}$ in the polynomial $\widetilde{M}$ introduced in (4) and compute $\tau_{l,j,k} := (P_j/Q_j)^{(k)}(\upsilon_l)$ for $j = 1, \ldots, n$, $k = 0, \ldots, \nu$, and $l = 1, 2$. If $\tau_1 := (\tau_{1,j,k})$ and $\tau_2 := (\tau_{2,j,k})$, we obtain the polynomials $P(\mathbf{y}) = M(\tau_1, \mathbf{y})$ and $Q(\mathbf{y}) = M(\tau_2, \mathbf{y})$.

Finally, we take $v = P(\mathbf{t})/Q(\mathbf{t})$. By Proposition 4 and Remark 5, if $\upsilon_1$ and $\upsilon_2$ lie outside the zero set of a known polynomial, the differential rational function $v$ is a Lüroth generator of $\mathcal{G}/\mathcal{F}$.

We point out that, even if the algorithm is easy to describe, the rapid increase of the number of variables and the degrees of the algebraic ideals involved, together with the

Please cite this article in press as: L. D'Alfonso et al., Quantitative aspects of the generalized differential Lüroth's Theorem, J. Algebra (2018), https://doi.org/10.1016/j.jalgebra.2018.01.050

fact that a specific elimination monomial ordering must be considered seem to be major constraints to obtain an output within a reasonable time for inputs of moderate size.

### 5.3. Example

Let $\mathcal{F}$ be a differential field of characteristic 0 and $\{t_1, t_2\}$ differential indeterminates over $\mathcal{F}$.

**Example.** Let $\mathcal{G} = \mathcal{F}\langle \dot{t}_1 t_2 + t_1 \dot{t}_2, t_1^2 t_2^2 \rangle$. Here, we have:

- $e = 1$, $n = 2$, $m = 2$,
- $\alpha_1 = \dot{t}_1 t_2 + t_1 \dot{t}_2$, $\alpha_2 = t_1^2 t_2^2$.

First, we check whether the differential transcendence degree of $\mathcal{G}/\mathcal{F}$ equals 1 applying Theorem 21. In this case, $\nu = \min\{n, m\}e = 2$ and so, we consider the Jacobian matrix of $\{\alpha_1, \dot{\alpha}_1, \alpha_1^{(2)}, \alpha_2, \dot{\alpha}_2, \alpha_2^{(2)}\}$ with respect to $\{t_1, t_2, \dot{t}_1, \dot{t}_2, t_1^{(2)}, t_2^{(2)}, t_1^{(3)}, t_2^{(3)}\}$:

$$\begin{pmatrix}
\dot{t}_2 & \dot{t}_1 & t_2 & t_1 & 0 & 0 & 0 & 0 \\
t_2^{(2)} & t_1^{(2)} & 2\dot{t}_2 & 2\dot{t}_1 & t_2 & t_1 & 0 & 0 \\
t_2^{(3)} & t_1^{(3)} & 3t_2^{(2)} & 3t_1^{(2)} & 3\dot{t}_2 & 3\dot{t}_1 & t_2 & t_1 \\
2t_1 t_2^2 & 2t_1^2 t_2 & 0 & 0 & 0 & 0 & 0 & 0 \\
2\dot{t}_1 t_2^2 + 4t_1 \dot{t}_2 t_2 & 4\dot{t}_1 t_1 t_2 + 2t_1^2 \dot{t}_2 & 2t_1 t_2^2 & 2t_1^2 t_2 & 0 & 0 & 0 & 0 \\
\dfrac{\partial \alpha_2^{(2)}}{t_1} & \dfrac{\partial \alpha_2^{(2)}}{t_2} & 4\dot{t}_1 t_2^2 + 8t_1 \dot{t}_2 t_2 & 8\dot{t}_1 t_1 t_2 + 4t_1^2 \dot{t}_2 & 2t_1 t_2^2 & 2t_1^2 t_2 & 0 & 0
\end{pmatrix}$$

where $\dfrac{\partial \alpha_2^{(2)}}{t_1} = 2t_1^{(2)} t_2^2 + 8\dot{t}_1 \dot{t}_2 t_2 + 4t_1 t_2^{(2)} t_2 + 4t_1 \dot{t}_2^2$ and $\dfrac{\partial \alpha_2^{(2)}}{t_2} = 4t_1^{(2)} t_1 t_2 + 4\dot{t}_1^2 t_2 + 8\dot{t}_1 t_1 \dot{t}_2 + 2t_1^2 t_2^{(2)}$. Since the rank of this matrix is 4, which is smaller than $2(\nu+1) = 6$, we conclude that the differential transcendence degree of $\mathcal{G}/\mathcal{F}$ equals 1.

In order to obtain a Lüroth generator, let

$$F_1 = x_1 - \dot{y}_1 y_2 - y_1 \dot{y}_2, \quad F_2 = x_2 - y_1^2 y_2^2$$

and, following Section 5.2, consider the algebraic polynomial ideal

$$\begin{aligned}
&(F_1, F_2, \dot{F}_1, \dot{F}_2, F_1^{(2)}, F_2^{(2)}) \\
&\quad = (x_1 - \dot{y}_1 y_2 - y_1 \dot{y}_2, x_2 - y_1^2 y_2^2, \dot{x}_1 - y_1^{(2)} y_2 - 2\dot{y}_1 \dot{y}_2 - y_1 y_2^{(2)}, \dot{x}_2 - 2\dot{y}_1 y_1 y_2^2 - 2y_1^2 \dot{y}_2 y_2, \\
&\qquad x_1^{(2)} - y_1^{(3)} y_2 - 3y_1^{(2)} \dot{y}_2 - 3\dot{y}_1 y_2^{(2)} - y_1 y_2^{(3)}, \\
&\qquad x_2^{(2)} - 2y_1^{(2)} y_1 y_2^2 - 2\dot{y}_1^2 y_2^2 - 8\dot{y}_1 y_1 \dot{y}_2 y_2 - 2y_1^2 y_2^{(2)} y_2 - 2y_1^2 \dot{y}_2^2)
\end{aligned}$$

A differential polynomial $M(\mathbf{x}, \mathbf{y})$ providing a Lüroth generator can be found in this polynomial ideal:

Please cite this article in press as: L. D'Alfonso et al., Quantitative aspects of the generalized differential Lüroth's Theorem, J. Algebra (2018), https://doi.org/10.1016/j.jalgebra.2018.01.050

$$M(\mathbf{x},\mathbf{y}) = M(x_1, \dot{x}_2, y_1, y_2) = \dot{x}_2 - 2x_1y_1y_2.$$

Now, we choose two specialization points for $(t_1, t_2, \dot{t}_1, \dot{t}_2, t_1^{(2)}, t_2^{(2)})$, for instance, $\upsilon_1 = (1,1,1,0,0,0)$ and $\upsilon_2 = (2,1,0,1,0,0)$, compute the corresponding specialization values for $(x_1, \dot{x}_2)$, namely, $(1,1)$ and $(2,4)$, respectively, and obtain:

- $P(y_1, y_2) = M(1,1,y_1,y_2) = 1 - 2y_1y_2$,
- $Q(y_1, y_2) = M(2,4,y_1,y_2) = 4 - 4y_1y_2$

and, as a consequence of Proposition 4, the Lüroth generator

$$v = \frac{P(t_1,t_2)}{Q(t_{1,2})} = \frac{1-2t_1t_2}{4-4t_1t_2}.$$

Note that this implies that $t_1t_2$ is also a Lüroth generator of the extension.

## Acknowledgments

The authors wish to thank Santiago Laplagne and the anonymous referees for their helpful remarks and suggestions.

## References

[1] 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.
[2] 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.
[3] L. D'Alfonso, G. Jeronimo, P. Solernó, Effective differential Lüroth's theorem, J. Algebra 406 (2014) 1–19.
[4] J. Freitag, W. Li, Simple differential field extensions and effective bounds, in: Mathematical Aspects of Computer and Information Sciences, in: Lecture Notes in Comput. Sci., vol. 9582, Springer, 2016, pp. 343–357.
[5] X. Gao, T. Xu, Lüroth's theorem in differential fields, J. Syst. Sci. Complex. 15 (4) (2002) 376–383.
[6] O. Golubitsky, M. Kondratieva, A. Ovchinnikov, Algebraic transformation of differential characteristic decompositions from one ranking to another, J. Symbolic Comput. 44 (2009) 333–357.
[7] P. Gordan, Uber biquadratische Gleichungen, Math. Ann. 29 (1887) 318–326.
[8] J. Heintz, Definability and fast quantifier elimination in algebraically closed fields, Theoret. Comput. Sci. 24 (3) (1983) 239–277.
[9] W.V.D. Hodge, D. Pedoe, Methods of Algebraic Geometry, vol. 1, Cambridge University Press, 1953.
[10] J. Igusa, On a theorem of Lüroth, Mem. Coll. Sci. Univ. Kyoto Ser. A: Math. 26 (1951) 251–253.
[11] E.R. Kolchin, Differential Algebra and Algebraic Groups, Academic Press, New York, 1973.
[12] E.R. Kolchin, Extensions of differential fields, II, Ann. of Math. (2) 45 (1944) 358–361.
[13] E.R. Kolchin, Extensions of differential fields, III, Bull. Amer. Math. Soc. 53 (1947) 397–401.
[14] M.V. Kondratieva, A.V. Mikhalev, E.V. Pankratiev, Jacobi's bound for systems of differential polynomials, in: Algebra, Moskov. Gos. Univ., Moscow, 1982, pp. 79–85 (in Russian).
[15] M.V. Kondratieva, A.V. Mikhalev, E.V. Pankratiev, Jacobi's bound for independent systems of algebraic partial differential equations, Appl. Algebra Engrg. Comm. Comput. 20 (1) (2009) 65–71.
[16] J. Lüroth, Beweis eines Satzes über rationale curven, Math. Ann. 9 (1876) 163–165.
[17] J.F. Ritt, Differential Equations from the Algebraic Standpoint, Amer. Math. Soc. Colloq. Publ., vol. XIV, 1932, New York.

Please cite this article in press as: L. D'Alfonso et al., Quantitative aspects of the generalized differential Lüroth's Theorem, J. Algebra (2018), https://doi.org/10.1016/j.jalgebra.2018.01.050

[18] J.F. Ritt, Differential Algebra, Amer. Math. Soc. Colloq. Publ., vol. 33, 1950, New York.
[19] 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.
[20] A. Seidenberg, Some basic theorems in differential algebra (characteristic $p$ arbitrary), Trans. Amer. Math. Soc. 73 (1952) 174–190.

Please cite this article in press as: L. D'Alfonso et al., Quantitative aspects of the generalized differential Lüroth's Theorem, J. Algebra (2018), https://doi.org/10.1016/j.jalgebra.2018.01.050