A. Ovchinnikov *et al*, (2022) "Bounds for Elimination of Unknowns in Systems of Differential-Algebraic Equations,"
International Mathematics Research Notices, Vol. 2022, No. 16, pp. 12342–12377
Advance Access Publication April 22, 2021
https://doi.org/10.1093/imrn/rnaa302

Bounds for Elimination of Unknowns in Systems of Differential-Algebraic Equations

Alexey Ovchinnikov[1,*], Gleb Pogudin[2,†], and Thieu N. Vo[3,‡]

[1]Department of Mathematics,CUNY Queens College, 65-30 Kissena Blvd, Queens, NY 11367 and CUNY Graduate Center, Ph.D. Programs in Mathematics and Computer Science, 365 Fifth Avenue, New York, NY 10016, USA, [2]LIX, CNRS, École Polytechnique, Institute Polytechnique de Paris, Palaiseau, France, and [3]Fractional Calculus, Optimization and Algebra Research Group, Faculty of Mathematics and Statistics, Ton Duc Thang University, Ho Chi Minh City, Vietnam

[*]*Correspondence to be sent to: e-mail: aovchinnikov@qc.cuny.edu*

Elimination of unknowns in systems of equations, starting with Gaussian elimination, is a problem of general interest. The problem of finding an a priori upper bound for the number of differentiations in elimination of unknowns in a system of differential-algebraic equations (DAEs) is an important challenge, going back to Ritt (1932). The first characterization of this via an asymptotic analysis is due to Grigoriev's result (1989) on quantifier elimination in differential fields, but the challenge still remained. In this paper, we present a new bound, which is a major improvement over the previously known results. We also present a new lower bound, which shows asymptotic tightness of our upper bound in low dimensions, which are frequently occurring in

[†]Gleb Pogudin's prior addresses: Johannes Kepler University, Institute for Algebra, Austria; New York University, Courant Institute of Mathematical Sciences, New York, NY, USA; Higher School of Economics, Moscow, Department of Computer Science, Russia. Gleb Pogudin's email address: gleb.pogudin@polytechnique.edu

[‡]Thieu Vo's prior address: Johannes Kepler University, RISC, Austria. Thieu Vo's email address: vongocthieu@tdtu.edu.vn

Received March 15, 2020; Revised September 2, 2020; Accepted October 2, 2020
Communicated by Brian Conrad

applications. Finally, we discuss applications of our results to designing new algorithms for elimination of unknowns in systems of DAEs.

1 Introduction

Consider a system of equations (e.g., linear, polynomial, or differential)

$$f_1(\boldsymbol{x}, \boldsymbol{y}) = \ldots = f_N(\boldsymbol{x}, \boldsymbol{y}) = 0 \tag{1}$$

in two sets of unknowns, $\boldsymbol{x}$ and $\boldsymbol{y}$. To *eliminate* the $\boldsymbol{x}$-variables is to find, if it exists, a nontrivial equation $g(\boldsymbol{y}) = 0$ involving only the $\boldsymbol{y}$-variables that holds for every solution of (1) (a stronger version of the problem is to describe all such equations). Elimination of unknowns for systems of equations of different types, starting from Gaussian elimination for linear systems, is a classical problem. In this paper, we study elimination of unknowns in systems of differential-algebraic equations (DAEs), existing applications of which include combinatorics [1], mathematical analysis of dynamic models [3, 9, 25, 30], and control theory [11, 12].

The first theoretical method for elimination of unknowns in systems of DAEs was developed in [47, §67] by Ritt, the founder of differential algebra. The method can be viewed as a far reaching generalization of Gaussian elimination and was further developed, for example, in [4, 27]. Ritt [47, §87-88] also proposed another approach, which is similar to the prolongation-relaxation strategy used in 1847–48 by Cayley [7, 8] and later by Macaulay [36, Chapter I] for polynomial equations. Their technique was to reduce elimination in a system of polynomial equations (1) to elimination in a system of linear equations via an upper bound B such that

(a) considering the *prolongation*

$$\boldsymbol{x}^{\alpha}\boldsymbol{y}^{\beta}f_i(\boldsymbol{x}, \boldsymbol{y}) = 0, \quad 1 \leqslant i \leqslant N, \ \ |\alpha| + |\beta| \leqslant B, \tag{2}$$

(b) polynomial elimination of $\boldsymbol{y}$ in (1) is possible if and only if $\boldsymbol{y}$ can be eliminated in (2) considered as a linear system in the monomials in $\boldsymbol{x}$ and $\boldsymbol{y}$ appearing in (2) using Gaussian elimination (*relaxation*).

Extending this idea, the approach to elimination of unknowns in a system (1) of DAEs proposed by Ritt was:

(a) *Prolongation*: for a non-negative integer B, consider the derivatives

$$f_i(\boldsymbol{x}, \boldsymbol{y}) = 0,\ f_i(\boldsymbol{x}, \boldsymbol{y})' = 0,\ \ldots,\ f_i(\boldsymbol{x}, \boldsymbol{y})^{(B)} = 0,\ \ 1 \leqslant i \leqslant N. \tag{3}$$

(b) *Relaxation*: apply polynomial elimination (e.g., using [47, §55-60]) to (3) viewed as polynomial equations in $\boldsymbol{x}, \boldsymbol{x}', \ldots, \boldsymbol{y}, \boldsymbol{y}', \ldots$.

The results of Ritt [47, §87-88] imply that, for every system (1) of DAEs, the integer B can be chosen large enough so that, if an elimination of $\boldsymbol{x}$ for (1) is possible, it can be performed using polynomial elimination applied to (3). Thus, Ritt posed the following challenge in 1932 [47, p. 118],

> (Ritt's Challenge) For the above process to become a genuine method of decomposition, it would be necessary to have a method for determining permissible integers B.

Since then, finding a bound for B has been a major problem. One of the classical results in model theory of differential fields is that the theory of differentially closed field of characteristic zero, DCF_0, has quantifier elimination [37, Theorem 2.4]. Using an algorithm for quantifier elimination as a black box, one can solve elimination problem, which can be encoded as an elimination of existential quantifiers for the unknowns to be eliminated. An asymptotic analysis for the computational complexity of quantifier elimination in the case of constant coefficients was established by Grigoriev in [19], more than 50 years after Ritt had posed the problem. The complexity was shown to be bounded by an expression triple-exponential in the number of variables to be eliminated, which also involved the number of other variables, the number of equations, and the size of coefficients. Thus, this analysis did not give an explicit bound yielding a reasonable algorithm, so the challenge remained. Yet not addressing the challenge, in the special case of $\boldsymbol{x} = \varnothing$, there has been progress, described in Related results.

We have overcome Ritt's challege, and our upper bound for B in Ritt's prolongation-relaxation process for elimination is of the form (see Theorem 1 for more details and Theorem 3 for a stronger version of the elimination problem):

$$d^{(\overline{m}+1)2^{m+1}},$$

where

- $\boldsymbol{f}(\boldsymbol{x}, \boldsymbol{y}) = 0$ is a system of DAEs,
- $n = |\boldsymbol{x}|$ is the number of unknowns to be eliminated (not the total number of unknowns),
- h is the order of $\boldsymbol{f}$ in $\boldsymbol{x}$ and $d \geqslant 2$ the degree of $\boldsymbol{f}$ in $\boldsymbol{x}, \boldsymbol{x}', \ldots, \boldsymbol{x}^{(h)}$,
- m and $\overline{m}$ are the dimension and codimension of the variety V defined by $\boldsymbol{f}(\boldsymbol{x}, \boldsymbol{x}', \ldots, \boldsymbol{x}^{(h)}, \boldsymbol{y}, \boldsymbol{y}', \ldots) = 0$ in the affine space $\mathbb{V}$ of dimension $n(h+1)$ with coordinates $\boldsymbol{x}, \boldsymbol{x}', \ldots, \boldsymbol{x}^{(h)}$ (over the field K of rational functions in $\boldsymbol{y}, \boldsymbol{y}', \ldots$).

The bound is polynomial in the degrees, exponential in the codimension, and doubly exponential in the dimension.

Furthermore, if the polynomial ideal generated by F is radical, then the bound is significantly better (see Theorem 2):

$$\sum_{i=0}^{m} D^{2(2^i-1)}, \qquad \text{singly exponential in the dimension}$$

where D is the degree of V (see [23, p. 246]). Concrete systems of differential equations arising in applications usually have this property, and many of them have $m = 0, 1$. For instance, if the parameter identifiability problem of ODE models is approached via input–output equations, then one solves an elimination problem for a prime (and therefore radical) differential ideals (see [35, 38–42, 50] and the references therein). The corresponding value of m is equal to $s - 2\ell$ (using Remark 2), where s is the number of state variables, and ℓ is the number of output variables (terminology/setup of the problem). Example 1 is a natural example with the resulting m being 0, more example can be found in [24, Appendix B] (half of benchmarks there have $m = 0, 1$). Examples 2 and 3 illustrate differential elimination problems in other contexts.

If $m = 0$, then the bound given by Theorem 2 is 1, which is tight. If $m = 1$, then the bound given by Theorem 2 is at most

$$D^2 + 1.$$

Our new lower bound for $m = 1$ is $\binom{D+2}{2} - 1 = D^2/2 + 3D/2$ (see Proposition 1), and so our upper bound is asymptotically tight for $m \leqslant 1$.

A bound for full elimination, which is finding all possible results of elimination of given order, is presented in Theorem 3.

Finally, we show how our bound can be used to design a randomized (Monte Carlo) algorithm with guaranteed probability of correctness: given $0 < p < 1$, the algorithm decides whether an elimination of unknowns is possible with probability at least p (see Section 5). The implementation and examples are available at https://github.com/pogudingleb/DifferentialElimination.git.

In the remainder of the introduction, we present an outline of the approach and difficulties to overcome, as well as discuss related results.

Outline of the approach

The conceptual flow of the derivation of the main results is as follows (Even though this derivation can also be viewed as a computational procedure, we are not suggesting to use this as an algorithm in practice (see Section 5 for an actual algorithm).):

1. We reduce the case of a general system of DAEs to the case in which the system of DAEs generates a radical equidimensional (i.e., all prime components have the same dimension) ideal of the polynomial ring $K[\mathbb{V}]$ (Section 4.3.3).
2. We then reduce the latter case to the case in which the system of DAEs generates a prime polynomial ideal I (Section 4.3.2).
3. The bound for the case of prime ideals is derived using the following divide-and-conquer approach (Section 4.3.1) with induction on $m := \dim I$:
   (a) In the base case $m = 0$, the ideal I is maximal. Then Lemma 2 implies that either $\sqrt{I^{(\infty)}} \cap K[\mathbb{V}] = I$, so the bound is 0, or $\sqrt{I^{(\infty)}} \cap K[\mathbb{V}] = I^{(1)} \cap K[\mathbb{V}] = K[\mathbb{V}]$, so the bound is 1.
   (b) Suppose now that $m > 0$. If $I^{(1)} \cap K[\mathbb{V}] = I$, then the bound is again 0 by Lemma 2, and we are done with this prime component. Otherwise, we proceed as follows:
      i. The key ingredient, Lemma 4, implies that there exists a polynomial $g \in I^{(1)} \cap K[\mathbb{V}]$ with $\deg g \leqslant D := \deg I$ such that $\dim\langle I, g\rangle < \dim I$ (getting this degree bound is one of the main subtleties, thus providing a key improvement of the method used in [10, 26]).
      ii. We pass to $\sqrt{\langle I, g\rangle}$ using Lemmas 6 and 7.
      iii. Since all prime components of $\sqrt{\langle I, g\rangle}$ are of dimension $m - 1$ (also the sum of their degrees is at most D^2), we apply the argument inductively to each of them.

iv. The bounds for the prime components are combined together using Lemma 8.

4. The above steps yield a general bound given in Proposition 4. The main results are deduced from the proposition as follows:

   - Theorem 2 follows from the proposition by restriction to radical ideals.
   - Theorems 1 and 3 are derived from the proposition by estimating the geometric data in terms of the combinatorial data (e.g., $D \leqslant d^{\overline{m}}$, where $\overline{m}$ is the codimension of the corresponding variety).

We derive the asymptotic tightness of our bound for $m = 1$ by finding a witness (for a quadratic lower bound) of the form $x' = 1$, $y' = y$, $P(x, y) = 0$, with $\deg P \leqslant D$, that nevertheless has an "approximate solution" $x(t) = t$, $y(t) = e^t$ (i.e., the equations in the system vanish at $t = 0$ up to order $\binom{D+2}{2} - 1$ after substituting (t, e^t)).

We derive a randomized (Monte Carlo) algorithm with guaranteed probability of correctness as follows:

- Theorems 1 and 2 reduce determining the possibility of elimination for a system of DAEs to determining the possibility of elimination for a polynomial system in q unknowns $\boldsymbol{z} = \left(\boldsymbol{x}, \boldsymbol{x}', \ldots, \boldsymbol{x}^{(B_1)}\right)$ and r unknowns $\boldsymbol{w} = \left(\boldsymbol{y}, \boldsymbol{y}', \ldots, \boldsymbol{y}^{(B_2)}\right)$ for suitable B_1 and B_2.
- An elimination of the $\boldsymbol{z}$ variables for a system $\boldsymbol{p}(\boldsymbol{z}, \boldsymbol{w}) = 0$ of polynomial equations is possible if and only if the projection π of the variety $X \subset \mathbb{A}^q \times \mathbb{A}^r$ defined by $\boldsymbol{p}(\boldsymbol{z}, \boldsymbol{w}) = 0$ to the $\boldsymbol{w}$-coordinates is not dominant.
- We check the dominance of π by determining whether the fiber over a random point on the $\boldsymbol{w}$-plane is not empty (cf. [46]). The dimension r of the search space is bounded by Theorems 1 and 2. If every coordinate of a random point is sampled from a finite set S (e.g., a finite set of integers), then the non-emptyness of the fiber is equivalent to the dominance of π with probability at least

$$1 - \deg X / |S|.$$

We show this by proving, in particular, that

$$\overline{\pi(X)} = \mathbb{A}^r \implies \frac{|S^r \cap Z|}{|S^r|} \leqslant \frac{\deg X}{|S|}, \quad Z := \mathbb{A}^r \setminus \pi(X).$$

Related results

There are related bounds for other problems about systems of DAEs:

- **Determining consistency.** To determine the consistency of a system of DAEs using the prolongation-relaxation strategy (also referred to as effective differential Nullstellensatz) is a special case of elimination in systems of DAEs because a system of DAEs is inconsistent if and only if it is possible to eliminate all of the unknowns (i.e., to derive a consequence of the form $1 = 0$). There has been significant progress in analyzing this problem [10, 17, 20, 51, 53]. However, it has been a challenge to find practical upper bounds for this problem, as the upper bounds obtained there
  - either are asymptotic and so cannot be used in a differential elimination algorithm directly,
  - or have values that make them impossible to be used even for small examples.

  Our results address both issues for DAEs for the consistency problem.
- **Differential resultants** can be used to give a solution to the elimination problem of generic systems of DAEs of a special form (see [15, 33, 34, 48, 49] and the references given there).
- **Counting solutions.** Unlike in usual applications to modeling and sciences, some systems of DAEs arising in algebraic number theory (see, e.g., [26, Section 5] and [14, Sections 5.1–5.2]) have only finitely many solutions, and an important problem is estimate this number. Such bounds were obtained and applied to number-theoretic problems in [2, 13, 14, 26]. Theorem 3 can be used to design a prolongation-relaxation algorithm for determining the number of solutions of a given DAE (see Remark 1).

2 Preliminaries and Main Results

2.1 Differential algebra

Throughout the paper, all fields are assumed to be of characteristic 0. Let R be a commutative ring.

Definition 1. (Differential rings)

- A map $D\colon R \to R$ satisfying $D(a+b) = D(a) + D(b)$ and $D(ab) = aD(b) + D(a)b$ for all $a, b \in R$ is called a *derivation*.
- A *differential ring* R is a ring with a specified derivation D. In this case, we will denote $D(x)$ by x' and $D^n(x)$ by $x^{(n)}$.
- A differential ring that is a field will be called a *differential field*.
- A differential ring A is said to be a *differential k-algebra* over a differential field k if A is a k-algebra and the restriction of the derivation of A on k coincides with the derivation on k.
- Let A be a differential k-algebra.
  - We consider the polynomial ring $A\left[x^{(0)}, x^{(1)}, x^{(2)}, \dots\right]$, where $x^{(0)}, x^{(1)}, x^{(2)}, \dots$ are algebraically independent variables. We will also use the notation x, x', x'' for $x^{(0)}, x^{(1)}, x^{(2)}$, respectively.
  - For $h \geqslant 0$, the polynomial algebra $A\left[x^{(0)}, x^{(1)}, \dots, x^{(h-1)}\right]$ is denoted by $A[x_h]$.
  - Extending, for a tuple $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_n) \in \mathbb{Z}^n_{\geqslant 0}$ and variables $\boldsymbol{x} = (x_1, \dots, x_n)$, the corresponding polynomial algebra is denoted by $A[\boldsymbol{x}_{\boldsymbol{\alpha}}]$.
  - Extending the derivation from A to $A\left[x^{(0)}, x^{(1)}, x^{(2)}, \dots\right]$ by $D(x^{(i)}) = x^{(i+1)}$, we obtain a differential algebra.
  - This algebra is called the *algebra of differential polynomials* in x over A and denoted by $A[x_\infty]$.
  - Iterating this construction, we define the algebra of differential polynomials in variables $\boldsymbol{x} := x_1, \dots, x_n$ over A and denote it by $A[\boldsymbol{x}_\infty]$. If A is a field, then the field of fractions of $A[\boldsymbol{x}_\infty]$ is denoted by $A(\boldsymbol{x}_\infty)$.

Definition 2. (Ideals)

- The ideal of a ring R generated by $a_1, \dots, a_n \in R$ will be denoted by $\langle a_1, \dots, a_n \rangle$.
- An ideal I of a differential ring R is said to be a *differential ideal* if $a' \in I$ for all $a \in I$.
- The differential ideal generated by $a_1, \dots, a_n \in R$ will be denoted by $\langle a_1, \dots, a_n \rangle^{(\infty)}$.
- For an ideal I (not necessarily differential) of $k[\boldsymbol{x}_\infty]$, $I^{(h)}$ denotes the ideal generated by all elements of the form $a^{(j)}$, where $a \in I$ and $j \leqslant h$. If $h = \infty$, then $I^{(h)}$ denotes $\langle I \rangle^{(\infty)}$.

- An ideal I is *radical* if, whenever $a^n \in I$ for some $n > 0$, $a \in I$. The smallest radical ideal containing $a_1, \ldots, a_n$ will be denoted by $\sqrt{\langle a_1, \ldots, a_n \rangle}$.
- For an ideal I and a non-negative integer i, the *equidimensional component* of I of dimension i is the intersection of prime components of $\sqrt{I}$ of dimension i.
- For a variety X, $\deg X$ denotes the degree of X (see [23, Definition 1 and Remark 2]).

The following is a version of Hilbert's Nullstellensatz for DAEs, which shows the correctness of the prolongation-relaxation approach to elimination for systems of DAEs.

- **Theorem [31, Theorem IV.2.1].** For all $f_1, \ldots, f_N \in k[\boldsymbol{x}_\infty, \boldsymbol{y}_\infty]$ and $g \in k[\boldsymbol{y}_\infty]$, the following are equivalent

  (a) for every $(\boldsymbol{x}^*, \boldsymbol{y}^*)$ in every differential field extension of k,

  $$f_1(\boldsymbol{x}^*, \boldsymbol{y}^*) = \ldots = f_N(\boldsymbol{x}^*, \boldsymbol{y}^*) = 0 \implies g(\boldsymbol{y}^*) = 0;$$

  (b) there exists M such that $g^M \in \langle f_1, \ldots, f_N \rangle^{(\infty)}$.

2.2 Main result

In this section, we state our main results, and their consequences. Proofs are postponed until Section 4.3.

Theorem 1 (Bound for an elimination). For all integers $s, t \geqslant 0$, tuples $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_s) \in \mathbb{Z}^s_{\geqslant 0}$, and $F \subset k(\boldsymbol{y}_\infty)[\boldsymbol{x}_\alpha]$,

$$\langle F \rangle^{(\infty)} \cap k[\boldsymbol{y}_\infty] = \{0\} \iff \langle F \rangle^{(B)} \cap k[\boldsymbol{y}_\infty] = \{0\},$$

where

- $B = \begin{cases} d^{(|\boldsymbol{\alpha}|-m+1)2^{m+1}}, & d \geqslant 2, \\ m+1, & d = 1, \end{cases}$
- $|\boldsymbol{\alpha}| = \alpha_1 + \ldots + \alpha_s$,
- $\boldsymbol{x} := (x_1, \ldots, x_s)$, $\boldsymbol{y} := (y_1, \ldots, y_t)$,
- $d = \max_{f \in F} \deg_{\boldsymbol{x}} f$, and
- $m = \dim \langle F \rangle$ in $k(\boldsymbol{y}_\infty)[\boldsymbol{x}_\alpha]$.

For many systems arising in applications, the ideal generated by F turns out to be radical (see examples in Section 3). In this situation, we present an improvement to Theorem 1, in Theorem 2. It follows from our proofs that this new upper bound is always smaller that one provided by Theorem 1.

Theorem 2 (Bound for an elimination for radical ideals). For all integers $s, t \geqslant 0$, tuples $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_s) \in \mathbb{Z}^s_{\geqslant 0}$, and $F \subset k(\boldsymbol{y}_\infty)[\boldsymbol{x}_\alpha]$, if the ideal $\langle F \rangle$ of $k(\boldsymbol{y}_\infty)[\boldsymbol{x}_\alpha]$ is radical, then

$$\langle F \rangle^{(\infty)} \cap k[\boldsymbol{y}_\infty] = \{0\} \iff \langle F \rangle^{(B)} \cap k[\boldsymbol{y}_\infty] = \{0\},$$

where

- $B = \sum_{0 \leqslant i \leqslant j \leqslant m} D_j^{2(2^i-1)}$,
- $\boldsymbol{x} := (x_1, \ldots, x_s)$, $\boldsymbol{y} := (y_1, \ldots, y_t)$,
- D_j is the degree of the equidimensional component of $\langle F \rangle$ of dimension j in $k(\boldsymbol{y}_\infty)[\boldsymbol{x}_\alpha]$, and
- we use the convention $0^0 = 0$.

For example, if $m = 0$, then $B = D_0^0$. If $m = 1$, then $B = D_1^2 + 1 + D_0^0$.

Theorem 3 (Bound for full elimination). For all integers $s, t \geqslant 0$, tuples $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_s) \in \mathbb{Z}^s_{\geqslant 0}$, $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_t) \in \mathbb{Z}^s_{\geqslant 0}$, and $F \subset k[\boldsymbol{x}_\alpha, \boldsymbol{y}_\beta]$,

$$\sqrt{\langle F \rangle^{(\infty)}} \cap k[\boldsymbol{y}_\beta] = \sqrt{\langle F \rangle^{(B)}} \cap k[\boldsymbol{y}_\beta],$$

where

- $B = \begin{cases} d^{(|\boldsymbol{\alpha}|+|\boldsymbol{\beta}|-m+1)2^{m+1}}, & d \geqslant 2, \\ m+1, & d = 1, \end{cases}$
- $\boldsymbol{x} := (x_1, \ldots, x_s)$, $\boldsymbol{y} := (y_1, \ldots, y_t)$,
- $|\boldsymbol{\alpha}| = \alpha_1 + \ldots + \alpha_s$, $|\boldsymbol{\beta}| = \beta_1 + \ldots + \beta_t$,
- $d = \max_{f \in F} \deg f$, and
- $m = \dim \langle F \rangle$ in $k[\boldsymbol{x}_\alpha, \boldsymbol{y}_\beta]$.

Remark. In Theorems 1 and 3, the expressions for the value of B can be replaced by the tighter ones obtained in inequality (19).

Proposition 1 (Lower bound for elimination). For every positive integer d, there exists an irreducible polynomial $P \in \mathbb{Q}[x, y]$ of degree at most d such that

$$1 \in \langle x' - 1, y' - y, P(x, y)\rangle^{(\infty)},$$
$$1 \notin \langle x' - 1, y' - y, P(x, y)\rangle^{(B-1)},$$

where $B = (\frac{d+2}{2}) - 1 = \frac{d(d+3)}{2}$.

Corollary 1. The bound in Theorem 2 is asymptotically tight for $m \leqslant 1$.

Remark 1. Consider $F \subset k[\mathbf{y}_\beta]$ with $\boldsymbol{\beta} \in \mathbb{Z}^t_{\geqslant 1}$. One can show that

$$\langle F\rangle^{(\infty)} \text{ has finitely many solutions} \iff \langle F\rangle^{(\infty)} \cap k[\mathbf{y}_1] \text{ has finitely many solutions,} \quad (4)$$

where $\mathbf{1} = (1, \ldots, 1)$. Furthermore, Theorem 3 implies that $\langle F\rangle^{(\infty)} \cap k[\mathbf{y}_1]$ is finite if and only if $\langle F\rangle^{(B)} \cap k[\mathbf{y}_1]$ is finite. Thus, using (4) and Theorem 3, one can design the following prolongation-relaxation algorithm for counting solutions of a system F of DAEs as follows:

1. Let B be the bound given by Theorem 3 applied $F \subset k[\mathbf{y}_\beta]$.
2. Successively taking N to be each integer from 1 to B, we check whether $\dim\left(\langle F\rangle^{(N)} \cap k[\mathbf{y}_1]\right) \leqslant 0$ and, if it is, stop and go to Step 3.
3. If, for all N from Step 2, $\dim\left(\langle F\rangle^{(N)} \cap k[\mathbf{y}_1]\right) > 0$, return ∞. Otherwise, we return the number of common zeros of the polynomials $\langle F\rangle^{(N)} \cap k[\mathbf{y}_\beta]$ that are also solutions of $F = 0$ as a system of DAEs.

3 Examples

In this section, we will show how our bounds can be used for elimination of unknowns in DAEs in practice. Our approach is general rather than *ad hoc*. Examples 1, 2, and 3 are from modeling, and $m = 0, 1$ in all of them (cf. Corollary 1). We have constructed Example 4 to show elimination for $m = 2$. All of the computational results below can be reproduced using our Maple code at https://github.com/pogudingleb/DifferentialElimination/tree/master/examples. The computation takes less than 30 seconds on a laptop.

Example 1 (Lotka–Volterra model). Consider the classical Lotka–Volterra equations (also known as the predator–prey equations),

$$\begin{cases} x' = \alpha x - \beta xy, \\ y' = \delta xy - \gamma y, \end{cases} \tag{5}$$

in which x and y are the populations of prey and predators, respectively. Frequently, one of these quantities, say y, cannot be measured in experiments. Using our main result, we can determine if there are relations among the parameters $\alpha, \beta, \gamma, \delta$ and the derivatives of x (the population of prey). Such relations can be further used to test the model against experimental data [21]. Finding the relations is the problem of eliminating y. In this case, we consider (5) in $\mathbb{Q}(\alpha, \beta, \gamma, \delta)(x_\infty)[y, y']$, which defines an affine variety of dimension zero ($m = 0$). Therefore, the bound provided by Theorem 2 is $B = 1$. The desired relation is

$$xx'' - x'^2 + x(\alpha x - x')(\delta x - \gamma) = 0.$$

Note that β does not appear in this relation as it is independent of $\alpha, \gamma, \delta, x, x', \ldots$ (cf. [25, Example 2.13]).

Example 2 (Van der Pol oscillator). The system

$$\begin{cases} y' = z, \\ (1 - y^2)z - y = 0, \end{cases} \tag{6}$$

is a limiting case of the Van der Pol oscillator [32, Example 1.7]. Consider the problem of eliminating y. System (6) is a system of a linear equation in y' with coefficients in $\mathbb{C}(z)$ and a quadratic equation in y with non-zero discriminant and with coefficients in $\mathbb{C}(z)$. Thus, (6) defines a zero-dimensional radical ideal in $\mathbb{C}(z)[y, y']$, and so $m = 0$. Hence, Theorem 2 implies that if elimination is possible, it is possible after one prolongation. After this one prolongation, one can now find the following consequence of (6) not involving y using only polynomial elimination:

$$z'^2 - z'z - 4z'z^3 + z^4 + 4z^6 = 0.$$

Remark 2. In Examples 4 and 3, we use the following observation. If $F \subset k(\boldsymbol{y}_\infty)[\boldsymbol{x}_\alpha]$ for some $\boldsymbol{\alpha} \in \mathbb{Z}^s_{\geqslant 0}$ and, for some $f \in F$, we have $f' \in k(\boldsymbol{y}_\infty)[\boldsymbol{x}_\alpha]$, then one can consider the

Table 1. Example 3

Equation in	(D_0, D_1)	Bound from Theorem 2	Elimination possible?
x	$(0, 2)$	5	No
y	$(0, 2)$	5	No
x, F_1	$(2, 0)$	1	No
y, F_2	$(2, 0)$	1	No

equivalent system $\{F, f'\}$ instead. For this new system, the bound given by Theorem 2 will be smaller or the same. This is not an ad hoc trick and can be used in an algorithm.

Example 3 (Pendulum). In this example, we will show how our bounds can be used to show the *impossibility* of elimination. Consider the following system from [16, p. 725]:

$$\begin{cases} x'' = Tx + F_1, \\ y'' = -Ty + 1 + F_2, \\ x^2 + y^2 = 1 \end{cases} \tag{7}$$

with added external force $\mathbf{F} = (F_1, F_2)$. System (7) describes a pendulum with unit mass, length, and gravity. The unknown functions x and y stand for the coordinates, and T denotes the string tension. Since differentiating the equation $x^2 + y^2 = 1$ twice does not introduce derivatives that do not appear in the system already, following Remark 2, we extend system (7) by

$$\begin{cases} xx' + yy' = 0, \\ x'^2 + xx'' + y'^2 + yy'' = 0. \end{cases} \tag{8}$$

We will consider problems of deriving differential equations in subsets of variables. The results are summarized in Table 1 (in all cases, $m = 0, 1$). The impossibility of elimination was established using the approach developed in Section 5 with probability at least 99%.

Table 2. Example 4

Equation in	(D_0, D_1, D_2)	Bound from Theorem 2	Elimination possible?
x_1, x_2	$(0, 2, 0)$	5	No
x_1, x_3	$(0, 0, 1)$	3	No
x_2, x_3	$(0, 0, 1)$	3	Yes

Example 4. We will now present an example that illustrates that the main result can also be used in $m = 2$ in practice whether or not elimination is possible. Consider

$$\begin{cases} x_1' = x_2 + u_1, \\ x_2' = x_1 + u_2, \\ x_3' = x_3(u_1 + u_2' - x_3). \end{cases} \tag{9}$$

One can think of u_1 and u_2 as control variables whose values can be prescribed in order to achieve a certain behavior for x_1, x_2, x_3. If there is a consequence of (9) involving only two of x_1, x_2, x_3, say x_1 and x_2, this would be a natural restriction on the trajectories on the (x_1, x_2)plane that can be achieved.

We consider all three possible pairs of variables to keep (x_1, x_2), (x_2, x_3), and (x_1, x_3). For the case (x_1, x_2), we additionally observe that one can add the derivative of the second equation from (9)

$$x_2'' = x_1' + u_2'$$

without changing α in the application of Theorem 2 (see Remark 2).

The results are summarized in Table 2 (in all cases, $m = 1, 2$). An equation only in x_2 and x_3 can be found using polynomial elimination after one prolongation. The impossibility of elimination in the cases (x_1, x_2) and (x_1, x_3) was established using the approach developed in Section 5 with probability at least 99%.

4 Proofs

The proofs are structured as follows. We first show, in Section 4.1, a new method that allows to build a dimension reduction procedure in such a way that the degree of the newly added equation is bounded by the degree of the ideal. In Section 4.2, we establish

a relation between differentiation and intersection of ideals, as well as gather results on the Noether exponent we will use later. Using these methods and results, the proof of the bound is finished in Section 4.3 along the following lines:

- we obtain a bound for the radical differential ideal membership problem for prime, radical equidimensional radical, and arbitrary polynomial ideals of the equations of the system to prove Proposition 4;
- From Proposition 4, we deduce a bound for the elimination problem given in Theorem 2. By estimating the geometric data in terms of the combinatorial data, we deduce bounds for the elimination problem given in Theorems 1 and 3 from Proposition 4.

Our proof of a new lower bound is given in Section 4.4.

For a field k, let $\overline{k}$ denote the algebraic closure of k. For $S \subset k[\boldsymbol{x}]$, the set of $\overline{k}$-points of the affine variety of S is denoted by $V(S)$.

4.1 Dimension reduction

In this section, we will show that if the intersection with a polynomial subring of $k[\boldsymbol{x}_\infty]$ of the form $k[\boldsymbol{x}_\alpha]$ and differentiation do not preserve a prime polynomial ideal, then this is witnessed by a polynomial of degree at most the degree of the ideal (see Lemma 4). This will be one of the keys in our inductive argument to prove the main result.

4.1.1 *General dimension reduction*

Let $\boldsymbol{x} = (x_1, \ldots, x_n)$ and $\mathbf{1} = (1, \ldots, 1) \in \mathbb{Z}^n$. We will use the following result, which is similar to [20, Lemma 3.1]:

Lemma 1. For every $\alpha \geqslant 1$ and prime ideal $I \subset k[\boldsymbol{x}_{\alpha\cdot\mathbf{1}}]$,

$$\langle I \cap k[\boldsymbol{x}_{(\alpha-1)\mathbf{1}}]\rangle^{(1)} \subset I \implies I = \sqrt{I^{(\infty)}} \cap k[\boldsymbol{x}_{\alpha\cdot\mathbf{1}}]. \tag{10}$$

Proof. Let π be the canonical homomorphism $\pi : k[\boldsymbol{x}_{\alpha\cdot\mathbf{1}}] \to B$, where

$$B = k[\boldsymbol{x}_{\alpha\cdot\mathbf{1}}]/I \supset A = k[\boldsymbol{x}_{(\alpha-1)\mathbf{1}}]\big/(I \cap k[\boldsymbol{x}_{(\alpha-1)\mathbf{1}}]).$$

We claim that the field of fractions $Q(B)$ of B satisfies the differential condition (see [20, p. 1146]). It is sufficient to show that, for every $f \in k[\boldsymbol{x}_{(\alpha-1)\mathbf{1}}]$ such that $\pi(f) = 0$, for the polynomial $g = f' \in k[\boldsymbol{x}_{\alpha\cdot\mathbf{1}}]$, the equality $\pi(g) = 0$ holds. $\pi(f) = 0$ implies that

$f \in I \cap k[\boldsymbol{x}_{(\alpha-1)\mathbf{1}}]$, so

$$g \in (I \cap k[\boldsymbol{x}_{(\alpha-1)\mathbf{1}}])^{(1)} \subset I.$$

Hence, $\pi(g) = 0$. Thus, by [43, Theorem 4.10], there exists an extension $K \supset Q(B)$, where K is a differential field, and the differential structure on K is compatible with that of $Q(A) \subset Q(B)$. Consider the differential homomorphism $\varphi\colon k[\boldsymbol{x}_\infty] \to K$ defined by $\varphi(x_i) = \pi(x_i)$, $1 \leqslant i \leqslant n$. Then, $\mathrm{Ker}\varphi \cap k[\boldsymbol{x}_{\alpha\cdot\mathbf{1}}] = I$, so

$$\sqrt{I^{(\infty)}} \cap k[\boldsymbol{x}_{\alpha\cdot\mathbf{1}}] \subset \mathrm{Ker}\varphi \cap k[\boldsymbol{x}_{\alpha\cdot\mathbf{1}}] = I.$$

The inverse inclusion is immediate. ■

Lemma 2. For every tuple $\boldsymbol{\alpha} \in \mathbb{Z}^n_{\geqslant 1}$ and prime ideal $I \subset k[\boldsymbol{x}_{\boldsymbol{\alpha}}]$,

$$\langle I \cap k[\boldsymbol{x}_{\boldsymbol{\alpha}-\mathbf{1}}]\rangle^{(1)} \subset I \implies I = \sqrt{I^{(\infty)}} \cap k[\boldsymbol{x}_{\boldsymbol{\alpha}}].$$

Proof. Let $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ and $\alpha = \max(\alpha_1, \ldots, \alpha_n)$, and, for every i, set $\delta_i = \alpha - \alpha_i$. We introduce new variables $\boldsymbol{y} = (y_1, \ldots, y_n)$. Let $\varphi\colon k[\boldsymbol{x}_\infty] \to k[\boldsymbol{y}_\infty]$ be the differential homomorphism defined by $\varphi(x_i) = y_i^{(\delta_i)}$ for all i. Then $J = k[\boldsymbol{y}_{\alpha\cdot\mathbf{1}}] \cdot \varphi(I)$ is a prime ideal in $k[\boldsymbol{y}_{\alpha\cdot\mathbf{1}}]$. Since

$$k[\boldsymbol{y}_{\alpha\cdot\mathbf{1}}] \cdot \varphi\big(\langle I \cap k[\boldsymbol{x}_{\boldsymbol{\alpha}-\mathbf{1}}]\rangle^{(1)}\big) = k[\boldsymbol{y}_{\alpha\cdot\mathbf{1}}] \cdot \langle J \cap k[\boldsymbol{y}_{(\alpha-1)\mathbf{1}}]\rangle^{(1)},$$

we obtain that $(J \cap k[\boldsymbol{y}_{(\alpha-1)\mathbf{1}}])^{(1)} \subset J$. Lemma 1 implies that $J = \sqrt{J^{(\infty)}} \cap k[\boldsymbol{y}_{\alpha\cdot\mathbf{1}}]$. Then

$$k[\boldsymbol{y}_\infty] \cdot \varphi\big(\sqrt{I^{(\infty)}}\big) = \sqrt{J^{(\infty)}} \implies I = \sqrt{I^{(\infty)}} \cap k[\boldsymbol{x}_{\boldsymbol{\alpha}}].$$

■

4.1.2 *Finding an equation of degree at most the degree of the ideal to lower the dimension*

For a non-negative integer D and an ideal $J \subset k[z_1, \ldots, z_N]$, let $J_D = \langle f \in J \mid \deg f \leqslant D\rangle$.

Lemma 3. For every non-negative integer D and prime ideal $J \subset k[z_1, \ldots, z_N]$ of degree D, there is a non-empty open subset $U \subset V(J)$ such that, for every $p \in U$,

$$J_{\mathfrak{m}} = (J_D)_{\mathfrak{m}}, \text{ where } \mathfrak{m} = I(p).$$

Proof. Without loss of generality, we can assume that $z_1, \dots, z_d$ form a transcendence basis of $k[z_1, \dots, z_N]$ modulo J. For every i, $d+1 \leqslant i \leqslant N$, we consider $P_i(z_1, \dots, z_d, z_i)$, a non-zero algebraic relation among $z_1, \dots, z_d, z_i$ modulo J of the smallest degree. Since P_i is a defining equation of the Zariski closure of the projection of $V(J)$ to the $(z_1, \dots, z_d, z_i)$ coordinates, for every i, $d+1 \leqslant i \leqslant N$, $\deg P_i \leqslant D$. Let

$$P := \frac{\partial P_{d+1}}{\partial z_{d+1}} \cdot \ldots \cdot \frac{\partial P_N}{\partial z_N}.$$

Let $U := V(J) \setminus V(P)$. Since $P_{d+1}, \dots, P_N$ are squarefree, P does not vanish everywhere on $Z(J)$, so $U \neq \varnothing$.

Let $p \in U$ and $\mathfrak{m} := I(p)$. The inclusion $J_D \subset J$ implies $(J_D)_{\mathfrak{m}} \subset J_{\mathfrak{m}}$. On the other hand, since P is the determinant of the Jacobian of $P_{d+1}, \dots, P_N$ with respect to $z_{d+1}, \dots, z_N$ and $P(p) \neq 0$, the polynomials $P_{d+1}, \dots, P_N$ form a system of local parameters of $V(J)$ at p. Then $P_{d+1}, \dots, P_N$ generate $J_{\mathfrak{m}}$ by [52, Theorem 2.5, p. 99]. ■

Lemma 4. For every tuple $\boldsymbol{\alpha} \in \mathbb{Z}^n_{\geqslant 1}$, if $I \subset k[\boldsymbol{x}_{\boldsymbol{\alpha}}]$ is a prime ideal such that $\langle I \cap k[\boldsymbol{x}_{\boldsymbol{\alpha}-\mathbf{1}}]\rangle^{(1)} \not\subset I$, then there exists $g \in \langle I \cap k[\boldsymbol{x}_{\boldsymbol{\alpha}-\mathbf{1}}]\rangle^{(1)}$ such that

$$\dim\langle I, g\rangle < \dim I \quad \text{and} \quad \deg g \leqslant \deg I.$$

Proof. Let $D := \deg I$. The inclusion $k[\boldsymbol{x}_{\boldsymbol{\alpha}-\mathbf{1}}] \subset k[\boldsymbol{x}_{\boldsymbol{\alpha}}]$ corresponds to a projection π. Let $X := V(I)$ and $X_0 := \overline{\pi(X)}$. [23, Lemma 2] implies that $\deg X_0 \leqslant \deg X$. Consider any $f \in I \cap k[\boldsymbol{x}_{\boldsymbol{\alpha}-\mathbf{1}}]$ such that $f' \notin I$. Then $X \setminus V(f')$ is a non-empty open subset of X. Applying Lemma 3 to the prime ideal $I \cap k[\boldsymbol{x}_{\boldsymbol{\alpha}-\mathbf{1}}]$, we obtain a non-empty subset $U \subset X_0$. Let

$$p \in \big(\pi^{-1}(U) \cap V(I)\big) \cap \big(V(I) \setminus V(f')\big).$$

Lemma 3 implies that there are polynomials $g_1, \dots, g_M \in I \cap k[\boldsymbol{x}_{\boldsymbol{\alpha}-\mathbf{1}}]$ of degree at most D and $a_1, \dots, a_M, b_1, \dots, b_M \in k[\boldsymbol{x}_{\boldsymbol{\alpha}-\mathbf{1}}]$ such that

$$f = \frac{a_1}{b_1} g_1 + \ldots + \frac{a_M}{b_M} g_M,$$

and, for all i, $1 \leqslant i \leqslant M$, $b_i(\pi(p)) \neq 0$. We clear the denominators and obtain

$$b_1 \cdot \ldots \cdot b_M \cdot f = c_1 \cdot g_1 + \ldots + c_M \cdot g_M$$

for suitable $c_1, \ldots, c_M \in k[\boldsymbol{x}_{\boldsymbol{\alpha}-\mathbf{1}}]$. We differentiate this equality and obtain

$$(b_1 \cdot \ldots \cdot b_M)' \cdot f + (b_1 \cdot \ldots \cdot b_M) \cdot f' = \left(c_1' \cdot g_1 + \ldots + c_M' \cdot g_M\right) + \left(c_1 \cdot g_1' + \ldots + c_M \cdot g_M'\right).$$

Since $f, g_1, \ldots, g_M$ vanish at p, and $b_1 \cdot \ldots \cdot b_M \cdot f'$ does not vanish at p, at least one of $g_1', \ldots, g_M'$, say g_1', does not vanish at p. Thus, we can set $g := g_1'$. ■

4.2 Multiplicity and differentiation

4.2.1 *Noether exponent*

For a field k, $\bar{k}$ will denote its algebraic closure.

Definition 3. Let I be an ideal in a commutative ring. The smallest positive integer μ (if it exists) such that $(\sqrt{I})^{\mu} \subset I$ is called *the Noether exponent* of I. The Noether exponent is welldefined for any ideal in a Noetherian ring.

Lemma 5. Let I be an ideal in a k-algebra A. Then

$$\bar{k} \otimes_k \sqrt{I} = \sqrt{\bar{k} \otimes_k I}.$$

Proof. Let $I_{\text{alg}} := \bar{k} \otimes_k I$ and $J := \bar{k} \otimes_k \sqrt{I}$. Then $J \subset \sqrt{I_{\text{alg}}}$. Since $A_{\text{alg}}/J \cong \bar{k} \otimes_k (A/\sqrt{I})$ and $A/\sqrt{I}$ is separable due to [5, Chapter V, §15, p. A.V.122, Theorem 1], A_{alg}/J is reduced, so J is a radical ideal. Let $a \in \sqrt{I_{\text{alg}}}$, then there exists N such that $a^N \subset I_{\text{alg}} \subset J$. Since J is radical, we have $a \in J$, and so $J = \sqrt{I_{\text{alg}}}$. ■

Corollary 2. Let I be an ideal in a k-algebra A with Noether exponent μ and $I_{\text{alg}} := \bar{k} \otimes_k I$. Then the Noether exponent of I_{alg} is at most μ.

Proof. By Lemma 5, $\sqrt{I_{\text{alg}}}$ is generated by any set of generators of $\sqrt{I}$, so $(\sqrt{I_{\text{alg}}})^{\mu} \subset I_{\text{alg}}$. ■

Lemma 6. Let $\boldsymbol{x} = (x_1, \ldots, x_n)$ and $\boldsymbol{\alpha} \in \mathbb{Z}^n_{\geqslant 0}$. For every prime ideal $I \subseteq k[\boldsymbol{x}_{\boldsymbol{\alpha}}]$ of degree D_0 and every $g \in k[\boldsymbol{x}_{\boldsymbol{\alpha}}]$ with $\deg g = D_1$, the Noether exponent of $\langle I, g \rangle$ does not exceed $D_0 D_1$.

Proof. If the ground field is algebraically closed, the lemma follows from [28, Corollary 4.6]. The case of not necessarily algebraically closed k follows from the lemma applied to $\bar{k} \otimes_k I$ and Corollary 2. ■

4.2.2 *Differentiation and intersection of ideals*

The following lemma follows from [45, Corollary 5.2] (see also [18, Theorem 2.2]).

Lemma 7. Let $\boldsymbol{x} = (x_1, \ldots, x_n)$. For all $q, m_1, \ldots, m_q \in \mathbb{N}$ and for all ideals (not necessarily differential) $I_1, \ldots, I_q \subset k[\boldsymbol{x}_\infty]$,

$$I_1^{(m_1)} \cdot \ldots \cdot I_q^{(m_q)} \subset \sqrt{(I_1 \cdot \ldots \cdot I_q)^{(m_1+\ldots+m_q)}}.$$

Lemma 8. Let $\boldsymbol{x} = (x_1, \ldots, x_n)$. For all $q, m_1, \ldots, m_q \in \mathbb{N}$ and for all ideals (not necessarily differential) $I_1, \ldots, I_q \subset k[\boldsymbol{x}_\infty]$,

$$I_1^{(m_1)} \cap \ldots \cap I_q^{(m_q)} \subset \sqrt{(I_1 \cap \ldots \cap I_q)^{(m_1+\ldots+m_q)}}.$$

Proof. We have

$$\left(I_1^{(m_1)} \cap \ldots \cap I_q^{(m_q)}\right)^q \subset I_1^{(m_1)} \cdot \ldots \cdot I_q^{(m_q)} \implies I_1^{(m_1)} \cap \ldots \cap I_q^{(m_q)} \subset \sqrt{I_1^{(m_1)} \cdot \ldots \cdot I_q^{(m_q)}}.$$

Lemma 7 implies that the latter radical is contained in $\sqrt{(I_1 \cdot \ldots \cdot I_q)^{(m_1+\ldots+m_q)}}$. Thus,

$$I_1^{(m_1)} \cap \ldots \cap I_q^{(m_q)} \subset \sqrt{(I_1 \cap \ldots \cap I_q)^{(m_1+\ldots+m_q)}}.$$

■

4.3 Proofs of the main results

Throughout this section, k denotes a differential field, and $\bar{k}$ denotes its algebraic closure. By [31, Lemma II.1], the derivation on k can be extended uniquely to $\bar{k}$. We introduce

$$B(m, D) := \sum_{i=0}^{m} D^{2(2^i-1)}. \tag{11}$$

The arguments in this section are structured as follows. We will start by showing that (11) is an upper bound for the number of differentiations in the radical differential ideal membership problem for polynomial prime and equidimensional radical ideals of

differential polynomials (see Propositions 2 and 3, respectively). This bound is adjusted to include arbitrary polynomial ideals of differential polynomials in Proposition 4. This results in the bound from Theorem 2, which we explain in Section 4.3.4, in which we also finish proving Theorems 1 and 3 by estimating B in (11) in terms of m, d, and $|\boldsymbol{\alpha}|$ or $|\boldsymbol{\alpha}|$ and $|\boldsymbol{\beta}|$, respectively.

4.3.1 *Prime ideals*

Proposition 2. For every positive integer n, tuple $\boldsymbol{\alpha} \in \mathbb{Z}^n_{\geqslant 0}$, prime ideal $I \subset \bar{k}[\boldsymbol{x}_{\boldsymbol{\alpha}}]$, and polynomial $f \in \bar{k}[\boldsymbol{x}_{\boldsymbol{\alpha}}]$, we have

$$f \in \sqrt{I^{(\infty)}} \iff f \in \sqrt{I^{(B(m,D))}},$$

where $m = \dim I$, $D = \deg I$, and $B(m, D)$ is defined in (11).

We will use the following lemma.

Lemma 9. For all

- $p(x) \in \mathbb{Z}_{\geqslant 0}[x]$ such that $p(0) = 1$ and $\deg p \geqslant 2$,
- $S, n \geqslant 1$ and tuples $(a_1, \ldots, a_n)$ of positive integers such that $\sum_{i=1}^{n} a_i = S$,

we have

$$\sum_{i=1}^{n} p(a_i) \leqslant p(S).$$

Proof. It is sufficient to prove that, for all $a, b \geqslant 1$,

$$p(a) + p(b) \leqslant p(a + b).$$

Let $p(x) = 1 + c_1 x + \ldots + c_d x^d$, where $d \geqslant 2$ and $c_d > 0$. We immediately have

$$\begin{aligned} c_1(a+b) + c_2(a^2 + b^2) + \ldots + c_{d-1}(a^{d-1} + b^{d-1}) &\leqslant c_1(a+b) \\ &+ c_2(a+b)^2 + \ldots + c_{d-1}(a+b)^{d-1}. \end{aligned}$$

So, it is sufficient to prove that $2 + c_d(a^d + b^d) \leqslant 1 + c_d(a+b)^d$. We have

$$1 + c_d(a+b)^d \geqslant 1 + c_d a^d + c_d \binom{d}{1} a b^{d-1} + c_d b^d \geqslant 2 + c_d(a^d + b^d).$$

■

Proof of Proposition 2. We will prove the proposition by induction on m. The base cases will be $m = 0, 1$.

- Case $m = 0$ follows from Lemma 2.
- Case $m = 1$. Then $B(m, D) = D^2 + 1$. Consider $f \in \sqrt{I^{(\infty)}} \cap \bar{k}[\boldsymbol{x}_{\alpha}]$. If $(I \cap \bar{k}[\boldsymbol{x}_{\alpha-1}])^{(1)} \subset I$, then Lemma 2 implies that $f \in I$. Otherwise, by Lemma 4, there exists $g \in (I \cap \bar{k}[\boldsymbol{x}_{\alpha-1}])^{(1)}$ such that

$$\dim I > \dim \langle I, g \rangle \quad \text{and} \quad \deg g \leqslant D.$$

Let $J = (I, g)$ and $J = Q_1 \cap \ldots \cap Q_s$ be a primary decomposition of J. Then

$$\sqrt{J} = I_1 \cap \ldots \cap I_s, \text{ where} I_j := \sqrt{Q_j} \text{ for} 1 \leqslant j \leqslant s.$$

Since $\dim I_j = 0$ for every j, $V(I_j) = p_j$ for some point p_j. Let

$$m_j = \dim_{\bar{k}} \bar{k}[\boldsymbol{x}_{\alpha}]/Q_j$$

be the multiplicity of J at the point p_j. Then $I_j^{m_j} \subset Q_j$. Bezout's theorem [22, Theorem 7.7, Chapter 1] implies that

$$m_1 + \ldots + m_s = \deg I \cdot \deg g \leqslant D^2.$$

The inclusions

$$f \in \sqrt{I_1^{(1)} \cap \ldots \cap I_s^{(1)}} \quad \text{and} \quad I_1^{m_1} \cdot \ldots \cdot I_s^{m_s} \subset Q_1 \cdot \ldots \cdot Q_s \subset J$$

together with Lemma 7 imply

$$\begin{aligned} f \in \sqrt{\left(I_1^{(1)}\right)^{m_1} \cdot \ldots \cdot \left(I_s^{(1)}\right)^{m_s}} &\subset \sqrt{\left(I_1^{m_1} \cdot \ldots \cdot I_s^{m_s}\right)^{(m_1+\ldots+m_s)}} \\ &\subset \sqrt{J^{(D^2)}} \subset \sqrt{I^{(1+D^2)}} = \sqrt{I^{(B(1,D))}}. \end{aligned}$$

- Inductive step for $m > 1$. Consider $f \in \bar{k}[\boldsymbol{x}_{\alpha}] \cap \sqrt{I^{(\infty)}}$. If $(I \cap \bar{k}[\boldsymbol{x}_{\alpha-1}])^{(1)} \subset I$, then Lemma 2 implies that $f \in I$. Otherwise, by Lemma 4, there exists $g \in (I \cap \bar{k}[\boldsymbol{x}_{\alpha-1}])^{(1)}$ such that

$$\dim I > \dim \langle I, g \rangle \quad \text{and} \quad \deg g \leqslant D.$$

Consider the minimal prime decomposition of $\sqrt{\langle I, g\rangle}$:

$$\widetilde{I} := \sqrt{\langle I, g\rangle} = I_1 \cap \ldots \cap I_s.$$

Then $\dim I_j = m - 1$ for all $1 \leqslant j \leqslant s$. Let $D_j := \deg I_j$ for every $1 \leqslant j \leqslant s$. [22, Theorem 7.7, Chapter 1] implies that $\sum_{j=1}^{s} D_i \leqslant D^2$. Since all $\sqrt{I_1^{(\infty)}}, \ldots, \sqrt{I_s^{(\infty)}}$ contain f, the inductive hypothesis implies that

$$f \in \sqrt{I_1^{(B(m-1,D_1))} \cap \ldots \cap I_s^{(B(m-1,D_s))}}.$$

By Lemma 8,

$$f \in \sqrt{\left(I_1 \cap \ldots \cap I_s\right)^{(B)}} = \sqrt{\widetilde{I}^{(B)}}, \quad \text{where} B := \sum_{i=1}^{s} B(m-1, D_i).$$

Lemma 6 implies that $\widetilde{I}^{D^2} \subset (I, g)$. Lemma 7 implies that

$$f \in \sqrt{\left(\widetilde{I}^{(B)}\right)^{D^2}} \subset \sqrt{\langle I, g\rangle^{(D^2 B)}} \subset \sqrt{I^{(D^2 B+1)}}. \tag{12}$$

$B(m-1, t)$ considered as a polynomial in t meets the requirements of Lemma 9. Applying Lemma 9 and using $\sum_{i=1}^{s} D_i \leqslant D^2$, we have

$$D^2 B + 1 = D^2 \sum_{i=1}^{s} B(m-1, D_i) + 1 \leqslant D^2 B(m-1, D^2) + 1 = B(m, D). \tag{13}$$

Combining (12) and (13), we show that $f \in \sqrt{I^{(B(m,D))}}$. ■

4.3.2 *Radical equidimensional ideals*

Proposition 3. For every positive integer n, tuple $\boldsymbol{\alpha} \in \mathbb{Z}^n_{\geqslant 0}$, radical equidimensional ideal $I \subset \bar{k}[\boldsymbol{x}_{\boldsymbol{\alpha}}]$, and polynomial $f \in \bar{k}[\boldsymbol{x}_{\boldsymbol{\alpha}}]$, we have

$$f \in \sqrt{I^{(\infty)}} \iff f \in \sqrt{I^{(B(m,D))}},$$

where $m = \dim I$, $D = \deg I$, and $B(m, D)$ is defined in (11).

Proof. Let $I = I_1 \cap I_2 \cap \ldots \cap I_s$ be the irreducible prime decomposition of I. Let $D_j := \deg I_j$ for $1 \leqslant j \leqslant s$. Consider $f \in \sqrt{I^{(\infty)}} \cap \bar{k}[\boldsymbol{x}_\alpha]$.

- Case $m > 0$. Since $f \in \sqrt{I_j^{(\infty)}}$ for all $1 \leqslant j \leqslant s$,

$$f \in \sqrt{I_1^{(B(m,D_1))} \cap \ldots \cap I_s^{(B(m,D_s))}}.$$

  Lemma 8 implies

$$f \in \sqrt{(I_1 \cap \ldots \cap I_s)^{(B)}}, \text{ where} B = \sum_{i=1}^{s} B(m, D_i).$$

  $B(m,t)$ as a polynomial in t meets the requirements of Lemma 9. Thus, $B \leqslant B(m,D)$.
- Case $m = 0$. Since $B(0,D) = 1$, $f \in \sqrt{I_j^{(1)}}$ for all $1 \leqslant j \leqslant s$. There exists an integer M such that $f^M \in I_j^{(1)}$ for all $1 \leqslant j \leqslant s$. Lemma 8 implies that

$$I_1 \cap \ldots \cap I_{j-1} \cap I_j^{(1)} \cap I_{j+1} \cap \ldots \cap I_s \subset \sqrt{I^{(1)}} \text{ for every} 1 \leqslant j \leqslant s.$$

  Hence,

$$\sum_{j=1}^{s} I_1 \cap \ldots \cap I_{j-1} \cap I_j^{(1)} \cap I_{j+1} \cap \ldots \cap I_s \subset \sqrt{I^{(1)}}.$$

  The left-hand side of the above inclusion contains the ideal

$$\sum_{j=1}^{s} I_1 \cap \ldots \cap I_{j-1} \cap \langle f^M \rangle \cap I_{j+1} \cap \ldots \cap I_s \supset \langle f^M \rangle \cdot \sum_{j=1}^{s} I_1 \cap \ldots \cap I_{j-1} \cap I_{j+1} \cap \ldots \cap I_s. \tag{14}$$

  Since $\sum_{j=1}^{s} I_1 \cap \ldots \cap I_{j-1} \cap I_{j+1} \cap \ldots \cap I_s$ is a sum of zero-dimensional ideals without a common zero, it is equal to $\bar{k}[\boldsymbol{x}_\alpha]$. Therefore, the right-hand side of (14) contains f^M. Thus $f \in \sqrt{I^{(1)}} = \sqrt{I^{(B(0,D))}}$. ■

4.3.3 *Arbitrary ideals*

Proposition 4. For every positive integer n, tuple $\boldsymbol{\alpha} \in \mathbb{Z}^n_{\geqslant 0}$, ideal $I \subset k[\boldsymbol{x}_\alpha]$, and $f \in k[\boldsymbol{x}_\alpha]$, we have

$$f \in \sqrt{I^{(\infty)}} \iff f \in \sqrt{I^{(B)}},$$

where

- $m = \dim I$,
- D_i is the degree of the equidimensional component of I of dimension i, $0 \leqslant i \leqslant m$,
- μ is the Noether exponent of I (which exists because $k[\boldsymbol{x}_\alpha]$ is Noetherian), and
- $B = \mu \cdot \sum_{i=0}^{m} B(i, D_i)$, where $B(m, D)$ is defined in (11).

Proof. We will first prove the proposition for an algebraically closed k. Consider $f \in \sqrt{I^{(\infty)}} \cap k[\boldsymbol{x}_\alpha]$. For each $0 \leqslant i \leqslant m$, let I_i be the radical ideal corresponding to the equidimensional component of dimension i of I. Proposition 3 implies that $f \in \sqrt{I_i^{(B(i,D_i))}}$ for every $0 \leqslant i \leqslant m$. Lemma 8 implies that

$$f \in \sqrt{\left(I_0 \cap I_1 \cap \ldots \cap I_m\right)^{(S)}} = \sqrt{\left(\sqrt{I}\right)^{(S)}}, \quad \text{where } S = \sum_{i=0}^{m} B(i, D_i).$$

Since $\left(\sqrt{I}\right)^{\mu} \subset I$, Lemma 7 implies that $\left(\sqrt{I}\right)^{(S)} \subseteq I^{(\mu \cdot S)}$. Hence, $f \in \sqrt{I^{(\mu \cdot S)}} = \sqrt{I^{(B)}}$.

We will finish the proof by considering the case of not necessarily algebraically closed k. For an ideal $J \subset k[\boldsymbol{x}_\alpha]$, we denote $J_{\text{alg}} = \bar{k} \otimes_k J$. Corollary 2 implies that the Noether exponent of I_{alg} is at most μ. Then the proposition applied to $I_{\text{alg}} \subset \bar{k}[\boldsymbol{x}_\alpha]$ implies that

$$\sqrt{(I_{\text{alg}})^{(\infty)}} \cap \bar{k}[\boldsymbol{x}_\alpha] = \sqrt{(I_{\text{alg}})^{(B)}} \cap \bar{k}[\boldsymbol{x}_\alpha].$$

Then we have

$$\begin{aligned} f \in \sqrt{I^{(\infty)}} &\implies f \in \sqrt{(I_{\text{alg}})^{(\infty)}} \cap k[\boldsymbol{x}_\alpha] \implies f \in \sqrt{(I_{\text{alg}})^{(B)}} \cap k[\boldsymbol{x}_\alpha] = \sqrt{\left(I^{(B)}\right)_{\text{alg}}} \cap k[\boldsymbol{x}_\alpha] \\ &= \left(\sqrt{I^{(B)}}\right)_{\text{alg}} \cap k[\boldsymbol{x}_\alpha] \subset \sqrt{I^{(B)}}, \end{aligned}$$

where we used Lemma 5. Finally, $f \in \sqrt{I^{(B)}} \implies f \in \sqrt{I^{(\infty)}}$ is by definition. ∎

4.3.4 *Bounds for elimination*

Proof. (Proof of Theorems 1 and 2) Let J be the ideal generated by F in $k(\mathbf{y}_\infty)[\mathbf{x}_\alpha]$.

- For each i, $0 \leqslant i \leqslant m$, let D_i be the degree of the equidimensional component of dimension i of $\sqrt{J}$.
- Let $\mu \geqslant 1$ be the Noether exponent of J.

Let

$$B := \mu \cdot \sum_{i=0}^{m} B(i, D_i). \tag{15}$$

Then Proposition 4 implies that

$$1 \in J^{(\infty)} \iff 1 \in J^{(B)}.$$

Thus,

$$\langle F \rangle^{(\infty)} \cap k[\mathbf{y}_\infty] \neq \{0\} \iff 1 \in J^{(\infty)} \iff 1 \in J^{(B)} \iff \langle F \rangle^{(B)} \cap k[\mathbf{y}_\infty] \neq \{0\}. \tag{16}$$

- Proof of Theorem 2. If J is radical, then $\mu = 1$, so $B = \sum_{i=0}^{m} B(i, D_i)$. Then the theorem follows from (16).
- Proof of Theorem 1. To finish the proof, it remains to estimate B in terms of m, d, and $|\alpha|$. Let $d_0 := \min_{f \in F} \deg_{\mathbf{x}} f$ and $r := |F|$. Therefore, $d_0 \leqslant d$.
- If $d = 1$, then $V(F)$ is an intersection of finitely many hyperplanes. Therefore, it is an irreducible variety of dimension m and degree $D_m = 1$. Thus, $B = m + 1$.
- We will now assume that $d \geqslant 2$. By [28, Corollary 4.6], we can bound the Noether exponent by

$$\mu \leqslant d_0 d^{\min\{r, |\alpha|\} - 1}. \tag{17}$$

For each i, we will estimate D_i. By [29, Lemma 3 and its proof], there exist $g_1, \ldots, g_{|\alpha|-i} \in k(\mathbf{y}_\infty)[\mathbf{x}_\alpha]$, where

(b) g_1 is the polynomial of minimal degree in F, so $\deg g_1 = d_0$, and

(b) $g_2, \ldots, g_{|\alpha|-i}$ are linear combinations of elements of F such that every component of $V(g_1, \ldots, g_{|\alpha|-i})$ of dimension greater than i is also a component of $V(F)$.

- Since $V(g_1, \ldots, g_{|\alpha|-i}) \supset V(F)$, the above implies that all components of $V(F)$ of dimension i are components of $V(g_1, \ldots, g_{|\alpha|-i})$ (but, maybe, there are some superfluous components of dimension i in $V(g_1, \ldots, g_{|\alpha|-i})$). Since $\deg g_j \leqslant d$ for all $j \geqslant 2$, [6, (8.28) Bézout Inequality] implies that the sum of the degrees of all components of $V(g_1, \ldots, g_{|\alpha|-i})$ does not exceed $d_0 d^{|\alpha|-i-1}$. Hence,

$$D_i \leqslant d_0 d^{|\alpha|-i-1}, \text{ for every } i = 0, \ldots, m. \tag{18}$$

By substituting (17) and (18) into (15), we obtain

$$B \leqslant d_0 d^{\min(|\alpha|,r)-1} \cdot \sum_{i=0}^{m} B\left(i, d_0 d^{|\alpha|-i-1}\right). \tag{19}$$

To achieve a simpler formula for the bound, we will replace d_0 by d. In particular, we have

$$B \leqslant d^{|\alpha|} \cdot \sum_{i=0}^{m} B\left(i, d^{|\alpha|-i}\right) = d^{|\alpha|} \cdot \sum_{i=0}^{m} \sum_{j=0}^{i} d^{(|\alpha|-i)(2^{j+1}-2)}. \tag{20}$$

Bounding the double sum by a geometric series with common ratio $\frac{1}{d^2}$ twice, we obtain, using $d \geqslant 2$,

$$\begin{aligned} \sum_{i=0}^{m} \sum_{j=0}^{i} d^{(|\alpha|-i)(2^{j+1}-2)} &\leqslant \frac{d^2}{d^2-1} \sum_{i=0}^{m} d^{(|\alpha|-i)(2^{i+1}-2)} \\ &\leqslant \left(\frac{d^2}{d^2-1}\right)^2 d^{(|\alpha|-m)(2^{m+1}-2)} \leqslant d^{(|\alpha|-m)(2^{m+1}-2)+1} \end{aligned}$$

Plugging this bound into (20), since $m \leqslant |\alpha| - 1$, we obtain

$$B \leqslant d^{|\alpha|+(|\alpha|-m)(2^{m+1}-2)+1} \leqslant d^{(|\alpha|-m)2^{m+1}+m} \leqslant d^{(|\alpha|-m+1)2^{m+1}}. \tag{21}$$

■

Proof of Theorem 3. By applying Proposition 4 to $I = \langle F \rangle \subset k[\boldsymbol{x}_\alpha, \boldsymbol{y}_\beta]$, we obtain

$$\sqrt{(F)^{(\infty)}} \cap k[\boldsymbol{x}_\alpha, \boldsymbol{y}_\beta] = \sqrt{(F)^{(B)}} \cap k[\boldsymbol{x}_\alpha, \boldsymbol{y}_\beta], \qquad \text{for } B = \mu \cdot \sum_{i=0}^{m} \sum_{j=0}^{i} D_i^{2^{j+1}-2},$$

where μ is the Noether exponent of I, and D_i is the degree of the equidimensional component of I of dimension i. By intersecting both sides with $k[\boldsymbol{y}_\infty]$, we obtain

$$\sqrt{(F)^{(\infty)}} \cap k[\boldsymbol{y}_\beta] = \sqrt{(F)^{(B)}} \cap k[\boldsymbol{y}_\beta].$$

Estimating B the same way we did in the proof of Theorem 1 in (19), (20), and (21), we obtain $B \leqslant d^{(|\boldsymbol{\alpha}|+|\boldsymbol{\beta}|-m+1)2^{m+1}}$. ■

4.4 Asymptotic tightness via a lower bound

In this section, we prove Proposition 1. We begin with two auxiliary lemmas.

Lemma 10. Let $\boldsymbol{x} = (x_1, \ldots, x_n)$. For all $g_1, \ldots, g_m \in \mathbb{C}[\boldsymbol{x}_\infty]$, positive integers N, and formal power series $f_1(t), \ldots, f_n(t) \in \mathbb{C}[\![t]\!]$,

$$\big(\forall i \;\; g_i(f_1(t), \ldots, f_n(t)) = \mathrm{O}(t^N),\ t \to 0\big) \implies 1 \notin \langle g_1, \ldots, g_m \rangle^{(N-1)}.$$

Proof. Consider the $\mathbb{C}$-algebra homomorphism $\varphi\colon \mathbb{C}[\boldsymbol{x}_\infty] \to \mathbb{C}$ defined by $\varphi\big(x_i^{(j)}\big) := f_i^{(j)}(0)$. Then $1 \notin \operatorname{Ker}\varphi$. We will prove the lemma by showing that

$$\langle g_1, \ldots, g_m \rangle^{(N-1)} \subset \operatorname{Ker}\varphi.$$

The chain rule implies that, for every i, $1 \leqslant i \leqslant m$, and $j \geqslant 0$,

$$g_i^{(j)}(x_1, \ldots, x_n)|_{x_i = f_i(t)} = \big(g_i(f_1(t), \ldots, f_n(t))\big)^{(j)}.$$

Then $\varphi(g_i^{(j)})$ is equal to the value of $\big(g_i(f_1(t), \ldots, f_n(t))\big)^{(j)}$ at $t = 0$. For every $j < N$ and i, since

$$\big(g_i(f_1(t), \ldots, f_n(t))\big)^{(j)} = \big(\mathrm{O}(t^N)\big)^{(j)} = \mathrm{O}(t^{N-j}),\ t \to 0,$$

the value of $\big(g_i(f_1(t), \ldots, f_n(t))\big)^{(j)}$ at $t = 0$ is zero. This proves the lemma. ■

Lemma 11. Let d be a positive integer and $P(x,y) \in \mathbb{C}[x,y]$ be a polynomial of degree at most d. If

$$P(t,e^t) = \mathrm{O}(t^{B+1}),\ t \to 0,\ \text{where } B = \binom{d+2}{2} - 1,$$

then $P(t,e^t) = 0$, and so P is the zero polynomial.

Proof. The function $P(t,e^t)$ is a $\mathbb{C}$-linear combination of $\{t^i e^j \mid 0 \leqslant i+j \leqslant d\}$. All these functions are annihilated by the following differential operator

$$D := \left(\tfrac{\partial}{\partial t}\right)^{d+1} \left(\tfrac{\partial}{\partial t} - 1\right)^{d} \left(\tfrac{\partial}{\partial t} - 2\right)^{d-1} \cdot \ldots \cdot \left(\tfrac{\partial}{\partial t} - d\right)$$

of order $B+1$ with constant coefficients, so $D(P(t,e^t)) = 0$. Every solution of D is uniquely determined by its first $B+1$ Taylor coefficients and 0 is a solution of D, so $P(t,e^t) = 0$. ■

Proof. (Proof of Proposition 1) We will show that

$$1 \in \left\langle x' - 1, y' - y, P(x,y) \right\rangle^{(\infty)} \tag{22}$$

holds for every $P(x,y) \in \mathbb{C}[x,y]$ such that $P(x,0) \neq 0$. Since system (22) has constant coefficients, it is consistent if and only if it has a solution in $\mathbb{C}[\![t]\!]$ (follows from [44, Proposition 3.2 and Corollary 3.6]). Every solution of $x' = 1,\ y' = y$ in $\mathbb{C}[\![t]\!]$ is of the form $x(t) = t + a,\ y = be^t$ for some $a, b \in \mathbb{C}$. If $b \neq 0$, then $P(x(t), y(t)) \neq 0$ due to the algebraic independence of t and e^t over $\mathbb{C}$. If $b = 0$, then $x(t)$ is a root of the non-zero polynomial $P(x,0)$ with constant coefficients. This is impossible.

For $0 \leqslant i+j \leqslant d$, let $f_{i,j} \in \mathbb{Q}[t]$ be the truncation of the power series $t^i \cdot e^{jt}$ to the degree B. If the polynomials $\{f_{i,j} \mid 0 \leqslant i+j \leqslant d\}$ were linearly dependent over $\mathbb{Q}$, there would exist $\lambda_{i,j} \in \mathbb{Q}$ not all zeros for $0 \leqslant i+j \leqslant d$ such that

$$f := \sum_{0 \leqslant i+j \leqslant d} \lambda_{i,j} t^i e^{jt} = \mathrm{O}(t^{B+1}),\ \ t \to 0.$$

The power series f is non-zero due to the algebraic independence of t and e^t. On the other hand, Lemma 11 implies that $f = 0$. The obtained contradiction implies that $\{f_{i,j} \mid 0 \leqslant i+j \leqslant d\}$ are linearly independent over $\mathbb{Q}$.

Since there are $B+1$ of the $f_{i,j}$, they form a basis of the $\mathbb{Q}$-vector space of polynomials of degree at most B. Thus, there exist $\mu_{i,j} \in \mathbb{Q}$ for $0 \leqslant i+j \leqslant d$ such that

$$g(t) := \sum_{0 \leqslant i+j \leqslant d} \mu_{i,j} t^i e^{jt} = t^B + \mathrm{O}(t^{B+1}), \quad t \to 0.$$

We define

$$P(x,y) := \sum_{0 \leqslant i+j \leqslant d} \mu_{i,j} x^i y^j.$$

We claim that $P(x,y)$ is irreducible. Assume the contrary, so $P(x,y) = P_1(x,y)P_2(x,y)$, where $\deg P_1 = d_1 \geqslant 1$ and $\deg P_2 = d_2 \geqslant 1$. Then there exist integers B_1 and B_2 such that $B_1 + B_2 = B$ and

$$P_i(t, e^t) = t^{B_i} + \mathrm{O}(t^{B_i+1}), \ t \to 0 \ \text{ for} i = 1, 2.$$

Since

$$B = \tfrac{(d+3)d}{2} > \tfrac{(d_1+3)d_1}{2} + \tfrac{(d_2+3)d_2}{2},$$

we have $B_i > \frac{(d_i+3)d_i}{2}$ for some i, say for $i = 1$. Then Lemma 11 applied to polynomial P_1 of degree d_1 implies that $P_1(t, e^t) = 0$. The obtained contradiction proves that $P(x,y)$ is irreducible.

Since $P(x,y)$ is irreducible, $P(x,0)$ is not zero. This implies that $x' - 1 = y' - y = P(x,y) = 0$ is inconsistent. Lemma 10 applied to

$$g_1 = x' - 1, \ g_2 = y' - y, \ g_3 = P(x,y), \ f_1(t) = t, \ f_2(t) = e^t, \ \text{and } N = B$$

implies

$$1 \notin \left\langle x' - 1, y' - y, P(x,y) \right\rangle^{(B-1)}.$$

■

Example 5. Based on the proof of Proposition 1, one can generate polynomial P using only linear algebra. For example, for $d = 2$, we obtain

$$P(x,y) = -2x^2 - 8xy + y^2 - 10x + 16y - 17.$$

Corollary 3. The bound in Theorem 2 is asymptotically tight for $m \leqslant 1$.

Proof. Let $I = \langle x' - 1, y' - y, P(x, y)\rangle$. We have

$$A := \mathbb{C}[x, y, x', y']/I \cong \mathbb{C}[x, y]/\langle P(x, y)\rangle.$$

Since P is irreducible, A is an integral domain, and so the ideal I is prime and, therefore, radical. Finally, $m = \dim(F) = 1$ and $D_1 = \deg I = \deg P$, and we have

$$D_1^2 + 1 \leqslant 2 \cdot \tfrac{D_1(D_1+3)}{2}.$$

For $m = 0$, one can take the system $x = 0$, $x' - 1 = 0$. Then $1 \in \langle x, x' - 1\rangle^{(1)}$ and $1 \notin \langle x, x' - 1\rangle$. ■

5 Dominance of projections of affine varieties and elimination in DAEs

In this section, we will address the problem of verifying whether the projection of an affine variety to an affine subspace is Zariski dense by analyzing the fibers of the projection. We will then connect this with an algorithm that verifies whether it is possible to eliminate a set of unknowns

- in a system of polynomial equations (see Section 5.1) and
- as a consequence of our main result, in a system of DAEs (see Section 5.2).

5.1 Dominance of projections of affine varieties

The possibility of elimination of a subset of unknowns for polynomial systems is equivalent to the dominance of the corresponding projection of affine varieties. Verifying whether the projection of an affine variety to an affine subspace is Zariski dense can be done by, for example, calculating Gröbner bases with respect to elimination monomial orderings. However, this could be very time-consuming. One can try the following naive approach:

- Consider the affine variety

$$xy - 1 = 0,$$

whose projection to the y-line is dominant. What if we consider the fiber of the projection over, say, $y = a$? Note that $xa - 1 = 0$ defines a non-empty variety if and only if $a \neq 0$.

- Consider the affine variety

$$x + y = 0, \quad x = 0,$$

whose projection to the y-plane is the point $\{0\}$, and so is not dominant. What if we again consider the fiber over $y = a$? In this case, $x + a = 0, x = 0$ defines an empty variety if and only if $a \neq 0$.

What we see in each of the above examples that, for all $a \neq 0$,

$$\text{the projection to the } y\text{-line is } \textit{dominant} \iff \text{the fiber over } a \text{ of the projection is } \textit{non-empty}. \tag{23}$$

Hence, for every field k and every finite subset $S \subset k$,

$$|\{a \in S \mid (23) \text{ holds}\}| \geqslant |S| - 1.$$

We will now show how to generalize this idea to arbitrary affine varieties bounding the size of the exceptional set of points $\boldsymbol{a}$ in a finite grid in $\mathbb{A}^r$ for which the dominance of a projection of an affine variety to $\mathbb{A}^r$ is not equivalent to the emptiness of the fiber over $\boldsymbol{a}$.

Proposition 5. For every

- affine variety $X \subset \mathbb{A}^q \times \mathbb{A}^r$ and
- finite subset $S \subset k$,

the number of points $\boldsymbol{a} = (a_1, \ldots, a_r) \in S^r \subset \mathbb{A}^r$ such that

$$\text{the projection of } X \text{ to } \mathbb{A}^r \text{ is dominant} \iff \text{the fiber over } \boldsymbol{a} \text{ of the projection is non-empty}$$

is at least

$$N := \left(1 - \frac{\deg X}{|S|}\right) \cdot |S|^r.$$

Proof. Let $\pi : \mathbb{A}^q \times \mathbb{A}^r \to \mathbb{A}^r$ be the projection. Assume that $\overline{\pi(X)} \neq \mathbb{A}^r$. [23, Lemma 2] implies that $\deg \overline{\pi(X)} \leqslant \deg X$, so there exists a polynomial $P_1 \in k[y_1, \ldots, y_r]$ of degree at most $\deg X$ [23, Proposition 3] such that $\overline{\pi(X)} \subset V(P_1)$. Thus,

$$P_1(\boldsymbol{a}) \neq 0 \implies \pi^{-1}(\boldsymbol{a}) \cap X = \varnothing.$$

Due to the Demillo–Lipton–Schwartz–Zippel lemma (see [54, Proposition 98]), $P_1(\boldsymbol{a}) \neq 0$ for at least

$$\left(1 - \frac{\deg P_1}{|S|}\right) \cdot |S|^r \geqslant N$$

many points $\boldsymbol{a} \in S^r$. Assume that $\overline{\pi(X)} = \mathbb{A}^r$. Then there exists an irreducible component $Z \subset X$ such that $\overline{\pi(Z)} = \mathbb{A}^r$. [25, Lemma 4.4] implies that there exists a proper subvariety $Y \subset \mathbb{A}^r$ such that

- $\deg Y \leqslant \deg Z$;
- for every $p \in \mathbb{A}^r \setminus Y$, $\pi^{-1}(p) \cap Z \neq \varnothing$.

Then there exists a polynomial $P_2 \in k[y_1, \ldots, y_r]$ with $\deg P_2 \leqslant \deg Y$ [23, Proposition 3] such that

$$P_2(\boldsymbol{a}) \neq 0 \implies \boldsymbol{a} \notin Y \implies \pi^{-1}(\boldsymbol{a}) \cap Z \neq \varnothing \implies \pi^{-1}(\boldsymbol{a}) \cap X \neq \varnothing.$$

Due to [54, Proposition 98] again, $P_2(\boldsymbol{a}) \neq 0$ for at least

$$\left(1 - \frac{\deg P_1}{|S|}\right) \cdot |S|^r \geqslant N$$

many points $\boldsymbol{a} \in S^r$. ■

5.2 Connection to elimination of unknowns in polynomial systems and in DAEs

By the Bézout theorem, Proposition 5 can be restated as follows.

Proposition 6. Let

- $f_1, \ldots, f_\ell \subset k[x_1, \ldots, x_q, y_1, \ldots, y_r]$ be polynomials, $\deg f_i \leqslant d$,
- $0 < p < 1$ be a real number,
- $S \subset k$ with $|S| = \left\lceil \frac{d^{q+r}}{1-p} \right\rceil$,

- $a_1, \dots, a_r$ be elements randomly, independently, and uniformly sampled from S, and
- $g_i := f_i|_{y_1=a_1,\dots,y_r=a_r}$, $1 \leqslant i \leqslant \ell$.

Then

$$\langle f_1, \dots, f_\ell \rangle \cap k[y_1, \dots, y_r] \neq \{0\} \iff 1 \in \langle g_1, \dots, g_\ell \rangle$$

with probability at least p.

Proof. By [29,Lemma 3], there exist $h_1, \dots, h_{q+r}$, linear combinations of $f_1, \dots, f_\ell$, such that $X := V(h_1, \dots, h_{q+r})$ and $Y := V(f_1, \dots, f_\ell)$ have the same prime components of dimension > 1. Thus, $\deg Y \leqslant \deg X$ and the Bézout inequality implies that $\deg X \leqslant d^{q+r}$. The proposition follows from Proposition 5 applied to the variety Y. ■

As a direct consequence, we obtain a Monte Carlo algorithm that verifies if an elimination of unknowns in a system of polynomial equations is possible with probability at least p. A deterministic algorithm based on similar geometric considerations was designed in [46]. Since degrees of polynomials do not increase under differentiation, using our main result (see Section 2.2), this can be used in a (deterministic or randomized) elimination algorithm for DAEs by

- calculating the data from the appropriate statements of the main results and then
- iterating differentiation and (deterministic or randomized) polynomial elimination successively until either an elimination is discovered or the bound from the appropriate main result is reached.

Our implementation of a randomized version as well as of a deterministic version is available at https://github.com/pogudingleb/DifferentialElimination.git.

Acknowledgments

The authors are grateful to S. Gorchinskiy, H. Hong, R. Hoobler, T. Scanlon, M.F. Singer, and referees for their suggestions. This work was partially supported by the National Science Foundations [CCF-0952591, CCF-1563942, DMS-1606334, DMS-1760448, DMS-1853650, DMS-1853482]; the National Security Agency [grant #H98230-15-1-0245]; City University of New York [CIRG #2248; PSC-CUNY #69827-00 47, 60098-00 48], the Austrian Science Fund FWF [Y464-N18]; and the strategic program "Innovatives OÖ 2020" by the Upper Austrian Government.

References

[1] Bernardi, O. and M. Bousquet-Mélou. "Counting coloured planar maps: differential equations." *Comm. Math. Phys.* 354, no. 1 (2017): 31–84. doi: 10.1007/s00220-017-2906-x.

[2] Binyamini, G. "Bezout-type theorems for differential fields." *Compositio Math.* 153, no. 4 (2017): 867–88. doi: 10.1112/S0010437X17007035.

[3] Boulier, F. "Differential Elimination and Biological Modelling." In *Grobner Bases in Symbolic Analysis*, vol. 2, 109–37, 2007.

[4] Boulier, F., F. Ollivier, D. Lazard, and M. Petitot. "Computing representations for radicals of finitely generated differential ideals." *Appl. Algebra Engrg. Comm. Comput.* 20, no. 1 (2009): 73–121. doi: 10.1007/s00200-009-0091-7.

[5] Bourbaki, N. *Algebra II. Chapters 4–7. Elements of Mathematics*. Berlin: Springer, 1990. doi: 10.1007/978-3-642-61698-3.

[6] Bürgisser, P., P. Clausen, and A. Shokrollahi. *Algebraic Complexity Theory*. Springer, 1997. doi: 10.1007/978-3-662-03338-8.

[7] Cayley, A. "On the Theory of Involution in Geometry." In *Cambridge and Dublin Mathematical Journal*, vol. II, 52–61, 1847.

[8] Cayley, A. "On the Theory of Elimination." In *Cambridge and Dublin Mathematical Journal*, vol III, 116–20 1848.

[9] Cruz-Victoria, J. C., R. Martínez-Guerra, and J. J. Rincón-Pasaye. "On nonlinear systems diagnosis using differential and algebraic methods." *J. Franklin Inst.* 345 (2008): 102–18. doi: 10.1016/j.jfranklin.2007.07.001.

[10] D'Alfonso, L., G. Jeronimo, and P. Solernó. "Effective differential Nullstellensatz for ordinary DAE systems with constant coefficients." *J. Complexity* 30, no. 5 (2014): 588–603. doi: 10.1016/j.jco.2014.01.001.

[11] Diop, S. "A State Elimination Procedure for Nonlinear Systems." In *New trends in Nonlinear Control Theory*, 190–8. Springer, 1989. doi: 10.1007/BFb0043028.

[12] Diop, S. "Elimination in control theory." *Math. Control Signals Systems* 4, no. 1 (1991): 17–32.

[13] Freitag, J. and O. León Sánchez. "Effective uniform bounds in partial differential fields." *Adv. Math.* 288 (2016): 308–36. doi: 10.1016/j.aim.2015.10.013.

[14] Freitag, J. and T. Scanlon. "Strong minimality and the j-function." *J. Eur. Math. Soc. (JEMS)* 20, no. 1 (2018): 119–36. doi: 10.4171/JEMS/761.

[15] Gao, X. S., W. Li, and C. M. Yuan. "Intersection theory in differential algebraic geometry: generic intersections and the differential chow form." *Trans. Amer. Math. Soc.* 365 (2013): 4575–632. doi: 10.1090/S0002-9947-2013-05633-4.

[16] Gear, C. and L. Petzold. "ODE methods for the solution of differential/algebraic systems." *SIAM J. Numer. Anal.* 21, no. 4 (1984): 716–28. doi: 10.1137/0721048.

[17] Golubitsky, O., M. Kondratieva, A. Ovchinnikov, and A. Szanto. "A bound for orders in differential Nullstellensatz." *J. Algebra* 322, no. 11 (2009): 3852–77. doi: 10.1016/j.jalgebra.2009.05.032.

[18] Goward, R. and K. Smith. "The jet scheme of a monomial scheme." *Comm. Algebra* 34, no. 5 (2006): 1591–8. doi: 10.1080/00927870500454927.

[19] Grigoriev, D. "Complexity of quantifier elimination in the theory of ordinary differential equations." *Lect. Notes Comput. Sci.* 378 (1989): 11–25. doi: 10.1007/3-540-51517-8_81.

[20] Gustavson, R., M. Kondratieva, and A. Ovchinnikov. "New effective differential Nullstellensatz." *Adv. Math.* 290 (2016): 1138–58. doi: 10.1016/j.aim.2015.12.021.

[21] Harrington, H. A., K. L. Ho, and N. Meshkat. "A parameter-free model comparison test using differential algebra." *Complexity* (2019). doi: 10.1155/2019/6041981.

[22] Hartshorne, R. *Algebraic Geometry In Number 52 in Graduate Texts in Mathematics*. Springer, 1977. doi: 10.1007/978-1-4757-3849-0.

[23] Heintz, J. "Definability and fast quantifier elimination in algebraically closed fields." *Theoret. Comput. Sci.* 24, no. 3 (1983): 239–77. doi: 10.1016/0304-3975(83)90002-6.

[24] Hong, H., A. Ovchinnikov, G. Pogudin, and C. Yap. "SIAN: software for structural identifiability analysis of ODE models." *Bioinformatics* 35, no. 16 (2019): 2873–4. doi: 10.1093/bioinformatics/bty1069.

[25] Hong, H., A. Ovchinnikov, G. Pogudin, and C. Yap. "Global identifiability of differential models." *Comm. Pure Appl. Math.* 73, no. 9 (2020): 1831–1879. doi: 10.1002/cpa.21921.

[26] Hrushovski, E. and A. Pillay. "Effective bounds for the number of transcendental points on subvarieties of semi-abelian varieties." *Am. J. Math.* 122, no. 3 (2000): 439–50. doi: 10.1353/ajm.2000.0020.

[27] Hubert, E. "Factorization-free decomposition algorithms in differential algebra." *J. Symbolic Comput.* 29, no. 4–5 (2000): 641–62. doi: 10.1006/jsco.1999.0344.

[28] Jelonek, Z. "On the effective Nullstellensatz." *Invent. Math.* 162, no. 1 (2005): 1–17. doi: 10.1007/s00222-004-0434-8.

[29] Jeronimo, G. and J. Sabia. "Effective equidimensional decomposition of affine varieties." *J. Pure Appl. Algebra* 169, no. 2 (2002): 229–48. doi: 10.1016/S0022-4049(01)00083-4.

[30] Jiafan, Z. "Nonlinear Systems Fault Diagnosis with Differential Elimination." In *2009 International Conference on Computational Intelligence and Natural Computing*, vol. 2, 186–9, 2009. doi: 10.1109/CINC.2009.38.

[31] Kolchin, E. *Differential Algebra and Algebraic Groups*. New York: Academic Press, 1973.

[32] Kunkel, P. and V. Mehrmann. *Differential-Algebraic Equations: Analysis and Numerical Solution*. European Mathematical Society, 2006.

[33] Li, W. and C. M. Yuan. "Elimination theory in differential and difference algebra." *J. Syst. Sci. Complex.* 32, no. 1 (2019): 287–316. doi: 10.1007/s11424-019-8367-x.

[34] Li, W., C. M. Yuan, and X. S. Gao. "Sparse differential resultant for Laurent differential polynomials." *Found. Comput. Math.* 15, no. 2 (2015): 451–517. doi: 10.1007/s10208-015-9249-9.

[35] Ljung, L. and T. Glad. "On global identifiability for arbitrary model parametrizations." *Automatica J. IFAC* 30, no. 2 (1994): 265–76. doi: 10.1016/0005-1098(94)90029-9.

[36] Macaulay, F. S. *The Algebraic Theory of Modular Systems*. Cambridge University Press, 1916.

[37] Marker, D. "Model theory of differential fields." In *Model Theory of Fields*, 38–113. Berlin: Springer, 1996. http://projecteuclid.org/euclid.lnl/1235423156.

[38] Meshkat, N., Z. Rosen, and S. Sullivant. "Algebraic Tools for the Analysis of State Space Models." In *The 50th Anniversary of Gröbner Bases*, 171–205, Tokyo, Japan, 2018. doi: 10.2969/aspm/07710171.

[39] Ollivier, F. "Le problème de l'identifiabilité structurelle globale: approche théorique, méthodes effectives et bornes de complexité." PhD thesis, Ecole Polytechnique, 1990.

[40] Ovchinnikov, A., A. Pillay, G. Pogudin, and T. Scanlon. "Computing all identifiable functions for ODE models." 2020. https://arxiv.org/abs/2004.07774.

[41] Ovchinnikov, A., G. Pogudin, and P. Thompson. "Input-output equations and identifiability of linear ODE models." 2020. https://arxiv.org/abs/1910.03960.

[42] Ovchinnikov, A., G. Pogudin, and P. Thompson. "Parameter identifiability and input-output equations." Appl. Algebra Engrg. Comm. Comput. (forthcoming). doi: 10.1007/s00200-021-00486-8.

[43] Pierce, D. "Fields with several commuting derivations." *J. Symb. Log.* 79, no. 1 (2014): 1–19.

[44] Pogudin, G. "A differential analog of the Noether normalization lemma." *Int. Math. Res. Not. IMRN* 2018, no. 4 (2018a): 1177–99. doi: 10.1093/imrn/rnw275.

[45] Pogudin, G. "Products of ideals and jet schemes." *J. Algebra* 502 (2018b): 61–78. doi: 10.1016/j.jalgebra.2018.01.027.

[46] Recio, T., R. Sendra, and C. Villarino. "The Importance of Being Zero." In *Proceedings of the ACM on 2018 International Symposium on Symbolic and Algebraic Computation*, 327–33, 2018. doi: 10.1145/3208976.3208981.

[47] Ritt, J. F. *Differential Equations from the Algebraic Standpoint*. Colloquium Publications. American Mathematical Society, 1932.

[48] Rueda, S. "Linear sparse differential resultant formulas." *Linear Algebra Appl.* 438, no. 11 (2013): 4296–321. doi: 10.1016/j.laa.2013.01.016.

[49] Rueda, S. and R. Sendra. "Linear complete differential resultants and the implicitization of linear DPPEs." *J. Symbolic Comput.* 45 (2010): 324–41. doi: 10.1016/j.jsc.2009.09.003.

[50] Saccomani, M., S. Audoly, and L. D'Angió. "Parameter identifiability of nonlinear systems: the role of initial conditions." Automatica, 39: 619–632, 2003. doi: 10.1016/S0005-1098(02)00302-3.

[51] Seidenberg, A. "An elimination theory for differential algebra." University of California publications in Mathematics III, no. 2 (1956): 31–66.

[52] Shafarevich, I. *Basic Algebraic Geometry 1*. University Lecture Series. Springer, 2013. doi: 10.1007/978-3-642-37956-7.

[53] Towsner, H. and W. Simmons. "Proof mining and effective bounds in differential polynomial rings." *Adv. Math.* 343 (2019): 567–623. doi: 10.1016/j.aim.2018.11.026.

[54] Zippel, R. *Effective Polynomial Computation*. Springer, 1993. doi: 10.1007/978-1-4615-3188-3.