Counting Solutions of Differential Equations

Von der Fakultät für Mathematik, Informatik und Naturwissenschaften
der RWTH Aachen University zur Erlangung des akademischen Grades
eines Doktors der Naturwissenschaften genehmigte Dissertation

vorgelegt von

Diplom-Computermathematiker

Markus Lange-Hegermann

aus Bottrop

Berichter: Universitätsprofessor Dr. Wilhelm Plesken
Universitätsprofessorin Dr. Julia Hartmann

Tag der mündlichen Prüfung: 17.01.2014

Contents

Introduction

> Newton's fundamental discovery, the one which he considered necessary to keep secret and published only in the form of an anagram, consists of the following: *Data aequatione quotcunque fluentes quantitae involvente fluxions invenire et vice versa.* In contemporary mathematical language, this means: "It is useful to solve differential equations".
>
> Vladimir Arnold
> in [Arn88]

Abstract. The aim of this thesis is a quantitative analysis of the set of solutions of a system of differential equations. For this aim, this thesis generalizes the differential dimension polynomial, and thereby makes it more accessible for algorithms. Furthermore, this thesis introduces the counting sequence and the differential counting polynomial to give a more detailed description of the size of the solution set of a system of differential equations. The Thomas decomposition algorithm, which is implemented as part of this thesis, is the algorithmic foundation for these descriptions of the size of solution sets. This algorithm partitions the solution set into solution sets of simple differential systems, and it allows to compute certain consequences of differential systems, independent of counting.

Motivation. Differential equations are ubiquitous when modeling continuously varying quantities, for example in physics, chemistry, biology, engineering, and economics. Solving systems of differential equations is important for simulations and other applications.

Systems of differential equations are notoriously hard to solve. Many systems of differential equations do not admit closed form solutions in "elementary" functions and hence cannot be solved symbolically. Despite this, increasingly good heuristics are implemented in computer algebra systems to find solutions [CTvB95, CTR08]. Given such a set of closed form solutions returned by a computer algebra system, the question remains whether this set is the *complete solution set* (cf. Examples 1.78, 2.67, 2.91, 2.92, and 2.94). With the notions of the size of solution sets given in this thesis, one can decide whether the solutions found by a heuristical solver form a proper subset of the set of all solutions.

Solutions of Differential Equations. This thesis concentrates on formal *power series* to avoid the following complications. For a formally consistent system of differential equations, formal power series solutions exist for any given suitable initial data (cf. Theorem 1.52); this is in contrast to smooth solutions, which do not exist in general for smooth initial data (cf. LEWY's counterexample [Lew57]). Formal power series can satisfactorily be described symbolically on a computer, which seems impossible for smooth or weak functions, as numerical methods only approximate them.

The Differential Dimension Polynomial. There exist several well-known measures in the literature that describe the size of the solution set of a system of differential equations. Subsection 1.6.4 recapitulates the CARTAN characters and the index of generality [CE79, CARTAN, 3.12.1929, Appendix III] [Car31], EINSTEIN's strength [Ein53a], the differential type, the differential dimension, the typical dimension, and the number of free functions. All these measures have a drawback: one can easily find two systems S_1 and S_2 of differential equations such that the solution set of S_1 is a proper subset of the solution set of S_2, but these two solution sets have identical measures (cf. Example 1.87). Thus, these measures cannot detect whether a set returned by a heuristical solver of differential equations contains the difference of the solution sets of S_2 and S_1.

KOLCHIN realized this problem and introduced the differential dimension polynomial as *finer measure* of the solution set of a system of differential equations given by a prime differential ideal [Kol64]. The differential dimension polynomial describes for any order the number of free power series coefficients up to that order, in the sense that generically these coefficients can be chosen arbitrarily. In particular, this polynomial carries enough information to reliably answer the question whether two full solution sets of differential prime ideals included in each other are equal. Additionally, in the case of prime ideals it determines all other mentioned measures of the size of solution sets. Even though it is in principle possible to decompose a set of differential equations into differential prime ideals, it is expensive in practice (cf. [Hub00], [BLOP09, §6.2]). Thus, there is a lack of practical methods which decide whether a subset of the solution set of differential equations is proper.

The first chapter of this thesis solves this problem for greater generality than full solution sets of prime differential ideals. It generalizes the differential dimension polynomial and its properties from prime ideals to ideals associated to simple differential systems (cf. Theorem 1.74). Decomposing a differential ideal into those is easier in practice than a decomposition into prime differential ideals. Most common differential systems can sufficiently be described by this generalization of the differential dimension polynomial (cf. Example 1.78).

Simple Systems and the THOMAS Decomposition. Simple differential systems are finite sets of differential equations and inequations with certain additional properties, which make them well-behaved (cf. Definition 1.14). The purpose of the differential inequations is to ensure these properties by guaranteeing that certain terms are non-zero. One of the properties of simple differential systems is passivity. The passivity condition builds on a calculus developed by JANET, which organizes the set of power series coefficients, and ensures that all *differential consequences* are obvious from the system (cf. Subsection 1.2.3). For a simple differential system this approach allows to read off the differential dimension polynomial as a closed formula (cf. Remark 1.77). Simplicity generically ensures that the requirements of RIQUIER's Existence Theorem 1.60 are met and, thus, simplicity generically implies local convergence of formal power series solutions.

The THOMAS Decomposition is the algorithmic keystone in this thesis. It transforms a system of differential equations and inequations into a set of simple differential systems by symbolic manipulation. The most important idea of the THOMAS decomposition is to use case distinctions to ensure the desirable properties of simple systems; this means that a system S is replaced by two *disjoint* systems $S \cup \{p \neq 0\}$ and $S \cup \{p = 0\}$

for some differential expression p. This disjointness distinguishes the Thomas decomposition from other algorithms. The Thomas decomposition has been implemented by the author (cf. Subsection 1.3.7, [BGLHR12, BLH12]). Experiments and examples computed with the software were a major inspiration for the results of this thesis.

The ideas of the Thomas decomposition go back to Riquier [Riq93] and Tresse[1] [Tre94], who were motivated to find and describe all analytic solutions of a set of differential equations. Janet made their ideas algorithmic for the case of linear differential equations and in doing so introduced his calculus [Jan21, Jan29]. Thomas, the eponym of the decomposition, generalized the theory to the nonlinear case [Tho37, Tho40, Tho62]. His ideas were largely ignored and only recently resurfaced [Wan98, Ger08]. In the meantime, Ritt developed the theory of characteristic sets [Rit50], which was extended by Seidenberg [Sei56] and Rosenfeld [Ros59]. Building on this work, the Rosenfeld-Gröbner algorithm by Boulier and coauthors [BLOP95, BLOP09] allowed decompositions of differential ideals; it is implemented by Boulier and Hubert. These algorithms are well-suited for certain problems, but the lack of disjointness complicates their application for detailed descriptions of solution sets.

Other Applications of the Thomas Decomposition. A Thomas decomposition of a system S of differential equations and inequations is of interest independent of the differential dimension polynomial. For example, it decides inconsistency of S, and it decides whether a given differential equation is implied by S using reduction (cf. Proposition 1.66). Furthermore, as all differential consequences are obvious in simple differential systems, these systems seem better suited as input for symbolic solvers (cf. Example 1.1). Another important application of the Thomas decomposition is differential elimination. This is a computational tool which produces differential consequences of a desired form, for example all differential equations only involving certain functions.

The Thomas decomposition sets itself apart from these other algorithms because it is both disjoint and does not compute the closure of the solution sets. These two properties of the Thomas decomposition are fundamental to the examples treated in Appendix A, which covers elimination. This appendix compares the laws of planetary motion of Kepler with those of Newton in detail and studies system theoretic properties of dynamical systems. In particular, for parametric dynamical systems the disjointness of the Thomas decomposition partitions the parameters, reflecting the behavior of the systems.

Genericity Conditions. The differential dimension polynomial does not describe the solution sets of systems of differential equations in adequate detail, as it assumes three different genericity conditions.

First, formal power series solutions show different behavior at different *centers of expansion* (cf. Example 1.50); simple differential systems only describe the generic behavior. The differential dimension polynomial only measures the number of free power series coefficients at a generic center of expansion. To make a virtue of necessity, this thesis introduces the set of non-centered power series as admissible solutions. These non-centered solutions have the advantage that the algorithms work without choosing the center of expansion and the choice of this center can be postponed (cf. Subsection 1.4.2). Furthermore, the non-centered solutions admit a Nullstellensatz (cf. Theorem 1.65) and, in contrast to universal differential fields, are suitable for algorithms.

The second genericity condition concerns *differential inequations*. These inequations are inserted into systems during a Thomas decomposition. A differential inequation

[1] According to [BC99], his results are wrong. Nevertheless, many of his ideas are quite helpful.

implies for a power series ansatz that one of the power series coefficients is non-zero, but it is unclear which coefficient (cf. Remark 1.49). To add insult to injury, the existence (and local convergence) is only clear for solutions that satisfy a certain genericity condition (cf. Lemma 1.47, Theorem 1.52, and Theorem 1.60).

Third, the dimension polynomial can not describe the size of the solution set of an arbitrary system, but it is restricted to describing the solution set of a differential ideal associated to a simple differential system. Additionally, the description of components with different differential dimension polynomials appears not to be *combinable*, as the associated primes of these ideals show the same generic behavior (cf. Proposition D.1, for example they all have the same differential dimension polynomial). This prevents a comparison of non-simple systems of differential equations using this ansatz.

These assumptions on genericity are a major obstacle to understand differential equations. The main goal of the second chapter of this thesis is to give a more *detailed, non-generic* description of a solution set of a system of differential equations. Therefore, it introduces the counting sequence and the differential counting polynomial, which avoid these three problems with genericity and generalize the differential dimension polynomial.

The Algebraic Counting Polynomial. The idea of the counting sequence and the differential counting polynomial is based on the algebraic counting polynomial (cf. [Ple09a, Ple09b] and Section 2.2).

The algebraic counting polynomial is an element $c(V) \in \mathbb{Z}[\infty]$ that describes the "size" of a constructible set V (i.e., given by polynomial equations and inequations) in affine n-space. Here, ∞ is a free indeterminate, which can be thought of as representing the cardinality of the algebraic closure of the base field. In that sense, the algebraic counting polynomial can "count" infinite sets, for example the counting polynomial of an affine i-space is $\infty^i \in \mathbb{Z}[\infty]$, and if V is a j-fold unramified cover of W, then $c(V) = j \cdot c(W) \in \mathbb{Z}[\infty]$.

Similarly to simple differential systems, there exist simple algebraic systems. The solution sets of simple algebraic systems form well-behaved covers (cf. Subsection 1.2.1), and the counting polynomial of the solution set of a simple algebraic system can be read off the degrees and orders of the equations and inequations in the system. An algebraic version of the THOMAS decomposition computes the algebraic counting polynomials of a constructible set, as the algebraic counting polynomial is additive with respect to disjoint decompositions and the THOMAS decomposition algorithm can also decompose an algebraic system into disjoint simple algebraic systems.

The most important property of the algebraic counting polynomial with regard to the description of solution sets of systems of differential equations is that two constructible sets $V \subseteq W$ included in each other are equal if and only if their algebraic counting polynomials $c(V)$ and $c(W)$ coincide (cf. Proposition 2.10 for the algebraic case and Theorem 2.34 for the differential case). Furthermore, the algebraic counting polynomial generalizes the dimension of a constructible set, as the dimension of a constructible set V is the degree of its algebraic counting polynomial $c(V)$ (cf. Proposition 2.23).

The Counting Sequence and the Differential Counting Polynomial The counting sequence and the differential counting polynomial combine the ideas of the differential dimension polynomial and the algebraic counting polynomial to give a more detailed overview over the size of the solution set of a system of differential equations. They generalize the differential dimension polynomial in the same sense as the algebraic counting polynomial generalizes the dimension (cf. Theorem 2.36). In particular, they also generalize all above-mentioned measures of the size of the solution set of a system of differential equations, like the CARTAN characters.

The counting sequence is the sequence of algebraic counting polynomials indexed by the order $\ell \in \mathbb{Z}_{\geq 0}$, which count the different TAYLOR polynomials of degree ℓ. These algebraic counting polynomials indexed by the order ℓ are called ℓ-th differential counting polynomials. If there exists a closed form polynomial that ultimately describes the ℓ-th differential counting polynomials, then this closed form is called the differential counting polynomial (cf. Definition 2.33).

Computing the counting sequence and the differential counting polynomial is hard. One would hope that it can be read off the degrees of equations and inequations, similarly to the algebraic case. However, as differential inequations have the above mentioned genericity restrictions, we need another means to ensure that terms are non-zero. Thus, we use polynomial inequations for power series coefficients; disjoint splittings necessitate complementary equations for power series coefficients. Section 2.3 introduces systems involving not only differential equations but also equations and inequations for power series coefficients. These systems provide the background for describing counting sequences and differential counting polynomials.

The definition of the counting sequence and the differential counting polynomial then depends on turning a system of differential equations into algebraic systems which only involve constraints for power series coefficients. Theorem 2.32 shows that this is possible in principle, but countably infinitely many systems might be needed, and these might involve countably infinitely many inequations. Thus, the problem of defining the counting sequence reduces to the problem of defining the algebraic counting polynomial for certain infinite algebraic systems (cf. Subsection 2.2.3). However, though unsolved in general, this problem turns out to be easy for all systems of differential equations encountered by the author. These infinite sets of inequations are necessary, e.g., in Example 2.93. In particular, the counting sequence is not a sequence of polynomials in $\mathbb{Z}[\infty]$ but needs an additional indeterminate $\aleph_0$ to describe countably infinite sets. The VESSIOT theory explains these countable infinite sets geometrically (cf. Appendix E).

Computation of the Differential Counting Polynomial. Determining the differential counting polynomial is not algorithmic. This is to be expected, as even in the case of a single inhomogeneous linear differential equation the problem of the existence of formal power series solutions can be reduced to HILBERT's tenth problem about DIOPHANTINE equations, which is known to be unsolvable (cf. [DL84] and Subsection 2.5.5). In particular, no general computational theory for formal power series solutions of systems of differential equations can exist. (Similar non-computability results hold for smooth solutions [PER81].) Still it makes sense to study the counting sequence and the differential counting polynomial in examples, as they provide a good description of the size of the solution set of a differential system.

These noncomputability results imply that at best one can hope for a collection of methods to compute the counting sequence and the differential counting polynomial of many important classes of systems of differential equations. Section 2.5 describes such methods and uses them to consider two big classes of interesting systems of differential equations. The first class consists of simple differential systems that do not involve inequations (cf. Theorem 2.72). This class contains all linear systems of differential equations and most common semilinear systems of differential equations. The second class contains first order ordinary differential equations of main degree one (cf. Theorem 2.79). The proofs for these classes are again given using non-centered solutions; Subsection 2.5.4 then describes the transfer to formal and convergent power series solutions.

The counting sequence and the differential counting polynomial solve the three genericity problems of the differential dimension polynomial. First, one can choose the center of expansion, but also keep it generic (cf. Example 2.3). Second, differential inequations are not needed for defining or computing the differential counting polynomial. Third, the counting sequence and the differential counting polynomial are *additive* with respect to disjoint decompositions; hence, in contrast to the differential dimension polynomial, it can describe and compare non-simple systems of differential equations.

Most important for applications, the counting sequence and the differential counting polynomial can decide whether an inclusion of two solutions sets is proper under suitable conditions: the case without countably infinite exceptional sets is tantamount to the case of the algebraic counting polynomial (cf. Theorem 2.34 and Examples 2.67, 2.91, 2.92, and 2.94). The condition that no countably infinite sets appear is necessary (cf. Remark 2.20). However, even if countably infinite sets appear, solution sets can still be compared by estimating counting sequences and differential counting polynomials (cf. Proposition 2.35).

Acknowledgements I thank all people who were part of my private and academic life in the past years.

In particular, I thank Prof. Wilhelm Plesken for his supervision, support, and his insistence on the existence of a differential counting polynomial. I thank Daniel Robertz, Mohamed Barakat, Thomas Bächler, Vladimir Gerdt, and Werner Seiler for teaching me during the last years and for their collaboration. I thank Prof. Bemelmans, Prof. Hartmann, Prof. Melcher, and Prof. Walcher for interesting lectures, seminars, helpful suggestions, and for pointing out relevant literature. I thank Alban Quadrat, Dongming Wang, François Boulier, François Lemaire, and Thomas Cluzeau for discussion related to this thesis (and other topics) on various conferences and visits.

I thank Thomas Bächler for taking care of "computer stuff" and Wolfgang Krass for combing through a draft of this thesis for typographical errors. I thank my colleagues (including student assistants) at Lehrstuhl B for thousands of small favors and a nice working atmosphere.

I thank my family, friends, "Sportsfreunde", and the "Teestunde" for constant support, encouragement, and food. I thank Carl Sagan for giving us a place in the cosmos.

This work was partially supported by the DFG Priority Program SPP 1489 and by the DFG Graduate School "Experimentelle und konstruktive Algebra".

Conventions

The following conventions are used throughout this thesis. All rings are associative, unitial, of characteristic zero, and all ring homomorphisms map the one to the one; all rings except for the skew polynomial rings from Subsection 1.3.4 are commutative. The Zariski topology is always used in the classical sense of closed points. Associated primes of an ideal are the preimages of the associated primes of its residue class ring. Applying functions $f : A \to B$ to a set $A' \subseteq A$ results in the set $f(A') := \{f(a') \mid a' \in A'\}$. The word "algebraic" is used for polynomial systems as a contrast to *differential* polynomial systems. A zero of a polynomial p is a solution of the equation $p = 0$. The term "(set of) admissible solutions" stands for the elements that are considered as solutions, i.e., the solutions of the empty set of equations. Examples and remarks are finished with a "$\triangleleft$" and proofs with a "$\square$".

Chapter 1

Simple Systems

1.1 An Overview

This expository section introduces simple systems and their properties by examples. It gives informal definitions; the precise ones can be found in the following sections.

Polynomial differential equations can be translated into an algebraic setting by replacing unknown functions and their derivatives in differential equations by variables. For example, the (left hand side of the) inviscid BURGERS' equation

$$\frac{\partial}{\partial t}u(x,t) + u(x,t) \cdot \frac{\partial}{\partial x}u(x,t) = 0$$

is represented by the differential polynomial

$$u_{0,1} + u_{0,0}u_{1,0} \ .$$

The set of differential polynomials is the differential polynomial ring denoted by $F\{U\}$, where F is a differential field, e.g., $F = \mathbb{C}$ or $F = \mathbb{C}(x,t)$, and U is the set of unknown functions. The variables $u_{\mathrm{i},\mathrm{j}}$ are called differential variables. This construction works for any number of independent variables instead of t and x. In examples it is often more convenient to use the jet notation for differential variables, e.g., write $u_{t,x,x}$ for $u_{1,2}$.

1.1.1 Simple Systems

The next step is to collect some desirable properties of differential systems. This leads to the definition of simple differential systems, i.e., differential systems that satisfy five properties given below.

Consider formal (or convergent) power series solutions. Simple systems allow to solve inductively for the power series coefficients, beginning from lower order, and determine one coefficient at a time. These coefficients are naturally in bijection to the differential variables. Therefore, fix a total order, called ranking, on the differential variables. Then, any non-trivial differential polynomial has a highest ranking differential variable called leader. For any differential polynomial one can substitute values for the lower ranking coefficients of a power series into all differential variables except for the leader. Thus, one ends up with a *univariate* polynomial in the leader. The zeros of this univariate polynomial are the possible values for the next power series coefficient. This works if each differential variables appears at most once as leader of an equation or inequation. This is the triangularity, the first property of simple systems.

The triangularity yields an overview[1] over the set of solutions. The existence of an equation (respectively inequation) with a certain leader implies that a power series coefficient can only take finitely (respectively all but finitely) many different values for fixed lower ranking values. The degree even determines the number of the solutions.

This shows that the leaders play an important role and one would like to have the leader of any differential polynomial well-defined, independent of the values of lower ranking variables. Therefore, as second property, demand that the leading coefficient, called the initial, of any differential polynomial in a system is non-zero for any solution of the system. Also the derivatives of differential equations should have a non-zero initial; it turns out that the initial of all derivatives of a differential polynomial $p \in F\{U\}$ is its separant. Thus, as third property, any differential polynomial should have a non-zero separant[2] for any solution of the system.

Additionally, all differential consequences should be included in the system. This is made formal below by the passivity[3], the fourth property for simple systems. The fifth condition is a minimality condition.

1.1.2 Thomas Decomposition

Many differential systems appearing "in nature" are not simple. However, it is possible to decompose those into a finite set of simple differential systems. This means that the set of solutions is partitioned into classes which are the solution set of simple differential systems. Such a decomposition is called (differential) Thomas decomposition.

The Thomas decomposition is algorithmic and has been implemented by the author. This implementation is used in many examples in this thesis. The following introductory example describes some commands of this implementation. The example was constructed by Robertz and shows that a Thomas decomposition can help symbolic solvers of differential equations.

Example 1.1.

```
restart;
```

Load the package `DifferentialThomas`.

```
with(DifferentialThomas):
```

Define the two independent variables x and y and the functions (called dependent variables) u and v.

```
ivar:=[x,y]:
dvar:=[u,v]:
```

The command `ComputeRanking` sets the ranking for all following computations. Its first parameter is a list of independent variables. If the second parameter is a list of lists of dependent variables, then a block ranking is used with previous blocks being higher, i.e., each differential variable involving a dependent variable in the first list is higher than each differential variable involving a dependent variable in the second list.

```
ComputeRanking(ivar,[[u],[v]]);
```

In this case write $u \gg v$. If the second parameter is given as a list of dependent variables, then use a degree-reverse lexicographical ranking, which is a well-behaved ranking in the sense that higher order implies higher ranking. For the following, decide to use such a ranking.

[1] The following is an oversimplification; see Chapter 2 for precise non-generic statements.

[2] As the separant is the partial derivative of p by its leader, p is square-free if its separant is non-zero.

[3] Passivity is the version of the confluence in differential algebra and the Thomas decomposition can be seen as a version of the Knuth-Bendix completion process [KB70].

```
ComputeRanking(ivar,dvar);
```

A differential variable like $u_{1,2}$ is encoded as

```
u[1,2];
```

$$u_{1,2}$$

For a differential polynomial like

```
p:=u[2,0]^2+u[0,2]+u[1,0]+u[0,1];
```

$$p := {u_{2,0}}^2 + u_{0,1} + u_{0,2} + u_{1,0}$$

the derivative can be computed using the following command.

```
PartialDerivative(p,x);
```

$$2\, u_{2,0} u_{3,0} + u_{1,1} + u_{1,2} + u_{2,0}$$

Given two lists of differential polynomials as input, a differential Thomas decomposition is computed using

```
res:=DifferentialThomasDecomposition([p],[]);
```

$$res := [DifferentialSystem, DifferentialSystem]$$

The differential polynomials in the first list of the input are treated as equations and the differential polynomials in the second list of the input are treated as inequations. This command returns a list of simple differential systems. In particular, the list is non-empty if and only if the input has solutions. Intersections of Thomas decompositions can be computed by the following command.

```
IntersectDecompositions(res,
   DifferentialThomasDecomposition([u[1,0]],[]));
```

$$[DifferentialSystem]$$

Equations and inequations of these systems can be extracted.

```
DifferentialSystemEquations(%[1]);
DifferentialSystemInequations(%%[1]);
```

$$[u_{1,0}, u_{0,1} + u_{0,2}]$$

$$[]$$

These simple differential systems can be printed using

```
PrettyPrintDifferentialSystem(res[1]);
```

$$[\left(\frac{\partial^2}{\partial x^2} u(x,y)\right)^2 + \frac{\partial}{\partial y} u(x,y) + \frac{\partial^2}{\partial y^2} u(x,y) + \frac{\partial}{\partial x} u(x,y) = 0,$$
$$\frac{\partial}{\partial y} u(x,y) + \frac{\partial^2}{\partial y^2} u(x,y) + \frac{\partial}{\partial x} u(x,y) \neq 0$$

and

```
MyPDSolve(res[1]);
MyPDSolve(res[2]);
```

$$\left\{u(x,y) = -1/12\, x^3 + 1/2\, \_C1\, x^2 - x\, \_C1^2 + x\, \_c_1 + \_C2 - \frac{\_C3}{e^y} - \_c_1 y + \_C4\right\}$$

$$\{u(x,y) = ((x+y+1)\, \_C2 - \_C3)\, e^{-y} + (x-y)\, \_C1 + \_C4\}$$

is a wrapper to the algorithms in dsolve and pdsolve of Maple [map] to solve differential equations (if possible). This set of solutions from the simple differential systems seems to be more straightforward than the set of solutions resulting from converting the differential equation into Maple language

```
JetList2Diff(p);
```

$$\left(\frac{\partial^2}{\partial x^2} u(x,y)\right)^2 + \frac{\partial}{\partial y} u(x,y) + \frac{\partial^2}{\partial y^2} u(x,y) + \frac{\partial}{\partial x} u(x,y)$$

and applying the solver from Maple directly:

```
pdsolve(%);
```

$$u(x,y) = \_F1(x) + \_F2(y), \text{where}$$
$$[\left\{ \left(\frac{d^2}{dx^2}\_F1(x)\right)^2 = \_c_1 - \frac{d}{dx}\_F1(x), \frac{d^2}{dy^2}\_F2(y) = -\_c_1 - \frac{d}{dy}\_F2(y) \right\}]$$

In particular, a decomposition into simple differential systems seems helpful when it comes to solving a system of differential equations.

```
JetList2Diff(p);
factor(expand(subs(subs({_c[1]=g(y)},MyPDSolve(res[1])),%)));
```

$$\left(\frac{\partial^2}{\partial x^2}u(x,y)\right)^2 + \frac{\partial}{\partial y}u(x,y) + \frac{\partial^2}{\partial y^2}u(x,y) + \frac{\partial}{\partial x}u(x,y)$$

$$x\frac{d}{dy}g(y) - \left(\frac{d}{dy}g(y)\right)y + x\frac{d^2}{dy^2}g(y) - \left(\frac{d^2}{dy^2}g(y)\right)y - 2\frac{d}{dy}g(y)$$

```
JetList2Diff(p);
factor(expand(subs(u(x, y) = _F1(x)+_F2(y),%)));
```

$$\left(\frac{\partial^2}{\partial x^2}u(x,y)\right)^2 + \frac{\partial}{\partial y}u(x,y) + \frac{\partial^2}{\partial y^2}u(x,y) + \frac{\partial}{\partial x}u(x,y)$$

$$\left(\frac{d^2}{dx^2}\_F1(x)\right)^2 + \frac{d}{dy}\_F2(y) + \frac{d^2}{dy^2}\_F2(y) + \frac{d}{dx}\_F1(x)$$

Example 2.67 revisits this example in the context of the differential counting polynomial and shows that most solutions of the differential equation are not among those found above. ◁

The first important application of simple differential systems is to decide whether a differential equation is a consequence of a system. For a simple differential system this can be decided by the algorithm Reduce described below. It uses suitable pseudo-reductions, a slight generalization of EUCLIDian division, to reduce a differential polynomial modulo derivatives of differential equations. If the reduced form is zero, then the polynomial is a consequence. This generalizes to non-simple differential systems: a differential THOMAS decomposition splits this system into simple differential systems, and then a differential polynomial is a consequence of the original system if it is a consequence of each of these simple differential systems.

Properties of parametric systems often depend on the values of their parameters.

Remark 1.2. An algebraic parameter a can be modeled as a new function. To make a constant, add the differential equations $\partial a = 0$ for all possible partial derivatives ∂ to the system of differential equations. ◁

The reduction with respect to simple differential system allows to prove theorems automatically in the form of deciding whether certain conditions are consequences of a differential system. The proof of the following well-known theorem is an example for this. It deals with the relation of two curves, the template and the tractrix. The template curve pulls the tractrix curve as if these two curves were connected by a fixed rod. The tractrix moves in the direction of the template but keeps a constant distance; thus, it is also called curve of pursuit. The template pushes the tractrix away when it moves in the direction of the tractrix. Thereby, one can model the parking process of a truck.

Theorem 1.3. *Let $(X(t), Y(t))$ be the template curve with tractrix $(x(t), y(t))$ for distance $d > 0$ and non-degeneracy condition $\dot{x}\dot{Y} - \dot{X}\dot{y} \neq 0$. The evolute of the tractrix is given by the intersection points of the normals of template and tractrix.*

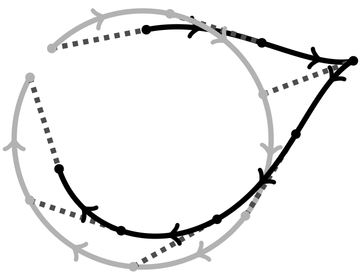


Figure 1.1: A demonstration of tractrix and template curves. The template curve is a light gray circle, the tractrix is the somewhat pear-shaped black curve, and the connecting rod is drawn in dotted gray. In the beginning, the template curve pushes the tractrix away. Then, the tractrix changes its direction and from that moment on, the template curve pulls the tractrix.

Proof.

```
restart;
with(DifferentialThomas):
```

Set the ranking. In the following, the algebraic variable d, which stands for the distance, always has the constraint $\frac{\partial}{\partial t}d = 0$, as explained in Remark 1.2.

```
ivar:=[t]:
dvar:=[x,y,X,Y,d]:
ComputeRanking(ivar,dvar);
```

The next simple procedure symbolically computes the normal ξ, η of a curve X, Y.

```
NormalDirection:=proc(X,Y)
   PartialDerivative(X,t)*(X-xi)+PartialDerivative(Y,t)*(Y-eta);
end proc:
```

The following differential equations describe the interrelation of template and tractrix curve.

```
L:=[
   (X[0]-x[0])^2+(Y[0]-y[0])^2-d^2,
   -y[1]*(X[0]-x[0])+x[1]*(Y[0]-y[0]),
   d[1]
]:
```

Symbolically compute the intersection of the normals of template and tractrix:

```
Ntrac:=NormalDirection(x[0],y[0]);
Ntemp:=NormalDirection(X[0],Y[0]);
s:=solve({Ntrac,Ntemp},{xi,eta});
```

$$\mathit{Ntrac} := x_1\,(x_0-\xi)+y_1\,(y_0-\eta)$$

$$\mathit{Ntemp} := X_1\,(X_0-\xi)+Y_1\,(Y_0-\eta)$$

$$s := \left\{\eta = -\frac{X_1X_0x_1 - X_1x_1x_0 - X_1y_1y_0 + Y_1Y_0x_1}{X_1y_1 - Y_1x_1}, \xi = \frac{y_1X_1X_0 + y_1Y_1Y_0 - Y_1x_1x_0 - Y_1y_1y_0}{X_1y_1 - Y_1x_1}\right\}$$

Compute the evolute:

```
evo:=solve({
   NormalDirection(x[0],y[0]),
   PartialDerivative(NormalDirection(x[0],y[0]),t)
   },{xi,eta});
```

$$\mathit{evo} := \left\{\eta = \frac{{x_1}^3 + y_0y_2x_1 + x_1{y_1}^2 - y_1y_0x_2}{y_2x_1 - y_1x_2}, \xi = \frac{y_2x_1x_0 - y_1x_2x_0 - y_1{x_1}^2 - {y_1}^3}{y_2x_1 - y_1x_2}\right\}$$

Check whether these two solutions are equivalent modulo our equations, i.e., whether their difference is zero modulo our equations. Compute simple differential systems from the equations

```
res:=DifferentialThomasDecomposition(L,[x[1]*Y[1]-X[1]*y[1]]);
```

$$\mathit{res} := [\mathit{DifferentialSystem}, \mathit{DifferentialSystem}]$$

and reduce the difference with respect to both systems to zero

```
differences:=[
   numer(subs(evo,eta)-subs(s,eta)),
   numer(subs(evo,zeta)-subs(s,zeta))]:
DifferentialSystemReduce(res[1],differences);
DifferentialSystemReduce(res[2],differences);
```

$$[0,0]$$
$$[0,0]$$

which implies the claim. □

1.1.3 The Differential Dimension Polynomial

The set of differential consequence of some set S differential polynomials has the structure of a differential ideal, denoted $\mathcal{I}(S)$. This means that it is an ideal which is closed under the action the prescribed derivation operators. One can assign the differential dimension polynomial to the differential ideal $\mathcal{I}(S)$ associated to a simple differential system S. The dimension polynomial was introduced by KOLCHIN to measure the size of the set of solutions of a differential system, and this thesis generalizes his approach from prime ideals to ideals associated to simple differential systems.

Example 1.4. Consider the differential equation $\frac{\partial}{\partial x}f(x,y)-f(x,y)=0$ and look for power series solutions $f(x,y)=\sum_{i,j=0}^{\infty} a_{i,j}\frac{x^iy^j}{i!j!}$ centered around zero. The power series coefficients $a_{0,j}$ for a solution are specified, then all other power series coefficients are determined by the differential equation. This gives an overview about the number of solutions by saying that up to order ℓ one can choose $\ell+1$ power series coefficients freely. The differential dimension function $\Omega(\ell)=\ell+1$ defined below formalizes this. ◁

Denote by $F\{U\}_{\leq\ell}$ the ring of differential polynomials of order $\leq \ell$ and for a differential ideal I define $I_{\leq\ell} := I \cap F\{U\}_{\leq\ell}$. Then the differential dimension function of I is defined using the KRULL dimension as

$$\Omega_I : \mathbb{Z}_{\geq 0} \mapsto \mathbb{Z}_{\geq 0} : \ell \mapsto \dim(F\{U\}_{\leq\ell}/I_{\leq\ell}) \ .$$

As in the example, the differential dimension function is a polynomial function for ℓ big enough. This polynomial is called differential dimension polynomial and the following theorem states its existence and other astonishing properties.

Theorem 1.5. *Let S, S' be simple differential systems and $I := \mathcal{I}(S), J := \mathcal{I}(S')$ the differentials ideals associated to S and S', respectively. Assume that $I \subseteq J$.*

- *There is a numerical polynomial*[4] $\omega_I(\ell) \in \mathbb{Q}[\ell]$ *called differential dimension polynomial such that* $\omega_I(\ell) = \Omega_I(\ell)$ *for sufficiently big* $\ell \in \mathbb{Z}_{\geq 0}$.
- $0 \leq \omega_I(\ell) \leq m\binom{\ell+n}{n}$. *In particular,* $d_I \leq n$ *for* $d_I := \deg_\ell(\omega_I)$.
- *The degree d_I and the leading coefficient of ω_I are invariant under differential birational maps*[5].
- $\omega_I \leq \omega_J$.

[4] I.e., a univariate polynomial $p(\ell) \in \mathbb{Q}[\ell]$ with $p(\ell) \in \mathbb{Z}$ for all $\ell \in \mathbb{Z}$. For two numerical polynomials $p, q \in \mathbb{Q}[\ell]$ define the total order $p \leq q$ if $p(\ell) \leq q(\ell)$ for all ℓ sufficiently large.

[5] Denote by $\mathrm{K}(R)$ the total quotient ring, i.e., the localization at the non-zero-divisors, of a commutative ring R. A differential birational map between two commutative rings R and R' is a ring isomorphism between $\mathrm{K}(R)$ and $\mathrm{K}(R')$ compatible with derivations.

- *Assume that $\omega_I = \omega_J$. Then, $I = J$ if and only if the equations of same leaders have the same degree.*

A more complete version of this theorem is given in Theorem 1.74 below.

The differential dimension polynomial implies many other values, which describe the set of solutions of a system of differential equations; examples are the CARTAN characters, EINSTEIN's strength and the differential type (cf. Subsection 1.6.4).

1.1.4 Differential Elimination

A differential THOMAS decomposition can not only decide whether a differential polynomial is a consequence but actually produce certain desirable consequences of differential systems. For example, given the (standard) NAVIER-STOKES equations it automatically produces the POISSON pressure equation and includes it into the system. More generally, by choosing a suitable ranking, one can force to include certain forms of differential consequences into a simple differential system, e.g., consequences of low order or consequences only involving certain differential indeterminates. The latter case is called differential elimination and it uses a block ranking as introduced in Example 1.1 above.

Example 1.6 (Cole-Hopf Transformation, [BC99, pp. 599-600])**.** Consider the heat equation $h = v_t + v_{xx}$ and the viscous BURGERS' equation $b = u_t + u_{xx} + 2u_x \cdot u$ for two unknown functions $u(t, x)$ and $v(t, x)$. Claim: Any non-zero solution for the heat equation can be transformed to a solution of BURGERS' equation using the COLE-HOPF transformation $\lambda : v \mapsto \frac{v_x}{v}$. A differential THOMAS decomposition of

$$\{h = 0, \underbrace{v \cdot u - v_x}_{\Leftrightarrow u=\lambda(v)} = 0, v \neq 0\}$$

consists of the single system $S = \{v_x - v \cdot u = 0, v \cdot u_x + v_t + v \cdot u^2 = 0, v \neq 0\}$, and one checks that the reduced form of b with respect to S is zero. This implies that λ maps any non-zero solution of the heat equation to a solution of BURGERS' equation.

Claim: λ is surjective. For the proof use any elimination ranking with $v \gg u$. A differential THOMAS decomposition of $\{h = 0, b = 0, v \cdot u - v_x = 0, v \neq 0\}$ consists of the single system

$$S = \{v_x - v \cdot u = 0, v \cdot u_x + v_t + v \cdot u^2 = 0, v \neq 0, b = 0\} .$$

The elimination ordering guarantees that the only constraint for u is BURGERS' equation $b = 0$. The simplicity of S implies that for any solution f of BURGERS' equation there exists a solution (g, f) of S; in particular, λ is surjective.

Claim: λ is not injective. Under any ranking, a differential THOMAS decomposition of $\{h = 0, v \cdot u - v_x = 0, u = 0\}$ consists of the single system

$$S = \{v_x = 0, v_t = 0, u = 0\} .$$

Thus, all constants are mapped to zero by the COLE-HOPF transformation.

Example 1.78 computes the differential dimension polynomials of these equations and uses it to show that MAPLE's pdsolve [map] only finds a subset of the solutions. ◁

Example 1.7. Consider the LOTKA-VOLTERRA (predator-prey) equations.

$$\frac{d}{dt}x(t) = x(t)\,(\alpha - \beta y(t))$$
$$\frac{d}{dt}y(t) = y(t)\,(-\gamma + \delta x(t))$$

In them x models the number of prey and y number of predators. Furthermore, α, β, γ, and δ are constants. The goal of this example is to demonstrate elimination for parameter identification, i.e., to express the parameters α, β, γ, and δ in terms of the functions x and y. The parameters cannot directly be measured in nature, but the amount of predator and prey can (to a certain extend). Therefore, use a block ranking with α, β, γ, δ $\gg x$, y. Remark 1.2 allows to model the parameters. For a better presentation, exclude the trivial cases where $\frac{\partial}{\partial t}x(t) = 0$ and $\frac{\partial}{\partial t}y(t) = 0$.

```
restart;
with(DifferentialThomas):
ivar:=[t]:
dvar:=[alpha,beta,gamma,delta,x,y]:
ComputeRanking(ivar,[dvar[1..4],dvar[5..6]]);
res:=DifferentialThomasDecomposition(
    [x[1]-x[0]*(alpha[0]-beta[0]*y[0]),
     y[1]-y[0]*(-gamma[0]+delta[0]*x[0]),
     alpha[1],beta[1],gamma[1],delta[1]],
    [x[1],y[1]]);
```

$$res := [DifferentialSystem]$$

The differential THOMAS decomposition results in a single simple differential system. In this system, one can solve for the constants:

```
zip((a,b)->print(a=rhs(isolate(JetList2Diff(
       DifferentialSystemEquations(res[1])[b])
    ,a(t)))),[alpha,beta,gamma,delta],[$1..4]):
```

$$\alpha = \frac{x(t)\left(\frac{d}{dt}x(t)\right)\frac{d}{dt}y(t) - x(t)\left(\frac{d^2}{dt^2}x(t)\right)y(t) + \left(\frac{d}{dt}x(t)\right)^2 y(t)}{(x(t))^2\frac{d}{dt}y(t)}$$

$$\beta = \frac{-x(t)\frac{d^2}{dt^2}x(t) + \left(\frac{d}{dt}x(t)\right)^2}{(x(t))^2\frac{d}{dt}y(t)}$$

$$\gamma = -\frac{-x(t)y(t)\frac{d^2}{dt^2}y(t) + x(t)\left(\frac{d}{dt}y(t)\right)^2 + \left(\frac{d}{dt}x(t)\right)y(t)\frac{d}{dt}y(t)}{\left(\frac{d}{dt}x(t)\right)(y(t))^2}$$

$$\delta = \frac{y(t)\frac{d^2}{dt^2}y(t) - \left(\frac{d}{dt}y(t)\right)^2}{\left(\frac{d}{dt}x(t)\right)(y(t))^2}$$

In particular, the right hand sides of the above are constant for solutions of the LOTKA-VOLTERRA equations. There exist two equations in x and y only, characterizing all possible solutions of the LOTKA-VOLTERRA equations, independent of the constants:

```
map(a->print(DifferentialSystemEquations(res[1])[a]),[5,6]):
```

$$x_0{}^2 x_2 y_2 - x_0{}^2 x_3 y_1 - x_0 x_1{}^2 y_2 + 3\, x_0 x_1 x_2 y_1 - 2\, x_1{}^3 y_1$$
$$x_1 y_0{}^2 y_3 - 3\, x_1 y_0 y_1 y_2 + 2\, x_1 y_1{}^3 - x_2 y_0{}^2 y_2 + x_2 y_0 y_1{}^2$$

◁

1.2 Simple Systems

> Differential algebra is easily described: it is (99 per cent or more) the work of RITT and KOLCHIN.
>
> IRVING KAPLANSKY
> in [Kap57, Preface]

> Differential algebra is no longer (99 per cent or more) the work of RITT and KOLCHIN
>
> DANIEL BERTRAND
> in [Ber96]

This section recalls basic definitions used throughout this work, both for the algebraic case of polynomial rings and for the differential case. Furthermore, it introduces the concepts of simple systems and the THOMAS decomposition. It sketches the combinatorial approach of JANET, which is used for the definition of simple differential systems and later to describe the freedom to choose a solutions of a system.

1.2.1 Algebraic Systems

This subsection looks at algebraic systems as a preparation for differential systems, because many properties of differential systems originate in properties of algebraic systems.

Let F be a field of characteristic 0 and $R := F[y_1, \ldots, y_n]$ be the polynomial ring in n variables. A total order $<$ on $\{1, y_1, \ldots, y_n\}$ with $1 < y_i$ for all $1 \leq i \leq n$ is called a **ranking**. An indeterminate x is called **leader**[6] of $p \in R$ if x is the $<$-largest variable occurring in p. In this case write $\mathrm{ld}(p) = x$. If $p \in F$, then define $\mathrm{ld}(p) = 1$. The degree $\mathrm{mdeg}(p)$ of p in $\mathrm{ld}(p)$ is called **main degree** of p. The leading coefficient $\mathrm{init}(p) \in F[\ z \mid z < \mathrm{ld}(p)\ ]$ of $\mathrm{ld}(p)^{\mathrm{mdeg}(p)}$ in p is called **initial** of p. For simplicity of this text always assume that $y_1 < \ldots < y_n$. The highest power of the leader appearing in a polynomial is often underlined for a better overview.

Given a polynomial $p \in R$, the symbols $p_=$ and $p_{\neq}$ denote the equation $p = 0$ and inequation $p \neq 0$, respectively[7]. Abusing notation, sometimes $p_=$ or $p_{\neq}$ also denote the underlying polynomial p. Call a set S of finitely many equations and inequations an **(algebraic) system** over R; its subset $S_{<x} := \{p \in S \mid \mathrm{ld}(p) < x\}$ is a system over $F[\ z \mid z < x\ ]$. The subsets of all equations $p_= \in S$ and all inequations $p_{\neq} \in S$ are denoted by $S^=$ and $S^{\neq}$, respectively. Define $S_x := \{p \in S \mid \mathrm{ld}(p) = x\}$. When it is clear that $|S_x| = 1$, write S_x to denote the unique element of S_x.

Denote by $\overline{F}$ the algebraic closure of F. For $\mathbf{a} \in \overline{F}^n$ define the **(complete) evalu-**

[6] In the context of algebraic triangular decompositions, the leader is usually called **main variable**. The term leader is used in [Tho37] and has later been adopted in differential algebra.

[7] However, especially in examples, equations and inequations are often denoted by $p = 0$ (and $p \neq 0$) when no confusion is possible with "p is (not) the zero polynomial".

ation homomorphism

$$\phi_{\mathbf{a}} : R \to \overline{F} : y_i \mapsto a_i \ .$$

Let $1 \leq j, k \leq n$ with $k \leq j+1$. For $\mathbf{a} \in \overline{F}^j$ define the **(partial) evaluation homomorphism**

$$\phi_{<y_k,\mathbf{a}} : R \to \overline{F}[y_k, \ldots, y_n] : \begin{cases} y_i \mapsto a_i, & i < k \\ y_i \mapsto y_i, & \text{otherwise} \end{cases} \ .$$

A **solution** of $p_=$ or $p_{\neq}$ is a tuple $\mathbf{a} \in \overline{F}^n$ with $\phi_{\mathbf{a}}(p) = 0$ or $\phi_{\mathbf{a}}(p) \neq 0$, respectively. Call $\mathbf{a} \in \overline{F}^n$ a solution of a system S if it is a solution of each element in S. The set of all solutions of S is denoted by $\mathfrak{Sol}(S)$.

A system S is **triangular** if $|S_{y_i}| \leq 1$ for all $1 \leq i \leq n$ and $S \cap \{c_=, c_{\neq} \mid c \in F\} = \emptyset$. The solutions of a triangular system can be found by iteratively finding zeros of a univariate polynomial and substituting the solution in the following polynomials. The following example demonstrates this and motivates further properties of algebraic system, collected in the definition of simple algebraic systems.

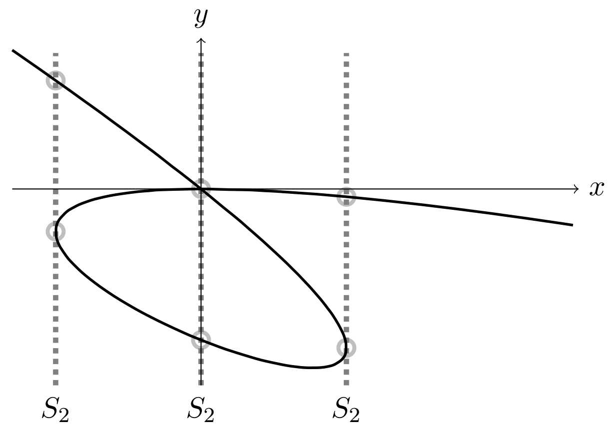
Example 1.8. The set of solutions over the complex numbers $\mathbb{C}$ of

$$p = \underline{y}^3 + (3x+1)y^2 + (3x^2+2x)y + x^3 = 0 \ .$$

equals the union of the solutions sets of the following two triangular (for $x < y$) systems.

$$\begin{array}{lrlr} S_1 := \{ & \underline{y}^3 + (3x+1)y^2 + (3x^2+2x)y + x^3 = 0, & 27\underline{x}^3 - 4x \neq 0 & \} \\ S_2 := \{ & 6\underline{y}^2 + (-27x^2+12x+6)y - 3x^2 + 2x = 0, & 27\underline{x}^3 - 4x = 0 & \} \end{array}$$

Substituting a solution of the univariate polynomial in x into the equation with leader y yields a univariate polynomial in y. Here, this univariate polynomial can be solved for y. In general triangular systems the univariate polynomial might degenerate to a non-zero constant. To prevent this, the initials of all polynomials need to be non-zero after substituting the solutions of lower ranking polynomials.



The geometric way of looking at this substitution are fibers of projections. The diagram shows the solutions of $\{p = 0\}$ in the real affine plane. The cardinality of the fibers of the projection onto the x-component along the y-axis depends on the x-value. However, when considering all solutions in the complex affine plane, this cardinality stays constant within each system; it is 3 for $27x^3 - 4x \neq 0$ corresponding to the degree of $(S_1)_y$ and 2 for $27x^3 - 4x = 0$ corresponding to the degree of $(S_2)_y$. ◁

As in this example, the THOMAS approach uses the evaluation homomorphisms $\phi_{<x,\mathbf{a}}$ to treat each polynomial $p \in S_x$ as the family of *univariate* polynomials $\phi_{<x,\mathbf{a}}(p) \in \overline{F}[x]$ for $\mathbf{a} \in \mathfrak{Sol}(S_{<x})$. In addition to triangularity, the following definition of simple (algebraic) systems formalizes that initials are non-zero and the fibers of all projections have the same cardinality. This equality of fiber cardinalities is ensured by square-freeness.

Definition 1.9. Let S be an algebraic system.

(1) S has **non-vanishing initials** if $\phi_{\mathbf{a}}(\mathrm{init}(S_{y_i})) \neq 0$ for all $\mathbf{a} \in \mathfrak{Sol}(S_{<y_i})$ and all $1 \leq i \leq n$.

(2) S is **square-free** if the univariate polynomial $\phi_{<y_i,\mathbf{a}}(S_{<y_i}) \in \overline{F}[y_i]$ is square-free for all $\mathbf{a} \in \mathfrak{Sol}(S_{<y_i})$ and all $1 \leq i \leq n$.

(3) S is called **simple** if it is triangular, has non-vanishing initials and is square-free.

Let S be a simple algebraic system and $1 \leq i \leq n$. Then, $S_{<y_i}$ is also a simple algebraic system in $F[y_1, \ldots, y_{i-1}]$ (and also in R). Furthermore, $\phi_{<y_i,\mathbf{a}}(S)$ is also a simple algebraic system in $F[y_i, \ldots, y_n]$ for all $\mathbf{a} \in \mathfrak{Sol}(S_{<y_i})$ [Ple09a, Lemma 3.2].

Remark 1.10. Every simple algebraic system S has a solution. In particular, if $\mathbf{b} \in \mathfrak{Sol}(S_{<x})$ and S_x is not empty, then $\phi_{<x,\mathbf{b}}(S_x)$ is a univariate polynomial with exactly $\mathrm{mdeg}(S_x)$ *distinct* roots. If S_x is an equation, each solution $\mathbf{b} \in \mathfrak{Sol}(S_{<x})$ extends to a solution $(\mathbf{b}, a) \in \mathfrak{Sol}(S_{\leq x})$ with $\mathrm{mdeg}(S_x)$ possible choices $a \in \overline{F}$. Otherwise, all but finitely many $a \in \overline{F}$ yield a solution $(\mathbf{b}, a) \in \mathfrak{Sol}(S_{\leq x})$, because an inequation S_x excludes $\mathrm{mdeg}(S_x)$ different a, and $S_x = \emptyset$ imposes no restriction on a.

Conversely, if $(a_1, \ldots, a_n) \in \mathfrak{Sol}(S)$, then $(a_1, \ldots, a_i) \in \mathfrak{Sol}(S_{\leq y_i})$ for any $1 \leq i \leq n$. More specific, $\mathfrak{Sol}(S_{\leq y_i})$ is equal to the projection of $\mathfrak{Sol}(S)$ onto its first i components. ◁

Properties (1) and (2) in the definition of simple algebraic systems are characterized via solutions of lower-ranking equations and inequations. If this set of solutions is infinite, then it is not feasible to check these properties for all solutions. Instead, use polynomial equations and inequations to *partition* the set of solutions of the lower-ranking system to ensure the above properties of simple algebraic systems. This leads to a THOMAS decomposition.

Definition 1.11. Let S be a system. A set $\{S_j | 1 \leq j \leq m\}$ or tuple $(S_j | 1 \leq j \leq m)$ of systems is called **decomposition** of S if

$$\mathfrak{Sol}(S) = \bigcup_{j=1}^{m} \mathfrak{Sol}(S_j) \ .$$

It is further called **disjoint** if $\mathfrak{Sol}(S_i) \cap \mathfrak{Sol}(S_j) = \emptyset \ \forall \ 1 \leq i < j \leq m$. A *disjoint* decomposition into *simple* algebraic systems is called **(algebraic) THOMAS decomposition**.

For any algebraic system S, there exists a THOMAS decomposition [Tho37, Tho62, Wan98]. The algorithm Decompose (cf. Algorithm 1.32) presented below provides another proof of this fact.

Example 1.12 (Quadratic Formula)**.** Consider $\left\{\left(p := a\underline{x}^2 + bx + c\right)_=\right\}$ in $\mathbb{Q}[a,b,c,x]$ with respect to $a < b < c < x$ and compute a THOMAS decomposition.

First, ensure that the initial $\operatorname{init}(p)$ of p is not zero. Therefore, insert $(\operatorname{init}(p))_{\neq} = (\underline{a})_{\neq}$ into the system. Since this restricts the solution set of this system, consider the complementary system $\{p_=, (\underline{a})_=\}$. This latter system simplifies to $\{(b\underline{x}+c)_=, (\underline{a})_=\}$. Similarly, add $(\underline{b})_{\neq}$ into this system to ensure $\operatorname{init}(b\underline{x}+c) \neq 0$ and get the special case system $\{(\underline{c})_=, (\underline{b})_=, (\underline{a})_=\}$. Up to this point, there are three systems, where the second and third one are easily checked to be simple:

$\underline{x}$	$\left(a\underline{x}^2+bx+c\right)_=$	$\underline{x}$	$(b\underline{x}+c)_=$	x	
c		c		$\underline{c}$	$(\underline{c})_=$
b		$\underline{b}$	$(\underline{b})_{\neq}$	$\underline{b}$	$(\underline{b})_=$
$\underline{a}$	$(\underline{a})_{\neq}$	$\underline{a}$	$(\underline{a})_=$	$\underline{a}$	$(\underline{a})_=$

Second, ensure that p is square-free by insertion of $\left(4a\underline{c}-b^2\right)_{\neq}$ into the first system. Again, consider the complementary system $\{(p)_=, \left(4a\underline{c}-b^2\right)_=, (\underline{a})_{\neq}\}$. As p is a square in this system, replace it by its square-free part $2a\underline{x}+b$. All systems are simple:

$\underline{x}$	$\left(a\underline{x}^2+bx+c\right)_=$	$\underline{x}$	$(2a\underline{x}+b)_=$	$\underline{x}$	$(b\underline{x}+c)_=$	x	
$\underline{c}$	$\left(4a\underline{c}-b^2\right)_{\neq}$	$\underline{c}$	$\left(4a\underline{c}-b^2\right)_=$	c		$\underline{c}$	$(\underline{c})_=$
b		b		$\underline{b}$	$(\underline{b})_{\neq}$	$\underline{b}$	$(\underline{b})_=$
$\underline{a}$	$(\underline{a})_{\neq}$	$\underline{a}$	$(\underline{a})_{\neq}$	$\underline{a}$	$(\underline{a})_=$	$\underline{a}$	$(\underline{a})_=$

$\triangleleft$

1.2.2 Differential Algebra and Differential Systems

This subsection introduces the standard setup of differential algebra, including the differential polynomial ring, the polynomial ring in the unknown functions and their derivatives, and differential algebras.

Let $\Delta = \{\partial_1, \ldots, \partial_n\}$ be a non-empty set of **derivation operators** and F a **differential ring**, i.e., the $\partial_j \in \Delta$ are commuting $\mathbb{Z}$-linear operators $\partial_j : F \to F$ satisfying the LEIBNIZ rule. Given a **differential indeterminate** u, the **differential polynomial ring** $F\{u\} := F\left[\, u_{\mathbf{i}} \mid \mathbf{i} \in \mathbb{Z}^n_{\geq 0} \,\right]$ is the polynomial ring generated by the infinite algebraically independent set $\{u\}_\Delta := \{u_{\mathbf{i}} \mid \mathbf{i} \in \mathbb{Z}^n_{\geq 0}\}$. The operation of $\partial_j \in \Delta$ on $\{u\}_\Delta$ is defined by $\partial_j u_{\mathbf{i}} = u_{\mathbf{i}+e_j}$, and this operation extends $\mathbb{Z}$-linearly and via the LEIBNIZ rule to $F\{u\}$. Let $U = \{u^{(1)}, \ldots, u^{(m)}\}$ be a non-empty set of differential indeterminates (also called the set of **dependent variables**). The multivariate differential polynomial ring is given by $F\{U\} := F\{u^{(1)}\} \ldots \{u^{(m)}\}$. Its generators $\{U\}_\Delta := \{u^{(j)}_{\mathbf{i}} \mid \mathbf{i} \in \mathbb{Z}^n_{\geq 0}, j \in \{1, \ldots, m\}\}$ are the **differential variables**. Call a finite set of equations and inequations, i.e., a subset of $F\{U\}^{\{=,\neq\}}$, a **(differential) system** over $F\{U\}$. Let $u^{(j)}_{\mathbf{i}}$ be a differential variable. Call $\operatorname{ord} u^{(j)}_{\mathbf{i}} := |\mathbf{i}| := \sum_{j=1}^n \mathbf{i}_j$ the **order** of $u^{(j)}_{\mathbf{i}}$ and $\operatorname{ord}_k u^{(j)}_{\mathbf{i}} := \mathbf{i}_k$ the **order** of $u^{(j)}_{\mathbf{i}}$ **in** ∂_k for $k = 1, \ldots, n$.

From now on let F be a **differential field** of characteristic zero, i.e., a field that is a differential ring. In many examples, the differential field contains elements $y_1, \ldots, y_n$ with $\partial_i y_j = \delta_{ij}$, where δ_{ij} denotes the KRONECKER delta, or more generally, F is a field of meromorphic functions in n complex variables $y_1, \ldots, y_n$. In these cases, call the elements $y_1, \ldots, y_n$ **independent variables**.

Slightly more general is the category of **differential** F**-algebras** over Δ; its object class are the F-algebras on which Δ operates as a set of commuting derivations, and its sets of morphisms are F-algebra homomorphism that commute with the derivations from

Δ. In an algorithmic setup one considers the full subcategory of **finitely differentially generated differential F-algebras** over Δ with objects that are generated as F-algebras by a finite set of elements and (consecutive) derivatives of these elements[8]. **Differential ideals** are ideals of a differential algebra that are closed under the action of Δ, and any finitely differentially generated differential F-algebra is the quotient of a finitely generated differential polynomial ring by a differential ideal. A **differential F-subalgebra** of a differential F-algebra is a subalgebra closed under derivations from Δ. A differential subalgebra is generated by some elements if it is the intersection of all differential subalgebras containing these elements.

1.2.3 Rankings and Janet Division

This subsection focuses on a combinatorial approach called Janet division [GB98a]. The Janet division organizes the infinite set of differential variables by partitioning them into finitely many cones. A combinatorial approach based on the Janet division guarantees inclusion of all integrability conditions in a differential system. This subsection presents an algorithm for inserting new equations into an existing set of equations and adjusting this cone decomposition accordingly. For an overview of modern development see [Ger05, Sei10], the original ideas are formulated in [Jan29].

A (differential) **ranking** $<$ is defined as a total order on the set of differential variables and 1 with $1 < u \ \forall\, u \in U$, such that

(1) $u < \partial_j u$ and

(2) $u < v$ implies $\partial_j u < \partial_j v$

for all $u, v \in \{U\}_\Delta$ and $\partial_j \in \Delta$. From now on let $<$ be an arbitrary and fixed differential ranking. For any finite set of differential variables, a differential ranking induces an algebraic ranking. Thereby, in accordance to the algebraic setting, define the largest differential variable $\mathrm{ld}(p)$ appearing in a differential polynomial $p \in F\{U\}$ as **leader**, which is set to 1 for $p \in F$. Furthermore, define $\mathrm{mdeg}(p)$ and $\mathrm{init}(p)$ as the **main degree**, i.e. degree in the leader, and the **initial**, i.e. coefficient of $\mathrm{ld}(p)^{\mathrm{mdeg}(p)}$, respectively. Note that $\mathrm{ld}(\partial p) = \partial\, \mathrm{ld}(p)$ for all $p \in F\{U\}$ and all $\partial \in \Delta$.

Special classes of rankings are used in different contexts. The first class of rankings is used for elimination. A (differential) ranking $<$ is called **block ranking** or **elimination ranking** if there is a partition $U = \biguplus_{i=1}^{k} B_i$ such that $u_{\mathbf{i}}^{(j)} < u_{\mathbf{i}'}^{(j')}$ if $u^{(j)} \in B_h$ and $u_{\mathbf{i}'}^{(j')} \in B_{h'}$ for $h < h'$. Write $B_1 \ll B_2 \ll \ldots \ll B_k$. The second class of rankings is useful for proving convergence of power series solutions. A ranking $<$ is called **Riquier** if $u_{\mathbf{i}}^{(j)} < u_{\mathbf{i}'}^{(j')}$ implies $u_{\mathbf{i}}^{(j')} < u_{\mathbf{i}'}^{(j)}$ for all $\mathbf{i}, \mathbf{i}' \in \mathbb{Z}_{\geq 0}^n$ and all $j, j' \in \{1, \ldots, m\}$. The next class of rankings is used for counting the set of solutions. A (differential) ranking $<$ is called **orderly ranking** if $|\mathbf{i}| < |\mathbf{i}'|$ implies $u_{\mathbf{i}}^{(j)} < u_{\mathbf{i}'}^{(j')}$ for any $\mathbf{i}, \mathbf{i}' \in \mathbb{Z}_{\geq 0}^n$ and any $j, j' \in \{1, \ldots, m\}$. The "standard" ranking is the **degree-reverse lexicographical ranking**, which is an orderly Riquier ranking. Here, $u_{\mathbf{i}}^{(j)} < u_{\mathbf{i}'}^{(j')}$ if and only if

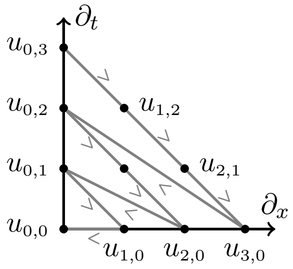
$$
\begin{array}{ll}
|\mathbf{i}| < |\mathbf{i}'| & \text{or} \\
|\mathbf{i}| = |\mathbf{i}'|,\ \mathbf{i}_n = \mathbf{i}'_n, \ldots,\ \mathbf{i}_{k+1} = \mathbf{i}'_{k+1},\ \text{and } \mathbf{i}_k < \mathbf{i}'_k & \text{or} \\
\ \mathbf{i} = \mathbf{i}' \text{ and } j < j' \ . &
\end{array}
$$

It is easy to see that rankings on $F\{U\}$ are in bijection to term orderings on $F[y_1, \ldots, y_n]^m$. Much work has been done on classification of term orderings and rank-

[8] The differential polynomial rings are the free objects in this category.

ings. The case $m = 1$ is treated in [Rob85, Wei87], Riquier rankings in [CS99], and the general case in [RR97].

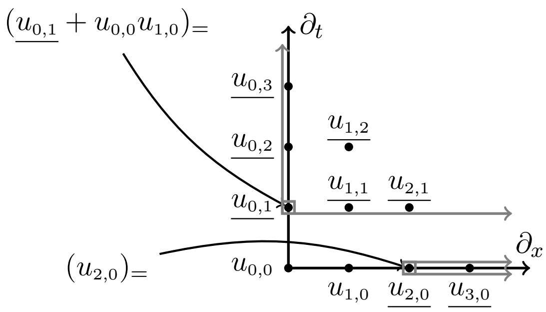
The following example demonstrates how to view rankings and uses them to motivate the Janet cone decomposition.



Example 1.13. Consider a differential indeterminate u and derivations $\Delta = \{\partial_x, \partial_t\}$. In this setting, any partial differential equation in one dependent variable and two independent variables with constant coefficients can be represented as a differential polynomial in $\mathbb{C}\{u\}$.

Let $<$ be the orderly ranking defined by $u_{i_1,i_2} < u_{j_1,j_2}$ if and only if either $i_1+i_2 < j_1+j_2$ or $i_1+i_2 = j_1+j_2$ and $i_2 < j_2$ holds. Thus, the smallest differential variables are: $u_{0,0} < u_{1,0} < u_{0,1} < u_{2,0} < u_{1,1} < u_{0,2} < u_{3,0}$. When considering the set of differential variables as a grid in the first quadrant of a plane, the diagram illustrates this ranking.

Consider $(\underline{u_{0,1}}+u_{0,0}u_{1,0})_=$ representing the inviscid Burgers' equation $\frac{\partial u}{\partial t}+u\frac{\partial u}{\partial x} = 0$. As in the algebraic part, the diagram visualizes equations by attaching them to their leaders. However, contrary to the algebraic part, differential equations imply their derivatives as consequences. Thus, a differential equation not only implies restrictions to its leader, but also to the derivatives of its leader. For example $\partial_t(\underline{u_{0,1}} + u_{0,0}u_{1,0}) = \underline{u_{0,2}} + u_{0,1}u_{1,0} + u_{0,0}u_{1,1}$. The diagram illustrates this by drawing a cone with apex $u_{0,1}$.



Now, consider solutions of the inviscid Burgers' equation linear in x. So, add the second equation $(\underline{u_{2,0}})_=$ to the system. This second equation also affects the derivatives of its leader. In particular, $(\underline{u_{0,1}}+u_{0,0}u_{1,0})_=$ and $(\underline{u_{2,0}})_=$ both affect the differential variable $u_{2,1}$ and its derivatives. This inhibits triangularity of the system. According to the approach suggested by Janet, disallow certain equations to be differentiated by certain partial derivations. In this example, allow $(\underline{u_{2,0}})_=$ to be differentiated only by ∂_x. The diagram illustrates this by drawing a (degenerate) cone with apex $u_{2,0}$ in direction of ∂_x. Thus, the differential consequence $(\partial_t \underline{u_{2,0}})_=$ is not yet considered and, so, consider it as a separate equation for further treatment in Example 1.40. ◁

The cones of the previous example are an important technical part of the simple systems, as they ensure the inclusion of all compatibility conditions. Furthermore, they provide the combinatorial background for counting.

A set W of differential variables is **closed** under the action of $\Delta' \subseteq \Delta$ if $\partial_i w \in W$ for all $\partial_i \in \Delta'$ and $w \in W$. The smallest set containing a differential variable w, which is closed under Δ', is called a **cone** and denoted by $\{w\}_{\Delta'}$. In this case, the elements of Δ' are called **reductive derivations**[9]. The Δ'-closed set generated by a set W of differential variables is defined as

$$\{W\}_{\Delta'} := \bigcap_{\substack{W_i \supseteq W \\ W_i\ \Delta'\text{-closed}}} W_i \subseteq \{U\}_\Delta .$$

[9] In [Ger99] and [Sei10, Chap. 7] the reductive derivations are called multiplicative variables and in [BGLHR10] they are called admissible derivations.

For a finite set $W = \{w_1, \dots, w_r\}$, the **Janet division** algorithmically assigns a set of reductive derivations to the elements of W such that the cones generated by the $w \in W$ are disjoint (cf. [GYB01] for a faster algorithm). The derivation $\partial_l \in \Delta$ is **Janet-reductive** for the cone generated by $w = u_{\mathbf{i}}^{(j)} \in W$ if and only if

$$\mathbf{i}_l = \max\left\{\mathbf{i}'_l \mid u_{\mathbf{i}'}^{(j)} \in W,\, \mathbf{i}'_k = \mathbf{i}_k \text{ for all } 1 \le k < l\right\}$$

holds [Ger05, Ex. 3.1]. Remark that j is fixed in this definition, i.e., only take into account other differential variables belonging to the same differential indeterminate. Denote the reductive derivations assigned to w by $\Delta(w, W) \subseteq \Delta$ and call $\{w\}_{\Delta(w,W)}$ the **Janet cone** of w with respect to W. Cones can be described by a pair of a differential variable and a subset of the derivations, i.e. and element of $\{U\}_\Delta \times \mathbb{P}(\Delta)$.

The Janet division ensures disjointness of cones but not necessarily that the union of cones equals $\{W\}_\Delta$. The problem is circumvented by enriching W to its **Janet completion** $\widetilde{W} \supseteq W$. This completion $\widetilde{W}$ is successively created by adding any

$$\tilde{w} = \partial_i w_j \notin \biguplus_{w \in \widetilde{W}} \{w\}_{\Delta(w,\widetilde{W})}$$

to $\widetilde{W}$, for $w_j \in \widetilde{W}$ and $\partial_i \in \Delta \setminus \Delta(w_j, \widetilde{W})$, leading to the disjoint **Janet decomposition**

$$\{W\}_\Delta = \biguplus_{w \in \widetilde{W}} \{w\}_{\Delta(w,\widetilde{W})}$$

that algorithmically separates a Δ-closed set $\{W\}_\Delta$ into finitely many cones $\{w\}_{\Delta(w,\widetilde{W})}$. For details and proofs see [Ger05, Def. 3.4] and [GB98a, Cor. 4.11].

Similarly, the complement of a Δ-closed set $\{W\}_\Delta$ can be decomposed into cones. An algorithm for this is given in Appendix B.

Extend the Janet decomposition from differential variables to differential polynomials according to their leaders, i.e., $\Delta(q, T) := \Delta(\mathrm{ld}(q), \mathrm{ld}(T))$ for finite $T \subset F\{U\}$ and $q \in T$. Call a derivative of an equation by a finite (possibly empty) sequence of derivations a **prolongation**. If all these derivations are reductive, the derivative is called a **reductive prolongation** of q with respect to T. Otherwise it is called a **non-reductive prolongation**.

A differential polynomial $p \in F\{U\}$ is called **reducible** modulo $q \in F\{U\}$ if there exists $\mathbf{i} \in \mathbb{Z}^n_{\ge 0}$ such that $\partial_1^{\mathbf{i}_1} \cdot \ldots \cdot \partial_n^{\mathbf{i}_n} \mathrm{ld}(q) = \mathrm{ld}(\partial_1^{\mathbf{i}_1} \cdot \ldots \cdot \partial_n^{\mathbf{i}_n} q) = \mathrm{ld}(p)$ and $\mathrm{mdeg}(\partial_1^{\mathbf{i}_1} \cdot \ldots \cdot \partial_n^{\mathbf{i}_n} q) \le \mathrm{mdeg}(p)$. For $\mathbf{i} \neq (0, \dots, 0)$ the condition on the main degree always holds. Now restrict to reductive prolongations: For a finite set $T \subset F\{U\}$, call a differential polynomial $p \in F\{U\}$ Janet-**reducible** modulo $q \in T$ w.r.t. T if p is reducible modulo q and $\partial_1^{\mathbf{i}_1} \cdot \ldots \cdot \partial_n^{\mathbf{i}_n} q$ is a reductive prolongation of q w.r.t. T, with $\mathbf{i} \in \mathbb{Z}^n_{\ge 0}$ from the reducibility conditions. Furthermore, p is Janet-**reducible** modulo T if there is a $q \in T$ such that p is Janet-reducible modulo q w.r.t. T.

1.2.4 Non-centered Power Series Solutions

All previous differential algebra definitions are purely formal and do not involve solutions. However, the definition of square-freeness or non-vanishing initials for simple systems require a set of admissible solutions. This subsection defines a set of admissible solutions for differential systems based on solutions of algebraic systems. Such a unified set of admissible solutions both for the algebraic and differential case allows unified algorithms, definitions, and proofs.

All fields are of characteristic zero.

Solutions for algebraic systems are n-tuples $\overline{F}^n \cong \overline{F}^{\{y_1,\dots,y_n\}}$ in the algebraic closure $\overline{F}$ of F, where each entry in the tuples is indexed by one of the n indeterminates. The admissible solutions considered here are tuples indexed by the differential variables, i.e., lie in $\overline{F}^{\{U\}_\Delta}$. Section 1.4 below connects this novel set of admissible solutions with formal and convergent power series.

To smooth notation, write the image of a differential variable $u_\mathbf{i}$ as coefficient of $z^\mathbf{i}$ in the formal power series ring $\overline{F}[[z_1,\dots,z_n]]$, where $z^\mathbf{i} := z_1^{i_1}\cdot\ldots\cdot z_n^{i_n}$. More formally, define the set of **non-centered power series**

$$E := \overline{F}[[z_1,\dots,z_n]]^U \equiv \bigoplus_{j=1}^{m} \overline{F}[[z_1,\dots,z_n]] \ ,$$

which is isomorphic as $\overline{F}$-vectorspace to $\overline{F}^{\{U\}_\Delta}$ by the **algebraization isomorphism**

$$\alpha : E \xrightarrow{\sim} \overline{F}^{\{U\}_\Delta} : \left(u^{(j)} \mapsto \sum_{\mathbf{i}\in\mathbb{Z}^n_{\geq 0}} a^{(j)}_\mathbf{i} \frac{z^\mathbf{i}}{\mathbf{i}!} \right) \mapsto \left(u^{(j)}_\mathbf{i} \mapsto a^{(j)}_\mathbf{i} \right)$$

where $\mathbf{i}! := i_1!\cdot\ldots\cdot i_n!$.

The name "algebraization isomorphism" indicates that a non-centered power series is turned into an (infinite) tuple, which is suitable for *algebraic* equations. The non-centered power series are a first step towards formal and convergent power series. They are already power series, but their coefficients lie in the differential field F. In all examples in this thesis F is a field of meromorphic functions. In this case the non-centered power series are power series with *variable coefficients*. For example, if $F = \mathbb{C}(y)$ and $U = \{u\}$, then $u \mapsto (1 + yz + \frac{1}{y}\frac{z^2}{2!} + \ldots) \in E$. They are called "non-centered", because one can specialize to (most) $\zeta \in \mathbb{C}$ as *center* of expansion by substituting y by ζ and z by $y-\zeta$ to get a formal power series $u \mapsto (1+\zeta(y-\zeta)+\frac{1}{\zeta}\frac{(y-\zeta)^2}{2!}+\ldots) \in \mathbb{C}[[y-\zeta]]^U$; of course, ζ should not be a pole of any coefficient. Non-centered solutions are *not* related with Taylor series of meromorphic functions at various centers of expansion (cf. Example 1.59). The definition of E delays the problem of choosing a suitable (non-singular) center and allows to concentrate on algorithms for now.

Now, the definition of solutions is the same as in the algebraic case. For $e \in E$, let

$$\phi_e : F\{U\} \to \overline{F} : u^{(j)}_\mathbf{i} \mapsto \alpha(e)(u^{(j)}_\mathbf{i})$$

be the F-algebra homomorphism evaluating the differential variables at e. A **differential equation** or **inequation** for m functions $U = \{u^{(1)},\dots,u^{(m)}\}$ in n indeterminates is an element $p \in F\{U\}^{\{=,\neq\}}$, written $p_=$ or $p_{\neq}$, respectively. A **non-centered (power series) solution** of $p_=$ or $q_{\neq}$ is an $e \in E$ with $\phi_e(\{p\}_\Delta) = \{0\}$ or $\phi_e(\{q\}_\Delta) \neq \{0\}$, respectively. Here, $\{p\}_\Delta := \{\partial^\mathbf{i} p \mid \mathbf{i} \in \mathbb{Z}^n_{\geq 0}\} \subset F\{U\}$. Furthermore, $e \in E$ is called a non-centered solution of a system S of differential equations and inequations if it is a non-centered solution of each element in S. Denote the set of non-centered solutions of S by $\mathfrak{Sol}_E(S) \subseteq E$.

The non-centered solutions are used in [BLOP09, Paragraph 7] under the name "formal power series solutions", however, without passing to an explicit center of expansion to obtain (actual) formal power series solutions over the field of constants.

Non-centered solutions connect solutions of differential ideals with algebraic solutions. Let $\mathrm{Mon}(\Delta)$ denote the free commutative monoid generated by Δ. The differential ideal $\langle P\rangle_\Delta$ generated by a set of equations $P := \{p_1, \dots, p_k\} \subset F\{U\}^{\{=\}}$ is equal to the algebraic ideal $\langle \mathrm{Mon}(\Delta)P\rangle$ generated by all derivations of the elements in P. Obviously, $\phi_e(\{p\}_\Delta) = \{0\}$ if and only if $\phi_e(\langle p\rangle_\Delta) = \{0\}$, as $\{p\}_\Delta$ generates the differential ideal $\langle p\rangle_\Delta$ in $F\{U\}$. Further connections of non-centered solutions and ideals follow from the Nullstellensatz for non-centered solutions (cf. Theorem 1.65).

In differential algebra one usually considers solutions in a universal differential field. However, in contrast to non-centered power series, this class of fields is highly non-constructive. Nonetheless, non-centered solutions are connected to solutions in the universal differential field and can be considered as such a solution. As the universal differential field take the universal closure $\widehat{F}$ of the algebraic closure $\overline{F}$. Then, $\overline{F}[[z_1, \dots, z_n]] \hookrightarrow \overline{F}((z_1, \dots, z_n)) \hookrightarrow \widehat{F}$, where the second embedding comes from the definition of universal differential fields [Kol73, §II.2 and §III.7].

1.2.5 Simple Differential Systems

These preparations allow the main definition in this chapter: simple differential systems.

Call a set of differential variables $T \subset \{U\}_\Delta$ **minimal**, if for any $S \subset \{U\}_\Delta$ with

$$\biguplus_{t\in T} \{t\}_{\Delta(t,T)} = \biguplus_{s\in S} \{s\}_{\Delta(s,S)}$$

the condition $T \subseteq S$ holds [GB98b, Def. 4.2]. Call a set of differential polynomials minimal, if the corresponding set of leaders is minimal.

Simple differential systems should contain all differential consequences. For this, it suffices to check whether the non-reductive prolongations of equations are already consequences. Let $p \in F\{U\}$ with $x = \mathrm{ld}(p)$ and define the **separant** $\mathrm{sep}(p) := \frac{\partial p}{\partial x}$. For a differential system of equations $S = S^=$ say that a differential polynomial $p \in F\{U\}$ **reduces to zero modulo** S if qp lies in the (algebraic) ideal generated by the elements of S and their reductive prolongations for at least one q in the monoid generated by the initials and separants of $S^=$. This definition means that p is a consequence of S, in the sense that it lies in the differential ideal associated to S (cf. Definition 1.64).

Definition 1.14 (Simple Differential Systems)**.** A differential system S is (JANET-) **passive** if all non-reductive prolongations of $(S_T)^=$ reduce to zero modulo $(S_T)^=$.

A differential system S is called **simple** if

(1) S is algebraically simple (in the finite set of differential variables appearing in it),

(2) S is passive,

(3) $S^=$ is minimal, and

(4) no inequation in $S^{\neq}$ is reducible modulo $S^=$.

A set $\{S_1, \dots, S_m\}$ or tuple $(S_j | 1 \le j \le m)$ of differential system is called **decomposition** of S if $\mathfrak{Sol}_E(S) = \bigcup_{j=1}^m \mathfrak{Sol}_E(S_j)$. It is further called **disjoint** if $\mathfrak{Sol}_E(S_i) \cap \mathfrak{Sol}_E(S_j) = \emptyset \ \forall\ 1 \le i < j \le m$. A *disjoint* decomposition into *simple differential systems* is called **(differential) THOMAS decomposition**.

Examples of simple differential systems and differential THOMAS decompositions can be found in the overview Section 1.1.

1.3 The Decomposition Algorithms

> In mathematics: "This isn't a proof. You can't have a whole step that's just 'Mathematica said so.'"
> In physics: "What a waste. Half of this proof could be replaced by 'mathematica said so.'"
>
> ZACHARY WEINERSMITH
> in [Wei, 2861]

This section presents an algorithm to compute algebraic and differential THOMAS decompositions as defined in the last section (cf. Definitions 1.11 and 1.14). It begins with the conceptually simpler algebraic case before presenting the differential algorithm. Most of this section grew out of joint work with THOMAS BÄCHLER, VLADIMIR GERDT and DANIEL ROBERTZ [BGLHR10, BGLHR12]. There exist easier describable THOMAS decomposition algorithms [Wan98, Ger08, Rob12, LHR13]. In contrast to these algorithms, the algorithms presented here lead to the definition of the differential counting polynomial (cf. Subsection 2.4.3) and yield a fast implementation.

Assume that the ground field F, both in the algebraic or differential setting, is computable[10] and of characteristic 0. Let $\Delta = \{\partial_1, \ldots, \partial_n\}$ be a non-empty set of derivation operators and $U = \{u^{(1)}, \ldots, u^{(m)}\}$ be a non-empty set of differential indeterminates.

In a nutshell, the main algorithm works as follows. Due to case distinctions, it needs to treat several systems successively until each system is simple. It represents each system as a pair consisting of a candidate simple system and a queue of unprocessed equations and inequations, similar to [GB98b, MM99]. In each step, the algorithm chooses a suitable polynomial from the queue, (pseudo-)reduces it, and both ensures a non-zero initial and square-freeness by a case distinction. Such a case distinction splits the system into two systems; it subjoins a new polynomial to the queue as an inequation and at the same time creates a new system with the same polynomial subjoined to the queue as an equation. Thereby, no solution is lost and the solution sets are disjoint. After the splitting, the algorithm subjoins the reduced polynomial to the candidate simple system. If there already is a polynomial in the candidate simple system with the same leader, then it combines both polynomials in one of the following three ways. First, for a pair of equations a generalization of the EUCLIDean algorithm computes the gcd; the degree of the gcd depends on more case distinctions. Second, the algorithm replaces an equation p and an inequation q by $p/\gcd(p, q)$ and, third, two inequations by their lcm. In the differential case, the algorithm additionally takes derivations of equations into account to ensure passivity.

Even though a system is a set of equations and inequations, this section often considers systems with an additional structure. View any system S as a pair of sets $S = (S_T, S_Q)$, such that S can be recovered from the union $S_T \cup S_Q$. Here, S_T represents the candidate simple system and S_Q is the queue. Triangularity is required for

[10] A field F is called computable if there exists an embedding $F \hookrightarrow \mathbb{Z}_{\geq 0}$ with a recursive image such that addition and multiplication are algorithmic. It follows that subtraction and division are algorithmic (cf. [Rab60]). Many examples sloppily talk about non-computable fields (mostly of complex numbers or finitely generated fields of functions over the complex numbers) instead of the computable differential subfield containing all relevant elements. In these cases assume that the algorithms are performed over a computable field which is contained in the larger field; this larger field is not computable but can be used for an interpretation of the solutions.

S_T, and $(S_T)_x$ denotes the unique (in)equation of leader x in S_T, if it exists. Moreover, S_T fulfills a weak form of the other simplicity conditions, i.e., for any indeterminate x where $(S_T)_x$ is non-empty $\phi_{\mathbf{a}}(\mathrm{init}((S_T)_x)) \neq 0$ and $\phi_{<x,\mathbf{a}}(S_{<x})$ is square-free for all $\mathbf{a} \in \mathfrak{Sol}((S_T)_{<x} \cup (S_Q)_{<x})$. In particular, S_T is simple if $S_Q = \emptyset$.

1.3.1 Algebraic Reduction

This subsection describes a reduction algorithm, a form of EUCLIDian division modulo a set of equations.

Let $R := F[y_1, \ldots, y_n]$ be a polynomial ring in n variables. From now on, let prem be any **pseudo remainder algorithm** in R and pquo the corresponding **pseudo quotient algorithm**. To be precise, if $p, q \in R$ with $\mathrm{ld}(p) = \mathrm{ld}(q) = x$, then

$$m \cdot p = \mathsf{pquo}(p, q, x) \cdot q + \mathsf{prem}(p, q, x) \tag{1.1}$$

holds, where $\deg_x(q) > \deg_x(\mathsf{prem}(p, q, x))$, $\mathrm{ld}(m) < x$ and $m \mid \mathrm{init}(q)^k$ for some $k \in \mathbb{Z}_{\geq 0}$. Note that $\phi_{\mathbf{a}}(\mathrm{init}(p)) \neq 0$ and $\phi_{\mathbf{a}}(\mathrm{init}(q)) \neq 0$ imply $\phi_{\mathbf{a}}(\mathsf{pquo}(p, q, x)) \neq 0$ and $\phi_{\mathbf{a}}(m) \neq 0$ for any $\mathbf{a} \in \overline{F}^n$. Clearly $\mathrm{ld}(\mathsf{pquo}(p, q, x)) \leq x$.

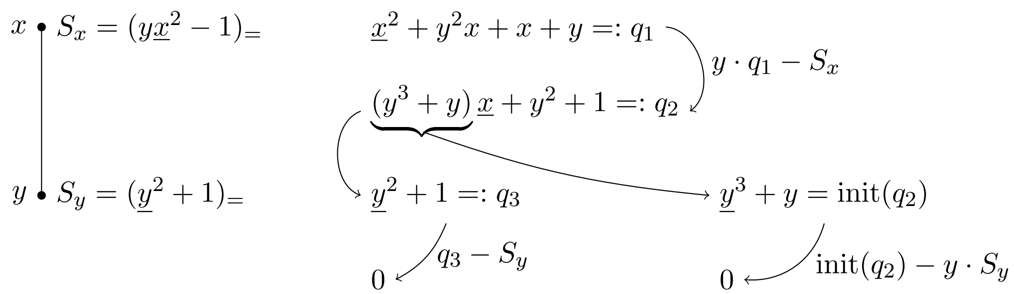
The following algorithm employs prem to reduce a polynomial modulo the candidate simple system S_T.

Algorithm 1.15 (Reduce).
Input: A system $S = (S_T, S_Q)$, a polynomial $p \in R$
Output: A polynomial q with $\phi_{\mathbf{a}}(q) = 0$ if and only if $\phi_{\mathbf{a}}(p) = 0$ for each $\mathbf{a} \in \mathfrak{Sol}(S)$. (Further properties of Reduce are stated in Remarks 1.17 and 1.18.)
Algorithm:

$x \leftarrow \mathrm{ld}(p)$; $q \leftarrow p$
while $x > 1$ and $(S_T)_x$ is an equation and $\mathrm{mdeg}(q) \geq \mathrm{mdeg}((S_T)_x)$ **do**
  $q \leftarrow \mathsf{prem}(q, (S_T)_x, x)$
  $x \leftarrow \mathrm{ld}(q)$
end while
if $x > 1$ and $\mathsf{Reduce}(S, \mathrm{init}(q)) = 0$ **then**
  return $\mathsf{Reduce}(S, q - \mathrm{init}(q)x^{\mathrm{mdeg}(q)})$
else
  return q
end if

Before giving a proof, the following example explains why the initial deserves special treatment in the reduction algorithm.

Example 1.16. Reduce $p := q_1 := x^2 + y^2x + x + y$ modulo the simple algebraic system $S = S_T = \{(y\underline{x}^2 - 1)_=, (\underline{y}^2 + 1)_=\}$, which is displayed on the left.



In the first reduction step, q_1 is pseudo-reduced modulo S_x. The result q_2 still has leader x, but a main degree smaller than S_x. The initial of q_2 reduces to 0, which removes the highest power of x from q_2. The resulting polynomial q_3 now pseudo-reduces to 0 modulo S_y, i.e. $\mathsf{Reduce}(\{S_x, S_y\}, p) = 0$. ◁

Proof of Algorithm 1.15. Each step decreases the main degree or leader of q. This can happen only a finite number of times. Similarly, the recursions in lines 6 and 7 are called with a polynomial either of lower main degree or lower leader. This proves termination.

Show correctness. There exists a product $m \in R \setminus \{0\}$ of (factors of) initials of elements in S_T with $\mathrm{ld}(m) < \mathrm{ld}(p)$ such that

$$\mathsf{Reduce}(S, p) = mp - \sum_{z \leq \mathrm{ld}(p)} c_z \cdot (S_T)_z \tag{1.2}$$

with $c_z \in R$ and $\mathrm{ld}(c_z) \leq \mathrm{ld}(p)$ if $(S_T)_z$ is an equation and $c_z = 0$ otherwise. The inequation $\phi_{\mathbf{a}}(m) \neq 0$ holds for all $\mathbf{a} \in \mathfrak{Sol}(S_{\leq \mathrm{ld}(p)})$ due to the requirements for S_T. This implies

$$\phi_{\mathbf{a}}(\mathsf{Reduce}(S, p)) = \underbrace{\phi_{\mathbf{a}}(m)}_{\neq 0} \phi_{\mathbf{a}}(p) - \sum_{z \leq x} \phi_{\mathbf{a}}(c_z) \underbrace{\phi_{\mathbf{a}}((S_T)_z)}_{=0},$$

and therefore $\phi_{\mathbf{a}}(p) = 0$ if and only if $\phi_{\mathbf{a}}(\mathsf{Reduce}(S, p)) = 0$. □

This algorithm is central for the application of simple algebraic systems. For example, Proposition 1.62 shows that this algorithm solves the radical ideal membership. The following remarks describe some easy properties of the reduction.

Remark 1.17. Let $S = S_T$ be a system and $p, q \in R$ with $q = \mathsf{Reduce}(S, p)$.

(1) If $S_{\mathrm{ld}(q)}$ is an equation, then $\mathrm{mdeg}(q) < \mathrm{mdeg}(S_{\mathrm{ld}(q)})$.

(2) If $q \neq 0$, then $\mathsf{Reduce}(S, \mathrm{init}(q)) \neq 0$.

(3) $\mathrm{ld}(q) \leq \mathrm{ld}(p)$ and if $\mathrm{ld}(q) = \mathrm{ld}(p)$ then $\mathrm{mdeg}(q) \leq \mathrm{mdeg}(p)$.

(4) If $q = 0$, then $\phi_{\mathbf{a}}(p) = 0 \ \forall\, \mathbf{a} \in \mathfrak{Sol}(S_{\leq \mathrm{ld}(p)})$.

◁

The next properties of the reduction solicit a proof.

Remark 1.18. Let $S = (S_T, S_Q)$ be a system and $p \in R$ with $\mathrm{ld}(p) = x$.

(1) If $(S_Q)^{=}_{<x} = \emptyset$ and $\mathsf{Reduce}(S, p) \neq 0$ hold, then either $\exists\, \mathbf{a} \in \mathfrak{Sol}(S_{<x} \cup \{(S_T)_x\})$ such that $\phi_{\mathbf{a}}(p) \neq 0$ or $\mathfrak{Sol}(S_{<x}) = \emptyset$.

(2) If $(S_Q)_{\leq x} = \emptyset$, i.e., $S_{\leq x} = (S_T)_{\leq x}$ is simple, then $\mathsf{Reduce}(S, p) \neq 0$ implies $\exists\, \mathbf{a} \in \mathfrak{Sol}(S_{\leq x})$ such that $\phi_{\mathbf{a}}(p) \neq 0$.

(3) Let $S = (S_T, \emptyset)$ be simple. Then $\mathsf{Reduce}(S, p) = 0$ if and only if $\phi_{\mathbf{a}}(p) = 0 \ \forall\, \mathbf{a} \in \mathfrak{Sol}(S_{\leq x})$.

◁

Proof. For the first part let $|\mathfrak{Sol}(S_{<x})| > 0$. Then $|\mathfrak{Sol}(S_{<x} \cup \{(S_T)_x\})| > 0$ holds, since $\mathrm{ld}((S_T)_x) = x$, $\mathrm{mdeg}((S_T)_x) > 0$, and the univariate polynomial $\phi_{<x,\mathbf{a}}((S_T)_x) \in \overline{F}[x]$ has positive degree for each $\mathbf{a} \in \mathfrak{Sol}(S_{<x})$. Assume that $\phi_{\mathbf{a}}(p) = 0 \ \forall\, \mathbf{a} \in \mathfrak{Sol}(S_{<x} \cup \{(S_T)_x\})$. Then $(S_T)_x$ is an equation and $\deg_x(p) \geq \deg_x((S_T)_x)$ and therefore $p \neq$

$\mathsf{Reduce}(S,p)$. In fact, the assumption further implies $\mathrm{ld}(\mathsf{Reduce}(S,p)) < x$, as otherwise $\deg_x(\mathsf{Reduce}(S,p)) \geq \deg_x((S_T)_x)$ would hold. By repeating the previous arguments, inductively conclude $\mathrm{ld}(\mathsf{Reduce}(S,p)) = 1$. As $\phi_{\mathbf{a}}(p) = 0$, conclude $\mathsf{Reduce}(S,p) = 0$, which is a contradiction.

The second part follows from the first part. The second part and Remark 1.17.(4) imply the third part (cf. [Wan98, Thm. 4]). □

Say that a polynomial p **reduces to q modulo S_T** if $\mathsf{Reduce}(S,p) = q$, and it is **reduced modulo S_T** if it reduces to itself. A polynomial $p \in F\{U\}$ is called **tail reduced** modulo S_T if its **tail** $p - \mathrm{init}(p)\,\mathrm{ld}(p)^{\mathrm{mdeg}(p)}$ and its initial $\mathrm{init}(p)$ are tail reduced modulo S_T, where a monomial in $F\{U\}$ is **tail reduced** modulo S_T if it is reduced modulo S_T.

1.3.2 Splitting

Let $R := F[y_1,\ldots,y_n]$ or $R = F\{U\}$.

The Thomas decomposition uses subalgorithms that decompose the solution set of a system into disjoint sets. These splitting algorithms are mostly based on subresultant methods (cf. [Hab48], [Mis93, Chap. 7], [Yap00, Chap. 3]). This subsection does not give the technical proofs based on the subresultant methods, as they were worked out by Thomas Bächler, and instead refers to [BGLHR12].

The following one-line algorithm underlies all splitting algorithms. It splits a system S into two systems with disjoint solution sets and thereby ensures a case distinction with respect to the solutions of another polynomial p.

Algorithm 1.19 (Split).
Input: A system $S = (S_T, S_Q)$, a polynomial $p \in R$
Output: The disjoint decomposition $(S \cup \{p_{\neq}\}, S \cup \{p_{=}\})$ of S.
Algorithm:

1: **return** $((S_T, S_Q \cup \{p_{\neq}\}), (S_T, S_Q \cup \{p_{=}\}))$

The following splitting subalgorithms are better understood when first described in the context of the main algorithm, which was sketched at the beginning of this section. Consider an equation or inequation q for which a property (like a non-zero initial) needs to be ensured with respect to a system S. Each such subalgorithm returns two systems for the input S and q. The first system S_1 contains this additional inequation, which ensures this additional property. The second system S_2 contains the complementary equation, and q is added back into the queue of S_2. The main algorithm then puts S_2 aside for later treatment. In each case $(S_1 \cup \{q\}, S_2)$ is a disjoint decomposition of $S \cup \{q\}$.

The first splitting algorithm $\mathsf{InitSplit}$ makes sure that an initial does not vanish.

Algorithm 1.20 (InitSplit).
Input: A system $S = (S_T, S_Q)$, an equation or inequation q with $\mathrm{ld}(q) = x$.
Output: Two systems S_1 and S_2, where $(S_1 \cup \{q\}, S_2)$ is a disjoint decomposition of $S \cup \{q\}$. Moreover, $\phi_{\mathbf{a}}(\mathrm{init}(q)) \neq 0$ holds for all $\mathbf{a} \in \mathfrak{Sol}(S_1)$ and $\phi_{\mathbf{a}}(\mathrm{init}(q)) = 0$ for all $\mathbf{a} \in \mathfrak{Sol}(S_2)$.
Algorithm:

1: $(S_1, S_2) \leftarrow \mathsf{Split}(S, \mathrm{init}(q))$
2: $(S_2)_Q \leftarrow (S_2)_Q \cup \{q\}$
3: **return** (S_1, S_2)

The further splitting algorithms need some preparation. Consider a multivariate polynomial $p \in R$ as the family of univariate polynomials $\phi_{<\mathrm{ld}(p),\mathbf{a}}(p)$ for certain $\mathbf{a} \in \overline{F}^n$. To ensure triangularity and square-freeness, compute the gcd of two polynomials, which in general depends on $\mathbf{a} \in \overline{F}^n$. Subresultants provide a generalization of the EUCLIDean algorithm that takes the tuple $\mathbf{a} \in \overline{F}^n$ into account.

Definition 1.21. Let $p, q \in R$ with both $\mathrm{ld}(p) = \mathrm{ld}(q) = x$ and $\deg_x(p) = d_p > \deg_x(q) = d_q$. Let $p, q, \mathsf{prem}(p, q, x), \ldots$ be the **subresultant polynomial remainder sequence** of p and q w.r.t. x, where each polynomial is a pseudo remainder of the previous two polynomials for a choice of prem. Denote this sequence by $\mathrm{SPRS}(p, q, x)$ and by $\mathrm{SPRS}_i(p, q, x)$, $i < d_q$ the polynomial of degree i in $\mathrm{SPRS}(p, q, x)$ if it exists, or 0 otherwise. Furthermore, $\mathrm{SPRS}_{d_p}(p, q, x) := p$, $\mathrm{SPRS}_{d_q}(p, q, x) := q$ and $\mathrm{SPRS}_i(p, q, x) := 0$, $d_q < i < d_p$. For $0 < i < d_p$ define $\mathrm{res}_i(p, q, x) := \mathrm{init}\,(\mathrm{SPRS}_i\,(p, q, x))$, $\mathrm{res}_{d_p}(p, q, x) := 1$ and $\mathrm{res}_0(p, q, x) := \mathrm{SPRS}_0\,(p, q, x)$. Note that $\mathrm{res}_0(p, q, x)$ is the usual resultant.

The subresultant polynomial remainder sequence is well-behaved with respect to evaluation. In particular, the subresultant polynomial remainder sequence yields a well-behaved sequence for the EUCLIDian algorithm when applying $\phi_{<\mathrm{ld}(p),\mathbf{a}}$. The $\mathrm{res}_i(p, q, x)$ lead to the case distinctions according to the various possibilities of the degrees of all possible gcds after evaluation with $\phi_{<\mathrm{ld}(p),\mathbf{a}}$ for $\mathbf{a} \in \mathfrak{Sol}(S_{<x})$.

Definition 1.22. Let $S = (S_T, S_Q)$ be a system and $p_1, p_2 \in R$ with $\mathrm{ld}(p_1) = \mathrm{ld}(p_2) = x$. If $|\mathfrak{Sol}(S_{<x})| > 0$, call

$$i := \min\left\{i \in \mathbb{Z}_{\geq 0} \mid \exists\ \mathbf{a} \in \mathfrak{Sol}(S_{<x}) \text{ such that } \deg_x(\gcd(\phi_{<x,\mathbf{a}}(p_1), \phi_{<x,\mathbf{a}}(p_2))) = i\right\}$$

the **fiber cardinality** of p_1 and p_2 w.r.t. S. Moreover, if $(S_Q)^{=}_{<x} = \emptyset$, then

$$\begin{aligned} i' := \min\{i \in \mathbb{Z}_{\geq 0}\ | &\mathsf{Reduce}(S_T, \mathrm{res}_i(p_1, p_2, x)) \neq 0, \\ &\mathsf{Reduce}(S_T, \mathrm{res}_j(p_1, p_2, x)) = 0\ \forall\ j < i\} \end{aligned}$$

is the **quasi fiber cardinality** of p_1 and p_2 w.r.t. S. A disjoint decomposition (S_1, S_2) of S such that

(1) $\deg_x(\gcd(\phi_{<x,\mathbf{a}}(p_1), \phi_{<x,\mathbf{a}}(p_2))) = i\ \forall\ \mathbf{a} \in \mathfrak{Sol}\,((S_1)_{<x})$

(2) $\deg_x(\gcd(\phi_{<x,\mathbf{a}}(p_1), \phi_{<x,\mathbf{a}}(p_2))) > i\ \forall\ \mathbf{a} \in \mathfrak{Sol}\,((S_2)_{<x})$

is called i-th **fibration split** of p_1 and p_2 w.r.t. S. A polynomial $r \in R$ with $\mathrm{ld}(r) = x$ such that $\deg_x(r) = i$ and

$$\phi_{<x,\mathbf{a}}(r) \sim \gcd(\phi_{<x,\mathbf{a}}(p_1), \phi_{<x,\mathbf{a}}(p_2))\ \forall\ \mathbf{a} \in \mathfrak{Sol}\,((S_1)_{<x})$$

is called i-th **conditional greatest common divisor** of p_1 and p_2 w.r.t. S, where $p \sim q$ if and only if $p \in (\overline{F} \setminus \{0\})q$. Furthermore, $q \in R$ with $\mathrm{ld}(q) = x$ and $\deg_x(q) = \deg_x(p_1) - i$ such that

$$\phi_{<x,\mathbf{a}}(q) \sim \frac{\phi_{<x,\mathbf{a}}(p_1)}{\gcd(\phi_{<x,\mathbf{a}}(p_1), \phi_{<x,\mathbf{a}}(p_2))}\ \forall\ \mathbf{a} \in \mathfrak{Sol}\,((S_1)_{<x})$$

is called i-th **conditional quotient** of p_1 by p_2 w.r.t. S. Replacing $\phi_{<x,\mathbf{a}}(p_2)$ in the above definition with $\frac{\partial}{\partial x}(\phi_{<x,\mathbf{a}}(p_1))$ results in an i-th **square-free split** and i-th **conditional square-free part** of p_1 w.r.t. S.

Example 1.23. Consider the system $S := \{(\underline{x}^3 + y)_=\}$ and the polynomial $q := \underline{x}^2 + x + y + 1$ with $y < x$. Compute $\mathrm{res}_0(S_x, q, x) = \underline{y}^3 + 7y^2 + 5y + 1$, $\mathrm{res}_1(S_x, q, x) = -\underline{y}$ and $\mathrm{res}_2(S_x, q, x) = 1$. The fiber cardinality of S_x and q w.r.t. S is 0. A zeroth fibration split is given by $S_1 := S \cup \{(\mathrm{res}_0(S_x, q, x))_{\neq}\}$ and $S_2 := S \cup \{(\mathrm{res}_0(S_x, q, x))_=\}$. The fiber cardinality w.r.t. S_2 is 1. A first fibration split is given by $S_{2,1} := S_2 \cup \{(-\underline{y})_{\neq}\}$ and $S_{2,2} := S \cup \{(-\underline{y})_=\}$. Note in this case that $\mathfrak{Sol}(S_{2,1}) = \mathfrak{Sol}(S_2)$ and $\mathfrak{Sol}(S_{2,2}) = \emptyset$. A zeroth conditional quotient of S_x and q is S_x. A first conditional gcd and a first conditional quotient are $-y\underline{x} + 2y + 1$ and $y^2\underline{x}^2 + (2y^2 + y)x + 4y^2 + 4y + 1$, respectively. ◁

The quasi fiber cardinality exists to give a lower bound to the fiber cardinality.

Lemma 1.24 ([BGLHR12, Lemma 2.16]). *Let $|\mathfrak{Sol}(S_{<x})| > 0$ and $(S_Q)^=_{<x} = \emptyset$. For p_1, p_2 as in Definition 1.22 with $\phi_{\mathbf{a}}(\mathrm{init}(p_1)) \neq 0\ \forall\ \mathbf{a} \in \mathfrak{Sol}(S_{<x})$ and $\mathrm{mdeg}(p_1) > \mathrm{mdeg}(p_2)$, let i be the fiber cardinality and i' the quasi fiber cardinality of p_1 and p_2 w.r.t. S. Then $i' \leq i$ with equality if and only if $|\mathfrak{Sol}(S_{<x} \cup \{\mathrm{res}_{i'}(p_1, p_2, x)_{\neq}\})| > 0$.*

It is in general hard to compute the fiber cardinality directly. However, in the case where the quasi fiber cardinality is strictly smaller than the fiber cardinality, the corresponding fibration split leads to one inconsistent system and one where the quasi fiber cardinality is increased. The following algorithm splits a system into subsystems, depending on the different quasi fiber cardinality of two given polynomials.

Algorithm 1.25 (ResSplit, [BGLHR12, Algorithm 2.18]).
Input: A system $S = (S_T, S_Q)$ with $(S_Q)^=_{<x} = \emptyset$, two polynomials $p, q \in R$ with $\mathrm{ld}(p) = \mathrm{ld}(q) = x$, $\mathrm{mdeg}(p) > \mathrm{mdeg}(q)$ and $\phi_{\mathbf{a}}(\mathrm{init}(p)) \neq 0$ for all $\mathbf{a} \in \mathfrak{Sol}(S_{<x})$.
Output: The quasi fiber cardinality i of p and q w.r.t. S and an i-th fibration split (S_1, S_2) of p and q w.r.t. S.
Algorithm:

1: $i \leftarrow \min\{i \in \mathbb{Z}_{\geq 0} \mid \mathsf{Reduce}(S_T, \mathrm{res}_j(p, q, x)) = 0\ \forall\ j < i$ and $\mathsf{Reduce}(S_T, \mathrm{res}_i(p, q, x)) \neq 0\}$
2: **return** $(i, S_1, S_2) := (i, \mathsf{Split}(S, \mathrm{res}_i(p, q, x)))$

Apply the fiber cardinality and fibration split to compute a gcd of a polynomial in S_T and some other polynomial.

Algorithm 1.26 (ResSplitGCD, [BGLHR12, Algorithm 2.19]).
Input: A system $S = (S_T, S_Q)$ with $(S_Q)^=_{<x} = \emptyset$, where $(S_T)_x$ is an equation, and an equation $q_=$ with $\mathrm{ld}(q) = x$. Furthermore, $\mathrm{mdeg}(q) < \mathrm{mdeg}((S_T)_x)$.
Output: Two systems S_1 and S_2 and an equation $\widetilde{q}_=$ such that:

a) $S_2 = \widetilde{S_2} \cup \{q\}$ where $\left(S_1, \widetilde{S_2}\right)$ is an i-th fibration split of $(S_T)_x$ and q w.r.t. S,
b) $\widetilde{q}$ is an i-th conditional gcd of $(S_T)_x$ and q w.r.t. S,

where i is the quasi fiber cardinality of p and q w.r.t. S.
Algorithm:

1: $(i, S_1, S_2) \leftarrow \mathsf{ResSplit}(S, (S_T)_x, q)$
2: $(S_2)_Q \leftarrow (S_2)_Q \cup \{q\}$
3: **return** $S_1, S_2, \mathrm{SPRS}_i((S_T)_x, q, x)_=$

Note that $i = 0$ yields an inconsistency, and so the main algorithm ensures $i > 0$ before calling ResSplitGCD by adding the resultant of two equations to the system.

The following algorithm is similar. It is used to divide an equation by its gcd with an inequation.

Algorithm 1.27 (ResSplitDivide, [BGLHR12, Algorithm 2.20]).
Input: A system $S = (S_T, S_Q)$ with $(S_Q)^{=}_{<x} = \emptyset$ and two polynomials p, q with $\operatorname{ld}(p) = \operatorname{ld}(q) = x$ and $\phi_{\mathbf{a}}(\operatorname{init}(p)) \neq 0$ for all $\mathbf{a} \in \mathfrak{Sol}(S_{<x})$. Furthermore, if $\operatorname{mdeg}(p) \leq \operatorname{mdeg}(q)$, then $\phi_{\mathbf{a}}(\operatorname{init}(q)) \neq 0$.
Output: Two systems S_1 and S_2 and a polynomial $\widetilde{p}$ such that:

a) $S_2 = \widetilde{S_2} \cup \{q\}$ where $\left(S_1, \widetilde{S_2}\right)$ is an i-th fibration split of p and q' w.r.t. S,

b) $\widetilde{p}$ is an i-th conditional quotient of p by q' w.r.t. S,

where i is the quasi fiber cardinality of p and q' w.r.t. S, with $q' = q$ for $\operatorname{mdeg}(p) > \operatorname{mdeg}(q)$ and $q' = \mathsf{prem}(q, p, x)$ otherwise.
Algorithm:

if $\operatorname{mdeg}(p) \leq \operatorname{mdeg}(q)$ **then**
  return $\mathsf{ResSplitDivide}(S, p, \mathsf{prem}(q, p, x))$
else
  $(i, S_1, S_2) \leftarrow \mathsf{ResSplit}\,(S, p, q)$
  if $i > 0$ **then**
    $\widetilde{p} \leftarrow \mathsf{pquo}(p, \operatorname{SPRS}_i(p, \mathsf{prem}(q, p, x), x), x)$
  else
    $\widetilde{p} \leftarrow p$
  end if
  $(S_2)_Q \leftarrow (S_2)_Q \cup \{q\}$
  return $S_1, S_2, \widetilde{p}$
end if

Applying the last algorithm to a polynomial p and $\frac{\partial}{\partial \operatorname{ld}(p)} p$ yields an algorithm to make p square-free.

Algorithm 1.28 (ResSplitSquareFree, [BGLHR12, Algorithm 2.21]).
Input: A system $S = (S_T, S_Q)$ with $(S_Q)^{=}_{<x} = \emptyset$ and a polynomial p with $\operatorname{ld}(p) = x$ and $\phi_{\mathbf{a}}(\operatorname{init}(p)) \neq 0$ for all $\mathbf{a} \in \mathfrak{Sol}(S_{<x})$.
Output: Two systems S_1 and S_2 and a polynomial r such that if $\operatorname{mdeg}(p) = 1$, then $S_1 = S$, $S_2 = \{1_=\}$, and $r = p$ or if $\operatorname{mdeg}(p) > 1$, then

a) $S_2 = \widetilde{S_2} \cup \{p\}$ where $\left(S_1, \widetilde{S_2}\right)$ is an i-th square-free split of p w.r.t. S,

b) r is an i-th conditional square-free part of p w.r.t. S,

where i is the quasi fiber cardinality of p and $\frac{\partial}{\partial x} p$ w.r.t. S.
Algorithm:

if $\operatorname{mdeg}(p) = 1$ **then**
  return $S, \{1_=\}, p$
end if
$(i, S_1, S_2) \leftarrow \mathsf{ResSplit}\left(S, p, \frac{\partial}{\partial x} p\right)$
if $i > 0$ **then**
  $r \leftarrow \mathsf{pquo}\left(p, \operatorname{SPRS}_i\left(p, \frac{\partial}{\partial x} p, x\right), x\right)$
else
  $r \leftarrow p$
end if
$(S_2)_Q \leftarrow (S_2)_Q \cup \{p\}$
return S_1, S_2, r

All $\mathsf{ResSplit}$-based algorithms require $(S_Q)^{=}_{<x} = \emptyset$ to ensure that all equations of a smaller leader than x are used when reducing modulo S_T. The order in which polynomials are treated by the main algorithm must therefore be restricted to incorporate low ranking equations into S_T as soon as possible. Any suitable order is a selection strategy in the sense defined below. Denote by $\mathbb{P}(M)$ the power set of a set M.

Definition 1.29 (Select)**.** A **selection strategy** is a map

$$\begin{aligned}\mathsf{Select}: \mathbb{P}\left(R^{\{=,\neq\}}\right) &\longrightarrow R^{\{=,\neq\}}: \\ Q &\longmapsto q \in Q\end{aligned}$$

with the following properties:

(1) If $\mathsf{Select}(Q) = q_=$ is an equation, then $Q^{=}_{<\mathrm{ld}(q)} = \emptyset$.

(2) If $\mathsf{Select}(Q) = q_{\neq}$ is an inequation, then $Q^{=}_{\leq\mathrm{ld}(q)} = \emptyset$.

These conditions are necessary for termination. The following example yields an infinite loop when they are violated.

Example 1.30. Consider $R := F[a, x]$ with $a < x$ and the system S with $S_T := \emptyset$ and $S_Q := \left\{(x^2 - a)_=\right\}$. To insert $(x^2 - a)_=$ into S_T, apply the $\mathsf{ResSplitSquareFree}$ algorithm: Calculate $\mathrm{res}_0(x^2 - a, \frac{\partial}{\partial x}(x^2 - a), x) = \mathrm{res}_0(x^2 - a, 2x, x) = -4a$, $\mathrm{res}_1(x^2 - a, 2x, x) = 2$ and $\mathrm{res}_2(x^2 - a, 2x, x) = 1$ according to Definition 1.21. The quasi fiber cardinality is 0 and $\mathsf{ResSplitSquareFree}$ yields two new systems S_1, S_2 with $(S_1)_T = \{(x^2-a)_=\}$, $(S_1)_Q = \{(-4a)_{\neq}\}$ and

$$(S_2)_T = \emptyset, (S_2)_Q = \{(x^2 - a)_=, (-4a)_=\} \ .$$

Now consider what happens with S_2. When selecting $(x^2 - a)_=$ as the next equation to be treated, in violation of the properties in Definition 1.29, $\mathsf{ResSplitSquareFree}$ splits up S_2 into $S_{2,1}$, $S_{2,2}$ with $(S_{2,1})_T = \{(x^2 - a)_=\}$, $(S_{2,1})_Q = \{(-4a)_{\neq}, (-4a)_=\}$ and

$$(S_{2,2})_T = \emptyset, (S_{2,2})_Q = \{(x^2 - a)_=, (-4a)_=, (-4a)_=\} \ .$$

As S_2 equals $S_{2,2}$ up to a duplicate equation, this results in an endless loop. ◁

1.3.3 The Algebraic Algorithm

Let $R := F[y_1, \ldots, y_n]$. The following trivial algorithm inserts a new equation into S_T. It is replaced with a non-trivial algorithm in the differential case. This algorithm is only applied in well-behaved situations in the main algorithm, where $(S_T)_x$ is superfluous.

Algorithm 1.31 ($\mathsf{InsertEquation}$)**.**
Input: A system $S = (S_T, S_Q)$ and an equation $r_=$ with $\mathrm{ld}(r) = x$ such that both $\phi_{\mathbf{a}}(\mathrm{init}(r)) \neq 0$ and $\phi_{<x,\mathbf{a}}(r)$ is square-free for all $\mathbf{a} \in \mathfrak{Sol}(S_{<x})$.
Output: A system S where $r_=$ is inserted into S_T.
Algorithm:

if $(S_T)_x$ is not empty **then**
    $S_T \leftarrow (S_T \setminus \{(S_T)_x\})$
end if
$S_T \leftarrow S_T \cup \{r_=\}$
return S

This subalgorithm allows to present the main algorithm. The general structure is as follows: In each iteration, a system S is selected from a list P of unfinished systems. An equation or inequation q is chosen from the queue S_Q according to the selection strategy. Then q is reduced modulo S_T and incorporated into the candidate simple system S_T with the splitting algorithms as described above. In doing so, the algorithm may add new systems S_i to P. Any obviously inconsistent system, i.e., a system containing an equation $c_=$ for $c \in F \setminus \{0\}$ or the inequation $0_{\neq}$, is discarded.

Algorithm 1.32 (Decompose).
Input: A system $S' = (\emptyset, (S')_Q)$.
Output: A Thomas decomposition of S'.
Algorithm: The algorithm is printed on page 39.

Demonstrate the algorithm with a simple example. All systems which are obviously inconsistent are omitted.

Example 1.33. Let $R := F[a, x]$ with $a < x$, and $S = (S_T, S_Q) := (\emptyset, \{(x^2 + x + 1)_=, (x + a)_{\neq}\})$. According to Select, $q := (x^2 + x + 1)_=$ is chosen. As $\operatorname{init}(q) = 1$ and $\operatorname{res}_0(q, \frac{\partial}{\partial x} q, x) = 1$, the original system S is replaced by $\big(\{(x^2 + x + 1)_=\}, \{(x + a)_{\neq}\}\big)$.

Now, the algorithm selects $q := (x + a)_{\neq}$ and ResSplitDivide$(S, (S_T)_x, q)$ computes $\operatorname{res}_0((S_T)_x, q, x) = \mathsf{prem}((S_T)_x, q, x) = a^2 - a + 1$, $\operatorname{res}_1((S_T)_x, q, x) = \operatorname{init}(q) = 1$, and $\operatorname{res}_2((S_T)_x, q, x) = 1$. As S_T contains no equation of leader a, none of these polynomials can be reduced. Then, decompose S into

$$S := (\underbrace{\{(x^2 + x + 1)_=, (a^2 - a + 1)_{\neq}\}}_{=S_T}, \underbrace{\{\}}_{=S_Q}) \ ,$$

which is already simple, and

$$S_1 := (\underbrace{\{(x^2 + x + 1)_=\}}_{=(S_1)_T}, \underbrace{\{(x + a)_{\neq}, (a^2 - a + 1)_=\}}_{=(S_1)_Q}) \ .$$

Replace S_1 by

$$S_1 := \big(\{(x^2 + x + 1)_=, (a^2 - a + 1)_=\}, \{(x + a)_{\neq}\}\big)$$

and apply ResSplitDivide$(S_1, ((S_1)_T)_x, q)$ to S_1 again. This time, Reduce$((S_1)_T, a^2 - a + 1) = 0$ holds and S_1 is replaced with

$$S_1 := (\{(\underbrace{x - a + 1}_{\mathsf{pquo}(x^2+x+1, x+a, x)})_=, (a^2 - a + 1)_=\}, \{1_{\neq}\}) \ .$$

Thus, a Thomas decomposition of $\{(x^2 + x + 1)_=, (x + a)_{\neq}\}$ is

$$\big(\{(x^2 + x + 1)_=, (a^2 - a + 1)_{\neq}\}, \{(x - a + 1)_=, (a^2 - a + 1)_=\}\big) \ . \qquad \triangleleft$$

The proof is postponed until after sketching how to compute a Thomas decomposition of set theoretic constructions. This also works in the differential case.

Proposition 1.34. *Let S, S_1, S_2 be simple systems over the same ring. A Thomas decomposition of the following sets can be computed.*

(1) $\mathfrak{Sol}(S_1) \cap \mathfrak{Sol}(S_2)$.

Algorithm 1.32 (Decompose)

$P \leftarrow \{S'\}$; $Result \leftarrow \emptyset$
while $|P| > 0$ **do**
Choose $S \in P$; $P \leftarrow P \setminus \{S\}$
if $|S_Q| = 0$ **then**
$Result \leftarrow Result \cup \{S\}$
else
$q \leftarrow \mathsf{Select}(S_Q)$; $S_Q \leftarrow S_Q \setminus \{q\}$
$q \leftarrow \mathsf{Reduce}(S_T, q)$; $x \leftarrow \mathrm{ld}(q)$
if $q \notin \{0_{\neq}, c_{=} \mid c \in F \setminus \{0\}\}$ **then**
if $x \neq 1$ **then**
if q is an equation **then**
if $(S_T)_x$ is an equation **then**
if $\mathsf{Reduce}(S_T, \mathrm{res}_0((S_T)_x, q, x)) = 0$ **then**
$(S, S_1, p) \leftarrow \mathsf{ResSplitGCD}(S, q)$; $P \leftarrow P \cup \{S_1\}$
$S \leftarrow \mathsf{InsertEquation}(S, p_{=})$
else
$S_Q \leftarrow S_Q \cup \{q_{=}, \mathrm{res}_0((S_T)_x, q, x)_{=}\}$
end if
else
if $(S_T)_x$ is an inequation[a] **then**
$S_Q \leftarrow S_Q \cup \{(S_T)_x\}$; $S_T \leftarrow S_T \setminus \{(S_T)_x\}$
end if
$(S, S_2) \leftarrow \mathsf{InitSplit}(S, q)$; $P \leftarrow P \cup \{S_2\}$
$(S, S_3, p) \leftarrow \mathsf{ResSplitSquareFree}(S, q)$; $P \leftarrow P \cup \{S_3\}$
$S \leftarrow \mathsf{InsertEquation}(S, p_{=})$
end if
else if q is an inequation **then**
if $(S_T)_x$ is an equation **then**
$(S, S_4, p) \leftarrow \mathsf{ResSplitDivide}(S, (S_T)_x, q)$; $P \leftarrow P \cup \{S_4\}$
$S \leftarrow \mathsf{InsertEquation}(S, p_{=})$
else
$(S, S_5) \leftarrow \mathsf{InitSplit}(S, q)$; $P \leftarrow P \cup \{S_5\}$
$(S, S_6, p) \leftarrow \mathsf{ResSplitSquareFree}(S, q)$; $P \leftarrow P \cup \{S_6\}$
if $(S_T)_x$ is an inequation **then**
$(S, S_7, r) \leftarrow \mathsf{ResSplitDivide}(S, (S_T)_x, p)$; $P \leftarrow P \cup \{S_7\}$
$(S_T)_x \leftarrow (r \cdot p)_{\neq}$
else if $(S_T)_x$ is empty **then**
$(S_T)_x \leftarrow p_{\neq}$
end if
end if
end if
end if
$P \leftarrow P \cup \{S\}$
end if
end if
end while
return $Result$

[a] Remember that $(S_T)_x$ might be empty, and thus neither an equation nor an inequation.

(2) $\overline{F}^n \setminus \mathfrak{Sol}(S)$*, the complement of the solutions of* S*.*

(3) $\mathfrak{Sol}(S_1) \setminus \mathfrak{Sol}(S_2)$*.*

(4) $\mathfrak{Sol}(S_1) \cup \mathfrak{Sol}(S_2)$*.*

Proof. For (1) just compute a THOMAS decomposition of $S_1 \cup S_2$.

Turn to (2). Let $k = |S|$ and p_i the i-th smallest polynomial in S according to the ranking, $1 \le i \le k$. For $p_1 \in S^=$ define $S^{(1)} := \{p_1 \neq 0\}$ and $T^{(1)} := \{p_1 = 0\}$. For $p_1 \in S^{\neq}$ define $S^{(1)} := \{p_1 = 0\}$ and $T^{(1)} := \{p_1 \neq 0\}$. Let $2 \le i \le k$. For $p_i \in S^=$ define $S^{(i)} := T^{(i-1)} \cup \{p_i \neq 0\}$ and $T^{(i)} := T^{(i-1)} \cup \{p_1 = 0\}$. For $p_i \in S^{\neq}$ define $S^{(i)} := T^{(i-1)} \cup \{p_i = 0\}$ and $T^{(i)} := T^{(i-1)} \cup \{p_1 \neq 0\}$. Claim that $\bigcup_{1 \le i \le k} \mathsf{Decompose}(S^{(i)})$ is a THOMAS decomposition of $\overline{F}^n \setminus \mathfrak{Sol}(S)$. For this show first disjointness of the solution sets of the $S^{(i)}$, second that the $S^{(i)}$ have no solution in common with S, and third that all elements that are not solutions of S are a solution of some $S^{(i)}$. For the first point it is clear by induction that the solutions of $S^{(i)}$ and $T^{(i)}$ are disjoint for all i. Then $T^{(j)} \subset S^{(i)}$ for $j < i$ implies the disjointness of $S^{(i)}$ and $S^{(j)}$. The second point follows as $p_i = 0$ in S implies $p_i \neq 0$ in $S^{(i)}$ and $p_i \neq 0$ in S implies $p_i = 0$ in $S^{(i)}$ for all $1 \le i \le k$. For the third point, let $\mathbf{a} \in \overline{F}^n \setminus \mathfrak{Sol}(S)$. Then, there exists a minimal i such that $\phi_{\mathbf{a}}(p_i) \neq 0$ if $p_i \in S^=$ or $\phi_{\mathbf{a}}(p_i) = 0$ if $p_i \in S^{\neq}$. Then, $\mathbf{a} \in \mathfrak{Sol}(S^{(i)})$.

Now, $\mathfrak{Sol}(S_1) \setminus \mathfrak{Sol}(S_2) = \mathfrak{Sol}(S_1) \cap \left(\overline{F}^n \setminus \mathfrak{Sol}(S_2)\right)$ and $\mathfrak{Sol}(S_1) \cup \mathfrak{Sol}(S_2) = (\mathfrak{Sol}(S_1) \setminus \mathfrak{Sol}(S_2)) \uplus (\mathfrak{Sol}(S_1) \cap \mathfrak{Sol}(S_2)) \uplus (\mathfrak{Sol}(S_2) \setminus \mathfrak{Sol}(S_1))$ imply (3) and (4). □

Proof (Correctness of Algorithm 1.32). First, note that it is easily verified that the input specifications of all subalgorithms are fulfilled (in particular, for lines 14 and 29, cf. Remark 1.17.(1)).

The following two loop invariants prove correctness of the $\mathsf{Decompose}$ algorithm.

(1) $P \cup \mathit{Result}$ is a disjoint decomposition of the input S'.

(2) For all systems $S \in P \cup \mathit{Result}$, S_T is triangular and

   (a) $\phi_{<x,\mathbf{a}}(p)$ is square-free and
   (b) $\phi_{\mathbf{a}}(\mathrm{init}(p)) \neq 0$

   for all $p \in S_T$ with $\mathrm{ld}(p) = x$ and all $\mathbf{a} \in \mathfrak{Sol}(S_{<x})$.

Begin with the first loop invariant. At the beginning of the algorithm, the loop invariant holds, as $P \cup \mathit{Result} = \{S'\}$. Assume that $P \cup \mathit{Result}$ is a disjoint decomposition of S' at the beginning of the main loop. It suffices to show that all systems added to P or *Result* add up to a disjoint decomposition of the system S, that is chosen in line 3. If $S_Q = \emptyset$ holds in line 4, the algorithm just moves S from P to *Result*.

In line 17, adding $\mathrm{res}_0((S_T)_x, q, x)_=$ to S does not change the solutions of S, as for each $\mathbf{a} \in \overline{F}^n$ the univariate polynomials $\phi_{<x,\mathbf{a}}((S_T)_x)$ and $\phi_{<x,\mathbf{a}}(q)$ have a common zero if and only if their resultant $\mathrm{res}_0(\phi_{\mathbf{a}}((S_T)_x), \phi_{\mathbf{a}}(q), x) \sim \phi_{\mathbf{a}}(\mathrm{res}_0((S_T)_x, q, x))$ is zero.

Note now that if (S, S_i) is the output of any of the $\mathsf{ResSplitGcd}$, $\mathsf{InitSplit}$, $\mathsf{ResSplitSquareFree}$ and $\mathsf{ResSplitDivide}$ algorithms, then $(S \cup \{q\}, S_i)$ is a disjoint decomposition of $S_0 \cup \{q\}$, where S_0 is the input of the respective algorithm. It remains to be shown that lines 15, 25, 30, 36 and 38 are equivalent to putting q back into the system S.

Let $\mathbf{a} \in \mathfrak{Sol}(S_{<x})$. In the context of line 15, $\mathsf{ResSplitGCD}$ guarantees

$$\phi_{<x,\mathbf{a}}(p) = 0 \Longleftrightarrow \phi_{<x,\mathbf{a}}((S_T)_x) = 0 \text{ and } \phi_{<x,\mathbf{a}}(q) = 0 \;.$$

In the context of line 30, ResSplitDivide ensures that

$$\phi_{<x,\mathbf{a}}(p) = 0 \Longleftrightarrow \phi_{<x,\mathbf{a}}((S_T)_x) = 0 \text{ and } \phi_{<x,\mathbf{a}}(q) \neq 0 \ .$$

In lines 25, 36 and 38, p has the same solutions as q, due to ResSplitSquareFree and

$$\phi_{<x,\mathbf{a}}(p) \sim \frac{\phi_{<x,\mathbf{a}}(q)}{\gcd(\phi_{<x,\mathbf{a}}(q), \phi_{<x,\mathbf{a}}(\frac{\partial}{\partial x}q))} = \frac{\phi_{<x,\mathbf{a}}(q)}{\gcd(\phi_{<x,\mathbf{a}}(q), \frac{\partial}{\partial x}\phi_{<x,\mathbf{a}}(q))} \ .$$

In addition, in line 36,

$$\phi_{<x,\mathbf{a}}(r) \sim \frac{\phi_{<x,\mathbf{a}}((S_T)_x)}{\gcd(\phi_{<x,\mathbf{a}}((S_T)_x), \phi_{<x,\mathbf{a}}(p))}$$

implies

$$\phi_{<x,\mathbf{a}}(r \cdot p) \sim \operatorname{lcm}(\phi_{<x,\mathbf{a}}((S_T)_x), \phi_{<x,\mathbf{a}}(p)) \ .$$

This concludes the proof of the first loop invariant.

Now, prove the second loop invariant. At the beginning, the loop invariant holds because $S'_T = \emptyset$ holds for the input system S'. Assume that the second loop invariant holds at the beginning of the main loop.

One easily checks that all steps in the algorithm allow only one polynomial $(S_T)_x$ in S_T for each leader x, thus triangularity obviously holds.

Show that all polynomials added to S_T have non-zero initial and are square-free. For $\mathfrak{Sol}(S_{<x}) = \emptyset$, the statement is trivially true. So, let $\mathbf{a} \in \mathfrak{Sol}(S_{<x})$.

For the equation $p_=$ added as conditional gcd of $(S_T)_x$ and q in line 15, it holds that $\phi_{<x,\mathbf{a}}(p)$ is a divisor of $\phi_{<x,\mathbf{a}}((S_T)_x)$. As $\phi_{<x,\mathbf{a}}((S_T)_x)$ is square-free by assumption, so is $\phi_{<x,\mathbf{a}}(p)$. The inequation added to S in ResSplitGCD is by Definition 1.21 the initial of $p_=$.

The equation $p_=$ inserted into S_T in line 25 and the inequation $p_{\neq}$ inserted in line 38 are square-free due to ResSplitSquareFree, and their initials are non-zero as p is either identical to q, or it is a pseudo quotient of q by $\mathrm{SPRS}_i\left(q, \frac{\partial}{\partial x}q, x\right)$ for some $i > 0$. On the one hand, if p equals q, the call of InitSplit for q ensures a non-zero initial for p. On the other hand, the polynomial $\mathrm{SPRS}_i\left(q, \frac{\partial}{\partial x}q, x\right)$ has initial $\mathrm{res}_i\left(q, \frac{\partial}{\partial x}q, x\right)$, which is added as an inequation by ResSplitSquareFree. This implies that the initial of the pseudo quotient is also non-zero.

The equation $p_=$ that replaces the old equation $(S_T)_x$ in line 30 is the quotient of $(S_T)_x$ by an inequation. It is square-free, because $\phi_{<x,\mathbf{a}}(p)$ is a divisor of $\phi_{<x,\mathbf{a}}((S_T)_x)$, which is square-free by assumption. Again, p is either identical to $(S_T)_x$ or a pseudo quotient of $(S_T)_x$ by $\mathrm{SPRS}_i\left((S_T)_x, q, x\right)$ for some $i > 0$, and, using the same arguments as in the last paragraph, the initial of p does not vanish.

Finally, consider the inequation $(r \cdot p)_{\neq}$ added in line 36 as a least common multiple of $((S_T)_x)_{\neq}$ and $p_{\neq}$. The inequation $\phi_{<x,\mathbf{a}}(p)$ is square-free and has non-vanishing initial for the same reasons as before. Due to $\phi_{<x,\mathbf{a}}(r) \sim \frac{\phi_{<x,\mathbf{a}}((S_T)_x)}{\gcd(\phi_{<x,\mathbf{a}}((S_T)_x), \phi_{<x,\mathbf{a}}(p))}$, the polynomials $\phi_{<x,\mathbf{a}}(r)$ and $\phi_{<x,\mathbf{a}}(p)$ have no common divisors. As $\phi_{<x,\mathbf{a}}(r)$ divides $\phi_{<x,\mathbf{a}}((S_T)_x)$, using the same arguments as before, $\phi_{<x,\mathbf{a}}(r)$ is square-free and has a non-vanishing initial. This completes the proof of the second loop invariant.

It is obvious that a system S with $S_Q = \emptyset$ for which these loop invariants hold is simple. Thus, the algorithm returns the correct result when it terminates. □

The next issue is termination. The system S chosen from P is treated in one of three ways: It is either discarded, added to *Result*, or replaced in P by at least one new system. For proving that P is empty after finitely many iterations, define an order on the systems and show that it is well-founded (cf. below). Thereby termination follows, since the systems in the tree of systems produced by the algorithm descend with respect to this well-founded order.

For transitive and asymmetric[11] partial orders $<_i$ for $i = 1, \ldots, m$, define the **composite order** " $<$ " $:= [<_1, \ldots, <_m]$ as follows: $a < b$ if and only if there exists $i \in \{1, \ldots, m\}$ such that $a <_i b$ and neither $a <_j b$ nor $b <_j a$ for $j < i$. The composite order is transitive and asymmetric. An order $<$ is **well-founded**, if each $<$-descending chain becomes stationary. If each $<_i$ is well-founded, so is the composite order $<$.

Now define the orders and show their well-foundedness:

Definition and Remark 1.35. Define the order $\prec$ on algebraic systems as the composite order $[\prec_1, \prec_2, \prec_3, \prec_4]$ of the four orders defined below. It is well-founded since the $\prec_i$ are.

(1) For $i = 1, \ldots, n$ define $\prec_{1,y_i}$ by $S \prec_{1,y_i} S'$ if and only if $\operatorname{mdeg}\left((S_T)^{=}_{y_i}\right) < \operatorname{mdeg}\left((S'_T)^{=}_{y_i}\right)$, with $\operatorname{mdeg}\left((S_T)^{=}_{y_i}\right) := \infty$ if $(S_T)^{=}_{y_i}$ is empty. Define the composite order $\prec_1$ as $[\prec_{1,y_1}, \ldots, \prec_{1,y_n}]$. Since degrees can only decrease finitely many times, the orders $\prec_{1,y_i}$ are clearly well-founded and, thus, $\prec_1$ is.

(2) Define a map μ from the set of all systems over R to $\{1, y_1, \ldots, y_n, y_\infty\}$, where $\mu(S)$ is minimal such that there exists an equation $p \in (S_Q)^{=}_{\mu(S)}$ with $\mathsf{Reduce}(S_T, p) \neq 0$, or $\mu(S) = y_\infty$ if no such equation exists. Then, $S \prec_2 S'$ if and only if $\mu(S) < \mu(S')$ with $1 < y_i$ and $y_i < y_\infty$ for $i \in \{1, \ldots, n\}$. The order $\prec_2$ is well-founded since $<$ is well-founded on the finite set $\{1, y_1, \ldots, y_n, y_\infty\}$.

(3) $S \prec_3 S'$ if and only if there is $p_{\neq} \in R^{\neq}$ and a finite (possibly empty) set $L \subset R^{\neq}$ with $\operatorname{ld}(q) < \operatorname{ld}(p)\ \forall\, q \in L$ such that $S_Q \uplus \{p_{\neq}\} = S'_Q \uplus L$ holds. Well-foundedness follows by induction on the highest appearing leader x in $(S_Q)^{\neq}$: For $x = 1$ a system S can only $\prec_3$-decrease by removing one of the finitely many inequations in $(S_Q)^{\neq}$. Assume that the statement is true for all indeterminates smaller x. By the induction hypothesis S can only $\prec_3$-decrease finitely many times without changing $(S_Q)^{\neq}_x$. To further $\prec_3$-decrease S, remove an inequation from $(S_Q)^{\neq}_x$. As $(S_Q)^{\neq}_x$ is finite, this process can only be repeated finitely many times until $(S_Q)^{\neq}_x = \emptyset$. Now, the highest appearing leader in $(S_Q)^{\neq}$ is smaller than x and by the induction hypothesis, the statement is proved.

(4) $S \prec_4 S'$ if and only if $|S_Q| < |S'_Q|$.

Proof (Termination of Algorithm 1.32). Tacitly use the fact that reduction never makes polynomials bigger in the sense of Remark 1.17.(3).

Denote the system chosen from P in line 3 by $\widehat{S}$ and the system added to P in line 43 by S. Prove that the systems $S, S_1, \ldots, S_7$ generated from $\widehat{S}$ are $\prec$-smaller than $\widehat{S}$. For $i = 1, \ldots, 4$ use the notation $S \not\precsim_i S'$ if neither $S \prec_i S'$ nor $S' \prec_i S$ holds.

For $j = 1, \ldots, 7$, $((S_j)_T)^{=} = (\widehat{S}_T)^{=}$ and thus $S_j \not\precsim_1 \widehat{S}$. The properties of Select in Definition 1.29 require that there is no equation in $(\widehat{S}_Q)^{=}$ with a leader smaller than x. However, the equation added to the system S_j returned from $\mathsf{InitSplit}$ is the initial of q, which has a leader smaller than x and does not reduce to 0 (cf. Remark 1.17.(2)).

[11] A relation $\prec$ is asymmetric, if $S \prec S'$ implies $S' \not\prec S$ for all S, S'. Asymmetry implies irreflexivity.

Furthermore, the equations added in one of the subalgorithms based on ResSplit have a leader smaller than x and do not reduce to 0. In each case $S_j \prec_2 \widehat{S}$ is proved.

It remains to show $S \prec \widehat{S}$. If q is reduced to $0_=$, then it is omitted from S_Q and so $S \prec_4 \widehat{S}$. As the system is otherwise unchanged, $S \not\succ_i \widehat{S}, i = 1, 2, 3$ and therefore $S \prec \widehat{S}$ holds. If q is reduced to $c_{\neq}$ for some $c \in F \setminus \{0\}$, then $S \prec_3 \widehat{S}$ and $S \not\succ_i \widehat{S}, i = 1, 2,$ since the only change was the removal of an inequation from S_Q. Otherwise, exactly one of the following cases will occur:

Lines 14-15 set $(S_T)_x$ to $p_=$ of smaller degree than $(\widehat{S}_T)_x$ and 20-25 add $(S_T)_x$ as a new equation. Both cases result in $S \prec_1 \widehat{S}$.

In line 17, $S_T = \widehat{S}_T$ implies $S \not\succ_1 \widehat{S}$. The polynomial q is chosen according to Select (cf. 1.29.(1)), which implies $(\widehat{S}_Q)^{=}_{<x} = \emptyset$ and $(S_Q)^{=}_{<x} = \{\mathrm{res}_0((S_T)_x, q, x)_=\}$. Line 13 ensures $\mathsf{Reduce}(S, \mathrm{res}_0((S_T)_x, q, x)) \neq 0$ and, thus, $S \prec_2 \widehat{S}$ follows.

Consider lines 29-30. If the degree of $(S_T)_x$ is smaller than the degree of $(\widehat{S}_T)_x$, then $S \prec_1 \widehat{S}$. In case the degree doesn't change and $S \not\succ_1 \widehat{S}$ and $(S_Q)^{=} = (\widehat{S}_Q)^{=}$ guarantees $S \not\succ_2 \widehat{S}$. However, q is removed from S_Q and replaced by an inequation of smaller leader, which implies $S \prec_3 \widehat{S}$.

In 31-39, obviously $S \not\succ_i \widehat{S}, i = 1, 2$. As before, q is removed from S_Q and replaced by an inequation of smaller leader, which once more implies $S \prec_3 \widehat{S}$. □

1.3.4 Skew Polynomial Rings and Ore Algebras

This subsection provides the language for compact description of the results of the differential reduction. The goal is to describe the ring $F\{U\}[\Delta]$ of differential operators with functions in $F\{U\}$ as coefficients.

This subsection follows [Rob12] to describe this ring in the context of Ore algebras, similar to many other classes of algebras "acting as linear operators" (cf. [CS98, Chy98, Rob06] as further references). A non-trivial example is the Weyl algebra, i.e. the non-commutative algebras of linear differential operators with polynomial coefficients. There exist Gröbner basis algorithms for many important Ore-algebras and rather general implementations of Ore-algebras, e.g., [LS03, CQR04, CQR07, Rob07].

In this subsection let A be a (not necessarily commutative) F-algebra and domain. Let ∂ be an indeterminate, $\rho : A \to A$ an F-algebra endomorphism and $\delta : A \to A$ a ρ-derivation, i.e. an F-linear map satisfying $\delta(ab) = \rho(a)\delta(b) + \delta(a)b$ for all $a, b \in A$. The **skew polynomial ring** $A[\partial; \rho, \delta]$ is the (not necessarily commutative) F-algebra generated by A and ∂ obeying the commutation rule $\partial a = \rho(a)\partial + \delta(a)$ for all $a \in A$.

If the F-algebra endomorphism $\rho : A \to A$ is injective, then $A[\partial; \rho, \delta]$ is a domain. In this case, the construction of skew polynomial rings can be iterated. Let $\Delta = \{\partial_1, \ldots, \partial_n\}$ be a set of indeterminates for some $n \in \mathbb{Z}_{\geq 0}$. The **Ore algebra**

$$B := A[\partial_1; \rho_1, \delta_1][\partial_2; \rho_2, \delta_2] \ldots [\partial_n; \rho_n, \delta_n]$$

is the (not necessarily commutative) F-algebra generated by A and Δ with relations $\partial_i d = \rho_i(d)\partial_i + \delta_i(d)$ for all $d \in A[\partial_1; \rho_1, \delta_1] \ldots [\partial_{i-1}; \rho_{i-1}, \delta_{i-1}]$ and all $i \in \{1, \ldots, n\}$. The maps ρ_i are F-algebra monomorphisms of $A[\partial_1; \rho_1, \delta_1] \ldots [\partial_{i-1}; \rho_{i-1}, \delta_{i-1}]$, and the δ_i are ρ_i-derivations of $A[\partial_1; \rho_1, \delta_1] \ldots [\partial_{i-1}; \rho_{i-1}, \delta_{i-1}]$ for all $i \in \{1, \ldots, n\}$ subject to

$$\begin{array}{lll} \rho_i(\partial_j) = \partial_j & \rho_i \circ \rho_j = \rho_j \circ \rho_i & \rho_i \circ \delta_j = \delta_j \circ \rho_i \\ \delta_i(\partial_j) = 0 & \delta_i \circ \delta_j = \delta_j \circ \delta_i & \delta_i \circ \rho_j = \rho_j \circ \delta_i \end{array}$$

for all $1 \le j \le i \le n$ as restrictions to $A[\partial_1; \rho_1, \delta_1] \ldots [\partial_{i-1}; \rho_{i-1}, \delta_{i-1}]$.

Denote the ring of linear differential operators[12] over F by $F[\Delta] := F[\partial_1, \ldots, \partial_n] := F[\partial_1; \mathrm{id}_F, \partial_1][\partial_2; \mathrm{id}, \partial_2] \ldots [\partial_n; \mathrm{id}, \partial_n]$. In general it is a non-commutative ring; it is commutative if and only if F is a field of constants, i.e., $\Delta F = \{0\}$. Any ranking induces a term order on $F[\Delta]$. The operation of the derivations ∂_i on $F\{U\}$ extends to a left module operation of $F[\Delta]$ on $F\{U\}$. The ring $F[\Delta]$ of linear differential operators over F is filtered by degree in Δ.

The **ring of differential operators with functions as coefficients** $F\{U\}[\Delta]$ is the iterated skew polynomial ring

$$F\{U\}[\Delta] := F\{U\}[\partial_1; \mathrm{id}_{F\{U\}}, \partial_1][\partial_2; \mathrm{id}, \partial_2] \ldots [\partial_n; \mathrm{id}, \partial_n] \ .$$

$F\{U\}$ is a $F\{U\}[\Delta]$-module, where $F\{U\}$ acts by multiplication and Δ by application.

1.3.5 Differential Thomas Algorithm

This subsection presents an algorithm for the differential Thomas decomposition and shows correctness and termination. Versions of the algorithms InsertEquation and Reduce, modified for the differential case, replace their algebraic counterparts.

The differential version of InsertEquation adds an equation p to $(S_T)^=$, with p not reducible modulo $(S_T)^=$. Then, it removes all polynomials from S_T that have a leader which is derivative of $\mathrm{ld}(p)$; this ensures minimality. In addition, when adding a new equation to $(S_T)^=$, it puts, according to Janet's cone decomposition, all minimal non-reductive prolongations into the queue S_Q; this ensures passivity.

Algorithm 1.36 (InsertEquation).
Input: A system $S' = (S'_T, S'_Q)$ and a polynomial $p_= \in F\{U\}$ not reducible modulo $(S'_T)^=$.
Output: A system S, where $(S_T)^= \subseteq (S'_T)^= \cup \{p_=\}$ is maximal satisfying

$$\emptyset = (\mathrm{ld}(S_T) \setminus \{\mathrm{ld}(p)\}) \cap \{\mathrm{ld}(p)\}_\Delta \quad \text{and}$$
$$S_Q = S'_Q \cup (S'_T \setminus S_T) \cup \{(\partial_i q)_= \mid q \in (S_T)^=, \partial_i \notin \Delta(q, (S_T)^=)\} \ .$$

Algorithm:

$S \leftarrow S'$
$S_T \leftarrow S_T \cup \{p_=\}$
for $q \in S_T \setminus \{p\}$ **do**
  if $\mathrm{ld}(q) \in \{\mathrm{ld}(p)\}_\Delta$ **then**
    $S_Q \leftarrow S_Q \cup \{q\}$
    $S_T \leftarrow S_T \setminus \{q\}$
  end if
end for
Reassign reductive derivations to $(S_T)^=$
$S_Q \leftarrow S_Q \cup \{(\partial_i q)_= \mid q \in (S_T)^=, \partial_i \notin \Delta(q, (S_T)^=)\}$
return S

Correctness and termination are obvious. A non-reductive prolongation might be added to S_Q several times in successive calls of InsertEquation; the implementation remembers which prolongations have been added before to avoid redundant computations.

The basic idea of the reduction is as follows. The Janet partition of certain differential variables into cones finds the unique reductor. This reductor is prolonged and used for a pseudo reduction.

[12] We do not expect confusion about the different meanings of ∂_i here.

Algorithm 1.37 (Reduce).
Input: A differential system $S = (S_T, S_Q)$ and a polynomial $p \in F\{U\}$.
Output: A polynomial q that is not JANET-reducible modulo S_T with the property $\phi_e(p) = 0$ if and only if $\phi_e(q) = 0$ for each $e \in \mathfrak{Sol}_E(S)$.
Algorithm:

1: $x \leftarrow \mathrm{ld}(p)$
2: **while** exists $q_= \in (S_T)^=$ and $\mathbf{i} \in \mathbb{Z}^n_{\geq 0}$ with $\mathbf{i}_j = 0$ for $\partial_j \notin \Delta(q, (S_T)^=)$ such that $\partial_1^{\mathbf{i}_1} \cdot \ldots \cdot \partial_n^{\mathbf{i}_n} \mathrm{ld}(q) = \mathrm{ld}(p)$ and $\mathrm{mdeg}(\partial_1^{\mathbf{i}_1} \cdot \ldots \cdot \partial_n^{\mathbf{i}_n} p) \geq \mathrm{mdeg}(q)$ hold **do**
3: $\quad p \leftarrow \mathsf{prem}(p, \partial_1^{\mathbf{i}_1} \cdot \ldots \cdot \partial_n^{\mathbf{i}_n} q, x)$
4: $\quad x \leftarrow \mathrm{ld}(p)$
5: **end while**
6: **if** $\mathsf{Reduce}(S, \mathrm{init}(p)) = 0$ **then**
7: $\quad$ **return** $\mathsf{Reduce}(S, p - \mathrm{init}(p) x^{\mathrm{mdeg}(p)})$
8: **else**
9: $\quad$ **return** p
10: **end if**

For a meaningful pseudo-reduction, initials (and initials of the prolongations) of reductors should be non-zero. The initial of any non-trivial prolongation of r is $\mathrm{sep}(r)$, and the separant of any square-free equation r is non-zero (cf. [Kol73, §I.8, Lemma 5] or [Hub03b, §3.1]). So, making sure that the equations have non-vanishing initials and are square-free, as in the algebraic case, ensures that reduction modulo all prolongations of r is legitimate. This provides the correctness of the reduction algorithm[13] and is used in Lemma 1.46 to establish a connection between simple algebraic and differential systems.

Termination of the reduction algorithm follows from DICKSON's Lemma 1.38. The differential variables of one differential indeterminate are in bijection to $\mathbb{Z}^n_{\geq 0}$. The leaders appearing in the reduction are a sequence of differential variables where no differential variable is a derivative of a previous one. These sequences are finite, i.e., the ranking $<$ is well-founded.

Lemma 1.38 (DICKSON, [CLO92, 2.4, Theorem 5], [Kol73, §0.17, Lemma 15])**.** *The partial order on $\mathbb{Z}^n_{\geq 0}$ given by componentwise comparison is a well-quasi-ordering, i.e., there is no infinite sequence $a \in \left(\mathbb{Z}^n_{\geq 0}\right)^{\mathbb{Z}_{\geq 0}}$ with $a_i \not\leq a_j$ for all $i < j$.*

As in the algebraic case, say that a polynomial p **reduces to** q **modulo** S_T if $\mathsf{Reduce}(S, p) = q$, and it is **reduced modulo** S_T if it reduces to itself. A polynomial $p \in F\{U\}$ is called **tail reduced** modulo S_T if its **tail** $p - \mathrm{init}(p)\,\mathrm{ld}(p)^{\mathrm{mdeg}(p)}$ and its initial $\mathrm{init}(p)$ are tail reduced modulo S_T, where a monomial in $F\{U\}$ is **tail reduced** modulo S_T if it is reduced modulo S_T.

The reduction algorithm is central for the application of simple differential systems. The first three properties of the algebraic reduction algorithm from Remark 1.17 also apply for the differential reduction algorithm. Furthermore, Proposition 1.66 shows that this algorithm solves the radical ideal membership. The following properties describe the (differential) linear combinations constructed by a reduction. These properties are

[13] In differential algebra, one often distinguishes a (full) differential reduction as used here and a partial (differential) reduction. Partial reduction only employs *proper* derivations of equations for reduction (cf. [Kol73, §I.9] or [Hub03b, §3.2]). This is useful for separation of differential and algebraic parts of the algorithm and for the use of ROSENFELD's Lemma (cf. [Ros59]), which is the theoretical basis for the ROSENFELD-GRÖBNER algorithm (cf. [BLOP09, BLOP95, Hub03b]).

direct consequences of the reduction algorithm Reduce and the properties of the pseudo reduction prem in equation (1.1) on page 31.

Remark 1.39. Let $S = (S_T, S_Q)$ be a differential system with $S^{=} = \{p_1, \ldots, p_s\}$ and $p \in F\{U\}$ with $\mathsf{Reduce}(S, p) = 0$. Then there exists $b_i \in F\{U\}[\Delta]$ (cf. Subsection 1.3.4 for the ring $F\{U\}[\Delta]$) for $i \in \{1, \ldots, s\}$ and $q \in F\{U\}$ with $qp = \sum_{i=1}^{s} b_i p_i$, such that the following additional properties are fulfilled:

(1) q is a (possibly empty) product of the initials and separants of $S^{=}$.

(2) $\operatorname{ord} q \leq \operatorname{ord} p$.

(3) $b_i \in F\{U\}[\Delta(p_i, S^{=})]$ for all $i \in \{1, \ldots, s\}$.

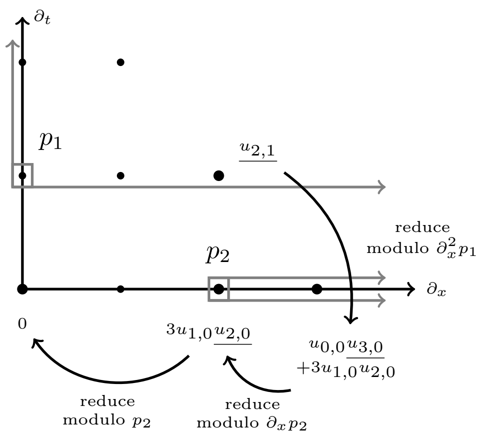
(4) $\operatorname{ord} b_i \leq \operatorname{ord} p$ for all $i \in \{1, \ldots, s\}$.

(5) $\deg_\Delta(b_i) + \operatorname{ord} p_i \leq \operatorname{ord} p$ for all $i \in \{1, \ldots, s\}$.

◁

Example 1.40. This continuation of Example 1.13 treats the remaining differential consequence $(\underline{u_{2,1}})_{=}$ and reduces it modulo the system S with

$$S_T := \left\{ p_1 := (\underline{u_{0,1}} + u_{0,0}u_{1,0})_{=}, p_2 := (\underline{u_{2,0}})_{=} \right\} .$$



The cone generated by $\operatorname{ld}(p_1)$ contains $\operatorname{ld}(\underline{u_{2,1}}) = u_{2,1}$. Thus, reduce $(\underline{u_{2,1}})$ modulo $\partial_x^2 p_1$ where the pseudo reduction yields $u_{0,0}\underline{u_{3,0}} + 3u_{1,0}u_{2,0}$. Second, reduce $u_{0,0}\underline{u_{3,0}} + 3u_{1,0}u_{2,0}$ modulo $\partial_x p_2$, because $u_{3,0}$ lies in the cone generated by $(\underline{u_{2,0}})_{=}$. This results in $3u_{1,0}\underline{u_{2,0}}$ and a third reduction step modulo p_2 produces zero. Thus, the only differential consequence is already implied by the system. Recall that this desirable situation without integrability conditions is called passivity. ◁

Now the differential decomposition algorithm can be stated.

Algorithm 1.41 (Decompose)**.**
Input: A differential system $S' = (\emptyset, S'_Q)$.
Output: A differential THOMAS decomposition of S'.
Algorithm: The algorithm is obtained from the algebraic algorithm Decompose (cf. Algorithm 1.32 and page 39) by replacing the two subalgorithms InsertEquation and Reduce with their differential counterparts Algorithm 1.36 and Algorithm 1.37, respectively.

Proof (Correctness of Algorithm 1.41). The correctness proof of the algebraic decomposition Algorithm 1.32 also holds verbatim for the differential case. In particular, the output is algebraically simple. The following additional three loop invariants for any system $S \in P \cup \mathit{Result}$ show correctness:

(1) $(S_T)^{=}$ is minimal.

(2) No inequation in $(S_T)^{\neq}$ is JANET-reducible modulo S_T.

(3) Let r be any non-reductive prolongation of $(S_T)^=$. Then r reduces to zero by using both conventional differential reductions[14] of $(S_Q)^=$ *and* reductions modulo reductive prolongations of $(S_T)^=$.

The first loop invariant is a purely combinatorial matter proved in [Ger02] for an algorithm using exactly the same combinatorial approach.

The second loop invariant is equally simple. On the one hand, a newly added inequation q in S_T is not JANET-reducible modulo $(S_T)^=$, since algorithm Reduce is applied to it before insertion. On the other hand, algorithm InsertEquation removes all inequations from S_T which are divisible by the newly added equation.

The third loop invariant holds at the beginning of the algorithm, as S_T is empty.

Claim that reduction of an equation $q_= \in S_Q$ by $(S_T)^=$ in line 8 does not affect the loop invariant, i.e. any non-reductive prolongation r reducing to zero beforehand reduces to zero afterwards. Prove this claim by performing a single reduction step on q, which generalizes by an easy induction. Let $q' := \mathsf{prem}(q,p,x) = m \cdot q - \mathsf{pquo}(q,p,x) \cdot p$ be a pseudo remainder identity (see (1.1) on page 31) reducing q to q' modulo p. Then a pseudo remainder identity $\mathsf{prem}(r,q,x) = m' \cdot r - \mathsf{pquo}(r,q,x) \cdot q$ describing a reduction of r modulo q can be rewritten as the iterated identity

$$\underbrace{m \cdot \mathsf{prem}(r,q,x)}_{\mathsf{prem}(\mathsf{prem}(r,p,x),q',x)} = m \cdot m' \cdot r - \mathsf{pquo}(r,q,x) \cdot q' - \mathsf{pquo}(r,q,x) \cdot \mathsf{pquo}(q,p,x) \cdot p.$$

Using the LEIBNIZ rule the same holds for reduction modulo partial derivatives of q. This holds especially for an equation $q_= \in S_Q$ reducing to 0 modulo $(S_T)^=$ in line 8, which can be removed from S_Q without violating the loop invariant.

Show that line 25, where InsertEquation inserts the square-free part $p_=$ of $q_=$ into S_T, does not violate the third loop invariant. First, the non-reductive prolongations in $\{(\partial_i r)_= \mid r \in (S_T)^= \partial_i \notin \Delta(r,(S_T)^=)\}$ are added to S_Q as equations. Thus, any of these reduce to 0 modulo $(S_Q)^=$. Second, moving equations from S_T back into S_Q in InsertEquation does not change the loop invariant either, because their reductive prolongations can still be used for reduction afterwards. Third, every non-reductive prolongation that reduced to zero using $q_= \in (S_Q)^=$ still reduces to zero after InsertEquation. This holds for two reasons. On the one hand, everything that reduces to zero modulo $q_=$, also reduces to zero modulo $p_=$. Write $m \cdot q = p \cdot q_1$ with $\mathrm{ld}(m) < x$ and $\phi_{\mathbf{a}}(m) \neq 0 \ \forall \mathbf{a} \in \mathfrak{Sol}_E(S_{<\mathrm{ld}(q)})$. Then p algebraically pseudo-reduces q to zero. Any derivative ∂q of q is reduced to zero modulo $p_=$ and $(\partial p)_=$, since $\partial(m \cdot q) = (\partial p) \cdot q_1 + p \cdot (\partial q_1)$ for any $\partial \in \Delta$. Inductively, the same holds for repeated derivatives of $q_=$. Therefore, $p_=$ implies all constraints given by $q_=$. On the other hand, all reduction steps modulo $p_=$ are either Janet-reductions modulo $p_=$ w.r.t. S_T or differential reductions modulo non-reductive prolongations of $p_=$. The latter equations have been added to S_Q.

When computing the gcd of two equations in line 14, the gcd of q and $(S_T)_x$ is inserted into S_T and reduces everything to zero that both q and $(S_T)_x$ did. As above, the non-reductive prolongations are covered by inserting them into S_Q, and the reductive prolongations are implied. Dividing an equation $(S_T)_x$ by an inequation $q_{\neq}$ in lines 29 and 30 also influences $(S_T)^=$. The new equation $p_=$, being a divisor of $(S_T)_x$, reduces everything to zero that $(S_T)_x$ and its non-reductive prolongations did by the same arguments as before. This proves the third loop invariant.

[14] i.e. modulo any prolongation

When the algorithm terminates, S_Q is empty and thus all non-reductive prolongations from $(S_T)^=$ Janet-reduce to zero modulo $(S_T)^=$. The system is therefore passive. Furthermore, the first loop invariant implies minimality and the second loop invariant implies that no inequation is reducible by an equation, since for a passive set reducibility is equivalent to Janet-reducibility. □

The termination proof uses six orders on differential systems, similar to the four orders used for the termination of the algebraic decomposition algorithm.

Definition and Remark 1.42. Define the orders $\prec_{1a}$, $\prec_{1b}$, $\prec_{1c}$, $\prec_2$, $\prec_3$, and $\prec_4$ for differential systems, and the composite order "$\prec$" := $[\prec_{1a},\prec_{1b},\prec_{1c},\prec_2,\prec_3,\prec_4]$.

$\prec_{1a}$: For $V \subseteq \{U\}_\Delta$ there is a unique minimal set $\nu(V) \subseteq V$ with $V \subseteq \{\nu(V)\}_\Delta$ [CLO92, Chap. 2, §4, exercise 7 and 8], called **canonical differential generators** of V. For a system S, define $\nu(S)$ as $\nu(\mathrm{ld}((S_T)^=))$. For systems S, S' define $S \prec_{1a} S'$ if and only if $\min_<(\nu(S) \setminus \nu(S')) < \min_<(\nu(S') \setminus \nu(S))$. An empty set is assumed to have y_∞ as minimum, which is $<$-larger than all differential variables. By Dickson's Lemma 1.38, $\prec_{1a}$ is well-founded.

$\prec_{1b}$: For systems S, S' define $S \prec_{1b} S'$ if and only if $S \not\succ\!\!\not\prec_{1a} S'$ and

$$\min_< \left(\mathrm{ld}((S_T)^=) \setminus \mathrm{ld}((S'_T)^=)\right) < \min_< \left(\mathrm{ld}((S'_T)^=) \setminus \mathrm{ld}((S_T)^=)\right) \ .$$

Minimality of $(S_T)^=$ at each step of the algorithm and a property of the Janet division [GB98a, Prop. 4.13] imply well-foundedness of $\prec_{1b}$ [GB98a, Thm. 4.14].

$\prec_{1c}$: For systems S and S' with $S \not\succ\!\!\not\prec_{1a} S'$ and $S \not\succ\!\!\not\prec_{1b} S'$, both $(S_T)^=$ and $(S'_T)^=$ have the same leaders $y_1, \ldots, y_\ell$. Define $S \prec_{1c,y_k} S'$ if and only if $\mathrm{mdeg}((S_T)^=_{y_i}) < \mathrm{mdeg}((S'_T)^=_{y_i})$. This order is clearly well-founded. For these systems define $S \prec_{1c} S'$ as $[\prec_{1c,y_1}, \ldots, \prec_{1c,y_\ell}]$, which is again well-founded as a composite order.

$\prec_2$: As in the algebraic case, define a map μ from the set of all systems over $F\{U\}$ to $\{1\} \cup \{U\}_\Delta \cup \{y_\infty\}$ with $\mu(S)$ minimal such that there exists an equation $p \in (S_Q)^=_{\mu(S)}$ with $\mathsf{Reduce}(S_T, p) \neq 0$ and $\mu(S) = y_\infty$ otherwise. Then, $S \prec_2 S'$ if and only if $\mu(S) < \mu(S')$ with $1 < u^{(j)}_{\mathbf{i}}$ and $u^{(j)}_{\mathbf{i}} < y_\infty$ for all $u^{(j)}_{\mathbf{i}} \in \{U\}_\Delta$. The order $\prec_2$ is well-founded since $<$ is well-founded by Dickson's Lemma.

$\prec_3$: This is verbatim the same condition as in the algebraic case. $S \prec_3 S'$ if and only if there is $p_{\neq} \in R^{\neq}$ and a finite (possibly empty) set $L \subset R^{\neq}$ with $\mathrm{ld}(q) < \mathrm{ld}(p)\ \forall\ q \in L$ such that $S_Q \uplus \{p_{\neq}\} = S'_Q \uplus L$ holds. For well-foundedness do a Noetherian induction instead of an ordinary induction.

$\prec_4$: This is identical to the algebraic case: $S \prec_4 S'$ if and only if $|S_Q| < |S'_Q|$.

Proof (Termination of Algorithm 1.41). Prove termination the same way as in the algebraic case. All arguments where systems get $\prec_2$, $\prec_3$, or $\prec_4$ smaller apply verbatim here. In the algebraic case a system $\prec_1$-decreases if and only if either an equation is added to S_T or the degree of an existing equation in S_T is decreased. Adapt this argument to the differential case: On the one hand, inserting a new equation with a leader that is not yet present in $\mathrm{ld}((S_T)^=)$ decreases either $\prec_{1a}$ or $\prec_{1b}$. On the other hand, if an existing equation in $(S_T)^=$ is replaced by one with the same leader and lower degree, the system $\prec_{1c}$-decreases. Thus, like in the algebraic termination proof, there is a strictly decreasing chain of systems which proves termination. □

1.3.6 An Example

The following example demonstrates a non-trivial application of the differential THOMAS decomposition. The example produces a non-trivial decomposition and deals with many systems. It uses other computer algebra packages, in particular differential equation solvers, to extract additional information from simple differential systems. As the question of this example concerns real solutions instead of non-real (complex) solutions, the example gets rid of systems only having complex solutions. Finally, it deals with certain non-polynomial differential equations, as explained in the following remark.

Remark 1.43. Many differential equations "in nature" are not polynomial in their unknown functions, for example differential equations involving a term of the form $f(u(t))$, e.g., $\sin(u(t))$ or $\sqrt{u(t)}$. Thus, the approach of differential algebra is not directly applicable. However, the THOMAS decomposition can still be applied to many of these cases. If f satisfies $\partial^\ell f = q(f, \partial f, \ldots, \partial^{\ell-1} f) = 0$, then add new dependent variables $g^{(0)}, \ldots, g^{(\ell-1)}$, where $g^{(i)}$ replaces $\partial^i f(u)$. Obviously, the relation $\partial g^{(\ell-1)} = (\partial u) \cdot q(g^{(0)}, g^{(1)}, \ldots, g^{(\ell-1)})$ holds and additionally the chain rule implies $\partial g^{(i)} = (\partial u) \cdot g^{(i+1)}$.

This generalizes to partial differential equations and to functions depending on more than one differential variable. Note that this has the drawback that initial conditions for the additional differential variables $g^{(i)}$ used to model $f(u)$ cannot be set. In particular the relations between the $g^{(i)}$ are no characterization of $f(u)$. ◁

Example 1.44 (LANDAU-LIFSHITZ-GILBERT equations)**.** This example automatically replicates some of the results about the LANDAU-LIFSHITZ-GILBERT equations from [Mül07] using the differential THOMAS decomposition.

```
restart;
with(DifferentialThomas):
with(LinearAlgebra):
with(jets):
```

The LANDAU-LIFSHITZ-GILBERT equations describe a unit magnetization vector

```
m:=<u(t),v(v),w(t)>;
```

$$m := \begin{bmatrix} u(t) \\ v(v) \\ w(t) \end{bmatrix}$$

with three dependent variables u, v, and w as entries.

```
ivar:=[t]:
dvar:=[u,v,w]:
ComputeRanking(ivar,dvar):
m:=<u[0],v[0],w[0]>:
```

Following [Mül07] assume a magnetic field

```
h_eff:=<0,0,h3-lambda*m[3]>;
```

$$h\_eff := \begin{bmatrix} 0 \\ 0 \\ -\lambda w_0 + h_3 \end{bmatrix}$$

for some $\lambda \in \{-1, 0, 1\}$. This means that there is a constant external field in the direction of the w-axis and a self interaction of the magnetic vector in the same direction. Assume an additional spin torgue term counteracting the damping. It is given by the following vector, which is also aligned in direction to the w-axis.

```
j:=<0,0,j3>;
```

$$j := \begin{bmatrix} 0 \\ 0 \\ j_3 \end{bmatrix}$$

Under these additional assumptions the LANDAU-LIFSHITZ-GILBERT equations can be given by the equations

$$(\alpha^2 + 1)\mathbf{m}_t = -\alpha\mathbf{m} \times \mathbf{m} \times \mathbf{h}_{\text{eff}} + \alpha\mathbf{m} \times \mathbf{j} - \mathbf{m} \times \mathbf{h}_{\text{eff}} - \mathbf{m} \times \mathbf{m} \times \mathbf{j}$$

```
LLG:=(alpha^2+1)*map(a->PartialDerivative(a,t),m)
       +CrossProduct(m,h_eff)
       -alpha*CrossProduct(m,CrossProduct(m,h_eff))
       +alpha*CrossProduct(m,j)
       +CrossProduct(m,CrossProduct(m,j)):
```

where α is a positive[15] real number indicating the strength of the damping.

The assumption that the vectors $(0, 0, h_3)$ and $(0, 0, j_3)$ are aligned implies that the LANDAU-LIFSHITZ-GILBERT equations are symmetric with respect to rotations around the w-axis. To show this, we use the MAPLE package `jets` [Bar01] and apply the rotational symmetry around the w-axis. This does not change the equations, i.e., the difference of the original equations and the transformed equations is zero.

```
CallJets(cchvec,[
   [t=t,u[0]=cos(beta)*u[0]-sin(beta)*v[0],
    v[0]=sin(beta)*u[0]+cos(beta)*v[0],w=w],
   [[LLG[1],[u[0]]],[LLG[2],[v[0]]],[LLG[3],[w[0]]]],
   ivar,dvar]):
```

```
simplify(LLG-convert(map(a->a[1],%),Vector));
```

$$\begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

This shows that all periodic solutions must be parallel to the equator, so add $\frac{\mathrm{d}}{\mathrm{d}\,t}w(t) = 0$ to the set of equations.

```
LLG:=[op(convert(LLG,list)),w[1]]:
```

The assumption that the magnetization vector has unit length has another consequence.

```
u(t)^2+v(t)^2+w(t)^2-1=0;
LLG:=[op(LLG),Diff2JetList(lhs(%))]:
```

$$(u(t))^2 + (v(t))^2 + (w(t))^2 - 1 = 0$$

The parameters α, λ, j_3, h_3 can be modelled by a differential indeterminates whose derivative is zero (cf. Remark 1.2).

```
LLG:=[op(LLG),alpha[1],j3[1],h3[1],lambda[1]]:
```

We use the inequation $\alpha \neq 0$, as $\alpha > 0$ is impossible in the complex setting. With hindsight, add the inequation $\alpha^2 + 1 \neq 0$ for α. This inequation is implied as α is a positive real constant, and it removes several systems of non-real (complex) solutions from the THOMAS decomposition. At last, assume that the external field and the spin torque are non-degenerate, i.e., that h_3 and j_3 are non-zero.

```
ineq:=[alpha[0],alpha[0]^2+1,h3[0],j3[0]]:
```

[15] Follow the convention of [Cim07] instead of [Mül07], which switches the signs of α and thereby has $\alpha > 0$ instead of $0 > \alpha$. Thereby, we can circumvent the inconsistency in the notation in [Mül07] assuming $\alpha > 0$ at the beginning of the introduction and silently switching to $0 > \alpha$ beginning from equation (2). As a consequence, some of the signs in our results differ from [Mül07].

Compute a THOMAS decomposition of this system.

```
ComputeRanking(ivar,[op(dvar),alpha,j3,h3,lambda]);
res:=DifferentialThomasDecomposition(LLG,ineq):
nops(res);
```

$$24$$

It consists of 24 simple systems. However, many of these systems contain only non-real (complex) solutions. Remove the systems with the following four pairs of constraints:

$$\begin{aligned} u(t)^2 + v(t)^2 &= 0, & v(t) &\neq 0; \\ j_3^2 + (h_3 - \lambda)^2 &= 0, & (h_3 - \lambda) &\neq 0; \\ j_3^2 + (h_3 + \lambda)^2 &= 0, & (h_3 + \lambda) &\neq 0; \\ j_3^2 + 4\lambda^2 &= 0, & \lambda &\neq 0. \end{aligned}$$

```
res:=remove(a->
   DifferentialSystemReduce(a,u[0]^2+v[0]^2)=0
      and v[0] in DifferentialSystemInequations(a), res):
res:=remove(a->
    DifferentialSystemReduce(a,j3[0]^2+(h3[0]-lambda[0])^2)=0
       and h3[0]-lambda[0] in DifferentialSystemInequations(a), res):
res:=remove(a->
   DifferentialSystemReduce(a,j3[0]^2+(h3[0]+lambda[0])^2)=0
      and h3[0]+lambda[0] in DifferentialSystemInequations(a), res):
res:=remove(a->
   DifferentialSystemReduce(a,j3[0]^2+4*lambda[0]^2)=0
      and lambda[0] in DifferentialSystemInequations(a), res):
nops(res);
```

$$6$$

We go through the remaining 6 systems. The simplicity of these systems allows to easily work with these systems. Furthermore, solutions with different behavior are split apart into different systems, and they can be examined individually.

The generic system results from the input by incorporating some inequations needed to imply the simplicity and by modifying the equations to equivalent equations. Thus, much information about the LANDAU-LIFSHITZ-GILBERT equations in this setup can be read off this system. First we observe the equation $\alpha h_3(t) - \alpha\lambda w(t) - j_3(t) = 0$ holds.

```
PrettyPrintDifferentialSystem(res[1])[3];
GenericEquation:=Diff2JetList(lhs(%)):
```

$$-\alpha(t)\,\lambda(t)\,w(t) + \alpha(t)\,h_3(t) - j_3(t) = 0$$

This equation holds whenenever $w(t) \neq \pm 1$. Confirm this for all systems:

```
map(b->DifferentialSystemReduce(b,w),
   select(
      a->0<>DifferentialSystemReduce(a,
         GenericEquation),
   res)
);
```

$$[-1, 1]$$

Thus, $w(t) = \pm 1$ in all systems where $\alpha h_3(t) - \alpha\lambda w(t) - j_3(t) = 0$ does not hold.

The simplicity allows to solve this system (and also the following ones). However, to simplify the solutions effectively, MAPLE should work with real numbers.

```
with(RealDomain):
```

We make some assumptions about signs of trigonometric functions to get a simplified form. Making the opposite assumption on this sign changes other signs in the solutions.

```
sol:=MyPDSolve(res[1]):
l:=[
   subs(sol,alpha(t))=alpha,subs(sol,lambda(t))=lambda,
   subs(sol,j3(t))=j3,subs(sol,h3(t))=h3]:
u(t)=simplify(factor(subs(l,subs(sol,u(t)))),trig) assuming alpha>0:
simplify(%) assuming cos(j3*signum(lambda)*(-t+_C5)/alpha)>0:
subs([-j3+alpha*h3+alpha*lambda=c1,-j3+alpha*h3-alpha*lambda=c2],%):
simplify(subs([c2=c3/c1],%)):
subs(c3=(-j3+alpha*h3+alpha*lambda)*(-j3+alpha*h3-alpha*lambda),%):
subs(signum(lambda)=lambda,%);
```

$$u(t) = \sqrt{-(\alpha h_3 - \alpha\lambda - j_3)(\alpha h_3 + \alpha\lambda - j_3)} \cos\left(\frac{j_3\lambda(C_5-t)}{\alpha}\right) \alpha^{-1} (|\lambda|)^{-1}$$

```
v(t)=simplify(factor(subs(l,subs(sol,v(t)))),trig) assuming alpha>0:
simplify(%) assuming cos(j3*signum(lambda)*(-t+_C5)/alpha)>0:
subs(signum(lambda)=lambda,%);
```

$$v(t) = -\sqrt{-(\alpha h_3 - \alpha\lambda - j_3)(\alpha h_3 + \alpha\lambda - j_3)} \sin\left(\frac{j_3\lambda(C_5-t)}{\alpha}\right) \alpha^{-1}\lambda^{-1}$$

```
w(t)=subs(l,subs(sol,w(t)));
```

$$w(t) = \frac{\alpha h_3 - j_3}{\alpha\lambda}$$

In this case u and v are phase shifted, and the angular velocity is $\pm\frac{j_3}{\alpha}$, as $\lambda \in \{-1, 0, 1\}$. The solutions are real if and only if

```
factor(subs([j3=j3_durch_alpha*alpha,lambda=1],
   -(-j3+alpha*h3-alpha*lambda)*(-j3+alpha*h3+alpha*lambda)))>0:
solve(subs(alpha=1,%),j3_durch_alpha) assuming j3_durch_alpha>0:
subs(j3_durch_alpha=j3/alpha,%);
```

$$\left\{\frac{j_3}{\alpha} < h_3 + 1, h_3 - 1 < \frac{j_3}{\alpha}\right\}$$

holds. (This last computation yields the same results for $\lambda = -1$.)

We move on to the second system.

```
sol:=MyPDSolve(res[2]):
l:=[
   subs(sol,alpha(t))=alpha,subs(sol,lambda(t))=lambda,
   subs(sol,j3(t))=j3,subs(sol,h3(t))=h3]:
u(t)=simplify(factor(subs(l,subs(sol,u(t)))),trig) assuming alpha>0:
simplify(%) assuming cos(j3*lambda*(-t+_C4)/alpha)>0:
subs(signum(lambda)=lambda,%);
```

$$u(t) = j_3\ (2\alpha\lambda - j_3) \left|\cos\left(\frac{j_3\lambda\ (C_4 - t)}{\alpha}\right)\lambda^{-1}\right| \alpha^{-1} \left(\sqrt{j_3\ (2\alpha\lambda - j_3)}\right)^{-1}$$

```
v(t)=simplify(factor(subs(l,subs(sol,v(t)))),trig) assuming alpha>0:
simplify(%) assuming cos(j3*lambda*(-t+_C4)/alpha)>0:
subs(signum(lambda)=lambda,%):
simplify(%) assuming cos(j3*lambda*(-t+_C4)/alpha)>0;
```

$$v(t) = -\sqrt{j_3\ (2\alpha\lambda - j_3)} \sin\left(\frac{j_3\lambda\ (C_4 - t)}{\alpha}\right) \alpha^{-1}\lambda^{-1}$$

```
w(t)=subs(l,subs(sol,w(t)));
```

$$w(t) = \frac{\alpha\lambda - j_3}{\alpha\lambda}$$

The "real" differential equations (in contrast to the parameter equations) are the same as in the last system with the additional constraint $h_3 = \lambda$. Similarly, the third system has the constraint $h_3 = -\lambda$.

These first three systems included the constraint $\lambda \neq 0$. In contrast, in the fourth system $\lambda = 0$ holds. It is a special case of the generic first systems with the following solutions.

```
sol:=MyPDSolve(res[4]):
l:=[
   subs(sol,alpha(t))=alpha,subs(sol,lambda(t))=lambda,
   subs(sol,j3(t))=j3,subs(sol,h3(t))=h3]:
u(t)=simplify(factor(subs(l,subs(sol,u(t)))),trig) assuming alpha>0:
simplify(%) assuming cos(h3*(-t+_C4))>0:
subs(signum(lambda)=lambda,%);
```

$$u(t) = \sqrt{-C_1{}^2 + 1}\cos(h_3\ (C_4 - t))$$

```
v(t)=simplify(factor(subs(l,subs(sol,v(t)))),trig) assuming alpha>0:
simplify(%) assuming cos(h3*(-t+_C4))>0:
subs(signum(lambda)=lambda,%);
```

$$v(t) = -\sin(h_3\ (C_4 - t))\sqrt{-C_1{}^2 + 1}$$

```
w(t)=subs(l,subs(sol,w(t)));
```

$$w(t) = C_1$$

The angular velocity seems independent of α for this system. However, the equation

```
JetList2Diff(DifferentialSystemEquations(res[4])[4])=0;
```

$$\alpha(t)\, h_3(t) - j_3(t) = 0$$

is included in this system and, thus, the angular velocity is still $\pm\frac{j_3}{\alpha}$.

The last two systems have the constant solution at the south pole and north pole.

```
MyPDSolve(res[5]);
```

$$\{\alpha(t) = C_3, h_3(t) = C_1, j_3(t) = C_2, \lambda(t) = C_4, u(t) = 0, v(t) = 0, w(t) = -1\}$$

```
MyPDSolve(res[6]);
```

$$\{\alpha(t) = C_3, h_3(t) = C_1, j_3(t) = C_2, \lambda(t) = C_4, u(t) = 0, v(t) = 0, w(t) = 1\}$$

Summing up, the Landau-Lifshitz-Gilbert equations with an additional spin torque term aligned to the self interaction have the following cyclic solutions and equilibrium points. The first four systems show that for $\frac{j_3}{\alpha} \in (h_3 - 1, h_3 + 1)$ there is a periodic cycle with angular velocity $\frac{j_3}{\alpha}$. The last two systems show that there are equilibrium points at $(u(t), v(t), w(t)) = (0, 0, \pm 1)$. ◁

1.3.7 Implementation

This subsection describes the implementation of the differential Thomas decomposition algorithm in the Maple [map] package `DifferentialThomas` [BLH12]. It also lists some typical optimizations to make the computations feasible and other implementations of triangular decomposition algorithms.

First, list some commands of this implementation not yet presented in the overview Section 1.1. The commands `Leader`, `Separant`, and `Initial` compute the leader, separant, and initial, respectively, for a given differential polynomial. The command `DifferentialSystemReduce` computes the result of a pseudo reduction with respect to a given system, `DifferentialSystemNormalForm` additionally divides the result of this pseudo reduction by the initials and separants that were multiplied to the input, and `DifferentialSystemLinearCombination` additionally outputs the linear combination (coefficients in $F\{U\}[\Delta]$) of the result. Using Proposition 1.34, the command `ComplementOfDecomposition` computes a Thomas decomposition of the complement of the solutions of a list of disjoint simple systems. Both commands `RemoveSuperfluousInequations` and `SimplifyInequationsInDifferentialSystem` apply certain heuristics to remove and simplify inequations in a simple differential system without changing the set of solutions. Further commands for invariants of the differential ideal associated to a simple differential system are described in Subsection 1.6.4.

Run time bounds for any algorithm in differential algebra are high. For example, a bound for orders in the differential Nullstellensatz is given in [GKOS09] by the Ackermann function. In contrast to these off-putting bounds, examples "from nature" have decent runtime in practice, as soon as algorithmic optimizations are used. Some of these optimizations used in the Decompose algorithm are described now.

Pseudo remainder sequences for the same pairs of polynomials are usually needed several times in different branches of the Decompose algorithm. As these calculations are expensive in general, the implementation always keeps the results in memory and reuses them when the same pseudo remainder sequence is requested again to *avoid repeated computations*.

To avoid coefficient growth, polynomials should be represented as compact as possible. Once the initial of a polynomial is known to be non-zero, the *content* of a polynomial (in the univariate sense) is non-zero, too. Thus, every time an initial is added to the system as an inequation, divide the polynomial by its content. Additionally, the multivariate content, which is an element of the field F, can be removed.

The reduction algorithms 1.15 and 1.37 do not recognize that non-leading coefficients are zero. However, one can reduce the coefficients modulo the polynomial equations of lower leader, in addition to reduction of the polynomial itself. Thereby, in some cases the sizes of coefficients decrease, in other cases they increase. The latter is partly due to multiplying the whole polynomials with the initials of the reductors. Finding a good heuristic for this *coefficient reduction* is crucial for efficiency. For testing examples it turns out that after each reduction done in the algorithm, one should to a tail reduction. Further tail reduction for the equations in a system, e.g., when new equations are present, do not speed up an implementation. To get a smaller output, it is usually good to do a tail reduction for the final systems.

Factorization of a polynomial improves computation time in many cases. More precisely, the system $S \uplus \{(p \cdot q)_=\}$ decomposes disjointly into $(S \cup \{p_=\}, S \cup \{p_{\neq}, q_=\})$ and the system $S \cup \{(p \cdot q)_{\neq}\}$ is equivalent to $S \cup \{p_{\neq}, q_{\neq}\}$. In fact, the algorithm keeps inequations factored at all times, which speeds up the computations and allows a better overview over the inequations, even though it contradicts the triangularity. In most cases, the computation of two smaller problems resulting from a factorization is (often much) cheaper than the computation of the big, original problem. This idea extends to factorizations over an extension of the base field: Let $Y_i := \left\{ y_j \mid y_j < y_i, (S_T)^{=}_{y_j} \neq \emptyset \right\}$ and $Z_i := \left\{ y_j \mid y_j < y_i, (S_T)^{=}_{y_j} = \emptyset \right\}$. Assume that $(S_T)^{=}_{y_i}$ is irreducible over the field $F_i := F(Z_i)[Y_i]/\langle (S_T)^{=}_{<y_i} \rangle$ for all $i \in \{1, \ldots, n\}$, where $\langle (S_T)^{=}_{<y_i} \rangle$ is the ideal generated by $(S_T)^{=}_{<y_i}$ in the polynomial ring $F(Z_i)[Y_i]$. Factorization over F_n instead of F may split the polynomial into more factors, but it is not clear whether this improves runtime. Tests show that factorization w.r.t. F should be preferred over factorization w.r.t. extension fields for $F = \mathbb{Q}$.

In the algebraic algorithm, polynomials need not be square-free when they are inserted into the candidate simple system. Efficiency can sometimes be improved by postponing the computation of the square-free split as long as possible. This differential equations need to be made square-free to ensure that their separant is non-zero, i.e.

non-trivial prolongations have a non-zero initial. However, tests show that postponing the square-freeness of inequations yields faster computations.

In the differential case, application of *criteria* can decrease computation time by avoiding useless reductions of non-reductive prolongations. JANET's combinatorial approach already avoids many reductions of Δ-polynomials, as used in other approaches (see [GY06]). In addition, use the involutive criteria 2-4 (cf. [GB98a, Ger05, AH05]), which together are equivalent to the chain criterion. Applicability of this criterion in the nonlinear differential case was shown in [BLOP09, §4, Prop. 5].

The algorithm should detect the inconsistencies as early as possible to discard them. One of the problems is that selection strategies postpone the costly treatment of inequations. A test detecting whether inequations in S_Q reduce to zero is comparably cheap and shows a big speed-up.

Another possible improvement is parallelization, since the main loop in Decompose (1.32) can naturally be used in parallel for different systems.

The axioms of a selection strategy (see Definition 1.29) already strongly limit the choice for the polynomial considered in the current step. However, the remaining freedom is another important aspect for the speed of an actual implementation. Consider two main approaches to selection strategies (see Definition 1.29).

(1) The "equations first" strategies: Select only chooses an inequation if Q does not contain any equations. Among the equations or inequations, it prefers the ones with smallest leader.

(2) The "leader first" strategies: Select always chooses an equation or inequation with the smallest leader occurring in Q. If there are both equations and inequations with that leader, it chooses an equation.

In experimental observation "leader first" strategies usually produce decompositions with less systems, while "equations first" strategies are more efficient.

Other systems perform a decomposition similar to the THOMAS decomposition (for benchmarks see [BGLHR12]).

The RegularChains package [LMMX05] is shipped with recent versions of MAPLE [map]. Its Triangularize command implements a decomposition of an algebraic variety given by a set of equations by means of regular chains. If the input also contains inequations, the resulting decomposition is represented by regular systems instead. It is possible to make these decompositions disjoint using the MakePairwiseDisjoint command.

The ϵpsilon package by [Wan03] implements different kinds of triangular decompositions in MAPLE. It is the only software package independent of this work that implements the algebraic THOMAS decomposition. It closely resembles the approach that [Tho37, Tho62] suggested, i.e., polynomials of higher leader are considered first. All polynomials of the same leader are combined into one common consequence, resulting in new conditions of lower leader. These are not taken into account right away and will be treated in later steps. Contrary to the approach here, one cannot reduce modulo an *unfinished* system. Therefore, one needs extra inconsistency checks to avoid spending too much time on computations with inconsistent systems. ϵpsilon implements such checks in order to achieve good performance.

The MAPLE packages diffalg [BH04] and DifferentialAlgebra by BOULIER and CHEB-TERRAB deal with ordinary and partial differential equations as described by [BLOP09]. They compute a radical decomposition of a differential ideal, i.e., a description of the vanishing ideal of the KOLCHIN closure [Kol73, §IV.1] of the set of solutions. Computation of integrability conditions is driven by reduction of Δ-polynomials [Ros59, Sect.

2], the analogon of s-polynomials in differential algebra. Just like in RegularChains, this approach does not give disjoint solution sets, although in principle disjointness might be achieved. The diffalg package is superseded by the package DifferentialAlgebra. DifferentialAlgebra is based on the BLAD-libraries [Bou09], a set of stand-alone C-libraries with an emphasis on usability for non-mathematicians and extensive documentation.

In contrast to other algorithms, the THOMAS decomposition only relies on computations over the ground field; neither algebraic [Rit50] nor transcendental [BLOP09, BLOP95] field extensions are necessary. Furthermore, polynomials need not be factored [Rit50] nor inverted [KRMS98].

1.4 Power Series Solutions

> We assume ϕ to be expanded in a TAYLOR series in the neighborhood of a point P (which presupposes the analytic character of ϕ). The totality of its coefficients describes then the function completely.
>
> ALBERT EINSTEIN
> in [Ein53a, First example]

> Some [...] argued that you may always consider any function as analytic [...] as they can be approximated with arbitrary precision by analytic ones. But, in my opinion, this objection would not apply, the question not being whether such an approximation would alter the data very little, but whether it would alter the solution very little.
>
> JACQUES HADAMARD
> in [Had53, I.II, p. 33]

Let F be a differential field of characteristic zero. Let $\Delta = \{\partial_1, \dots, \partial_n\}$ be a non-empty set of derivation operators and $U = \{u^{(1)}, \dots, u^{(m)}\}$ be a non-empty set of differential indeterminates.

Formal or convergent power series solutions are solutions in $\mathbb{C}[[y_1 - \zeta_1, \dots, y_n - \zeta_n]]$ for $\zeta_1, \dots, \zeta_n \in \mathbb{C}$. In contrast, recall the definition of the set of non-centered power series

$$E := \overline{F}[[z_1, \dots, z_n]]^U \cong \bigoplus_{j=1}^{m} \overline{F}[[z_1, \dots, z_n]]$$

from Subsection 1.2.4. Taking them as admissible solutions suits the THOMAS decomposition algorithms in the last section and, using the algebraization isomorphism $\alpha : E \to \overline{F}^{\{U\}_\Delta}$, they are solutions of the differential system viewed as algebraic system. However, they are different from the set of formal or convergent power series solutions, and they can be thought of as formal power series at a generic center of expansion if F is a field of meromorphic functions over $\mathbb{C}$.

Non-centered solutions can be turned into formal power series solutions by substituting the center of expansion into the elements of F if F is a field of meromorphic functions. For example the non-centered power series $(1 + yz + \frac{1}{y}z^2 + \dots) \in \mathbb{C}(y)[[z]]$ yields a formal power series in $\mathbb{C}[[y - \zeta]]$ when substituting z by $y - \zeta$ and y in the coefficients by $\zeta \in \mathbb{C}$. However, two regularity conditions need to be satisfied for this. First, the non-centered solutions need to be regular in the sense that they come from algebraic solutions. Second, the center ζ of expansion needs to be regular in the sense that no poles appear when evaluating the coefficients of the equation at ζ and that initials and separants are not zero when evaluated at ζ. Both kinds of regularities are generic properties. This section introduces these regularity conditions and shows that regular non-centered solutions yield formal power series solutions at regular points and that these formal power series solutions converge for convergent initial conditions. The case of non-regular points or solutions is studied in Chapter 2.

Fix an orderly[16] ranking $<$. Then, there are only finitely many differential variables not ranking higher than any differential variable $u_{\mathbf{i}}^{(j)} \in \{U\}_\Delta$. Denote the polynomial ring of these differential variables by $F\{U\}_{\leq u_{\mathbf{i}}^{(j)}}$ and denote the polynomial ring of all differential variables up to order $\ell \in \mathbb{Z}_{\geq 0}$ by $F\{U\}_{\leq \ell}$.

1.4.1 Regular Non-centered Solutions

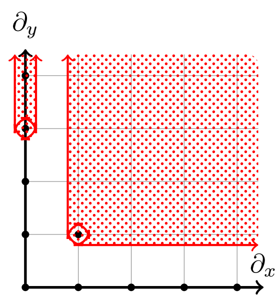
This subsection shows that each simple differential system has a non-centered solution. In doing so, it describes the subset $\mathfrak{Sol}_E^o$ of regular non-centered solutions that allows a good passage to formal power series solutions.

Let S be a simple differential system and $u_{\mathbf{i}}^{(j)} \in \{U\}_\Delta$ a differential variable. Define the **simple algebraic system up to $u_{\mathbf{i}}^{(j)}$ associated to S** as

$$S_{\leq u_{\mathbf{i}}^{(j)}} := \left(\{\delta p \mid p \in S^=, \delta \in \mathrm{Mon}(\Delta(p, S^=))\} \cup S^{\neq}\right) \cap F\{U\}_{\leq u_{\mathbf{i}}^{(j)}} ,$$

where $\mathrm{Mon}(\Delta(p, S^=))$ is the free commutative monoid generated by the reductive prolongations $\Delta(p, S^=)$ from the Janet cone decomposition. Let $\ell \in \mathbb{Z}_{\geq 0}$. Define the **simple algebraic system up to order ℓ associated to S** as $S_{\leq \ell} := S_{\leq u_{\mathbf{i}}^{(j)}}$, where $u_{\mathbf{i}}^{(j)} \in \{U\}_\Delta$ is the largest differential variable of order ℓ w.r.t. the chosen ranking.

Example 1.45. Consider $F = \mathbb{C}(x, y)$, $U = \{u\}$ and $\Delta = \{\partial_x, \partial_y\}$ with respect to the degree-reverse lexicographical ranking. Let $S := \{u_{xy} = 0, u_{yyy} = 0, u_x \neq 0\}$ be a simple system. As indicated by the cones in the diagram, the reductive derivations of the equation u_{xy} are $\Delta(u_{xy}, S^=) = \{\partial_x, \partial_y\}$ and those of u_{yyy} are $\Delta(u_{yyy}, S^=) = \{\partial_y\}$. Some simple algebraic systems associated to S are:



$$S_{\leq 0} = \emptyset, \quad S_{\leq 1} = \{u_x \neq 0\}$$
$$S_{\leq 2} = S_{\leq 1} \uplus \{u_{xy} = 0\}$$
$$S_{\leq 3} = S_{\leq 2} \uplus \{u_{xxy} = 0, u_{xyy} = 0, u_{yyy} = 0\}$$

These systems are simple. This is true in general and explains the name *simple* algebraic system associated to S. ◁

Lemma 1.46. *Let S be a simple differential system and $u_{\mathbf{i}}^{(j)} \in \{U\}_\Delta$ a differential variable. The simple algebraic system $S_{\leq u_{\mathbf{i}}^{(j)}}$ up to $u_{\mathbf{i}}^{(j)}$ associated to S is a simple algebraic system in $F\{U\}_{\leq u_{\mathbf{i}}^{(j)}}$. In particular, this holds for $F\{U\}_{\leq \ell}$.*

Proof. No two inequations with the same leader exist, since $S_{\leq u_{\mathbf{i}}^{(j)}} = S^{\neq} \cap F\{U\}_{\leq u_{\mathbf{i}}^{(j)}}$, which is triangular. No two equations with the same leader exist, since the Janet decomposition into cones is disjoint. No inequation in $S^{\neq}$ is reducible modulo $S^=$, and thus no inequation in $S_{\leq u_{\mathbf{i}}^{(j)}}$ has the same leader as a reductive prolongation of an equation. The triangularity follows.

[16] The results of this section generalize to the case of weighted orderly rankings.

The initials of elements in S do not vanish, since S is simple. The initials of prolongations of equations in S do not vanish, since these initials are the separants of the equations in S, which do not vanish because of the square-freeness.

The elements of S are square-free, since S is a simple algebraic system. The prolongations of equations in S are square-free, since their main degree is 1. $\square$

Let S be a simple differential system in $F\{U\}$. Recall that the set of non-centered power series E are isomorphic to $\overline{F}^{\{U\}_\Delta}$ using the algebraization α (cf. page 28). Using the inverse of α turns (algebraic) solutions of the simple algebraic system associated to S into (differential) non-centered solution. Define the **regular non-centered solutions** of S as

$$\mathfrak{Sol}^o_E(S) := \alpha^{-1}(\bigcap_{\ell\in\mathbb{Z}_{\geq 0}} \mathfrak{Sol}(S_{\leq \ell})) \subseteq E \ ,$$

where the algebraic systems $S_{\leq \ell}$ are considered as systems in $F\{U\}$ instead of $F\{U\}_{\leq \ell}$. These solutions are only defined for *simple* differential systems, as they depend on the Thomas decomposition. Simple systems have a solution by Remark 1.10, hence clearly $\mathfrak{Sol}^o_E(S) \neq \emptyset$.

Lemma 1.47. *Let S be a simple differential system. Then $\mathfrak{Sol}^o_E(S) \subseteq \mathfrak{Sol}_E(S)$, and, in particular, $\mathfrak{Sol}_E(S) \neq \emptyset$.*

Proof. Recall that a non-centered solution of $p_=$ or $q_{\neq}$ is defined as an $e \in E$ with $\phi_e(\{p\}_\Delta) = \{0\}$ or $\phi_e(\{q\}_\Delta) \neq \{0\}$, respectively. If $q \in S^{\neq}$, then $\phi_e(q) \neq 0$ by construction and, thus, $\phi_e(\{q\}_\Delta) \neq \{0\}$. Let $p \in S^=$. By construction $\phi_e(\partial_1^{b_1}\dots\partial_n^{b_n}p) = 0$ for all reductive prolongations $\partial_1^{b_1}\dots\partial_n^{b_n}p$ of p, i.e., for all $\partial_1^{b_1}\cdot\dots\cdot\partial_n^{b_n} \in \Delta(p, S^=)$. So consider $\partial_1^{b_1}\dots\partial_n^{b_n}p$ for general $\partial_1^{b_1}\dots\partial_n^{b_n}$. By the passivity condition for simple systems and Remark 1.39, there is a product q of initials and separants of equations in $S^=$ such that

$$q\cdot\partial_1^{b_1}\dots\partial_n^{b_n}p = \sum_{s\in S^=} c_s(\partial)s$$

for an operator $c_s(\partial) \in F[\Delta(s, S^=)]$. As S is simple, $\phi_e(q) \neq 0$ and by construction $\phi_e(c_s(\partial)s) = 0$ for all $s \in S$. This implies $\phi_e(\partial_1^{b_1}\dots\partial_n^{b_n}\cdot p) = 0$. $\square$

In general, $\mathfrak{Sol}^o_E(S) \neq \mathfrak{Sol}_E(S)$ for S simple:

Example 1.48. Let $F = \mathbb{C}$, $\Delta = \{\partial_t\}$ and $U = \{u\}$, and consider the simple differential system $S := \{u_1 - 1 = 0, u_0 \neq 0\}$. Its sets of solutions are given by

$$\mathfrak{Sol}_E(S) = \{\ z + a \in \mathbb{C}[[z]] \mid a \in \mathbb{C}\ \} \text{ and}$$
$$\mathfrak{Sol}^o_E(S) = \{\ z + a \in \mathbb{C}[[z]] \mid 0 \neq a \in \mathbb{C}\ \}\ .$$

Note that the inequation $u_0 \neq 0$ is satisfied on all solutions of the equation $u_1 - 1 = 0$. $\lhd$

Differential variables can be classified depending on how much freedom of choice they allow for a solution of a simple differential system S. Partition the set of differential variables $\{U\}_\Delta$ into three sets $B^=$, $B^{\neq}$ and B^0. A differential variable belongs to $B^=$ if it lies in the cone generated by equations of S. These differential variables are called **principal**. A differential variable $u_{\mathbf{i}}^{(j)}$ belongs to $B^{\neq}$ and is called **generically parametric** if there is an inequation $q \in S^{\neq}$ with $\mathrm{ld}(q) = u_{\mathbf{i}}^{(j)}$. Because of both the triangularity and reduced inequations (cf. Definition 1.14.(4)), $B^= \cap B^{\neq} = \emptyset$ holds. The differential variables in $B^0 := \{U\}_\Delta \setminus \left(B^= \cup B^{\neq}\right)$ are called **parametric**.

Remark 1.49. Let S be a simple differential system. Any solution $e \in \mathfrak{Sol}_E^o(S)$ satisfies $\phi_e(q) \neq 0$ for any inequation $q_{\neq}$ (cf. proof of Lemma 1.47). However, for a non-centered solution it would suffice that any *derivative* of q is non-zero when evaluated by ϕ_e. It seems algorithmically hard to say whether a choice of a generically parametric power series coefficient yields a non-centered solution. This also means that if S does not have any inequation, then $\mathfrak{Sol}_E^o(S) = \mathfrak{Sol}_E(S)$. Section 2.3 replaces the infinitely many derivations of an inequation by another infinite process, leading to the counting polynomial. ◁

Certain inequations from a simple differential system can be removed. If all solutions of an inequation $q \neq 0$ are solutions of $\{p_1 = 0, \ldots, p_k = 0\}$, then the inequation $q \neq 0$ is superfluous, as is the case if the system $\{p_1 = 0, \ldots, p_k = 0, q = 0\}$ with q inserted as *equation* has no solution. `RemoveSuperfluousInequations` implements this.

1.4.2 Formal Power Series Solutions

This subsection describes how to turn non-centered solutions into formal power series solutions centered around a point $\zeta = (\zeta_1, \ldots, \zeta_n) \in \mathbb{C}^n$. Many results of this section are similar to the ones in [P97], which shows these results without the detour over non-centered solutions. Assume without loss of generality[17] for the rest of this section that the differential field F is a field of meromorphic functions in n complex variables $y_1, \ldots, y_n$ defined on $\mathbb{C}^n$, as all statements are local, and $\partial_i = \frac{\partial}{\partial y_i}$. Additionally, for better legibility, assume for the rest of this section, that F contains the complex numbers. This means that the field of constants of F is $\mathbb{C}$, where an element $f \in F$ is called a **constant** if $\Delta f = \{0\}$ and the set of constant elements of F is called the **field of constants** of F. If F is equal to its field of constants, then F is called field of constants.

The meromorphic functions in F can be evaluated at the point ζ. Denote by ψ_ζ the **evaluation** of elements in F **at the point** ζ, i.e.,

$$\psi_\zeta : F \to \mathbb{C} \cup \{\infty\} : f(y_1, \ldots, y_n) \mapsto f(\zeta_1, \ldots, \zeta_n) \ .$$

In the following, meromorphic functions are only evaluated at points which are not poles. By abuse of notation extend ψ_ζ to $F\{U\} \to \mathbb{C}\{U\} \cup \{\infty\}$ and to $E \mapsto \mathbb{C}[[y_1 - \zeta_1, \ldots, y_n - \zeta_n]]^U \cup \{\infty\}$ by applying it to every coefficient, substituting z_i by $y_i - \zeta_i$, and assigning ∞ if one coefficient has a pole.

Example 1.50. Consider the ordinary linear differential equation $p := y^2 u_1 - u + y = 0$ over the differential field $F = \mathbb{C}(y)$. The set of non-centered solutions depends on one parameter $a_0 \in F$, and each such solutions is of the following form.

$$e(a_0) := a_0 + \frac{a_0 - y}{y^2} z^1 + \frac{(1-2y)a_0 + y^2 - y}{y^4} \frac{z^2}{2} + \ldots \in E$$

Any $0 \neq \zeta \in \mathbb{C}$ specializes such a solution to a formal power series solution

$$\psi_\zeta(e(a_0)) = a_0 + \frac{a_0 - \zeta}{\zeta^2} \frac{(y-\zeta)^1}{1!} + \frac{(1-2\zeta)a_0 + \zeta^2 - \zeta}{\zeta^4} \frac{(y-\zeta)^2}{2!} + \ldots \in \mathbb{C}[[y - \zeta]] \ .$$

The set of these formal power series solutions depends on one parameter as the set of non-centered solutions, and all formal power series converge locally (cf. Theorem 1.60).

[17] A differential system can be considered over the differential field generated by its coefficients. Such a field is finitely differentially generated and Seidenberg's embedding theorem (cf. [Sei58, Sei69]) applies. This theorem states that every finitely differentially generated differential field of characteristic zero is differentially isomorphic to a differential field of meromorphic functions in n complex variables.

There is a different behavior around the center $\zeta = 0$, which is a zero of the initial of p. A computations yields a unique formal power series

$$\sum_{i=1}^{\infty}(i-1)!\,y^i \in \mathbb{C}[[y]]$$

there, and this formal power series does not converge in any neighborhood.

Thus, the number of formal power series solutions depends on the center ζ. ◁

We use three regularity conditions[18] for the point ζ with respect to a system S. The first condition implies that no poles appear in S at ζ, the second condition implies that finding solutions of S is easy at ζ, and the third condition implies that a THOMAS decomposition can be sensibly interpreted around ζ.

Definition 1.51. Let S be a (*not* necessarily simple) differential system over F. A point $\zeta \in \mathbb{C}^n$ is called **weakly regular** with respect to S if $\psi_\zeta(p) \neq \infty$ for all $p \in S$.

Let S be a *simple* differential system over F. Then a point $\zeta \in \mathbb{C}^n$ is called **regular** with respect to S if it is weakly regular with respect to S and $\psi_\zeta(\mathrm{init}(p)) \neq 0$ and $\psi_\zeta(\mathrm{sep}(p)) \neq 0$ for all $p \in S$.

Let S be a (*not* necessarily simple) differential system over F. Call $\zeta \in \mathbb{C}^n$ **strongly regular** with respect to S if there is a differential $\mathbb{C}$-subalgebra A of F such that

(1) $\psi_\zeta(a) \in \mathbb{C}$ for all $a \in A$,

(2) $S \subset A\{U\}^{\{=,\neq\}}$, and there is an associated THOMAS decomposition $\{S_1, \ldots, S_k\}$ of S which can be obtained by computations over $A\{U\}$ such that no inequation $q_{\neq}$ with a trivial leader and a zero at ζ is removed (cf. line 7 in Decompose), and

(3) the point ζ is regular with respect to each of the systems $S_1, \ldots, S_k$ of the associated THOMAS decomposition.

We define formal power series solutions in the ring $\mathbb{C}[[y_1 - \zeta_1, \ldots, y_n - \zeta_n]]$ of power series centered around ζ. Therefore, we expand the coefficients of a differential polynomial into formal power series centered around ζ using a map Ψ_ζ, and we substitute the differential variables by suitable derivatives of formal power series centered around ζ. The operation of $\partial_i \in \Delta$ on $\mathbb{C}[[y_1 - \zeta_1, \ldots, y_n - \zeta_n]]$ is given by $\partial_i y_i = 1$ and $\partial_i y_j = 0$ for $i \neq j$. Denote by F_ζ the subring of F whose elements do not have a pole at ζ. A holomorphic function can be expressed locally as a power series, and thus there exists a differential homomorphism of $\mathbb{C}$-algebras

$$\Psi_\zeta : F_\zeta \to \mathbb{C}[[y_1 - \zeta_1, \ldots, y_n - \zeta_n]]$$

called **expansion around** ζ. In contrast to the evaluation ψ_ζ at ζ, the expansion around ζ yields a formal power series. It can be extended to differential polynomials by applying it to the coefficients, which yields a differential homomorphism of $\mathbb{C}$-algebras

$$\Psi_\zeta : F_\zeta\{U\} \to \mathbb{C}[[y_1 - \zeta_1, \ldots, y_n - \zeta_n]]\{U\}\ .$$

Differential variables can be evaluated at a formal power series $f \in \mathbb{C}[[y_1 - \zeta_1, \ldots, y_n - \zeta_n]]^U$ in a differentially compatible way. Formally, define the **differential extension of** f, the homomorphism of differential F-algebras

$$\Phi_f : \mathbb{C}[[y_1 - \zeta_1, \ldots, y_n - \zeta_n]]\{U\} \to \mathbb{C}[[y_1 - \zeta_1, \ldots, y_n - \zeta_n]] : u_{\mathbf{i}}^{(j)} \mapsto \partial^{\mathbf{i}} f(u^j)\ .$$

[18] This is similar to [PR05] and [Rob12, Remark 2.1.66, Remark 2.1.68]. Note that the first source has an omission and the second one gives no proofs.

Now, the usual definition of formal power series solutions can be given in this setting. Let S be a differential system and $\zeta \in \mathbb{C}^n$ a weakly regular point with respect to S. Define the set $\mathfrak{Sol}_{\mathbb{C},\zeta}(S)$ of **formal power series solutions of S around ζ** as

$$\{f \in \mathbb{C}[[y_1 - \zeta_1, \ldots, y_n - \zeta_n]]^U | \Phi_f(\Psi_\zeta(p)) = 0, \Phi_f(\Psi_\zeta(q)) \neq 0 \text{ for all } p \in S^=, q \in S^{\neq}\}.$$

The next theorem yields the connection between formal power series solutions and non-centered solutions.

Theorem 1.52. *Let $F \supseteq \mathbb{C}$ be a differential field of meromorphic functions in n complex variables and $\zeta \in \mathbb{C}^n$ a regular point with respect to a simple differential system S. Let $e \in \mathfrak{Sol}^o_E(S)$ such that no $\phi_e(u^{(j)}_{\mathbf{i}})$ has a pole in ζ for a parametric or generically parametric differential variable $u^{(j)}_{\mathbf{i}}$. Then, $\psi_\zeta(e) \in \mathfrak{Sol}_{\mathbb{C},\zeta}(S)$.*

The proof is postponed to the end of this subsection. Call the set of these formal power series solutions constructed in this theorem **regular formal power series solutions (with respect to S)** and denote them by $\mathfrak{Sol}^o_{\mathbb{C},\zeta}(S)$. This theorem implies the following corollary, as $\mathfrak{Sol}^o_E(S) \neq \emptyset$ for S, and the parametric and generically parametric can be chosen as constants.

Corollary 1.53. *Let $F \supseteq \mathbb{C}$ be a differential field of meromorphic functions in n complex variables and $\zeta \in \mathbb{C}^n$ a regular point with respect to a simple differential system S over $F\{U\}$. Then, $\mathfrak{Sol}_{\mathbb{C},\zeta}(S) \neq \emptyset$.*

The proof of the following proposition shows that the detection of most strongly regular points $\zeta \in \mathbb{C}^n$ with respect to a differential system S over $F\{U\}$ is possible after a Thomas decomposition $\{S_1, \ldots, S_k\}$ of S is computed.

Proposition 1.54. *Let $F = \mathbb{C}(y_1, \ldots, y_n)$ and S a simple differential system over F. The set of strongly regular points with respect to S is Zariski-open in $\mathbb{C}^n$*

Proof. Compute a Thomas decomposition $\{S_1, \ldots, S_k\}$ of S. Let G be a set of all field elements by which one divides during the algorithm. Let $\{T_1, \ldots, T_{k'}\}$ be the set of all intermediate T-lists (cf. Section 1.3) during the algorithm. For each $p \in S_i$ for $1 \leq i \leq k$ or $p \in T_i$ for $1 \leq i \leq k'$ let I'_p be the ideal generated by the F-coefficients of $\mathrm{init}(p)$, I''_p be the ideal generated by the F-coefficients of $\mathrm{sep}(p)$, and $I_p := I'_p \cap I''_p$. Then the set of strongly regular points is given by the complement of the zero set in $\mathbb{C}^n$ of

$$\bigcap_{g \in G} \langle g \rangle \cap \bigcap_{1 \leq i \leq k} \bigcap_{p \in S_i} I_p \cap \bigcap_{1 \leq i \leq k'} \bigcap_{p \in T_i} I_p$$

where all ideals are taken in the polynomial ring $\mathbb{C}[y_1, \ldots, y_n]$. □

The next proposition shows that formal power series solutions are compatible with splitting a system into simple differential systems.

Proposition 1.55. *Let $F \supseteq \mathbb{C}$ be a differential field of meromorphic functions in n complex variables and $\zeta = (\zeta_1, \ldots, \zeta_n) \in \mathbb{C}^n$ a strongly regular point with respect to a system S of differential equations and inequations over $F\{U\}$ and $\{S_1, \ldots, S_k\}$ the associated Thomas decomposition. Then, the set of formal power series solutions around ζ of the systems in this differential Thomas decomposition partitions the set of solutions of S around ζ, i.e.,*

$$\mathfrak{Sol}_{\mathbb{C},\zeta}(S) = \biguplus_{i=1}^{k} \mathfrak{Sol}_{\mathbb{C},\zeta}(S_i) \ .$$

Proof. This follows similar to the proof of the Decompose-algorithms (cf. Algorithm 1.41 and Algorithm 1.32): Every splitting (cf. Split, i.e., Algorithm 1.19) partitions the set of non-centered solutions of the system. This is clearly also true for formal power series solutions centered around ζ. The conditions for strong regularity ensure that one does not divide by zero or get poles during the computation. □

The following lemma is used in the proof of Theorem 1.52.

Lemma 1.56. *Let $F \supseteq \mathbb{C}$ be a differential field of meromorphic functions in n complex variables and $\zeta = (\zeta_1, \ldots, \zeta_n) \in \mathbb{C}^n$ a regular point with respect to a simple differential system S over $F\{U\}$. Let $e \in \mathfrak{Sol}^o_E(S)$ such that no $\phi_e(u^{(j)}_{\mathbf{i}})$ has a pole in ζ for a parametric or generically parametric differential variable $u^{(j)}_{\mathbf{i}}$. Then $\psi_\zeta(e) \in \mathbb{C}[[y_1 - \zeta_1, \ldots, y_n - \zeta_n]]$.*

Proof. For the proof it suffices to show that $\phi_e(u^{(j)}_{\mathbf{i}})$ does not have a pole in ζ for *any* differential variable $u^{(j)}_{\mathbf{i}} \in \{U\}_\Delta$. For principal differential variables show that the zeros of equations solved in the definition of $\mathfrak{Sol}^o_E$ are holomorphic at ζ. These polynomial equations have holomorphic coefficients by the choice of (generically) parametric differential variables, the definition of (weakly) regular points and by induction over the differential variables in order of their ranking. Furthermore, the initial of these polynomials does not have a zero at ζ by the definition of regular points and, hence, the inverse of the initial is still a holomorphic function. Thus, the zero is a zero of a polynomial with initial 1 and holomorphic coefficients. By Hensel's Lemma its zeros are again holomorphic[19]. The claim follows. □

The following lemma clarifies the connection between the different evaluation maps. It can be proved by a lengthy but straight forward computation.

Lemma 1.57. *Let $e \in E$, $p \in F\{U\}$. Then, $\psi_\zeta(\Phi_{\psi_\zeta(e)}(\Psi_\zeta(p))) = \psi_\zeta(\phi_e(p))$ if $\zeta \in \mathbb{C}^n$ regular w.r.t $\{p_=\}$.*

Proof of Theorem 1.52. Lemma 1.56 states that everything done here is well-defined and does not yield poles. Let $p \in S^=$ and $q \in S^{\neq}$. We have to show that $\Phi_{\psi_\zeta(e)}(\Psi_\zeta(p)) = 0$ and $\Phi_{\psi_\zeta(e)}(\Psi_\zeta(q)) \neq 0$. Let $r \in F\{U\}$. The formal power series $\Phi_{\psi_\zeta(e)}(\Psi_\zeta(r)) \in \mathbb{C}[[y_1-\zeta_1, \ldots, y_n-\zeta_n]]$ is zero if and only if all its coefficients are. The coefficient of $(y_1 - \zeta_1)^{i_1} \ldots (y_n - \zeta_n)^{i_n}$ is zero if and only if $\psi_\zeta(\partial^{\mathbf{i}}\Phi_{\psi_\zeta(e)}(\Psi_\zeta(r))) = 0$. Thus, all power series coefficients are zero if and only if $\psi_\zeta(\{\Phi_{\psi_\zeta(e)}(\Psi_\zeta(r))\}_\Delta) = \{0\}$. As $\Phi_{\psi_\zeta(e)}$ and Ψ_ζ are homomorphisms of differential $\mathbb{C}$-algebras this is equivalent to $\psi_\zeta(\Phi_{\psi_\zeta(e)}(\Psi_\zeta(\{r\}_\Delta))) = \{0\}$. The claim follows from Lemma 1.57, as $\phi_e(\{p\}_\Delta) = \{0\}$ and $\phi_e(\{q\}_\Delta) \neq \{0\}$. □

The end of this subsection gives some concluding remarks. First, computing a formal power series solution up to some order is straight forward using reduction. A so-called quadratic Newton-like method exists for regular differential systems [HLR03]. However, contrary to the claims in this paper, the set of formal power series solutions is not invariant under decomposing a system into regular differential systems[20]. Another approach can be seen in the unpublished work [BL07].

Second, the results of this subsection can be strengthened in the case of constant coefficients.

[19]Furthermore, these zeros are distinct, since the separant of the polynomial is non-zero at ζ.

[20]The decomposition in the sense of [HLR03] makes solution sets larger, e.g. $\{u_t = 0, u \neq 0\}$ is decomposed into $\{u_t = 0\}$, adding the zero function as solution.

Corollary 1.58. *Let S be a system of differential equations and inequations over $\mathbb{C}\{U\}$. The isomorphism $E \to \mathbb{C}[[y_1-\zeta_1,\dots,y_n-\zeta_n]]^U : \sum a_{\mathbf{i}}^{(j)} \frac{z^{\mathbf{i}}}{\mathbf{i}!} \mapsto \sum a_{\mathbf{i}}^{(j)} \frac{(y_1-\zeta_1)^{\mathbf{i}_1}\cdot\ldots\cdot(y_1-\zeta_n)^{\mathbf{i}_n}}{\mathbf{i}!}$ restricts to a bijection between $\mathfrak{Sol}_E(S) \subset E$ and $\mathfrak{Sol}_{\mathbb{C},\zeta}(S)$ for every $\zeta \in \mathbb{C}^n$.*

Third, there is the following peculiar effect that constructing formal power series solutions from non-centered solutions depends on the chosen center. This is particularly noticeably in the bijection from the previous corollary.

Example 1.59. Consider $F = \mathbb{C}$, $U = \{u\}$, $\Delta = \{\partial_y\}$ and the system $S = \{u_{yy} = 0\}$ consisting of a single ordinary differential equation. Then, $e := z \in \mathfrak{Sol}_E(S) \subset \mathbb{C}[[z]]$. Consider the two points $\zeta = 0 \in \mathbb{C}^1$ and $\zeta' = 1 \in \mathbb{C}^1$. Then, the bijection from Corollary 1.58 maps the non-centered solution e to $y \in \mathfrak{Sol}_{\mathbb{C},\zeta}(S) \subset \mathbb{C}[[y]]$ for the point ζ and to $y-1 \in \mathfrak{Sol}_{\mathbb{C},\zeta'}(S) \subset \mathbb{C}[[y-1]]$ for the point ζ'. ◁

1.4.3 Convergent Power Series Solutions

Riquier's existence theorem ensures that the regular formal power series solutions in the sense of Theorem 1.52 of simple differential systems are convergent under mild assumptions. For proofs see [Riq10], [Tho29, Tho34, Tho40] or [Rit50, chap. VIII]. Additionally, [BR78, §4.6] proves the special case of one ordinary differential equation of order two in an elegant way.

Let $F \supseteq \mathbb{C}$ be a differential field of meromorphic functions in n complex variables $y_1,\dots,y_n$, $\partial_i = \frac{\partial}{\partial y_i}$, and $\zeta \in \mathbb{C}^n$ a regular point with respect to a simple differential system S. Let $V = \{v_1,\dots,v_k\} \subset \{U\}_\Delta$ be a cone decomposition of the complement of $\{\mathrm{ld}(S^=)\}_\Delta$ in $\{U\}_\Delta$ with corresponding set of reductive prolongations $\Delta(v_i,V)$ for each v_i, $1 \le i \le n$. Let $f := \psi_\zeta(e) \in \mathfrak{Sol}^o_{\mathbb{C},\zeta}(S)$. Call f a **regular formal power series solution of S with analytical initial conditions around** ζ if the formal power series $\left(\partial_{y_1}^{\mathbf{i}_1}\dots\partial_{y_n}^{\mathbf{i}_n} f(u^{(j)})\right)(w_1,\dots,w_n)$ represents an analytical function around ζ for all $u_{\mathbf{i}}^{(j)} \in V$, where $w_i = y_i - \zeta_i$ if $\partial_i \in \Delta(u_{\mathbf{i}}^{(j)},V)$ and $w_i = \zeta_i$ otherwise. Denote the set of these solutions by $\mathfrak{Sol}^{ho}_{\mathbb{C},\zeta}(S)$.

This means that the parametric and generically parametric differential variables are partitioned into a finite set of classes. Each of these classes corresponds to a formal power series in at most n indeterminates. If all of these formal power series are convergent, then the corresponding solutions are also convergent under mild assumptions:

Theorem 1.60 (Riquier)**.** *Let $<$ be an orderly* Riquier *ranking. Let F be a differential field of meromorphic functions in n complex variables, S be a simple differential system in $F\{U\}$, and $\zeta \in \mathbb{C}^n$ a regular point with respect to S. Then all elements in $\mathfrak{Sol}^{ho}_{\mathbb{C},\zeta}(S)$ have positive radius of convergence.*

[Ger09] states a casual version of Theorem 1.60 without the conditions of a regular point and regular solutions. However, the assumptions of Theorem 1.60 are sharp. Example 1.50 shows that ζ needs to be regular, and Example 2.90 shows that the restriction to $\mathfrak{Sol}^0_{\mathbb{C},\zeta}$ instead of $\mathfrak{Sol}_{\mathbb{C},\zeta}$ is necessary. Furthermore, the theorem in [Ger09] states a uniqueness, which is only satisfied in the quasi-linear case (cf. Example 2.78).

This theorem is a reformulation of the original result from [Riq10] in the context of simple differential systems. Theorem 1.60 follows from the version in [Rit50] because of the following reasons. [Rit50] needed the system to be tail reduced. This can be done without loss of generality for S without changing the set of solutions. The system needs to have equations which have all main degree one in [Rit50]. However, replacing a differential equation in a simple differential system by its derivatives with respect to reductive prolongations ensures that all equations are of main degree one and conserves simplicity. Doing this enlarges the set of solutions. An algebraic equation for the coefficients of the power series rectifies this problem. For details see Subsection 2.5.1.

1.5 Ideals and Simple Systems

> For want of proper algebraic viewpoints, questions which date from the beginning of mathematical analysis remained without systematic treatment. [...] The problem of the number of arbitrary constants [...] failed to receive even a sound formulation.
>
> JOSEPH RITT
> in [Rit38a]

This section treats the differential ideal associated to a simple differential system. It contains all differential polynomials vanishing on all solutions of the simple system or, equivalently, the elements that reduce to zero with respect to the simple systems. These ideals are the basis for differential elimination (cf. Appendix A) and the differential dimension polynomial (cf. Section 1.6).

1.5.1 Simple Algebraic Systems and their Ideals

This subsection introduces ideals associated to simple algebraic systems. Let F be a field of characteristic zero and denote its algebraic closure by $\overline{F}$.

Definition 1.61. Let S be an algebraic system over $\overline{F}[y_1, \dots, y_n]$ and q the product of all initials of the equations in $S^=$, i.e. $q := \prod_{p \in S^=} \operatorname{init}(p)$. Call

$$\begin{aligned}\mathcal{I}(S) &:= \langle S^= \rangle_{\overline{F}[y_1,\dots,y_n]} : q^\infty \\ &= \left\{ p \in \overline{F}[y_1, \dots, y_n] \middle| q^r \cdot p \in \langle S^= \rangle_{\overline{F}[y_1,\dots,y_n]} \text{ for some } r \in \mathbb{Z}_{\geq 0} \right\}\end{aligned}$$

the **ideal associated to the system** S. In particular, if S is a simple algebraic system over $\overline{F}[y_1, \dots, y_n]$, then call $\mathcal{I}(S)$ the **ideal associated to the simple system** S.

For $X \subseteq \overline{F}^n$ denote the **vanishing ideal** of X in $\overline{F}[y_1, \dots, y_n] = \mathcal{O}(\overline{F}^n)$ by

$$\mathcal{I}(X) := \left\{ p \in \overline{F}[y_1, \dots, y_n] \middle| \phi_x(p) = 0 \text{ for all } x \in X \right\} .$$

By HILBERT's Nullstellensatz the vanishing ideal is radical, and radical ideals are in inclusion reverting bijection with closed sets in the ZARISKI topology on $\overline{F}^n$. The ideal of a simple algebraic system S describes the ZARISKI closure of the solutions of S.

Proposition 1.62 ([Rob12, Proposition 2.2.7])**.** *Let S be a simple algebraic system over $\overline{F}[y_1, \dots, y_n]$. Then,*

$$\mathcal{I}(S) = \mathcal{I}(\mathfrak{Sol}(S)) .$$

In particular, $\mathcal{I}(S)$ is a radical ideal[21]*. Furthermore, a polynomial $p \in \overline{F}[y_1, \dots, y_n]$ is an element of $\mathcal{I}(S)$ if and only if the remainder of an iterated pseudo-reduction of p modulo $S^=$ is zero, i.e.* $\mathsf{Reduce}(S, p) = 0$.

[21] The radicalness of $\mathcal{I}(S)$ is an implication of the square-freeness of simple systems. Saturation is only needed with respect to initials, whereas in other contexts (cf. [Hub03a, Theorem 7.5,Proposition 7.6]) a saturation with respect to the initials *and* separants is necessary for a radical ideal.

Another description of the ideal associated to the simple algebraic system S is given by saturating with respect to inequations instead of with respect to initials. This, however, only gives the ideal up to powers, i.e., $\mathcal{I}(S) = \sqrt{\langle S^{=}\rangle : \overline{q}^{\infty}}$ where $\overline{q} := \prod_{p\in S^{\neq}} p$ [Rob12, 2.2.42]. Note that neither the initials of equations nor the inequations of a simple algebraic system S are zero-divisors modulo $\mathcal{I}(S)$.

The solution set of a simple algebraic system is smooth.

Proposition 1.63. *For a simple algebraic system S in $\overline{F}[y_1,\ldots,y_n]$ the set $\mathfrak{Sol}(S)$ is smooth.*

Proof. Let $\mathfrak{m} = \langle y_1,\ldots,y_n\rangle$ be the maximal ideal in $R := \overline{F}[y_1,\ldots,y_n]$ corresponding to a point in $\mathfrak{Sol}(S)$ and $\widehat{R}$ the completion of R with respect to $\mathfrak{m}$. The ideal $\widehat{R}\otimes_R\mathcal{I}(S)$ is generated by $S^{=}$, as the initials of $S^{=}$ are units in $\widehat{R}$. In the following, Hensel's lemma (in the form that it yields a unique root [Eis95, Theorem 7.4]) is applicable, as $\mathrm{sep}(p) \notin \mathfrak{m}$ for each $p \in S^{=}$ due to the square-freeness of S. Thereby, the polynomial p in $S^{=}$ of lowest leader x factors into a unit and a non-unit $\widehat{p}$ of main degree 1 in the ring $\widehat{R}$. Thus, replace p by $\widehat{p}$ in the set of generators of $\widehat{R}\otimes_R\mathcal{I}(S)$. Iteratively, substituting x in the higher polynomials, $\widehat{R}\otimes_R\mathcal{I}(S)$ is generated by $|S^{=}|$ polynomials of degree one. Thus, these polynomials are linear independent modulo $\widehat{R}\otimes_R\mathfrak{m}$. In particular, $\widehat{R}/(\widehat{R}\otimes_R\mathcal{I}(S))$ is a regular local ring. As $\widehat{R}$ is a flat R-module, also the completion of $R/\mathcal{I}(S)$ with respect to $\mathfrak{m}$ is a regular local ring. Thus, $\mathcal{I}(S)$ is smooth at $\mathfrak{m}$. □

1.5.2 Simple Differential Systems and their Ideals

For this subsection let F be a differential field of characteristic zero, $\Delta = \{\partial_1,\ldots,\partial_n\}$ a non-empty set of derivation operators, and $U = \{u^{(1)},\ldots,u^{(m)}\}$ a non-empty set of differential indeterminates.

This subsection introduces ideals associated to simple differential systems and their most important properties. In general, differential ideals can be rather complicated, for example there are differential ideals which are not finitely generated or even not recursive [GMO91]. In contrast, ideals associated to simple differential systems have manageable properties.

Definition 1.64. Let S be a differential system over $F\{U\}$ and q the product of all initials and separants[22] of the equations in $S^{=}$, i.e. $q := \prod_{p\in S^{=}}(\mathrm{init}(p)\cdot\mathrm{sep}(p))$. Call

$$\begin{aligned}\mathcal{I}(S) &:= \langle S^{=}\rangle_\Delta : q^\infty\\ &= \{p\in F\{U\} | q^r\cdot p \in \langle S^{=}\rangle_\Delta \text{ for some } r\in\mathbb{Z}_{\geq 0}\}\end{aligned}$$

the **ideal associated to the system** S. In particular, if S is a simple differential system over $F\{U\}$, then call $\mathcal{I}(S)$ the **ideal associated to the simple system** S.

The Kolchin topology is the differential algebra analogon of the Zariski topology (cf. [Kol73, Chapter IV], [BC99]). A set $X\subseteq E$ is **Kolchin closed** if there is a differential ideal I in $F\{U\}$ such that $X = \mathfrak{Sol}_E(I)$. The Kolchin closed sets form the closed sets of the **Kolchin topology**. The **vanishing ideal** of $X\subseteq E$ in $\overline{F}\{U\}$ is

$$\mathcal{I}(X) := \mathcal{I}_{F\{U\}}(X) := \{p\in F\{U\} | \phi_e(p) = 0 \text{ for all } e\in X\}\ .$$

The closure of a set $X\subseteq E$ in the Kolchin topology is given by $\overline{X} = \mathcal{I}(\mathfrak{Sol}_E(X))$.

[22] In contrast to the algebraic case, saturation with respect to the separants is necessary, as they are the initials of derivations of differential equations.

The notion of the vanishing ideal in differential algebra depends on the set of admissible solutions. However, it is independent of sets of admissible solution with a Nullstellensatz, as stated below. In classical differential algebra this set of solutions lies in a differential fields. There exists a Nullstellensatz of RITT and RAUDENBUSH. RITT proved that theorem for the case of differential equations with meromorphic coefficients and power series at a generic center of expansion as solutions (cf. [Rit32, Theorem in §VII]) and RAUDENBUSH the general case of differential fields (cf. [Rau34, Theorem 9]). A Nullstellensatz for non-centered solutions is easy to prove.

Theorem 1.65 (Nullstellensatz). *Let I be a radical differential ideal in $F\{U\}$.*

(1) $I \neq \langle 1\rangle_\Delta$ implies $\mathfrak{Sol}_E(I) \neq \emptyset$.

(2) $f \in F\{U\}$ with $f(\mathfrak{Sol}_E(I)) = \{0\}$ then $f \in I$.

Proof. Any radical differential ideal is finitely differentially generated [Kol73, Corollary III.4.1] and, thus, has a non-trivial decomposition into simple differential systems. Lemma 1.47 implies the existence of a solution for each of these systems, which proves (1). Part (2) follows using the RABINOWITZ-trick; see [Rit32, §85] for details. □

There is no Nullstellensatz for formal power series solutions at a fixed center, as $t\frac{\partial u}{\partial t}(t) - 1$ has no such solution around zero. (The solutions are $\log(t) + c$ for $c \in \mathbb{C}$.)

Proposition 1.66 (cf. [Rob12, Proposition 2.2.31, Lemma 2.2.42]). *Let S be a simple differential system in $F\{U\}$. Then*

$$\mathcal{I}(S) = \mathcal{I}(\mathfrak{Sol}_E(S)) \ .$$

In particular, $\mathcal{I}(S)$ is a radical ideal. Furthermore, a differential polynomial $p \in F\{U\}$ is an element of $\mathcal{I}(S)$ if and only if the remainder of an iterated differential pseudo-reduction of p module $S^=$ is zero, i.e. $\mathsf{Reduce}(S, p) = 0$.

Again, $\mathcal{I}(S) = \sqrt{\langle S^=\rangle_\Delta : \overline{q}^\infty}$ for a simple differential system S where $\overline{q} := \prod_{p\in S^{\neq}} p$ [Rob12, Lemma 2.2.42]. In particular, neither initials and separants of equations nor inequations are zero-divisors modulo $\mathcal{I}(S)$.

Corollary 1.67. *The maps $\mathfrak{Sol}_E$ and $\mathcal{I}$ form an inclusion reverting bijection between closed sets in the KOLCHIN topology on E and radical differential ideals.*

A THOMAS decomposition is compatible with decomposition of the associated ideals.

Proposition 1.68 ([Rob12, 2.2.51]). *Let S be a (not necessarily simple) differential system over $F\{U\}$. Let $S_1, \dots, S_k$ be a THOMAS decomposition of S. Then*

$$\mathcal{I}(S) = \bigcap_{i=1}^{k} \mathcal{I}(S_i) \ .$$

By the last two propositions, membership to a radical differential ideal can therefore be decided by reducing modulo every simple differential system of a THOMAS decomposition.

Corollary 1.69. *Let $p_1, \dots, p_\ell \in F\{U\}$ and $S_1, \dots, S_k$ a THOMAS decomposition of $\{p_1 = 0, \dots, p_\ell = 0\}$. Let $r \in F\{U\}$. Then*

$$r \in \sqrt{\langle p_1, \dots, p_\ell\rangle} \quad \Leftrightarrow \quad \mathsf{Reduce}(S_i, r) = 0 \text{ for all } i = 1, \dots, k \ .$$

The following proposition shows that prime ideals can be described by simple differential systems. It is true in both the algebraic and the differential case.

Proposition 1.70 ([Rob12, Proposition 2.2.45, 2.2.46])**.** *For every prime ideal I in $F[y_1, \dots, y_n]$ resp. $F\{U\}$ there exists a simple algebraic resp. differential system S with $I = \mathcal{I}(S)$.*

Proposition D.1 gives a sufficient criterion that $\mathcal{I}(S)$ is prime for a simple algebraic or differential system S: all equations in $S^{=}$ have main degree one.

1.6 The Differential Dimension Polynomial

"For many questions this number is sufficient to prove that two systems are not equivalent"

Élie Cartan
in [CE79, Cartan, 29.4.1932]

The differential dimension polynomial is an important description of a simple differential system and it measures the restrictiveness of aforementioned system on admissible solutions. Though it gives less information than the differential counting polynomial (cf. Section 2.3), the dimension polynomial has the advantage that it is fully algorithmic (cf. Remark 1.77) and has stronger invariance conditions (cf. Theorem 1.74). This section extends the differential dimension polynomial from prime differential ideals to differential ideals associated to simple differential systems, and thereby makes the differential dimension polynomial much more suitable for algorithmic computations.

For this section, let F be a differential field of characteristic zero, $<$ an orderly ranking, $\Delta = \{\partial_1, \dots, \partial_n\}$ be a non-empty set of derivation operators, and $U = \{u^{(1)}, \dots, u^{(m)}\}$ be a non-empty set of differential indeterminates.

Preliminaries on Numerical Polynomials The differential dimension polynomial is a numerical polynomial, i.e., a rational polynomial that maps an integer to an integer. The following lemma is well-known.

Lemma 1.71. *The $\mathbb{Z}$-module of numerical polynomials of degree $\leq i$ is free with basis*

$$\left\{ \binom{\ell+k}{k} \in \mathbb{Q}[\ell] \middle| 0 \leq k \leq i \right\} .$$

Remark 1.72. Define a total order on the numerical polynomials $p = \sum_{k=0}^{d} a_k \binom{\ell+k}{k}$ and $q = \sum_{k=0}^{d} b_k \binom{\ell+k}{k}$ by $p \leq q$ if $p(\ell) \leq q(\ell)$ for all ℓ sufficiently large. Then $p \leq q$ if and only if either $p = q$ or there is a $j \in \{0, \dots, d-1\}$ such that $a_k = b_k$ for all $k > j$ and $a_j < b_j$. In the second case write $p < q$. If $p(\ell - \ell_0) \leq q(\ell) \leq p(\ell + \ell_0)$ for some ℓ_0 and all ℓ large enough, then the degrees and leading coefficients of p and q coincide. ◁

The next lemma shows how to express binomial coefficients in the standard basis from Lemma 1.71. It can inductively be proved using Pascal's rule $\binom{a-1}{b} = \binom{a}{b} - \binom{a-1}{b-1}$.

Lemma 1.73. *Let $\ell, k, d \in \mathbb{Z}_{\geq 0}$. Then*

$$\binom{\ell+k-d}{k} = \sum_{i=0}^{\min(k,d)} (-1)^i \binom{d}{i} \binom{\ell+k-i}{k-i} .$$

1.6.1 The Differential Dimension Polynomial

The existence and fundamental properties of the differential dimension polynomial for prime ideals were first announced by Kolchin in [Kol64]. A first proof was published by his student Johnson in [Joh69a] using differentials to reduce the problem to the case of modules over a commutative ring. The originally announced proof by counting cardinalities of transcendence bases was then published in Kolchin's book [Kol73,

§II.12]. A good historical reference for this topic is [BC99, §1.11], and a rich compilation of result on dimension polynomials can be found in the monograph [KLMP99]. Recently, Levin generalized the differential dimension polynomial to describe certain subsets of the full solution set of a prime differential ideal [Lev10]. For other recent development, especially with respect to difference dimension polynomials, see [Doe09].

This subsection relaxes the condition of primeness from KOLCHIN's Theorem to ideals associated to a simple differential system. This generalization is important for constructive mathematics; a decomposition into prime ideals is computationally much harder than a decomposition into simple differential systems.

The dimension polynomial yields invariants under differential birational maps. Recall that for a commutative ring R the **total quotient ring** $\mathrm{K}(R)$ is the localization $\mathrm{K}(R) := Q^{-1}R$, where $Q \subset R$ the multiplicatively closed set of non-zero-divisors. The natural homomorphism $R \to \mathrm{K}(R) : 1 \mapsto 1$ is a monomorphism. Let R and R' be two differential algebras. A **differential birational map** from R to R' is given by an isomorphism $\varphi : \mathrm{K}(R) \to \mathrm{K}(R')$ of F-algebras that commutes with derivations.

The **differential dimension function**

$$\Omega_I : \mathbb{Z}_{\geq 0} \mapsto \mathbb{Z}_{\geq 0} : \ell \mapsto \dim(F\{U\}_{\leq \ell}/I_{\leq \ell}) \ .$$

measures the size of the solution set of a differential ideal $I \subseteq F\{U\}$ using the KRULL dimension. It depends on the filtration and is not invariant under birational maps.

The differential dimension polynomial implies certain invariants. A **differential transcendence basis** of a differential F-algebra over Δ is a set $\{r_1, \ldots, r_d\} \subset R$ of maximal cardinality with $\biguplus_{i=1}^{d} \{r_i\}_\Delta$ algebraically independent over F. The **differential dimension** of R is defined[23] as the cardinality d of a differential transcendence basis. For example, a differential transcendence basis of $F\{U\}$ is $U = \{u^{(1)}, \ldots, u^{(m)}\}$, and its differential dimension is m.

This allows to state the main theorem, the full version of Theorem 1.5.

Theorem 1.74. *Let S be a simple differential system with respect to an orderly ranking $<$ and $I := \mathcal{I}(S) \subseteq F\{U\}$ the differential ideal associated to S. Then:*

*(1) There is a numerical polynomial $\omega_I(\ell) \in \mathbb{Q}[\ell]$ called **differential dimension polynomial** such that $\omega_I(\ell) = \Omega_I(\ell)$ for sufficiently big $\ell \in \mathbb{Z}_{\geq 0}$.*

(2) $0 \leq \omega_I(\ell) \leq m\binom{\ell+n}{n}$. In particular, $d_I := \deg_\ell(\omega_I) \leq n$. Furthermore, ω_I can be written uniquely as $\omega_I(\ell) = \sum_{i=0}^{n} a_i \binom{\ell+i}{i}$ with $a_i \in \mathbb{Z}$ for all $i \in \{0, \ldots, n\}$ by Lemma 1.71.

*(3) The values d_I and a_i for $i \geq d_I$ are invariant under differential birational maps and, thus, only depend on the isomorphism class of $\mathrm{K}(F\{U\}/I)$. Call a_{d_I} the **typical dimension** of I.*

(4) a_n is equal to the differential dimension of $F\{U\}/I$.

Let S' be a further simple differential systems with respect to $<$, and $J := \mathcal{I}(S') \subseteq F\{U\}$. Assume that $I \subseteq J$. Then:

(5) $\omega_I \geq \omega_J$.

Additionally, assume that $\omega_I = \omega_J$. Then:

[23] For a prime differential ideal I the differential dimension is often defined as m-th coefficient of the differential dimension polynomial [Kol73, KLMP99]. The definition above includes non-prime differential ideals. In the special case the definitions are equivalent by [KLMP99, Theorem 5.4.4].

(6) $\operatorname{ld}(S^=) = \operatorname{ld}((S')^=)$.

(7) $I = J$ *if and only if* $\deg_x(S_x) = \deg_x(S'_x)$ *for all* $x \in \operatorname{ld}(S^=) = \operatorname{ld}((S')^=)$.

Section 1.7 is dedicated to the proof of this theorem.

Remark 1.75. This theorem can be slightly strengthened, as $I \subseteq J$ and $\omega_I = \omega_J$ already imply $\deg_x(S_x) \leq \deg_x(S'_x)$ for all $x \in \operatorname{ld}(S^=)$ by Appendix D. Thus, $I = J$ if and only if $\prod_{x\in\operatorname{ld}(S^=)} \deg_x(S_x) = \prod_{x\in\operatorname{ld}(S^=)} \deg_x(S'_x)$. ◁

Remark 1.76. The degrees of the equations used in Theorem 1.74.(7) depend on the chosen orderly ranking. This is not a problem for the comparison of two different sets of solutions using Theorem 1.74.(7), as the dimension polynomials for both ideals only need to be computed with respect to the same ranking. ◁

The differential dimension polynomial can be computed based on the Janet decomposition, as the proof in Section 1.7 shows that the dimension polynomial can be interpreted as the number of free differential variables in a simple differential system. The formula follows from the next Subsection 1.6.2 about Hilbert-Samuel polynomials, which are the “filtered version” of the Hilbert polynomials.

Remark 1.77. Let $I = \mathcal{I}(S)$ be the differential ideal associated to a simple differential system S. The differential dimension polynomial of I is the Hilbert-Samuel polynomial HS_S of S defined in the next subsection. For its computation let $S^= = \{p_1, \ldots, p_k\}$, $\theta_i := \operatorname{ord}(p_i)$, and, using the Janet decomposition, let $\eta_i = |\Delta(p_i, S^=)|$ the number of reductive prolongations of p_i. Then,

$$\begin{aligned}\omega_I(\ell) = HS_S(\ell) &= m\binom{\ell+n}{n} - \sum_{i=1}^{k}\binom{\eta_i+\ell-\theta_i}{\ell-\theta_i}\\ &= m\binom{\ell+n}{n} - \sum_{i=1}^{k}\binom{\eta_i+\ell-\theta_i}{\eta_i}\end{aligned}$$ ◁

Example 1.92 below presents the implementation of the dimension polynomial.

Example 1.78. Consider the heat equation $h = v_t + v_{xx}$ and the viscous Burgers' equation $b = u_t + u_{xx} + 2u_x \cdot u$ from Example 1.6. MAPLE's pdsolve [map] finds the following sets of solutions.

$$\left\{v(t,x) = F_1(t)F_2(x) \,\middle|\, \frac{d}{dt}F_1(t) = c_1F_1(t), \frac{d^2}{dx^2}F_2(x) = -c_1F_2(x), c_1 \in \mathbb{C}\right\}$$
$$\left\{u(t,x) = c_4\tanh(c_3t + c_4x + c_2) - \frac{c_3}{2c_4} \,\middle|\, c_2, c_3, c_4 \in \mathbb{C}\right\}$$

These sets of solutions only depend on a finite number of parameters. Both the singleton consisting of the heat equation and the singleton consisting of the viscous Burgers' equation are a simple differential system, and both these systems consist of one equation with a leader of order two. In particular, their differential dimension polynomials

$$\omega_{\mathcal{I}(\{h_=\})} = \omega_{\mathcal{I}(\{b_=\})} = 1\cdot\binom{\ell+2}{2} - \binom{2+\ell-2}{2} = 2\ell+1$$

show that the set of solutions depends on an infinite number of parameters and that the solutions found by MAPLE's pdsolve only account for a small subset of all solutions. ◁

1.6.2 Hilbert Polynomials

Sets of differential variables closed under the action of the derivations in Δ and their complements allow to compute the differential dimension polynomial and to prove its properties. This subsection describes certain combinatorial information given by the Janet decompositions, which can be encoded in numerical polynomials. For details and proofs see [Kol73, §0.17], [Rob12], [Cou95, §9], or [GP08, §5].

Let W be a set of differential variables closed under the action of Δ. Let $\widetilde{W} = \{w_1, \ldots, w_k\} \subset W$ be a cone decomposition of W, i.e. $W = \biguplus_{w \in \widetilde{W}} \{w\}_{\Delta(w,\widetilde{W})}$. The **Hilbert function** of W is defined as

$$\widetilde{h} : \mathbb{Z}_{\geq 0} \to \mathbb{Z}_{\geq 0} : \ell \mapsto \left| W \cap \left\{ u_{\mathbf{i}}^{(j)} \middle| \operatorname{ord} u_{\mathbf{i}}^{(j)} = l \right\} \right| .$$

Lemma 1.79. *Let $\widetilde{W} = \{w_1, \ldots, w_k\} \subset W$ be a disjoint cone decomposition of some set of differential variables $W = \biguplus_{w \in \widetilde{W}} \{w\}_{\Delta(w,\widetilde{W})}$. Let η_i be the number $\left|\Delta(w_i, \widetilde{W})\right|$ of reductive prolongations of w_i and $\theta_i := \operatorname{ord}(w_i)$. The* Hilbert *function $\widetilde{h}$ equals*

$$\widetilde{h}_W(\ell) = \sum_{i=1}^{k} \binom{\eta_i - 1 + \ell - \theta_i}{\ell - \theta_i} = \sum_{i=1}^{k} \binom{\eta_i - 1 - \theta_i + \ell}{\eta_i - 1}$$

for $\ell \geq \max\{\theta_i | 1 \leq i \leq k\}$. This is a numerical polynomial called the ***Hilbert polynomial*** *and denoted by $H_W(\ell)$. In particular, the* Hilbert *function is ultimately a polynomial function. An important special case is $H_{\{U\}_\Delta}(\ell) = m\binom{\ell+n-1}{n-1}$.*

Also the complement $\{U\}_\Delta \setminus W$ of a set W of differential variables closed under the action of Δ defines a **Hilbert function**

$$\widetilde{h}_{\{U\}_\Delta \setminus W}(\ell) := m\binom{\ell + n - 1}{n - 1} - \widetilde{h}_W(\ell) ,$$

which is ultimately a polynomial function. A cone decomposition of this complement (cf. Algorithm B.1) computes the Hilbert function with the same formulas as above.

Instead of the number of differential variables *in* order ℓ, the **Hilbert-Samuel function**

$$\widetilde{hs}_W : \mathbb{Z}_{\geq 0} \to \mathbb{Z}_{\geq 0} : \ell \mapsto \left| W \cap \left\{ u_{\mathbf{i}}^{(j)} \middle| \operatorname{ord} u_{\mathbf{i}}^{(j)} \leq \ell \right\} \right| .$$

of a set W of differential variables closed under the action of Δ counts the number of differential variables *up to* order ℓ.

Lemma 1.80. *Let $\widetilde{W} = \{w_1, \ldots, w_k\} \subset W$ be a disjoint cone decomposition of a set of differential variables $W = \biguplus_{w \in \widetilde{W}} \{w\}_{\Delta(w,\widetilde{W})}$. Let η_i be the number $\left|\Delta(w, \widetilde{W})\right|$ of reductive prolongations of w_i and by $\theta_i := \operatorname{ord}(w_i)$. The* Hilbert-Samuel *function $\widetilde{hs}$ is*

$$HS_W(\ell) = \sum_{i=1}^{k} \binom{\eta_i + \ell - \theta_i}{\ell - \theta_i} = \sum_{i=1}^{k} \binom{\eta_i + \ell - \theta_i}{\eta_i}$$

for $\ell \geq \max\{\theta_i | 1 \leq i \leq k\}$. This is a numerical polynomial called the ***Hilbert-Samuel polynomial*** *and denoted by $HS_W(\ell)$. In particular, the* Hilbert-Samuel *function is ultimately a polynomial function and $HS_{\{U\}_\Delta}(\ell) = m\binom{n+\ell}{n}$.*

Again, the same definitions hold for a complement $\{U\}_\Delta \backslash W$ of a set W of differential variables closed under the action of Δ. Define the **Hilbert-Samuel function**

$$\widetilde{hs}_{\{U\}_\Delta \backslash W}(\ell) := m\binom{\ell+n}{n} - \widetilde{hs}_W(\ell) ,$$

which is ultimately a polynomial function and can be computed by a cone decomposition of the complement of W.

For a differential system S define above functions and polynomials according to the complement of the Δ-closed set generated by the leaders of the equations, i.e.,

$$H_S(\ell) := H_{\{U\}_\Delta \backslash \{\mathrm{ld}(S^=)\}_\Delta}(\ell) \qquad \text{the } \textbf{Hilbert polynomial} \text{ of } S,$$
$$HS_S(\ell) := HS_{\{U\}_\Delta \backslash \{\mathrm{ld}(S^=)\}_\Delta}(\ell) \qquad \text{the } \textbf{Hilbert-Samuel polynomial} \text{ of } S.$$

These numerical polynomials can be described in the standard basis.

Lemma 1.81. *Let $\widetilde{W} = \{w_1, \ldots, w_k\} \subset W$ be a disjoint cone decomposition of a set of differential variables W, i.e. $W = \biguplus_{w \in \widetilde{W}} \{w\}_{\Delta(w,\widetilde{W})}$. Denote by η_i the number $\left|\Delta(w, \widetilde{W})\right|$ of reductive prolongations of w_i and by θ_i the order* $\mathrm{ord}(w_i)$. *For $\ell \geq$* $\max\{\theta_i | 1 \leq i \leq k\}$ *the following identities hold for the* Hilbert *polynomial H and* Hilbert-Samuel *polynomial HS.*

$$\begin{aligned}
H_W(\ell) &= \sum_{i=1}^{k} \binom{(\eta_i - 1) + \ell - \theta_i}{(\eta_i - 1)} && \textit{by Lemma 1.79}\\
&= \sum_{i=1}^{k} \sum_{j=0}^{\min(\theta_i, \eta_i - 1)} (-1)^j \binom{\theta_i}{j} \binom{\ell + (\eta_i - 1) - j}{(\eta_i - 1) - j} && \textit{by Lemma 1.73}\\
HS_W(\ell) &= \sum_{i=1}^{k} \binom{\eta_i + \ell - \theta_i}{\eta_i} && \textit{by Lemma 1.80}\\
&= \sum_{i=1}^{k} \sum_{j=0}^{\min(\theta_i, \eta_i)} (-1)^j \binom{\theta_i}{j} \binom{\ell + \eta_i - j}{\eta_i - j} && \textit{by Lemma 1.73}
\end{aligned}$$

1.6.3 Examples

For each differential prime ideal I there exists a simple differential system S with $I = \mathcal{I}(S)$ Proposition 1.70. Thus, the differential dimension polynomial defined above includes the version of Kolchin. Furthermore, there exist ideals which are not prime but are associated to a simple differential system.

Example 1.82. Consider $F = \mathbb{C}$, $U = \{u, v\}$, $\Delta = \{\partial_t\}$, $p = u_1^2 - v$, $q = v_1^2 - v$, and $S = \{p = 0, q = 0, v \neq 0\}$. The differential ideal $I := \mathcal{I}(S)$ associated to S is not prime, as $p - q = u_1^2 - v_1^2 = (u_1 - v_1)(u_1 + v_1)$. ◁

In the original theorem of Kolchin two differential prime ideals $I \subseteq J$ are equal if and only if $\omega_I = \omega_J$. The version of the theorem given here needs the degrees of the equations in the simple differential system as additional criterion for equality of ideals associated to simple differential systems contained in each other (cf. Theorem 1.74.(7)). The following example shows that this extra complication is necessary.

Example 1.83. Consider the differential ideals $\langle u_0 \cdot (u_0 - 1)\rangle_\Delta \subsetneq \langle u_0\rangle_\Delta$ in $F\{u\}$. Both ideals are associated to a simple differential system that contains only the ideals generator as equation, and both ideals have differential dimension polynomial 0. However, these ideals are not equal. ◁

The next example shows that using an orderly ranking is needed for the computation of the differential dimension polynomial.

Example 1.84 ([CE79, Einstein, 16.5.1932])**.** Let $F = \mathbb{C}(x,t)$, $U = \{u\}$ and $\Delta = \{\frac{\partial}{\partial x}, \frac{\partial}{\partial t}\}$. The heat equation $u_t + u_{xx} = 0$ has leader u_{xx} for any orderly ranking. Thus, the dimension polynomial is $2\ell + 1$. However, "illegally" considering the formula of the differential dimension polynomial for a ranking with $u_t > u_{xx}$ yields the dimension polynomial $\ell + 1$. In particular, the leading coefficient does change. ◁

1.6.4 Interpretation of the Dimension Polynomial

This subsection describes information[24] that the dimension polynomial yields about a differential ideal. This is motivated by the following demonstrative example.

Example 1.85 ([CE79, Cartan, 3.12.1929, Appendix I])**.** Consider the $m = 7$ differential indeterminates $U = \{X, Y, Z, r, u, v, w\}$, $n = 4$ derivations $\Delta = \{\frac{\partial}{\partial t}, \frac{\partial}{\partial x}, \frac{\partial}{\partial y}, \frac{\partial}{\partial z}\}$, and the system S consisting of the following differential equations.

$$\begin{aligned}
\underline{Z_y} - Y_z &= 0,\\
\underline{Z_x} - X_z &= 0,\\
\underline{Y_x} - X_y &= 0,\\
\underline{X_x} + Y_y + Z_z + 4\,\pi\, f r &= 0,\\
\underline{r_t} + r_x u + r u_x + r_y v + r v_y + r_z w + r w_z &= 0,\\
\underline{u_t} + u u_x + v u_y + w u_z - X &= 0,\\
\underline{v_t} + u v_x + v v_y + w v_z - Y &= 0,\\
\underline{w_t} + u w_x + v w_y + w w_z - Z &= 0
\end{aligned}$$

This systems is simple with respect to the degree-reverse lexicographical ranking.

The dimension polynomial is given by

$$\omega_{\mathcal{I}(S)}(\ell) = l^3 + \frac{13}{2}\ell^2 + \frac{25}{2}\ell + 7 = 6\binom{\ell+3}{\ell} + \binom{\ell+2}{\ell}\ .$$

The second representation in the free basis of numerical polynomials is more useful. For example, in the cone decomposition of the parametric differential variables

$$\{X, Y\}_{\{\frac{\partial}{\partial t}, \frac{\partial}{\partial y}, \frac{\partial}{\partial z}\}} \uplus \{Z\}_{\{\frac{\partial}{\partial t}, \frac{\partial}{\partial z}\}} \uplus \{r, u, v, w\}_{\{\frac{\partial}{\partial x}, \frac{\partial}{\partial y}, \frac{\partial}{\partial z}\}}$$

there are 6 cones of dimension 3 and 1 cone of dimension 2, similar to the coefficients of the dimension polynomial.

The regular non-centered solutions $\mathfrak{Sol}^o_E(S)$ yield all formal power series solutions of the system S by Remark 1.49, as S contains no inequations. In particular, the Janet

[24] Regard all descriptions of the solution set presented in this subsection as global descriptions, as is standard in differential algebra. However, from the standpoint of differential geometry, they only describe local properties, which are correct generically. Recall that the ranking $<$ is orderly.

cone decomposition shows exactly which coefficients can be chosen freely and which coefficients are determined by these choices, i.e., providing (convergent) power series

$$X(t,0,y,z), Y(t,0,y,z), Z(t,0,0,z), r(0,x,y,z), u(0,x,y,z), v(0,x,y,z), w(0,x,y,z)$$

uniquely determines a solution (which by RIQUIER's Existence Theorem 1.60 converges). There are 6 functions in 3 indeterminates and 1 function in 2 indeterminates, as the coefficients of the dimension polynomial. CARTAN called the number of freely choosable functions of the highest number of indeterminates the degré d'arbitraire or generality index.

The dimension polynomial counts parametric differential variable *up to* a certain order. For the number *in* a certain order, the HILBERT polynomial agrees with the correct number on all but finitely many orders. For this example it is

$$H_S(\ell) = 3\ell^2 + 10\ell + 7 = 6\binom{\ell+2}{\ell} + \binom{\ell+1}{\ell}.$$

Again, 6 and 1 appear as coefficients. EINSTEIN compared this polynomial to the number $\binom{\ell+n-1}{\ell} = \binom{\ell+3}{\ell}$ of power series coefficients freely choosable for an arbitrary function in order ℓ. He compared their asymptotic behavior by

$$\frac{3\ell^2+10\ell+7}{\binom{\ell+3}{\ell}} = 18\frac{1}{\ell} + \mathcal{O}\left(\left(\frac{1}{\ell}\right)^2\right)$$

and 18 is called the strength of the (determined) differential system. It also equals

$$18 = \underbrace{\deg_\ell(\binom{\ell+3}{\ell})!}_{=(n-1)!=3!=6} \cdot \underbrace{\operatorname{init}(3\ell^2+10\ell+7)}_{=\frac{6}{(n-2)!}=3} = 6(n-1)$$

where, again, the leading coefficient 6 of the dimension polynomial appears. ◁

CARTAN characters and the index of generality The CARTAN characters and the index of generality are well-known descriptions of the size of solutions. We follow [Sei10, Definition 6.2.1] and define them dependent on the coordinates. However, in a dense subset of coordinates, the δ-regular coordinates, this definition coincides with the intrinsic definition given in [Pom94, Definition III.B.11]. The intrinsic CARTAN characters are the smallest ones.

Let S be a simple differential system in $F\{U\}$ and $\ell \in \mathbb{Z}_{\geq 0}$ larger than any order of a differential variable appearing in an equation of S. Similarly to Algorithm B.1 one can compute a decomposition of $\{\Delta^\ell U\}_\Delta \setminus \{\operatorname{ld}(S^=)\}_\Delta$ into cones. It is easy to see that such a decomposition is possible by using only cone generators of order ℓ, and all cones have at least one reductive derivation. Define the **CARTAN characters** $\alpha_\ell^{(j)}$ as the number of these cones with j reductive derivations for $1 \leq j \leq n$.

The CARTAN characters do not determine the number of parametric differential variables in order less than ℓ, but they do determine it in order at least ℓ. Thus, the dimension polynomial determines the CARTAN characters, but the CARTAN characters determine the dimension polynomial up to a constant.

Proposition 1.86. *Let the dimension polynomial of a simple differential system S be given as*

$$\omega_{\mathcal{I}(S)}(\ell) = \sum_{i=0}^{n} a_i \binom{\ell+i}{\ell}.$$

Then, the CARTAN *characters of S are*

$$\alpha_\ell^{(j)} k = \sum_{i=j}^{n} \binom{\ell - 1 + i - j}{i - j} a_i \ .$$

From this representation one sees that the highest j such that $\alpha_\ell^{(j)} \neq 0$ is independent of ℓ and is equal to the degree of the dimension polynomial. For this j it holds that $\alpha_\ell^{(j)} = a_j$, independent of ℓ. This number is called the **index of generality** or **degré d'arbitraire** or highest non-zero CARTAN character.

The HILBERT polynomial The dimension polynomial determines the HILBERT polynomial. Let S be a simple differential system in $F\{U\}$ with dimension polynomial

$$\omega_{\mathcal{I}(S)}(\ell) = \sum_{i=0}^{n} a_i \binom{\ell + i}{\ell} \ .$$

Then, the HILBERT polynomial is

$$H_S(\ell) := \sum_{i=1}^{n} a_i \binom{\ell + i - 1}{\ell} \ .$$

However, the HILBERT polynomial contains less information than the dimension polynomial, more precisely one cannot recover the coefficient a_0 from H_S.

The Hilbert polynomial cannot decide whether containment of ideals is proper, even in the case of linear differential equations.

Example 1.87. Consider $S_1 = \{u_x = 0\}$ in $\mathbb{C}\{u\}$ and $S_2 = \{u_{xx} = 0, u_{xy} = 0\}$ with $\Delta = \{\partial_x, \partial_y\}$. Then $\mathcal{I}(S_2) \subseteq \mathcal{I}(S_1)$ and $H_{S_1}(\ell) = 1 = H_{S_2}(\ell)$. However, $\mathcal{I}(S_2) \neq \mathcal{I}(S_1)$, as $\omega_{\mathcal{I}(S_1)}(\ell) = l + 1 \neq l + 2 = \omega_{\mathcal{I}(S_2)}(\ell)$.

The HILBERT polynomial implies all other values in this subsection describing the solution set of a set of differential equations. In particular, also these values cannot decide whether $\mathcal{I}(S_1) \neq \mathcal{I}(S_2)$. ◁

The CARTAN characters yield the same information as the HILBERT polynomial, which can be shown by a computation using Lemma 1.81. In particular, the CARTAN characters cannot decide whether ideals contained in each other are equal.

Proposition 1.88. *Given a simple differential system S in $F\{U\}$ for an orderly ranking $<$ with* CARTAN *characters $\alpha_k^{(1)}, \ldots, \alpha_k^{(n)}$. Then the* HILBERT *polynomial is*

$$H_S(\ell) = \sum_{i=1}^{n} \alpha_k^{(i)} \binom{(\ell - k) + i - 1}{(\ell - k)} \ ,$$

and it is independent of k (cf. [Sei94, Section III]) for k large enough. The coefficients of the HILBERT *polynomial in basis $H_S(\ell) := \sum_{i=1}^{n} a_i \binom{\ell+i-1}{\ell}$ are given by*

$$a_i = \sum_{j=i}^{n} \alpha_k^{(j)} (-1)^{j-i} \binom{k}{j - i} \ .$$

Free functions The number of free functions one can choose to get a formal power series solution is strongly linked to the previous values. A similar approach can be found in [Sei94] and [Sei10, Section 8.2]. Let S be a simple differential system in $F\{U\}$, $\ell \in \mathbb{Z}_{\geq 0}$ larger than any order of a differential variable appearing in any equation or inequation of S, and $\alpha_\ell^{(1)}, \dots, \alpha_\ell^{(n)}$ the CARTAN characters of S. Denote by W the set of parametric differential variables of order smaller than ℓ. One can arbitrarily (i.e., only restricted by inequations) choose the power series coefficients corresponding to W and the $\alpha_\ell^{(j)}$ formal power series in j indeterminates for $1 \leq j \leq n$ corresponding to the cones constructed for the CARTAN characters. All these choices lead to $\prod_{p \in S^=} \operatorname{mdeg}(p)$ solutions.

EINSTEIN's Strength Often, in physical applications the number of arbitrary power series in n indeterminates is zero and there is a non-zero number of arbitrary power series in $n-1$ indeterminates. For this case EINSTEIN introduced the strength of a system in [Ein53a, Ein53c]. The strength was used in mathematical physics and calculated for many examples [Mar74, Hoe77, Mat87, Mat92, Sei95]. The paper [Sch75] gives the connection between the strength and the number of arbitrary power series in $n-1$ indeterminates for semilinear[25] systems and generalizes the strength to the case of power series in an arbitrary number of indeterminates. The connection to the other values is described by [Sué91] and generalized to the nonlinear case in [Sei94, Sei10].

Let S be a simple differential system in $F\{U\}$. Consider the HILBERT polynomial $H_S(k)$ of S and asymptotically compare it to the number $\binom{n+\ell-1}{\ell}$ of coefficients in order ℓ of a formal power series. Develop $\frac{H_S(\ell)}{\binom{n+\ell-1}{\ell}}$ by powers of $\frac{1}{\ell}$ to get

$$\frac{H_S(\ell)}{\binom{n+\ell-1}{\ell}} = Z^{(0)} + Z^{(1)}\frac{1}{\ell} + \mathcal{O}\left(\frac{1}{\ell^2}\right)$$

In EINSTEIN's examples there was always $Z^{(0)} = 0$ and $Z^{(1)} \neq 0$. The integer $Z^{(1)}$ is called the **strength**[26] of the system S. HILBERT polynomial, dimension polynomial, and CARTAN characters imply the strength. For a different formula see [Sei94].

Proposition 1.89. *Let S be a simple differential system in $F\{U\}$ for an orderly ranking $<$ with HILBERT polynomial $H_S(\ell) = \sum_{i=1}^n a_i \binom{\ell+i-1}{\ell}$, $\ell \in \mathbb{Z}_{\geq 0}$ larger than any order of a differential variable appearing in any equation or inequation of S, and $\alpha_\ell^{(1)}, \dots, \alpha_\ell^{(n)}$ the CARTAN characters of S. Then the following holds.*

$$Z^{(0)} = a_n = \alpha_\ell^{(n)}$$
$$Z^{(1)} = (n-1)a_{n-1} = (n-1)\left(-\ell\alpha_\ell^{(n)} + \alpha_\ell^{(n-1)}\right)$$

In differential algebra The following corollaries about invariants in differential algebra follow easily from Theorem 1.74 and the previous results in this subsection. Always assume that ℓ is large enough for the CARTAN characters to be defined. The general reference is [KLMP99, Section 5.6].

Corollary 1.90. *Let S be a simple differential system in $F\{U\}$. The differential dimension of $\mathcal{I}(S)$ is also equal to the highest CARTAN character $\alpha_\ell^{(n)}$. Furthermore, the*

[25] I.e., systems where all equations have an initial in F and are of main degree one.

[26] The term strength is used for $Z^{(1)}$ in the literature. However, in [Ein53a] EINSTEIN did not call $Z^{(1)}$ the strength of a system but "coefficient of freedom". More paradoxical, a system is stronger (in the sense of EINSTEIN) if the strength $Z^{(1)}$ is smaller.

differential dimension is equal to the number of arbitrary formal power series in $n = |\Delta|$ indeterminates which can be chosen arbitrarily for a solution.

Let $d_{\mathcal{I}(S)}$ be the largest index such that $a_{d_{\mathcal{I}(S)}} \neq 0$ ($a_{d_{\mathcal{I}(S)}} \neq 0$ is the typical dimension). Call $d_{\mathcal{I}(S)}$ the **differential type** of $\mathcal{I}(S)$. The differential type can be characterized similarly to the KRULL dimension by chains of prime ideals [Joh69b]. By Theorem 1.74 both the differential type and typical dimension are invariants of $\mathcal{I}(S)$ under differential birational maps.

Corollary 1.91. *Let S be a simple differential system in $F\{U\}$ for an orderly ranking $<$. The differential type of $\mathcal{I}(S)$ is equal to the index of the highest non-zero* CARTAN *character, and the typical dimension $d_{\mathcal{I}(S)}$ is also equal to the generality index. These numbers are invariant under differential birational maps.*

Several of the values describes in this subsection allow an a-priori estimation. Some of these estimates from the literature are collected in Appendix C.

Example 1.92. The computation of the differential dimension polynomial is implemented. Consider the incompressible NAVIER-STOKES-Equations.

```
restart;
with(DifferentialThomas):
ivar:=[t,x,y,z]:  dvar:=[u,v,w,p]:
ComputeRanking(ivar,dvar);
L := [
   u[1,0,0,0]+u[0,0,0,0]*u[0,1,0,0]+v[0,0,0,0]*u[0,0,1,0]
         +w[0,0,0,0]*u[0,0,0,1]+p[0,1,0,0]
         -1/rl*(u[0,2,0,0]+u[0,0,2,0]+u[0,0,0,2]),
   v[1,0,0,0]+u[0,0,0,0]*v[0,1,0,0]+v[0,0,0,0]*v[0,0,1,0]
         +w[0,0,0,0]*v[0,0,0,1]+p[0,0,1,0]
         -1/rl*(v[0,2,0,0]+v[0,0,2,0]+v[0,0,0,2]),
   w[1,0,0,0]+u[0,0,0,0]*w[0,1,0,0]+v[0,0,0,0]*w[0,0,1,0]
         +w[0,0,0,0]*w[0,0,0,1]+p[0,0,0,1]
         -1/rl*(w[0,2,0,0]+w[0,0,2,0]+w[0,0,0,2]),
   u[0,1,0,0]+v[0,0,1,0]+w[0,0,0,1]
]:
res:=DifferentialThomasDecomposition(L,[]);
```

$$res := [DifferentialSystem]$$

A THOMAS decomposition yields one simple differential system, which only adds the POISON pressure equation as compatibility condition to the input. We compute the dimension polynomial and also its representation in the free basis.

```
DifferentialSystemDimensionPolynomial(res[1]);
```

$$s^3 + 11/2\, s^2 + 17/2\, s + 4$$

```
DifferentialSystemDimensionPolynomialCanonicalBase(res[1]);
```

$$6\binom{3+s}{s} - \binom{2+s}{s} - 1 - s$$

Furthermore, the HILBERT polynomial can be computed,

```
DifferentialSystemHilbertPolynomial(res[1]);
```

$$3\, s^2 + 8\, s + 4$$

```
DifferentialSystemHilbertPolynomialCanonicalBase(res[1]);
```

$$-2 + 6\binom{2+s}{s} - s$$

as can the strength,

```
DifferentialSystemStrength(res[1]);
```

$$18$$

and the CARTAN characters. The latter ones are a list of numbers and are measured depending on the differentiation order. When called with a system as sole parameter, the following command computes the CARTAN characters in the smallest reasonable order. A positive interger given as a second parameter is used for the order.

```
DifferentialSystemCartanCharacters(res[1]);
```

$$2,\ [15, 11, 6, 0]$$

```
DifferentialSystemCartanCharacters(res[1],3);
```

$$3,\ [32, 17, 6, 0]$$

Older implementations are cited in [KLMP99, IX.§1], which also shows alternative approaches to compute the differential dimension polynomial. ◁

1.7 Proofs for the Differential Dimension Polynomial

This section proves Theorem 1.74 about the differential dimension polynomial. First it reduces the crucial parts of the statements to the case of algebraic systems. Then, it studies KRULL dimensions and zero-divisors in the case of simple algebraic systems. This allows to prove the theorem. The proof uses elementary facts from commutative algebra (cf. [Eis95, §2, §3, §8]).

Let F be a differential field of characteristic zero, $<$ an orderly ranking, $\Delta = \{\partial_1, \dots, \partial_n\}$ be a non-empty set of derivation operators, and $U = \{u^{(1)}, \dots, u^{(m)}\}$ be a non-empty set of differential indeterminates.

1.7.1 A Reduction to the Algebraic Case

The following lemma, which is essential for the proof of the Theorem 1.74, is a consequence of passivity. Define $\mathcal{I}(S)_{\leq \ell} := \mathcal{I}(S) \cap F\{U\}_{\leq \ell}$.

Lemma 1.93. *Let S be a simple differential system in $F\{U\}$, $\ell \in \mathbb{Z}_{\geq 0}$, and $<$ an orderly ranking. Then the equality*

$$\mathcal{I}_{F\{U\}_{\leq \ell}}(S_{\leq \ell}) = \mathcal{I}(S)_{\leq \ell}$$

of algebraic ideals in $F\{U\}_{\leq \ell}$ holds, where $S_{\leq \ell}$ is the simple algebraic system up to order ℓ associated to S (cf. Subsection 1.4.1).

Proof. Let $p \in F\{U\}_{\leq \ell}$. Then $p \in \mathcal{I}(S_{\leq \ell})$ if and only if $\mathsf{Reduce}(S_{\leq \ell}, p) = 0$ (cf. Proposition 1.62). This is equivalent to the existence of a (possibly empty) product q of initials of equations in $(S_{\leq \ell})^{=}$ and the existence of $a_s \in F\{U\}_{\leq \ell}$ for all $s \in (S_{\leq \ell})^{=}$ such that $qp = \sum_{s \in (S_{\leq \ell})^{=}} a_s s$. As the initial of a derivative ∂p for $\partial \in \Delta$ and $p \in F\{U\}$ is the separant $\operatorname{sep}(p)$, this holds if and only if there exists a product q of initials and separants of equations in $(S_{\leq \ell})^{=}$ and there exist $a_t \in F\{U\}_{\leq \ell}[\Delta(t, S^{=})]$ such that $\deg_{\Delta}(a_t) \cdot \operatorname{ord}(t) \leq \ell$ for all $t \in S^{=} \cap F\{U\}_{\leq \ell}^{\{=\}}$ with $qp = \sum_{S^{=} \cap F\{U\}_{\leq \ell}^{\{=\}}} a_t t$; this equivalence follows from [Rob12, 2.2.42], which implies that the ideals associated to simple systems are saturated with respect to inequations, in particular separants. This is equivalent to $\mathsf{Reduce}(S, p) = 0$ (cf. Remark 1.39) and to $p \in \mathcal{I}(S)$ (cf. Proposition 1.66). □

1.7.2 The Algebraic Case - Zero Divisors and Dimension

Lemma 1.93 reduces certain questions about differential ideals to questions about algebraic ideals. Now, the proof of Theorem 1.74 about the differential dimension polynomial needs statements about ideals associated to simple algebraic systems.

Certain invariants of an ideal associated to a simple algebraic system can directly be read off the simple algebraic system. This subsection discusses the (Krull-)dimension and zero-divisors of ideals associated to simple algebraic systems.

It turns out that the dimension is equal to the number of indeterminates that do not show up as leaders of equations. A similar result is valid for regular chains (cf. [Hub03a, Theorem 4.4]).

Theorem 1.94. *Let S be a simple algebraic system in $R = F[y_1, \dots, y_n]$. Then $R/\mathcal{I}(S)$ is equidimensional*[27] *of dimension* $\dim(R/\mathcal{I}(S)) = n - |S^=|$.

Further results on prime decompositions of algebraic and differential ideals associated to simple algebraic systems are collected in Appendix D.

For the proof one needs to look at zero-divisors of ideals associated to simple algebraic systems. They are used in this and other proofs and also clarify the connection between simple systems and regular chains. It is clear from the definition by saturation of an ideal $\mathcal{I}(S)$ associated to a simple algebraic system S that none of the initials of equations are zero-divisors modulo $\mathcal{I}(S)$. This lemma is a stronger version of this statement:

Lemma 1.95. *Let S be a simple algebraic system in $F[y_1, \dots, y_n]$ where S_{y_n} is an equation. Then* $\operatorname{init}(S_{y_n})$ *is not a zero-divisor in $F[y_1, \dots, y_n]/\mathcal{I}(S_{<y_n})$.*

Proof. By definition of simple systems $\phi_{\mathbf{a}}(\operatorname{init}(S_{y_n})) \neq 0 \ \forall \ \mathbf{a} \in \mathfrak{Sol}(S_{<y_n})$ holds (cf. Definition 1.9.(1)). In particular, $\mathfrak{Sol}(\operatorname{init}(S_{y_n}))$ is not a superset of any irreducible component of $\overline{\mathfrak{Sol}(S_{<y_n})}$. Thus, $\operatorname{init}(S_{y_n})$ is not contained in any associated prime of $\mathcal{I}(S_{<y_n})$. Since the set containing zero and zero-divisors is the union of the associated primes the claim follows. □

Corollary 1.96. *Let S be a simple algebraic system in $F[y_1, \dots, y_n]$ and $1 \leq i \leq n$. Then*

$$\mathcal{I}(S_{<y_i}) = \mathcal{I}(S) \cap F[y_1, \dots, y_{i-1}] \ .$$

A system S is called a **regular chain** if S does not contain an inequation, $\operatorname{init}(p_=)$ is not a zero-divisor modulo $\mathcal{I}(S_{<x})$ for every $p_= \in S^=$ with $\operatorname{ld}(p_=) = x$, and S is weakly triangular[28], i.e., $\operatorname{ld}(S_{y_i})$ is not a derivative of $\operatorname{ld}(S_{y_j}) \ \forall \ 1 \leq i \neq j \leq n$ and $S \cap \{c_= \mid c \in F\} = \emptyset$. The above results imply that the equations of a simple systems which are not needed for the Janet completion form a regular chain. Thus, many results about regular chains (cf. [Hub03a, §5]) hold for simple systems and their ideals; we do not use these statements.

Subsection 1.5.1 shows that inequations of a simple system S are not zero-divisors modulo $\mathcal{I}(S)$. The next lemma generalizes this to all polynomials that vanish on none of the points of $\mathfrak{Sol}(S)$.

Lemma 1.97. *Let S be a simple algebraic system in $R = F[y_1, \dots, y_n]$ and $q \in R$ such that $\mathfrak{Sol}(\{q_=\} \cup S) = \emptyset$. Let Q be the commutative multiplicative monoid generated by all inequations in S. Then, $\langle q, \mathcal{I}(S)\rangle \cap Q \neq \emptyset$. In particular, $\mathcal{I}(S) : q^\infty = \mathcal{I}(S)$.*

[27] In the sense that R/P has the same dimension for all associated primes in $R/\mathcal{I}(S)$.

[28] Being weakly triangular is a stronger condition than being triangular.

Proof. Use $(Q^{-1}\langle S^=\rangle) \cap R = \mathcal{I}(S)$ from the following Lemma 1.98. Since q has no solutions in common with S, the Nullstellensatz implies that the ring $Q^{-1}(R/\langle q, S^=\rangle)$ is trivial. In particular, $\mathfrak{m} \cap Q \neq \emptyset$ for all maximal ideals $\mathfrak{m}$ of $R/\langle q, \mathcal{I}(S)\rangle$ and, as $S^{\neq}$ generates Q and $\mathfrak{m}$ is maximal, $\mathfrak{m} \cap S^{\neq} \neq \emptyset$. The Nullstellensatz implies $\prod_{s \in S^{\neq}} s \in \sqrt{\langle q, \mathcal{I}(S)\rangle}$. Thus, there is a $k \in \mathbb{Z}_{\geq 1}$ with $Q \ni \prod_{s \in S^{\neq}} s^k \in \langle q, \mathcal{I}(S)\rangle$. □

Lemma 1.98. *Let S be a simple algebraic system in $R = F[y_1, \ldots, y_n]$ and Q the multiplicatively monoid generated by* $\mathrm{init}(S^=)$. *Then*

(1) $R/\mathcal{I}(S)$ embeds into $Q^{-1}(R/\mathcal{I}(S))$,

(2) $Q^{-1}\mathcal{I}(S)$ is generated by $S^=$ in $Q^{-1}R$, and

(3) $Q^{-1}\mathcal{I}(S) \cap R = \mathcal{I}(S)$.

Proof. The embedding follows from Lemma 1.95. The second statement follows as the initials of $S^=$ are units in $Q^{-1}R$ and so the saturation from Definition 1.61 is trivial. The last statement is trivial as $\mathcal{I}(S)$ embeds into $Q^{-1}\mathcal{I}(S)$. □

The last ingredient for the proof of Theorem 1.94 is a form of the Gauss lemma.

Lemma 1.99 (Gauss, cf. [Eis95, Exercise 3.4])**.** *Let R be a* Noetherian *ring. Let $p \in R[x]$ and denote by I the ideal in R generated by the coefficients of p. Then I contains a non-zero-divisor of R if and only if p is a non-zero-divisor of $R[x]$.*

Proof of Theorem 1.94. Using the notation from Lemma 1.98, we examine the localization $Q^{-1}(R/\mathcal{I}(S))$. By the Gauss Lemma 1.99 an equation S_{y_i} is not a zero-divisor modulo $Q^{-1}\mathcal{I}(S_{<y_i})$, as its leading coefficient is invertible. Thus, $S^=$ is a regular sequence in $Q^{-1}R$. Since this regular sequence generates the ideal $Q^{-1}\mathcal{I}(S)$ by Lemma 1.98, the ring $Q^{-1}(R/\mathcal{I}(S))$ is a complete intersection. Thus, $Q^{-1}(R/\mathcal{I}(S))$ is Cohen-Macaulay. By the Unmixedness Theorem [Eis95, Corollary 18.14] every associated prime of $Q^{-1}(R/\mathcal{I}(S))$ has the same codimension $n - |S^=|$.

The results from $Q^{-1}(R/\mathcal{I}(S))$ transfer back to $R/\mathcal{I}(S)$. Let P be an associated prime of $\mathcal{I}(S)$. It can be written as $P = P' \cap R$ for an associated prime P' of $Q^{-1}\mathcal{I}(S)$ as $Q^{-1}\mathcal{I}(S) \cap R = \mathcal{I}(S)$. The codimension of P' and P are equal as codimensions of an ideal in localizations and the codimension the intersection of the ideal with the original ring are equal. So every associated prime of $\mathcal{I}(S)$ has codimension $n - |S^=|$ and, thus, $\mathcal{I}(S)$ has codimension $n - |S^=|$. □

The dimension formula in Theorem 1.94 follows more easily by integral ring extensions after the localization with Q; this would not have implied equidimensionality.

Corollary 1.100. *Let S be a simple algebraic system in $R = F[y_1, \ldots, y_n]$. The set $\{y_1, \ldots, y_n\} \setminus \mathrm{ld}(S^=)$ forms a transcendence basis for every associated prime of $\mathcal{I}(S)$.*

Proof. By Lemma 1.95 an associated prime contains no initial of an element in $S^=$. This implies that the elements of $\mathrm{ld}(S^=)$ are algebraic over $Y := \{y_1, \ldots, y_n\} \setminus \mathrm{ld}(S^=)$. Now, Y is a transcendence basis due to dimension arguments from Theorem 1.94. □

Lemma D.3 is a stronger form of this corollary. It states that this transcendence basis $\{y_1, \ldots, y_n\} \setminus \mathrm{ld}(S^=)$ is minimal with respect to the ranking.

Corollary 1.96 states that the intersection of ideals associated to simple algebraic systems with subrings is well-behaved. This holds in a stronger version for the associated primes of $\mathcal{I}(S)$ (cf. also [Hub03a, Proposition 5.8]).

Lemma 1.101. *Let S be a simple algebraic system in $R = F[y_1, \ldots, y_n]$ and $1 \le i \le n$. Then an ideal P is an associated prime of $\mathcal{I}(S_{<y_i})$ if and only if there exists an associated prime Q of $\mathcal{I}(S)$ such that $P = Q \cap F[y_1, \ldots, y_{i-1}]$.*

Note that $\mathcal{I}(S_{<y_i}) = \mathcal{I}(S) \cap F[y_1, \ldots, y_{i-1}]$, which follows easily from the reduction statement in Proposition 1.62 (cf. also Proposition A.1).

Proof. For the one direction let Q be an associated prime of $\mathcal{I}(S)$. Then, $P := Q \cap F[y_1, \ldots, y_{i-1}]$ is still a prime ideal that contains $\mathcal{I}(S_{<y_i})$. Thus, it must contain a minimal associated prime P' of $\mathcal{I}(S_{<y_i})$. There exists a simple algebraic system S' such that $\mathcal{I}(S') = Q$ (cf. Proposition 1.70) and the set $\operatorname{ld}((S')^{=})$ is the same as $\operatorname{ld}(S^{=})$ by Corollary 1.100. The residue class ring of the ideal $P = \mathcal{I}(S'_{<y_i})$ has the same transcendence basis as that of P' by Corollary 1.96. Thus, the ideals are equal, since prime ideals of the same dimension that are contained in each other are equal.

For the converse let $Q_1, \ldots, Q_k$ be the associated primes of $\mathcal{I}(S)$. Then

$$\begin{aligned}
\mathcal{I}(S_{<y_i}) &= \mathcal{I}(S) \cap R_{<y_i} && \text{Corollary 1.96}\\
&= Q_1 \cap \ldots \cap Q_k \cap R_{<y_i} && \mathcal{I}(S) \text{ radical and equidimensional}\\
&= (Q_1 \cap R_{<y_i}) \cap \ldots \cap (Q_k \cap R_{<y_i}) \;.
\end{aligned}$$

The first part of the proof shows that each $Q_j \cap R_{<y_i}$ is an associated prime of $\mathcal{I}(S_{<y_i})$. The ideal $\mathcal{I}(S_{<y_i})$ is the intersection of its associated prime as it is radical (cf. Proposition 1.62), and this intersection is minimal as $\mathcal{I}(S_{<y_i})$ is equidimensional (cf. Theorem 1.94). So any associated prime of $\mathcal{I}(S_{<y_i})$ must be among the $Q_j \cap R_{<y_i}$. □

This lemma directly implies the following proposition.

Proposition 1.102. *Let S be a simple algebraic system in $F[y_1, \ldots, y_n]$ and $1 \le i \le n$. If $0 \ne p \in F[y_1, \ldots, y_{i-1}]$ is not a zero-divisor modulo $\mathcal{I}(S_{<y_i})$, then p is not a zero-divisor modulo $\mathcal{I}(S)$.*

1.7.3 The Proof

These preparations allow to prove most of Theorem 1.74. The proof of Theorem 1.74.(3) follows on page 86, and the proof of Theorem 1.74.(6) and (7) follows on page 87.

Proof of Theorem 1.74.(1), (2), (4), and (5). Lemma 1.93 implies $I_{\le \ell} = \mathcal{I}(S_{\le \ell})$. Then, Theorem 1.94 states that $\dim(F\{U\}_{\le \ell}/I_{\le \ell})$ equals the number of differential variables in $F\{U\}_{\le \ell}$ minus the number of equations in $S_{\le \ell}$. Now, the number of differential variables in the complement of a set closed under Δ follows easily from the combinatorial approach by Janet (cf. Lemma 1.71 and Lemma 1.80). This proves (1) and (2).

For (4) let d denote the differential dimension of $F\{U\}/I$.

We first show the inequality $a_n \le d$. Note that there are a_n cones of dimension n in the Janet decomposition of the complement of the Δ-closed set of differential variables $\operatorname{ld}(S^{=})$. For each differential indeterminate u associated to such a cone there cannot be a differential equation in S with a leader associated to u, as otherwise at least one such equation has a cone of dimension n and the complement cannot have a cone of dimension n. Thus, these a_n differential indeterminates are differentially independent, since any constraint between these differential indeterminates would reduce to zero with respect to S.

For the other inequality $a_n \ge d$ of (4) let $\{p_1, \ldots, p_d\}$ be a differential transcendence basis of $F\{U\}/I$ and denote by θ_i the order of p_i for $1 \le i \le d$ and $\theta_0 := \max_i \theta_i$

the maximal order. Then, the differential F-subalgebra $F\{p_1, \ldots, p_d\}$ generated by $p_1, \ldots, p_d$ has an induced filtration $F\{p_1, \ldots, p_d\}_{\leq \ell} := F\{U\}_{\leq \ell} \cap F\{p_1, \ldots, p_d\}$. As the p_i are a differential transcendence basis,

$$\dim(F\{p_1, \ldots, p_d\}_{\leq \ell}) = \sum_{i=1}^{d} \binom{n + (\ell - \theta_i)}{n} .$$

for $\ell \geq \theta_0$. Since $F\{p_1, \ldots, p_d\}/(I \cap \{p_1, \ldots, p_d\})$ is a subalgebra of $F\{U\}/I$,

$$\begin{aligned}
\omega_I(\ell) &= \sum_{i=0}^{n} a_i \binom{\ell + i}{i} \\
&\geq \dim(F\{p_1, \ldots, p_d\}_{\leq \ell}) \\
&= \sum_{i=1}^{d} \binom{n + (\ell - \theta_i)}{n} \\
&\geq d \binom{n + (\ell - \theta_0)}{n}
\end{aligned}$$

for $\ell \geq \theta_0$. In particular, the leading coefficient a_n of ω_I fulfills $a_n \geq d$, as the total order on numerical polynomials is equivalent to the order defined by the comparison of the coefficients (cf. Remark 1.72).

The proof of (5) is trivial: $I \subseteq J$ implies $I_{\leq \ell} \subseteq J_{\leq \ell}$ for all $\ell \geq 0$. In particular, the map from $F\{U\}_{\leq \ell}/I_{\leq \ell}$ to $F\{U\}_{\leq \ell}/J_{\leq \ell}$ is surjective and, thus, $\dim(F\{U\}_{\leq \ell}/I_{\leq \ell}) \geq \dim(F\{U\}_{\leq \ell}/J_{\leq \ell})$. □

Kolchin's classical Theorem about the differential dimension polynomial states that the degree, leading coefficient and coefficient of degree n of the dimension polynomial are birational invariants of a prime differential ideal. This is claimed above for the more general case of differential ideals associated to simple differential systems. The next aim is to prove this invariance condition. We begin by showing that the filtration on the differential polynomial ring $F\{U\}/\mathcal{I}(S)$ induces a filtration on the total quotient ring $\mathrm{K}(F\{U\}/\mathcal{I}(S))$. This allows to use standard techniques of filtrations adapted from Kolchin's proof [Kol73, §II.12].

The differential polynomial ring $F\{U\}$ admits a filtration by finitely generated F-algebras $F\{U\}_{\leq i}$; call it the **orderly filtration**. It is not true for all differential ideals I that the orderly filtration on the ring $F\{U\}/I$ induces a filtration on $\mathrm{K}(F\{U\}/I)$.

Example 1.103. Consider $\Delta = \{\partial_t\}$ and $U = \{u, v\}$. Let I be the differential ideal generated by $u_0 \cdot v_1$. The differential polynomial u_0 is not a zero-divisor in $F\{U\}_{\leq 0} \cong F[u_0, v_0]$ modulo $I_{\leq 0} = \{0\}$. But obviously, $u_0 \cdot v_1 = 0$ in $F\{U\}/I$.

The first total quotient ring of the filtration $\mathrm{K}(F\{U\}_{\leq 0}/I_{\leq 0}) = \mathrm{K}(F[u_0, v_0]) = F(u_0, v_0)$ contains the element $\frac{1}{u_0}$, and the first total quotient ring

$$\mathrm{K}(F\{U\}_{\leq 1}/I_{\leq 1}) = \mathrm{K}(F[u_0, v_0, u_1, v_1]/\langle u_0 \cdot v_1 \rangle)$$

does not. ◁

Recall from Subsection 1.3.4 that the ring $F[\Delta]$ of linear differential operators is filtered by order and that $F\{U\}$ is a (left) $F[\Delta]$-module. The orderly filtration of $F\{U\}$ is compatible with the $F[\Delta]$-module structure of $F\{U\}$, since $\Delta(F\{U\}_{\leq i}) \subseteq F\{U\}_{\leq i+1}$.

Let R be a $F[\Delta]$-algebra with a filtration $(R_{\leq i})_{i=0}^{\infty}$ and $R_{\leq 0} = F$. This filtration is called **exhaustive** if $\bigcup_i R_{\leq i} = R$. The filtration on $F\{U\}/I$ induced by the orderly filtration is exhaustive for any differential ideal I in $F\{U\}$. If the differential ideal is associated to a simple differential system, then there is an induced exhaustive filtration on the total quotient ring of $F\{U\}/I$.

Lemma 1.104. *Let S be a simple differential system in $F\{U\}$ and $I := \mathcal{I}(S)$. Then,*

$$\mathrm{K}(F\{U\}_{\leq \ell}/I_{\leq \ell}) \hookrightarrow \mathrm{K}(F\{U\}_{\leq \ell+1}/I_{\leq \ell+1})$$

induced by $F\{U\}_{\leq \ell}/I_{\leq \ell} \hookrightarrow F\{U\}_{\leq \ell+1}/I_{\leq \ell+1}$ is a monomorphism for all $\ell \in \mathbb{Z}_{\geq 0}$. In particular, the total quotient ring $\mathrm{K}(F\{U\}/I)$ has an exhaustive filtration by the total quotient rings $\mathrm{K}(F\{U\}_{\leq \ell}/I_{\leq \ell})$.

Proof. Every non-zero-divisor p of $F\{U\}_{\leq \ell}/I_{\leq \ell}$ is a non-zero-divisor when considered in $F\{U\}_{\leq \ell+1}/I_{\leq \ell+1}$. This is the statement of Proposition 1.102, which also holds for the differential cases due to Lemma 1.46. Thus, such a p maps to a unit in $\mathrm{K}(F\{U\}_{\leq \ell+1}/I_{\leq \ell+1})$ by the canonical map. This implies that the map $F\{U\}_{\leq \ell}/I_{\leq \ell} \to \mathrm{K}(F\{U\}_{\leq \ell+1}/I_{\leq \ell+1})$ factors over $\mathrm{K}(F\{U\}_{\leq \ell}/I_{\leq \ell})$ by the universal property of localizations.

Show that this map $\mathrm{K}(F\{U\}_{\leq \ell}/I_{\leq \ell}) \to \mathrm{K}(F\{U\}_{\leq \ell+1}/I_{\leq \ell+1})$ is monic. Let the ideal $J \subseteq \mathrm{K}(F\{U\}_{\leq \ell}/I_{\leq \ell})$ be the kernel of $\mathrm{K}(F\{U\}_{\leq \ell}/I_{\leq \ell}) \to \mathrm{K}(F\{U\}_{\leq \ell+1}/I_{\leq \ell+1})$. As there is a bijection between ideals in $\mathrm{K}(F\{U\}_{\leq \ell}/I_{\leq \ell})$ and ideals in $F\{U\}_{\leq \ell}/I_{\leq \ell}$ not containing zero-divisors, the intersection $J \cap F\{U\}_{\leq \ell}/I_{\leq \ell}$ would be non-zero if and only if J is non-zero. However, $J \cap F\{U\}_{\leq \ell}/I_{\leq \ell}$ is also the kernel of the monic composition $F\{U\}_{\leq \ell}/I_{\leq \ell} \hookrightarrow F\{U\}_{\leq \ell+1}/I_{\leq \ell+1} \hookrightarrow \mathrm{K}(F\{U\}_{\leq \ell+1}/I_{\leq \ell+1})$ and, thus, zero. □

The following lemma describes this filtration under differential birational maps.

Lemma 1.105. *Let I and J be a differential ideals associated to simple differential systems in the differential polynomial rings $F\{U\}$ and $F\{V\}$, respectively. Let $\varphi : \mathrm{K}(F\{U\}/I) \to \mathrm{K}(F\{V\}/J)$ be a differential birational map from $F\{U\}/I$ to $F\{V\}/J$ and φ^{-1} its inverse. Then, for the filtrations from Lemma 1.104 there exists an $\ell_0 \in \mathbb{Z}_{\geq 0}$ such that*

$$\varphi(\mathrm{K}(F\{U\}_{\leq \ell}/I_{\leq \ell})) \subseteq \mathrm{K}(F\{V\}_{\leq \ell+\ell_0}/J_{\leq \ell+\ell_0}) \quad \textit{and}$$
$$\varphi^{-1}(\mathrm{K}(F\{V\}_{\leq \ell}/J_{\leq \ell})) \subseteq \mathrm{K}(F\{U\}_{\leq \ell+\ell_0}/I_{\leq \ell+\ell_0})$$

Proof. It suffices to show only one of the two inclusions; the other inclusion follows by symmetry and taking ℓ_0 to be the maximum of the ℓ_0's of both inclusions.

For legibility write $R := F\{U\}/I$ and $R' := F\{V\}/J$. Then

$$R_{\leq \ell} = F[\Delta]_{\leq \ell} R_{\leq 0} \ . \tag{1.3}$$

The orderly filtration on $F\{V\}/J$ is exhaustive. Thus, there exists an $\ell_0 \in \mathbb{Z}_{\geq 0}$ with

$$\varphi(R_{\leq 0}) \subseteq \mathrm{K}(R'_{\leq \ell_0}) \ . \tag{1.4}$$

Then the claim follows:

$$\begin{aligned}
\varphi(\mathrm{K}(R_{\leq \ell})) &= \mathrm{K}(\varphi(R_{\leq \ell})) \\
&= \mathrm{K}(\varphi(F[\Delta]_{\leq \ell} R_{\leq 0})) && \text{by (1.3)} \\
&= \mathrm{K}(F[\Delta]_{\leq \ell} \varphi(R_{\leq 0})) && \text{as } \varphi \text{ commutes with } \Delta \\
&\subseteq \mathrm{K}(F[\Delta]_{\leq \ell} \mathrm{K}(R'_{\leq \ell_0})) && \text{by (1.4)} \\
&\subseteq \mathrm{K}(R'_{\leq \ell+\ell_0})
\end{aligned}$$

□

The KRULL-dimension is well-behaved for finitely generated F-algebras. However, information about the KRULL-dimension is lost when passing to the total quotient ring. For example $\dim(F[x]) = 1$ but $\dim(\mathrm{K}(F[x])) = \dim(F(x)) = 0$. Thus, use $\max_{P\in\mathrm{Ass}(R)} \mathrm{trdeg}_F(\mathrm{K}(R/P))$ as notion of dimension, which is better-behaved when passing to the total quotient ring. This dimension coincides with the KRULL-dimension for finitely generated F-algebras R, i.e., $\dim(R) = \max_{P\in\mathrm{Ass}(R)} \mathrm{trdeg}_F(\mathrm{K}(R/P))$. It is well-behaved when passing to the total quotient ring:

$$\dim(R) = \max_{P\in\mathrm{Ass}(R)} \mathrm{trdeg}_F(\mathrm{K}(R/P)) = \max_{P\in\mathrm{Ass}(\mathrm{K}(R))} \mathrm{trdeg}_F(\mathrm{K}(\mathrm{K}(R)/P)) \ . \tag{1.5}$$

For this notion of dimension, the dimensions of both $F\{U\}_{\le\ell}/I_{\le\ell}$ and its quotient ring agree. This allows to give the next part of the proof.

Proof of Theorem 1.74.(3). By Lemma 1.105 there exists an $\ell_0 \in \mathbb{Z}_{\ge 0}$ with

$$\varphi(\mathrm{K}(F\{U\}_{\le\ell}/I_{\le\ell})) \subseteq \mathrm{K}(F\{V\}_{\le\ell+\ell_0}/J_{\le\ell+\ell_0}) \ .$$

Since φ is a monomorphism,

$$\begin{aligned}\mathrm{K}(F\{U\}_{\le\ell}/I_{\le\ell}) &\cong \varphi(\mathrm{K}(F\{U\}_{\le\ell}/I_{\le\ell}))\\ &\subseteq \mathrm{K}(F\{V\}_{\le\ell+\ell_0}/J_{\le\ell+\ell_0})\end{aligned}$$

which implies

$$\begin{aligned}\dim(F\{U\}_{\le\ell}/I_{\le\ell}) &= \max_{P\in\mathrm{Ass}(\mathrm{K}(F\{U\}_{\le\ell}/I_{\le\ell}))} \mathrm{trdeg}_F(\mathrm{K}(\mathrm{K}(F\{U\}_{\le\ell}/I_{\le\ell})/P))\\ &\le \max_{P\in\mathrm{Ass}(\mathrm{K}(F\{V\}_{\le\ell+\ell_0}/J_{\le\ell+\ell_0}))} \mathrm{trdeg}_F(\mathrm{K}(\mathrm{K}(F\{V\}_{\le\ell+\ell_0}/J_{\le\ell+\ell_0})/P))\\ &= \dim(F\{V\}_{\le\ell+\ell_0}/J_{\le\ell+\ell_0})\end{aligned}$$

using (1.5) twice. This implies $\omega_I(\ell) \le \omega_J(\ell+\ell_0)$ and by symmetry $\omega_J(\ell) \le \omega_I(\ell+\ell_0)$. At last, Remark 1.72 proves the claim. □

The proof of Theorem 1.74.(6) and (7) uses relations between ideals and equations in simple algebraic systems, which are presented in the following two propositions.

Proposition 1.106. *Let S, S' be simple algebraic systems in $R = F[y_1,\ldots,y_n]$ with $\mathcal{I}(S) \subseteq \mathcal{I}(S')$ and $|S^=| = |S'^=|$. Then the sets of leaders of the equations of S and S' coincide, i.e., $\mathrm{ld}(S^=) = \mathrm{ld}(S'^=)$.*

Proof. Let $\{P_1,\ldots,P_k\}$ the associated primes of $\mathcal{I}(S)$ and $\{Q_1,\ldots,Q_\ell\}$ the associated primes of $\mathcal{I}(S')$. The condition $|S^=| = |S'^=|$ implies that all P_i and Q_i are of the same dimension (cf. Theorem 1.94). Further, the intersections $\mathcal{I}(S) = \bigcap_{i=1}^k P_i$ and $\mathcal{I}(S') = \bigcap_{i=1}^\ell Q_i$ are minimal, and all ideals are radical (cf. Proposition 1.62). The condition $\mathcal{I}(S) \subseteq \mathcal{I}(S')$ now implies $k \ge \ell$ and $\{P_1,\ldots,P_k\} \supseteq \{Q_1,\ldots,Q_\ell\}$. By renaming, assume without loss of generality that $\{P_1,\ldots,P_\ell\}$ are the associated primes of $\mathcal{I}(S')$.

Assume that the claim does not hold. Let $x \in \{y_1,\ldots,y_n\}$ such that S has an equation of leader x and S' does not has an equation of leader x. Then $\mathsf{reduce}(S', S_x) = 0$ as $S_x \in \mathcal{I}(S) \subseteq \mathcal{I}(S')$ (cf. Proposition 1.62). This implies $\mathsf{reduce}(S', q) = 0$ for $q := \mathrm{init}(S_x)$ as there is no equation in S' with leader x to reduce S_x. This initial q is not a zero-divisor module $\mathcal{I}(S)$ and, thus, not contained in any associated prime ideal $P_1,\ldots,P_k$ of $\mathcal{I}(S)$. However, q is contained in each one of $P_1,\ldots,P_\ell$ as $q \in \mathcal{I}(S')$. This implies $k = 0$ and $\mathcal{I}(S) = \langle 1\rangle$. Hence S has no solutions, which is a contradiction to every simple algebraic system having a solution (cf. Remark 1.10). □

Proposition 1.107. *Let S, S' be simple algebraic systems in $R = F[y_1, \ldots, y_n]$ with $\mathcal{I}(S) \subseteq \mathcal{I}(S')$ and $|S^{=}| = |S'^{=}|$. Then, $\mathcal{I}(S) = \mathcal{I}(S')$ if and only if $\deg_x(S_x) = \deg_x(S'_x)$ for all $x \in \mathrm{ld}(S^{=}) = \mathrm{ld}((S')^{=})$ (for this last equality $\mathrm{ld}(S_x) = \mathrm{ld}(S'_x)$ see Proposition 1.106).*

Proof. Assume that $\deg_x(S_x) = \deg_x(S'_x)$ for all $x \in \mathrm{ld}(S^{=})$ and show $\mathcal{I}(S) = \mathcal{I}(S')$. The statement is clear for $\mathcal{I}(S_{\leq y_1}) = \mathcal{I}(S'_{\leq y_1})$ as these are principle ideals contained in each other and generated by a polynomial of the same degree. Assume by the induction that $\mathcal{I}(S)_{<y_i} = \mathcal{I}(S')_{<y_i}$ and let $p \in R$ with $\mathrm{ld}(p) = y_i$. Thus, $\mathrm{init}(p) \in \mathcal{I}(S)$ if and only if $\mathrm{init}(p) \in \mathcal{I}(S')$ as $\mathrm{ld}(\mathrm{init}(p)) < y_i$. Furthermore, there is an equation in S of leader y_i if and only if there is in S', and if they exist they have the same degree in y_i. Thus, p can be reduced with respect to S if and only if it can be with respect to S' as can easily be seen by the reduction algorithm reduce (cf. Algorithm 1.15).

Assume that there is an $x \in \mathrm{ld}(S^{=})$ with $\deg_x(S_x) > \deg_x(S'_x)$ and show $\mathcal{I}(S) \neq \mathcal{I}(S')$. (The methods of this proof easily imply that $\deg_x(S_x) < \deg_x(S'_x)$ contradicts $\mathcal{I}(S) \subseteq \mathcal{I}(S')$.) Then, $\mathsf{reduce}(S, S'_x) = 0$ holds, since $S'_x \in \mathcal{I}(S)$ and this implies $\mathsf{reduce}(S, q) = 0$ for $q := \mathrm{init}(S'_x)$ as there is no equation in S with leader x to reduce S'_x. So $q \in \mathcal{I}(S)$. Now, $\mathcal{I}(S) = \mathcal{I}(S')$ would contradict $\mathcal{I}(S')$ being saturated with respect to q by the definition of ideals associated to simple algebraic systems (cf. Definition 1.61). □

Proof of Theorem 1.74.(7). Again, Lemma 1.93 reduces the statements to the algebraic case. In this case, Proposition 1.106 implies (6), and (7) follows from Proposition 1.107, because the only equations of main degree greater one in $S_{\leq \ell}$ are those of S for every $\ell \in \mathbb{Z}_{\geq 0}$. □

Chapter 2

Differential Counting Polynomials

This chapter discusses the size of the set of power series solutions of systems of differential equations in detail, using counting polynomials. This yields a more precise overview over the solutions than the differential dimension polynomial. However, computing the differential version of the counting polynomial is not algorithmic. In particular, the differential THOMAS decomposition is not used in this chapter, and instead we rely on certain modifications of the algebraic THOMAS decomposition for equations and inequations, which both restrict the power series coefficients. Another result of this chapter are certain phenomena of differential equations that involve countable infinite sets.

2.1 An Overview

This expository section introduces the algebraic counting polynomial, the counting sequence, and the differential counting polynomial and its properties by examples. It gives informal definitions; the precise ones can be found in the following sections.

2.1.1 Algebraic Counting Polynomial

The motivation for the differential counting polynomial originates from the algebraic counting polynomial, which in a certain sense describes the cardinality of the solution set of an algebraic system over $F[y_1, \ldots, y_n]$ for a field F of characteristic zero. The algebraic counting polynomial can be read off a simple algebraic system, and it can be computed for any algebraic system using an algebraic THOMAS decomposition.

Simple systems over the univariate polynomial ring motivate the algebraic counting polynomial. If such a system is given by a square-free equation of degree d, then its solution set is finite and its algebraic counting polynomial is d. If such a system is given by a square-free inequation of degree d, then its solution set is cofinite in $\overline{F}$ and its algebraic counting polynomial is $\infty - d$. Here, ∞ is a formal indeterminate of the polynomial ring $\mathbb{Z}[\infty]$ and might be interpreted as the cardinality of the algebraic closure $\overline{F}$ of F.

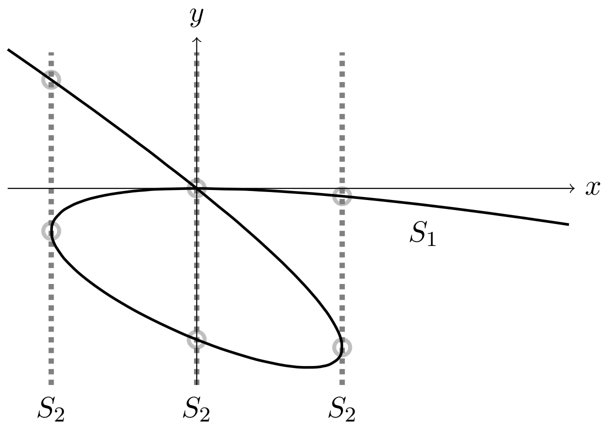
This generalizes for any simple algebraic system S using the fibration of the space induced by the ranking. There exists a covering projection from the solution set of $S_{\leq y_n}$ to the solution set of the restricted simple algebraic system $S_{\leq y_{n-1}}$ viewed in $\overline{F}^{n-1}$. View the elements in the fibres of this covering projection as elements in $\overline{F}$. Each such fiber has the same cardinality or cocardinality in $\overline{F}$, which depends only on the degree of the equation or inequation of S with leader y_n. Then the counting polynomial of $S_{\leq y_n}$ is defined as the algebraic counting polynomial of any such fiber multiplied by the algebraic counting polynomial of $S_{<y_n}$. A THOMAS decomposition allows to examine the solution sets of arbitrary systems.

Example 2.1. Recall from Example 1.8 that a THOMAS decomposition of

$$\{p := \underline{y}^3 + (3x+1)y^2 + (3x^2+2x)y + x^3 = 0\}$$

is given by

$$\begin{array}{ll} S_1 := \{ & \underline{y}^3 + (3x+1)y^2 + (3x^2+2x)y + x^3 = 0, \quad 27\underline{x}^3 - 4x \neq 0\} \\ S_2 := \{ & 6\underline{y}^2 + (-27x^2+12x+6)y - 3x^2 + 2x = 0, \quad 27\underline{x}^3 - 4x = 0\} \end{array}$$



The image shows the solution set of $\{p = 0\}$ in the real affine plane. The cardinality of the fibers of the projection onto the x-component along the y-axis depends on y and is constant within each system; i.e., the fibers of the projection onto the x-component are of cardinality 3 and 2 in the solution sets of S_1 and S_2, respectively. (This image cannot show certain complex, non-real solutions of S_1.)

Rephrasing this, the system S_1 implies that for each x-value in $\overline{F}$ except the three solutions of $27x^3 - 4x = 0$ there are 3 solutions of $\{p = 0\}$. This set of solutions can be described by $(\infty - 3) \cdot 3$. The system S_2 implies that for three solutions of $27x^3 - 4x = 0$ there are 2 solutions of $\{p = 0\}$. This set of solutions can be described by $3 \cdot 2$. Adding up, the solution set of the system $\{p = 0\}$ has algebraic counting polynomial $(\infty - 3) \cdot 3 + 3 \cdot 2 = 3\infty - 3 \in \mathbb{Z}[\infty]$. ◁

2.1.2 Motivating Examples for the Differential Counting

In a nutshell, the idea when counting solutions of differential equations is to give the algebraic counting polynomial for the set of TAYLOR polynomials of degree ℓ for each $\ell \in \mathbb{Z}_{\geq 0}$. The sequence of these algebraic counting polynomials is called counting sequence, and the ℓ-th element of this sequence is called the ℓ-th differential counting polynomial. Furthermore, if these differential counting polynomials can ultimately be given by a closed formula, then this closed formula is called the differential counting polynomial. We give some expository examples for this.

Example 2.2. Consider the heat equation $u_{xx} - u_t = 0$ with u_{xx} as leader. Then, for a power series solution ansatz

$$u(t,x) = \sum_{i,j=0}^{\infty} g_{i,j} \frac{t^i x^j}{i!j!}$$

a coefficient $g_{i,j+2}$ is uniquely determined by the coefficient $g_{i+1,j}$ for all $i, j \geq 0$. The linearity of these equations implies that a power series coefficient can either be chosen freely (the $g_{0,i}$'s and $g_{1,i}$'s) or is uniquely determined. In particular, $2\ell + 1$ coefficients can be chosen freely up to order ℓ. The counting sequence is $\ell \mapsto \infty^{2\ell+1}$, the ℓ-th differential counting polynomial is $\infty^{2\ell+1}$ for all $\ell \in \mathbb{Z}_{\geq 0}$, and the differential counting polynomial is $\infty^{2\ell+1}$. ◁

The degree of the algebraic counting polynomial of a variety is equal to its KRULL dimension. Also the dimension polynomial is defined using the KRULL dimension. This allows the differential counting polynomial to generalize the dimension polynomial in a way made precise by Theorem 2.36.

This generalization can easily be understood for a set of differential equations with constant coefficients over the complex numbers $\mathbb{C}$, as in the previous example. Any such linear system can be transformed into one simple differential system S, and the number of free power series coefficients is given by the differential dimension function $\Omega_{\mathcal{I}(S)}$, i.e., the counting sequence is

$$\ell \mapsto \infty^{\Omega_{\mathcal{I}(S)}(\ell)} ,$$

and the differential counting polynomial is $\infty^{\omega_{\mathcal{I}(S)}(\ell)}$, using the differential dimension polynomial $\omega_{\mathcal{I}(S)}(\ell)$. Thus, for the linear case, the counting sequence holds no more information than the differential dimension function and essentially no more information than the differential dimension polynomial. Such a formula also holds for certain nonlinear systems of equations. In the case of one simple differential system S over the complex numbers without inequations, for each power series coefficient there are as many choices as the degree of the equation for this coefficient, once all lower power series coefficients are fixed. Thus, the counting sequence is

$$\ell \mapsto \prod_{\substack{1 \leq i \leq s \\ \operatorname{ord}(p_i) \leq \ell}} \operatorname{mdeg}(p_i) \cdot \infty^{\Omega_{\mathcal{I}(S)}(\ell)} ,$$

(cf. Theorem 2.72) and the differential counting polynomial is

$$\prod_{1 \leq i \leq s} \operatorname{mdeg}(p_i) \cdot \infty^{\omega_{\mathcal{I}(S)}(\ell)} .$$

The next example allows variable coefficients. It turns out that the differential counting polynomial depends on the chosen center for a power series solution.

Example 2.3. Consider the BESSEL equation

$$p := t^2 \cdot u'' + t \cdot u' + (t^2 - \alpha^2) \cdot u = 0$$

for a constant coefficient[1] $\alpha \in \mathbb{C}$ and consider power series solutions of the form

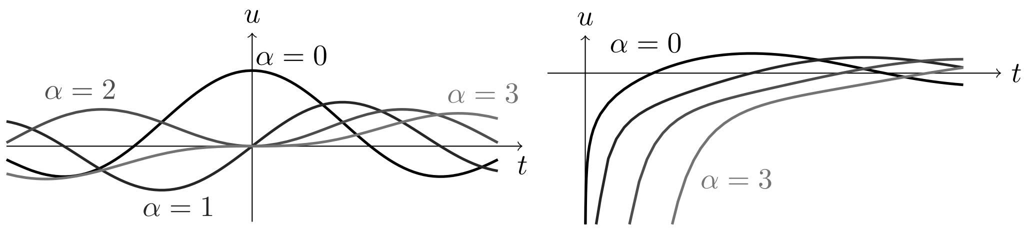
$$u(x) = \sum_{k=0}^{\infty} g_i \frac{(t - t_0)^k}{k!}$$

expanded around the center t_0.

In this example we show that for $t_0 \neq 0$ the differential counting polynomial for formal power series solutions is ∞^2; for $t_0 = 0$ it is ∞ if $\alpha \in \mathbb{Z}$, and it is 1 if $\alpha \notin \mathbb{Z}$. All of these solutions are locally convergent power series.

[1] Many applications restrict to $\alpha \in \frac{1}{2}\mathbb{Z}$ or $\alpha \in \mathbb{Z}$.

Figure 2.1: Bessel functions of the first and second kind in the left resp. right plot for the values 0, 1, 2, and 3 of α.



We begin with an expansion point $t_0 \neq 0$. In this case the initial of the equation is non-zero and one can use $\partial_t^k p$ to solve for the coefficient g_{k+2}. Thus, only the coefficients g_0 and g_1 can be chosen freely. In particular, the zeroth differential counting polynomial is ∞ and the ℓ-th differential counting polynomials are ∞^2 for all $\ell \geq 1$. Riquier's Existence Theorem 1.60 implies that all these solutions converge locally. The solutions are the linear combinations of the Bessel functions of the first and second kind.

Now, let $t_0 = 0$ and consider the derivatives

$$\partial_t^k p = t^2 \cdot u_{k+2} + (1+2k) \cdot t \cdot u_{k+1} + (k^2 + t^2 - \alpha^2) \cdot u_k \\ + 2k \cdot t \cdot u_{k-1} + (k^2 - k) \cdot u_{k-2}$$

of p. After substituting of t by 0 all coefficients of these prolongations of the differential equation vanish except for the third and fifth one; the equation $(k^2 - \alpha^2)g_k + (k^2 - k)g_{k-2} = 0$ remains.

In case of $\alpha \notin \mathbb{Z}$ the coefficient of g_k in this equation is non-zero for all k. Furthermore, the cases $k = 0$ and $k = 1$ imply that the power series coefficients g_0 and g_1 of order 0 and 1 are zero. Thus, the only analytical solution is the zero solution[2], since the k-th coefficient is computed as a multiple of the $(k-2)$-th coefficient. This yields the constant sequence $\ell \mapsto 1$ as counting sequence.

In case of $\alpha \in \mathbb{Z}$ the power series coefficients smaller than order $|\alpha|$ of the solution are zero, as in the previous case $\alpha \notin \mathbb{Z}$. However, the coefficient of $g_{|\alpha|}$ when substituting $t = 0$ in $\partial_t^{|\alpha|} p$ does vanish, and this prolongation finds $g_{|\alpha|-2} = 0$, again. So there is no equation for the power series coefficient of order $|\alpha|$, which can therefore be chosen freely. All further coefficients are determined[3] and, thus, the ℓ-th differential counting polynomial is ∞ for $\ell \geq |\alpha|$ and 1 for $\ell < |\alpha|$. The solutions are the Bessel functions of the first kind. ◁

For certain classes of differential equations the differential counting polynomial can be given by a closed formula.

Theorem 2.4 (cf. Theorem 2.79). *Let $p := A(u)u_1 + B(u) \in \mathbb{C}\{u\}$ and ordinary differential equation with $A(u), B(u) \in \mathbb{C}[u]$ and $A(u)$ not the zero polynomial. The differential counting polynomial of the set of solutions of $p = 0$ is*

$$\infty - b + d + e$$

at a generic center of expansion. Here $b \in \mathbb{Z}$ is the number of distinct zeros of A, $d \in \mathbb{Z}$ is the number of distinct common zeros of A and B, and $e \in \mathbb{Z}$ is the number of distinct common zeros of A and B that appear in A and B with the same multiplicity.

[2] The other solutions $\frac{c \cdot \sin(t)}{\sqrt{t}}$ for $c \in \mathbb{C} \setminus \{0\}$ do not have a power series expansion around 0.

[3] Every second coefficient from order $|\alpha|$ on is non-zero, provided that the coefficient of order $|\alpha|$ was chosen non-zero.

2.1.3 A Geometric Interpretation and Demotivating Example

So far, the counting sequences and the differential counting polynomials were rather well-behaved. However, in general, more involved behavior appears. The following example is intended to give some geometric intuition for possible behaviors. Its descriptive plots shows certain kinds of singularities which prevent the existence of formal power series solutions. This approach is sketched in Appendix E and explains *why* a certain ansatz for a formal power series does not yield a solution.

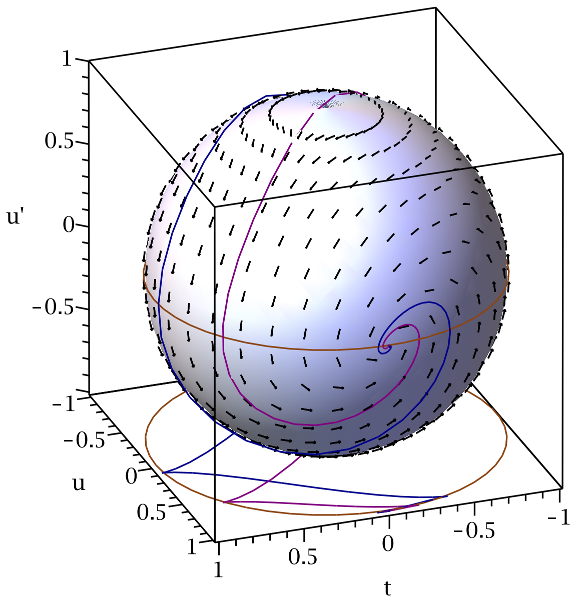
Example 2.5 ([KS12])**.** Consider the differential sphere equation $p = u_t^2 + u^2 + t^2 - 1 = 0$ and complex formal power series solutions of the form

$$u(x) = \sum_{k=0}^{\infty} g_i \frac{(t-t_0)^k}{k!}$$

as set of admissible solutions. It turns out that for $g_0^2 + t_0^2 - 1 = 0$ and $t_0 \neq 0$ no formal power series solution exists and for $t_0 = 1$ and $g_0 = \pm 1$ two formal power series solutions exist. This example gives plausibility arguments for this (cf. Example 2.91 for details).

The geometric approach interprets (possible) solutions as points on the variety given by the equation p, i.e., the sphere, in the space with coordinates t, u, and u_t. On these three coordinates remains a differential structure, the contact distribution. It determines the direction any solution of a differential equation might take in the space given by the coordinates t, u, and u_t. Further, a solution of a differential equation should move along the surface of the sphere. This motivated the definition of the VESSIOT space, the intersection of the contact distribution with the tangent space of the sphere. The sphere and its VESSIOT space are plotted in Figure 2.2.

Figure 2.2: The sphere $u_1^2 + u^2 + t^2 - 1 = 0$ and its VESSIOT spaces in a real picture.



Integrating along the VESSIOT space yields a generalized (called "geometric") solution in this jet space of order one. Two of these solutions are plotted on the surface of the sphere. Each of these geometric solutions is smooth when crossing the equator, plotted in brown. However, after projection to the t-u-plane plotted below the sphere, these geometric solutions have a singularity in the sense that the function cannot be extended and "goes back". In particular, they admit no expansion into a formal power series. Such points are called regular singularities (more specifically impasse points or cusps). This can be explained by the VESSIOT spaces being transversal with respect to the projection to the t-u-plane everywhere except for the equator.

This behavior appears everywhere along the equator except for the two points with $t = 0$. At these two points the VESSIOT space is singular in the sense that it is two-dimensional. Example 2.91 shows that each of these points admits two complex formal power series solutions. These points are called irregular singularities and at these points various behavior is possible. ◁

This example indicates that at regular singularities there exists no formal power series solution. What happens at the irregular singularities is more involved; in general, the behavior at such a singularity is not decidable by looking at any finite order.

2.1.4 Algebraic Complications

In general, differential equations show much more tantalizing behavior than the examples in this overview. The order ℓ can appear in the coefficients of the counting polynomials, e.g., Example 2.92 has the following counting sequence.

$$l \mapsto \begin{cases} \infty^{\ell+2} - \infty^{\ell+1} + (\ell+1)\infty^{\ell} - \ell\infty^{\ell-1}, & \ell \geq 1 \\ \infty^2 - \infty + 1, & \ell = 0 \end{cases}$$

Other examples can have countably many infinite exceptional cases, e.g., Example 2.93 has counting sequence

$$l \mapsto \begin{cases} \infty^3 - \infty^2 + \infty - \aleph_0, & \ell \geq 1 \\ \infty^2 - \infty + 1, & \ell = 0 \end{cases},$$

where $\aleph_0$ is a new indeterminate, which can be interpreted as the cardinality of a countable set. Furthermore, there are examples where the center of expansion changes the counting sequence on a countably infinite set (cf. Example 2.90)

These examples demonstrate that certain aspects of the cardinality of the set of solutions of differential equations can only be described using countably infinite sets. Such involved behavior can only appear at irregular singularities from the geometric approach.

2.2 Algebraic Counting Polynomials

" Wenn ein Gebilde von n Parametern [...] abhängt, [...] so nimmt das Gebilde ∞^n verschiedene Lagen an, wenn die Parameter variieren. So giebt es z. B. auf der Geraden ∞^1, in der Ebene ∞^2, im Räume ∞^3 Punkte, denn die Lage des Punktes hängt von bez. 1, 2, 3 Parametern (Coordinaten) ab. Ferner giebt es in der Ebene ∞^3 Kreise, da zur Bestimmung des Kreises drei Grössen [...] genügen, u. s. w."

Sophus Lie
in [Lie67, p. 2]

This section begins with the algebraic counting polynomial for constructible sets, i.e., sets in the affine space given by equations, inequations, and unions. Describing the solution set of systems of differential equations requires a generalization to systems with countably many inequations and countably many such systems. This section introduces these generalizations.

Let F be a field of characteristic zero, $\overline{F}$ its algebraic closure, and $R = F[y_1, \ldots, y_n]$. Certain affine projections induced by the ranking $y_1 < \ldots < y_n$ on R are important for the algebraic counting polynomial.

Remark 2.6. Consider the indeterminates $y_1, \ldots, y_n$ of R as coordinate system of an affine n-space W over $\overline{F}$. The ranking $y_1 < \ldots < y_n$ induces an ascending filtration of affine subspaces W_i of W, where W_i is the zero set of $y_{i+1}, \ldots, y_n$. For all $1 \leq i \leq n$ this induces a unique affine projection $\pi_i : W \to W$ commuting with $y_1 \oplus \ldots \oplus y_i$ and having image W_i. Abusing notation, denote by π_i the corestriction $W \to W_i$ of π_i. The coordinates y_i identify $W \equiv \overline{F}^n$; then $\pi_i : \overline{F}^n \to \overline{F}^i : (a_1, \ldots, a_n) \mapsto (a_1, \ldots, a_i)$. ◁

2.2.1 The Counting Polynomial of Algebraic Systems

The idea of the algebraic counting polynomial is as follows. Let $\pi_{i-1} : \overline{F}^n \to \overline{F}^i$, $1 < i \leq n$ be a projection induced by the ranking $<$ and $(\pi_{i-1})_{|\overline{F}^i} : \overline{F}^i \to \overline{F}^{i-1}$ its restriction. The properties of a simple algebraic system S correspond to the following fibration structure on its solution set. For any solution $\mathbf{a} \in \mathfrak{Sol}(S_{<y_i})$, denote its fiber by $s_{i,\mathbf{a}} := (\pi_{i-1})^{-1}_{|\overline{F}^i}(\{\mathbf{a}\})$; this fibre is interpreted as subset of $\overline{F}$. If S_{y_i} is an equation, then the fiber cardinality is $|s_{i,\mathbf{a}}| = \mathrm{mdeg}(S_{y_i})$. If S_{y_i} is an inequation, then $s_{i,\mathbf{a}} = \overline{F} \setminus \tilde{s}_{i,\mathbf{a}}$ with $|\tilde{s}_{i,\mathbf{a}}| = \mathrm{mdeg}(S_{y_i})$. If S_{y_i} is empty, then $s_{i,\mathbf{a}} = \overline{F}$. The cardinalities of $s_{i,\mathbf{a}}$ or $\tilde{s}_{i,\mathbf{a}}$ are independent of the choice of the solution $\mathbf{a} \in \mathfrak{Sol}(S_{<y_i})$ (cf. Remark 1.10).

Let ∞ be a free indeterminate in the polynomial ring $\mathbb{Z}[\infty]$. It represents the cardinality of $\overline{F}$. Define the **type** of constraints the following way. An equation $p_= \in R^{\{=\}}$ has type $\tau(p_=) := \mathrm{mdeg}(p) \in \mathbb{Z}[\infty]$. An inequation $p_{\neq} \in R^{\{\neq\}}$ has type $\tau(p_{\neq}) := \infty - \mathrm{mdeg}(p) \in \mathbb{Z}[\infty]$. The empty set has type $\tau(\emptyset) := \infty \in \mathbb{Z}[\infty]$.

Definition 2.7. Let S be a simple algebraic system over R. The **algebraic counting polynomial** $c(S) = c(S, \infty)$ of S is given by

$$c(S) := \prod_{i=1}^{n} \tau(S_{y_i}) \ .$$

For (not necessarily simple) systems S define the **algebraic counting polynomial** by

$$c(S) := \sum_{i=1}^{k} c(S_i) \ ,$$

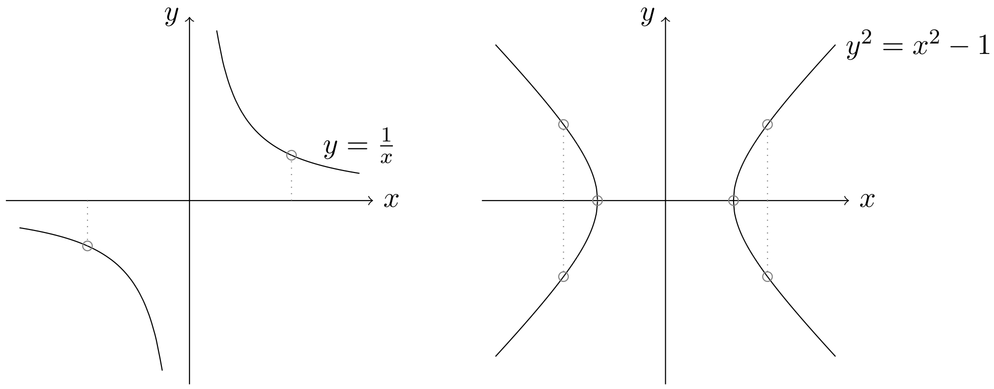
where $\{S_1, \dots, S_k\}$ is a THOMAS decomposition of S. (This is independent of the THOMAS decomposition by Proposition 2.12 or [Ple09a, Proposition 3.3].)

A **constructible set** in $\overline{F}^n$ is a union of solution sets of algebraic systems. Let $V \subseteq \overline{F}^n$ be a constructible set. Call a set $\{S_1, \dots, S_k\}$ of disjoint simple algebraic systems with $V = \biguplus_{i=1}^{k} \mathfrak{Sol}(S_i)$ a **THOMAS decomposition** of V. This is algorithmic using Proposition 1.34 if V is given as the (not necessarily disjoint) union of algebraic systems. Define the **algebraic counting polynomial** of V as $c(V) = c(V, \infty) := \sum_{i=1}^{k} c(S_i)$, where $\{S_1, \dots, S_k\}$ is a THOMAS decomposition[4] of V. The THOMAS decomposition clearly implies that an affine projection of a constructible set is again constructible.

Example 2.8. The algebraic counting polynomial of the empty set is $0 \in \mathbb{Z}[\infty]$, of a singleton it is $1 \in \mathbb{Z}[\infty]$, and of the affine i-space it is $\infty^i \in \mathbb{Z}[\infty]$. ◁

The algebraic counting polynomial of constructible sets in $\overline{F}^n$ is not invariant under the change of ranking and not invariant under the action of $\mathrm{GL}_n(\overline{F})$, as the following example shows. The generic counting polynomial of [Ple09a] is coordinate invariant.

Example 2.9. Consider $p := x\underline{y} - 1 \in \mathbb{C}[x, y]$ and $V := \mathfrak{Sol}(\{p = 0\})$. A THOMAS decomposition of V is given by $\{\{\underline{x} \neq 0, p = 0\}\}$ for the ranking $x < y$, and the counting polynomial is $c(V) = \infty - 1$. The polynomial $\widetilde{p} := (x - y)(x + y) - 1 = -\underline{y}^2 + x^2 - 1 \in \mathbb{C}[x, y]$ arises from p by an invertible linear transformation. A THOMAS decomposition of $\widetilde{V} := \mathfrak{Sol}(\{\widetilde{p} = 0\})$ for the ranking $x < y$ is given by $\{\{\underline{x}^2 - 1 \neq 0, \widetilde{p} = 0\}, \{x^2 - 1 = 0, \underline{y} = 0\}\}$ and the algebraic counting polynomial is $c(\widetilde{V}) = 2(\infty - 2) + 2 = 2\infty - 2$, which does not equal $c(V)$.



The (real) pictures shows the fiber cardinalities. For p the fibers of the projection on the x-axis have cardinality 1 everywhere except over 0, and for $\widetilde{p}$ the fibers of this projection have cardinality 2 everywhere except over ± 1. ◁

The following proposition states the fundamental properties of the algebraic counting polynomial. Define the total order $\leq$ on $\mathbb{Z}[\infty]$ by $p \leq q$ if the leading coefficient of $q - p$ is non-negative ($p, q \in \mathbb{Z}[\infty]$).

Proposition 2.10 ([Ple09a, Corollary 3.4, 3.5])**.** *Let $V, W \subseteq \overline{F}^n$ and $U \subseteq \overline{F}^m$ be constructible sets.*

[4] Again, this is independent of the THOMAS decomposition [Ple09a, Proposition 3.3].

(1) $c(V \cup W) + c(V \cap W) = c(V) + c(W)$

(2) *Let* $V \subseteq W$*. Then* $c(V) \leq c(W)$ *with equality if and only if* $V = W$*.*

(3) $V \times U \subseteq \overline{F}^n \times \overline{F}^m \simeq \overline{F}^{n+m}$ *is constructible and* $c(V \times U) = c(V)c(U)$*.*

In particular, the decision whether for two THOMAS decompositions $\{S_1, \ldots, S_k\}$ and $\{S'_1, \ldots, S'_\ell\}$ satisfying $\bigcup_{i=1}^k \mathfrak{Sol}(S_i) \subseteq \bigcup_{i=1}^\ell \mathfrak{Sol}(S'_i)$ the equality $\bigcup_{i=1}^k \mathfrak{Sol}(S_i) = \bigcup_{i=1}^\ell \mathfrak{Sol}(S'_i)$ of solutions sets holds is algorithmic by computing the algebraic counting polynomials of the THOMAS decompositions.

Similarly to Proposition 2.10 one easily verifies the following.

Lemma 2.11. *Let* $1 \leq i \leq n$ *and* $\pi_i : \overline{F}^n \to \overline{F}^i$ *be a projection associated to the ranking (cf. Remark 2.6). If* $V \subset \overline{F}^n$ *is constructible such that for a* $1 \leq i \leq n$ *each non-empty fiber* U *of* π_i *has the same algebraic counting polynomial, then* $c(V) = c(U) \cdot c(\pi_i(V))$*.*

The algebraic counting polynomial can be characterized axiomatically. For a similar characterization see [BP, Proposition 2.1]

Proposition 2.12. *Let* $\overline{F}^n$ *be an affine* n*-space with projections* $\pi_i : \overline{F}^n \to \overline{F}^i$ *as in Remark 2.6. Let* C *be the set of constructible sets in* $\overline{F}^n$*. Then there is a unique map* $\widetilde{c} : C \to \mathbb{Z}[\infty]$ *with the following properties.*

(1) $\widetilde{c}(\{a\}) = 1$ *for all* $a \in \overline{F}^n$*.*

(2) $\widetilde{c}(A) = \infty$ *for all affine* 1*-spaces* A *over* $\overline{F}$*.*

(3) $\widetilde{c}(V \uplus W) = \widetilde{c}(V) + \widetilde{c}(W)$ *for all disjoint constructible sets* $V, W \subseteq \overline{F}^n$*.*

(4) *If* $V \subset \overline{F}^n$ *is constructible such that for a* $1 \leq i \leq n$ *each non-empty fiber* U *of* π_i *has the same value under* $\widetilde{c}$*, then* $\widetilde{c}(V) = \widetilde{c}(U) \cdot \widetilde{c}(\pi_i(V))$*.*

The algebraic counting polynomial c *fulfills these conditions and, hence, is equal to* $\widetilde{c}$*.*

This proof is given by a generalization of [Ple09a, Proposition 3.3], which is sketched in [BP, Proposition 2.1]

The uniqueness of the algebraic counting polynomial implies the following.

Corollary 2.13. *Let* $V \subseteq W$ *be constructible sets. Then* $c(W \setminus V) = c(W) - c(V)$*.*

Corollary 2.14. *Let* $\emptyset \neq V \subseteq \overline{F}^n$ *be a constructible set and* $c(V) = \sum_{i=0}^d a_i \infty^i$ *be its algebraic counting polynomial with* $a_i \in \mathbb{Z}$*,* $0 \leq i \leq d$*, and* $a_d \neq 0$*. Then* $a_d > 0$*.*

Proof. By the additivity from Proposition 2.12.(3), assume without loss of generality that V can be described by one simple algebraic system S. We prove the claim by an induction on the dimension n. If $n = 0$, then V is the singleton and $c(V) = 1$. If $n = 1$, then V is finite and $c(V) = |V|$ or V is cofinite and $c(V) = \infty - |\overline{F}^1 \setminus V|$. Assume that the claim is true for $n-1$ and let $\pi_{n-1} : \overline{F}^n \to \overline{F}^{n-1}$ be the projection. Then the leading coefficient of $c(\pi_{n-1}(V))$ is positive by the induction hypothesis. The algebraic counting polynomials of each fiber $U = \pi_{n-1}^{-1}(\{v\})$, $v \in V$, of π_{n-1} are identical and have an algebraic counting polynomial with positive leading coefficient, by the case $n = 1$. Now, Proposition 2.12.(4) implies $c(V) = c(\pi_{n-1}(V)) \cdot c(U)$, and this polynomial has positive leading coefficient as product of two polynomials with positive leading coefficient. □

Even though the algebraic counting polynomial is not coordinate invariant, the algebraic counting polynomial implies the (coordinate independent) EULER characteristic[5]. This was pointed out by FRANK-OLAF SCHREYER. See [Mar11] for similar work.

Theorem 2.15. *Let $F = \mathbb{C}$, V a constructible set in $\mathbb{C}^n$, and $c(V)(\infty) \in \mathbb{Z}[\infty]$ its algebraic counting polynomial. Then the* EULER *characteristic $\chi(V)$ of V is given by*

$$\chi(V) = c(V, 1) = c(V)_{|\infty=1} \ .$$

Proof. The EULER characteristic maps disjoint unions into addition and set difference of two sets contained in each other into a difference [Ful93, p. 92]. The same holds for the algebraic counting polynomial (cf. Proposition 2.12.(3)). This implies that without loss of generality V is the solution set of a simple algebraic system S over $F[y_1, \dots, y_n]$.

Show the claim by induction over the dimension n. For $n = 1$ there are two possibilities for V. If V is finite, then both the algebraic counting polynomial and the EULER characteristic are equal to the cardinality $|V|$. If V is cofinite in $\overline{F}$, then both the algebraic counting polynomial is $c(V)(\infty) = \infty - |\mathbb{C} \setminus V|$. In this case the EULER characteristic is given by $\chi(\mathbb{C}) = \chi(V) = \chi(\mathbb{C}) - \chi(\mathbb{C} \setminus V) = 1 - |\mathbb{C} \setminus V| = c(V, 1)$.

For $n > 1$ the system S either an equation with leader y_n, an inequation with leader y_n, or no constraint. In the first case, V is a $\mathrm{mdeg}(S_{y_n})$-sheeted covering space of $\mathfrak{Sol}_{\mathbb{C}^{n-1}}(S_{<y_n})$. On the one hand, $\chi(V) = \mathrm{mdeg}(S_{y_n}) \cdot \chi(\mathfrak{Sol}_{\mathbb{C}^{n-1}}(S_{<y_n}))$ (cf. e.g. [Spa81, Theorem 9.3.1]). On the other hand,

$$c(V) = c(S) = \mathrm{mdeg}(S_{y_n}) \cdot c(S_{<y_n}) = \mathrm{mdeg}(S_{y_n}) \cdot c\left(\mathfrak{Sol}_{\mathbb{C}^{n-1}}(S_{<y_n})\right) \ .$$

In the second case, $V = (\mathbb{C} \times \mathfrak{Sol}_{\mathbb{C}^{n-1}}(S_{<y_n})) \setminus \mathfrak{Sol}(S_{<y_n} \cup \{(S_{y_n})_=\})$. The EULER characteristic behaves multiplicatively with respect to $\times$. Thus,

$$\chi(V) = \chi(\mathbb{C}) \cdot \chi\left(\mathfrak{Sol}_{\mathbb{C}^{n-1}}(S_{<y_n})\right) - \chi\left(\mathfrak{Sol}(S_{<y_n} \cup \{(S_{y_n})_=\})\right) \ .$$

The first case implies $\chi(\mathfrak{Sol}(S_{<y_n} \cup \{(S_{y_n})_=\})) = \mathrm{mdeg}(S_{y_n}) \cdot \chi(\mathfrak{Sol}_{\mathbb{C}^{n-1}}(S_{<y_n}))$. Thus,

$$\begin{aligned}\chi(V) &= 1 \cdot \chi\left(\mathfrak{Sol}_{\mathbb{C}^{n-1}}(S_{<y_n})\right) - \mathrm{mdeg}(S_{y_n}) \cdot \chi\left(\mathfrak{Sol}_{\mathbb{C}^{n-1}}(S_{<y_n})\right) \\ &= (1 - \mathrm{mdeg}(S_{y_n})) \cdot \chi\left(\mathfrak{Sol}_{\mathbb{C}^{n-1}}(S_{<y_n})\right) \ .\end{aligned}$$

At last, $c(V) = (\infty - \mathrm{mdeg}(S_{y_n})) \cdot \chi(\mathfrak{Sol}_{\mathbb{C}^{n-1}}(S_{<y_n}))$ completes the proof of the second case. Finally, the third case of no constraint is trivial. □

The following corollary is a typical application of the EULER characteristic. It uses the knowledge of all but one coefficient of the algebraic counting polynomial and of the EULER characteristic to deduce the missing coefficient.

Corollary 2.16. *Fix the Ranking $x > y$, and let $f(x) \in \mathbb{C}[x]$ of degree $\deg(f) \geq 1$. The algebraic counting polynomial of the system $S := \{y - f(x) = 0\}$ is*

$$c(S) = \deg(f) \cdot \infty - (\deg(f) - 1)$$

Proof. When exchanging the order of the variables into $y > x$ the system describes the graph of a function and, thus, has algebraic counting polynomial ∞. In particular, $\deg(c(S)) = 1$, as the degree of the algebraic counting polynomial is coordinate independent. Since generically the projection of $\mathfrak{Sol}(\{y - f(x) = 0\})$ onto the y-axis is a $\deg(f)$-sheeted covering, the coefficient of ∞ in $c(S)$ is $\deg(f)$. The EULER characteristic formula implies $c(S)(1) = 1$. This determines the constant coefficient of $c(S)$. □

[5]The EULER characteristics with or without compact support coincide for the case of locally closed sets [Ful93, p. 92-95]

Proposition D.1 implies a sufficient criterion for prime ideals. The following version of the criterion involves the algebraic counting polynomial. If the solution set of a simple algebraic system S has an algebraic counting polynomial with leading coefficient one, then $\mathcal{I}(S)$ is prime.

2.2.2 Simple Algebraic σ-Systems

For counting the number of solutions of algebraic systems there are only finitely many exceptional values for each indeterminate. However, for a differential system there can be countably many exceptional values for one indeterminate (cf. Example 2.93). Thus, we need countably many inequations (for the generic case) and countably many (special) cases. This subsection generalizes simple algebraic systems to this context.

Let I be a countable index set. Let F be a field of characteristic 0 and denote by $\overline{F}$ the algebraic closure of F. Let $R := F[y_i|i \in I]$ be the polynomial ring (in possibly infinitely many variables). A well-founded total order $<$ on $\{1, y_i|i \in I\}$ with $1 < y_i$ for all $i \in I$ is called a **ranking**. The concepts of leader, main degree, and initial are the same as in the case of finitely many indeterminates. For readability, assume a natural total order on I by setting either $I = \mathbb{Z}_{>0}$ or $I = \{1, \dots, n\}$ for $n \in \mathbb{Z}_{>0}$ such that $i < j$ implies $y_i < y_j$. For $\mathbf{a} \in \overline{F}^I$ define the **(complete) evaluation homomorphism**

$$\phi_{\mathbf{a}} : R \to \overline{F} : y_i \mapsto a_i \ .$$

Let $j, k \in I$ with $k - 1 \le j$. Define the **(partial) evaluation homomorphism**

$$\phi_{<y_k,\mathbf{a}} : R \to \overline{F}[y_i|i \in I, k \le i] : \begin{cases} y_i \mapsto a_i, & i < k \\ y_i \mapsto y_i, & \text{otherwise} \end{cases}$$

for $\mathbf{a} \in \overline{F}^j$ or $\mathbf{a} \in \overline{F}^I$. A **solution** of an equation or inequation p is a tuple $\mathbf{a} \in \overline{F}^I$ with $\phi_{\mathbf{a}}(p) = 0$ or $\phi_{\mathbf{a}}(p) \neq 0$, respectively. Call $\mathbf{a} \in \overline{F}^I$ a solution of a set S of equations and inequations, if it is a solution of each element in S. The set of all solutions of S is denoted by $\mathfrak{Sol}(S)$. Again, for a set S of equations and inequations define $S^{=}, S^{\neq}$, S_x, $S_{<x}$, and $S_{\le x}$ as the subsets of all equations, inequations, elements of leader x, elements of leader smaller x, and elements of leader smaller or equal x, respectively.

Call a set of finitely many equations and countably many inequations an **(algebraic) σ-system** over R. Non-vanishing initials of σ-systems is defined exactly as for systems. Furthermore, square-freeness of equations is defined as for systems and a set T of inequations with the same leader is square-free if and only if all products of all finite subsets of T are square-free in the sense of systems.

Definition 2.17. Let S be a σ-system. Call S **weakly triangular** if $|S^{=}_{y_i}| \le 1 \ \forall\ 1 \le i \le n$, $S \cap \{c_{=}, c_{\neq} \mid c \in F\} = \emptyset$, and if $|S^{=}_{y_i}| = 1$, then $S^{\neq}_{y_i} = \emptyset$, $1 \le i \le n$. Call S **simple** if it is weakly triangular, has non-vanishing initials, and is square-free.

A simple algebraic σ-system S over R shares many properties with simple algebraic systems. For example, $S_{<y_i}$ is also a simple algebraic σ-system in $F[y_1, \dots, y_{i-1}]$ for all $i \in I$. If $\mathbf{a} \in \mathfrak{Sol}(S_{<y_i})$, then $\phi_{<y_i,\mathbf{a}}(S)$ is also a simple algebraic σ-system in $F[y_j|j \ge i, j \in I]$ for all $i \in I$. Furthermore, every simple algebraic σ-system S has a solution. In particular, if $\mathbf{b} \in \mathfrak{Sol}(S_{<x})$, then $\phi_{<x,\mathbf{b}}(p)$ is a univariate polynomial with exactly $\operatorname{mdeg}(S_x)$ *distinct* roots for all $p \in S_x$. Conversely, if $(a_i|i \in I) \in \mathfrak{Sol}(S)$, then $(a_1, \dots, a_i) \in \mathfrak{Sol}(S_{\le y_i})$ for any $i \in I$. Thus, $\pi_i(\mathfrak{Sol}(S)) = \mathfrak{Sol}(S_{\le y_i})$ for a simple algebraic σ-system, where π_i is the projection from Remark 2.6. (This remark easily generalizes to the context of infinite dimensional affine spaces.)

Let S be a σ-system. A family $(S_j)_{j\in J}$ of σ-systems for a (not necessarily finite) index set J is called **algebraic σ-decomposition** of S if $\mathfrak{Sol}(S) = \bigcup_{j\in J}\mathfrak{Sol}(S_j)$. A *disjoint* decomposition of a system into simple algebraic σ-systems is called **algebraic Thomas σ-decomposition**.

2.2.3 The Counting Polynomial for Algebraic σ-Systems

This subsection extends the algebraic counting polynomial to algebraic σ-systems in finitely many indeterminates. This is motivated, as counting in the differential case requires counting polynomials of algebraic σ-systems. Therefore, take the defining conditions for the algebraic counting polynomial in Proposition 2.12 as axioms. The algebraic counting polynomial is not unique in this case of algebraic σ-systems.

Countable infinite exceptional sets are the reason for introducing σ-systems. For the representation of these countably infinite exceptional sets, use the additional symbol $\aleph_0$. This symbol is necessary for example for the σ-system $S := \{x - i \neq 0 | i \in \mathbb{Z}_{\geq 0}\}$ in $\mathbb{C}[x]$. Its solution set is given by $\mathfrak{Sol}(S) = \mathbb{C} \setminus \mathbb{Z}_{\geq 0}$. Think of the cardinality of this set as the cardinality of $\mathbb{C}$ minus a countable set and write $\infty - \aleph_0$ for its algebraic counting polynomial.

Remark 2.18. To avoid problems that the cardinality of fields is also countable, assume that the cardinality of ground field F is not countable. Otherwise, the system $S := \left\{x - i \neq 0 \middle| i \in \overline{\mathbb{Q}}\right\}$ in $\overline{\mathbb{Q}}[x]$ would have algebraic counting polynomial $\infty - \aleph_0$ but no solutions. ◁

Call a subset of $\overline{F}^n$ **elementarily describable** if it is a solution set of a σ-system. Call $V \subseteq \overline{F}^n$ **describable** if it is a countable union of elementarily describable sets. Let $\mathbb{Z}[\infty, \aleph_0]$ be the polynomial ring in two indeterminates ∞ and $\aleph_0$.

Definition 2.19. Let $\overline{F}^n$ be the affine n-space with projections $\pi_i : \overline{F}^n \to \overline{F}^i$ from Remark 2.6. Let V be a describable set in $\overline{F}^n$. Then, call *any* element $c(V) \in \mathbb{Z}[\infty, \aleph_0]$ that results from applying the following five axioms an **algebraic counting polynomial** of V.

(1) $c(\{a\}) = 1$ for all $a \in \overline{F}^n$.

(2) $c(A) = \infty$ for all affine 1-spaces A over $\overline{F}$.

(3) $c(V \uplus W) = c(V) + c(W)$ for all disjoint describable sets $V, W \subseteq \overline{F}^n$.

(4) If $V \subset \overline{F}^n$ is describable such that for a $1 \leq i \leq n$ each non-empty fiber U of π_i has a same value under c, then $c(V) = c(U) \cdot c(\pi_i(V))$.

(5) $c(\overline{F}^1 \setminus M) = \infty - \aleph_0$ for $M \subset \overline{F}^1$ is countably infinite.

For an algebraic σ-system S define the algebraic counting polynomial $c(S)$ as $c(\mathfrak{Sol}(S))$.

We comment on the definition of the algebraic counting polynomial.

Remark 2.20. The algebraic counting polynomial is not unique; for example, the set $\mathfrak{Sol}_{\mathbb{C}}(\{x - i \neq 0 | i \in \mathbb{Z}_{\geq 0}\}) = \mathfrak{Sol}_{\mathbb{C}}(\{x - i \neq 0 | i \in \mathbb{Z}_{\geq 1}\}) \uplus \{0\}$ can have both counting polynomial $\infty - \aleph_0$ and $\infty - \aleph_0 + 1$. Hence, Proposition 2.10.(2), which states that the algebraic counting polynomial decides equality of contained sets, does not hold anymore. However, it holds for the important special case of well-fibred sets (cf. Theorem 2.29). ◁

Remark 2.21. It seems unreasonable to "add" infinitely many algebraic counting polynomials. If we did this by a kind of "σ-additivity", then the following might happen.

For example, the set $\mathbb{C} \setminus \{0\}$ has algebraic counting polynomial $\infty - 1$, but we can decompose this set into $\mathbb{C} \setminus \mathbb{Z}_{\geq 0} \uplus \biguplus_{i \in \mathbb{Z}_{\geq 1}} \{i\}$, and the σ-additivity yields the algebraic counting polynomial

$$c\Big((\mathbb{C} \setminus \mathbb{Z}_{\geq 0}) \uplus \biguplus_{i \in \mathbb{Z}_{\geq 1}} \{i\}\Big) = \underbrace{(\infty - \aleph_0)}_{c(\mathbb{C} \setminus \mathbb{Z}_{\geq 0})} + \sum_{i \in \mathbb{Z}_{>0}} \underbrace{1}_{c(\{i\})} = (\infty - \aleph_0) + \aleph_0 = \infty \ .$$

To avoid this problem, the definition of the algebraic counting polynomial for σ-systems only includes additivity (cf. Definition 2.19.(3)), but no σ-additivity. The axiomatic definition of the algebraic counting polynomial means that it is not defined for every countable infinite union of σ-systems, for example it is not defined for the set $\mathbb{Z}_{\geq 0}$. Instead, the algebraic counting polynomial is much more "unique" and definitive. ◁

Remark 2.22. Similarly[6] to Corollary 2.14 one shows that any algebraic counting polynomial of an elementarily describable set has a leading coefficient in $\mathbb{Z}_{\geq 1}$ when considered as a polynomial in the indeterminate ∞ with coefficients in $\mathbb{Z}[\aleph_0]$. In particular, $\aleph_0$ does not appear in the leading coefficient. By Lemma 2.63 below, the degree and leading coefficient in the indeterminate ∞ is well-defined (once a ranking is fixed).

This also holds for any describable set that allows a description by (possibly infinitely many) simple algebraic σ-systems $\{S_j | j \in J\}$ such that the number of σ-systems S_j with $|S_j^=| = \min\big\{|S_j^=| \big| j \in J\big\}$ is finite. ◁

Recall that the number of equations in a σ-system is finite. Ideals associated to a σ-system S can be defined using the same formula $\mathcal{I}(S) := \langle S^= \rangle : q^\infty$ for $q := \prod_{p \in S^=} \operatorname{init}(p)$ as in Definition 1.61.

Proposition 2.23. *Let S be a simple algebraic system or simple algebraic σ-system in $R = \overline{F}[y_1, \ldots, y_n]$. Then,* $\dim(R/\mathcal{I}(S)) = \deg_\infty(c(S))$

Proof. For a system S this follows directly from Theorem 1.94. For a σ-system S this follows as $\mathcal{I}(S)$ only depends on $S^=$. □

The examples in this thesis utilize two constructions for an algebraic counting polynomial. The first construction works for elementarily countable sets and uses an extension of the type, which was defined at the beginning of Subsection 2.2.1. A finite set of inequations $Q \subset F[y_1, \ldots, y_n]$ with the same leader x has **type** $\tau(Q) = \infty - \sum_{q \in Q} \deg_x(q)$. A countably infinite set of inequations $Q \subset (F[y_1, \ldots, y_n] \setminus F)^{\{\neq\}}$ with the same leader has **type** $\tau(Q) = \infty - \aleph_0$. With these definitions, this construction is proved as a natural generalization of Proposition 2.12.

Lemma 2.24. *Let S be a simple algebraic σ-system in $F[y_1, \ldots, y_n]$. Then a* ***counting polynomial*** *$c(S)$ of S can be given by $c(S) := \prod_{i=1}^n \tau(S_{y_i})$.*

The second construction for an algebraic counting polynomial works for certain infinite unions of algebraic σ-systems. This shows how to "add" the algebraic counting polynomials of infinitely many simple algebraic σ-systems of a certain form. Note, that the resulting algebraic counting polynomial does not involve $\aleph_0$ if none of the σ-systems does.

[6] Here, one cannot assume that the algebraic counting is independent of the decomposition. However, that set has to be decomposed for axiom (4) being applicable, and this axiom is the only axiom that allows to increase dimensions. Just take this decomposition for the proof.

Lemma 2.25. *Let $P := \{T_j | j \in \mathbb{Z}_{\geq 0}\}$ be a family of algebraic simple algebraic σ-systems over $R = F[y_1, \ldots, y_n]$. Assume that P satisfies the following conditions.*

(1) The sets $\mathfrak{Sol}_{\overline{F}}((T_j)_{\leq y_1})$, $j \in \mathbb{Z}_{\geq 0}$, partition $\overline{F}$.

(2) For all $j \in \mathbb{Z}_{\geq 1}$ the set $\mathfrak{Sol}_{\overline{F}}((T_j)_{\leq y_1})$ is finite.

(3) Let $\mathbf{a}_j \in \mathfrak{Sol}(T_j)$, and let $T'_j := \phi_{\leq y_1, \mathbf{a}_j}(T_j)$ be the corresponding simple algebraic σ-systems in $F[y_2, \ldots, y_n]$ for all $j \in \mathbb{Z}_{\geq 0}$. Then there is a $k \in \mathbb{Z}_{>0}$ such that $c(T'_j)$ exists for all $j \in \mathbb{Z}_{>k} \cup \{0\}$ and $c(T'_j) = c(T'_0)$ for all $j > k$.

(4) Let k be as in (3). For all $j \in \{1, \ldots, k\}$ there exists an algebraic counting polynomial $c(T_j) \in \mathbb{Z}[\infty, \aleph_0]$, and $c(T_j) \notin \mathbb{Z}[\infty]$ for at most one of those j.

Let $d := \left|\biguplus_{j=1}^{k} \mathfrak{Sol}_{\overline{F}}((T_j)_{\leq y_1})\right|$. Then an algebraic counting polynomial of P is given by

$$c(P) := (\infty - d) \cdot c(T'_0) + \sum_{j=1}^{k} c(T_j) \in \mathbb{Z}[\infty, \aleph_0] \ ,$$

where the sum and product is taken in the ring $\mathbb{Z}[\infty, \aleph_0]$.

Proof. Let k be as in condition (3). Then, $c(\biguplus_{j=0}^{\infty} \mathfrak{Sol}_{\overline{F}}((T_j)_{\leq y_1})) = c(\overline{F}) = \infty$ by condition (1) and Definition 2.19.(2). Due to (1), Definition 2.19.(3) implies

$$\begin{aligned}
\infty &= c\Big(\biguplus_{j=0}^{\infty} \mathfrak{Sol}_{\overline{F}}((T_j)_{\leq y_1}) \Big) \\
&= c\Big(\biguplus_{j=1}^{k} \mathfrak{Sol}_{\overline{F}}((T_j)_{\leq y_1}) \Big) + c\Big(\mathfrak{Sol}_{\overline{F}}((T_0)_{\leq y_1}) \uplus \biguplus_{j=k+1}^{\infty} \mathfrak{Sol}_{\overline{F}}((T_j)_{\leq y_1}) \Big) \\
&= d + c\Big(\mathfrak{Sol}_{\overline{F}}((T_0)_{\leq y_1}) \uplus \biguplus_{j=k+1}^{\infty} \mathfrak{Sol}_{\overline{F}}((T_j)_{\leq y_1}) \Big) \ ,
\end{aligned}$$

as $d = c(\biguplus_{j=1}^{k} \mathfrak{Sol}_{\overline{F}}((T_j)_{\leq y_1}))$ by Definition 2.19.(1) and Definition 2.19.(3). Thus,

$$c\Big(\mathfrak{Sol}_{\overline{F}}((T_0)_{\leq y_1}) \uplus \biguplus_{j=k+1}^{\infty} \mathfrak{Sol}_{\overline{F}}((T_j)_{\leq y_1}) \Big) = \infty - d \ .$$

By condition (3), $c(T_j) = c(T'_0)$ for all $j > k$. Thus, Definition 2.19.(4) implies

$$c\Big(\mathfrak{Sol}_{\overline{F}}(T_0) \uplus \biguplus_{j=k+1}^{\infty} \mathfrak{Sol}_{\overline{F}}(T_j) \Big) = (\infty - d) \cdot c(T'_0) \ .$$

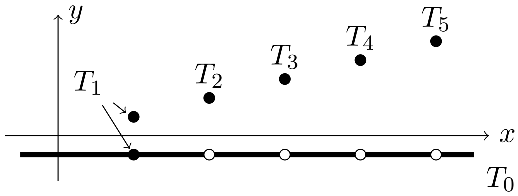
Due to the disjointness of the systems in P, Definition 2.19.(3) implies the claim. □

Example 2.26. Consider the simple algebraic σ-systems

$$\begin{aligned}
T_0 &:= \{x - j \neq 0, y + 1 = 0 | j \in \mathbb{Z}_{\geq 1}\}, \\
T_1 &:= \{x - 1 = 0, 4y^2 - 1 = 0\}, \text{ and} \\
T_j &:= \{x - j = 0, 2y - j = 0\} \text{ for } j \geq 2
\end{aligned}$$

over $\mathbb{C}[x, y]$ with $x < y$. Let $P := \{T_j | j \in \mathbb{Z}_{\geq 0}\}$. The assumptions of Lemma 2.25 are satisfied with $k = 1$ and, thus, $c(P) = (\infty - 1) \cdot 1 + 2 = \infty + 1$. ◁

Figure 2.3: Diagram of the solutions of Example 2.26



2.2.4 Well-fibred Sets and the Avoidance of Countable Sets

Countable exceptional sets and the corresponding symbol $\aleph_0$ complicate the use of the algebraic counting polynomial for σ-systems in applications (cf. Remark 2.20). This subsection describes sets that do not lead to such complications. Call a describable set V with $c(V) \in \mathbb{Z}[\infty]$ **well-fibred**. Example 2.26 shows that well-fibred sets are more general than constructible sets. These sets show a similar behavior regarding counting polynomials as constructible sets, in particular the algebraic counting polynomial for these sets is strong enough to decide equality of sets contained in each other.

We begin with some lemmas describing properties of well-fibred systems. To state the first lemma, call a set $W \subset \overline{F}^n$ **elementarily well-fibred** if either $n = 1$ and W is constructible or $n > 1$, $\pi_{n-1}(W) \subseteq \overline{F}^{n-1}$ is elementarily well-fibred, and the fibres of $\pi_{n-1}^{-1}(\{w\})$ for $w \in \pi_{n-1}(W)$ are constructible with the same counting polynomials. Note that elementarily well-fibred sets admit an algebraic counting polynomial in $\mathbb{Z}[\infty]$.

Lemma 2.27. *Let V be a well-fibred set. Then, there exists a finite partition $V = \biguplus_{i=1}^{k} W_i$ of V into elementarily well-fibred sets W_i.*

Proof. The claim clearly holds for $n = 1$. The only axiom that allows to increase the dimension n is axiom (4). In general, one needs to partition V before applying axiom (4), but this partition needs to be finite, as otherwise axiom (3) is not applicable to recombine the counting polynomials of these systems. Elementarily well-fibred sets are exactly the sets for which axiom (4) is applicable without previous splittings. □

Lemma 2.28. *Let V be a well-fibred set. Then, the algebraic counting polynomial of V is unique.*

Proof. The proof of [Ple09a, Proposition 3.3] regarding the uniqueness of counting polynomials holds for well-fibred sets. One only needs to replace a decomposition into simple systems with a decomposition into elementarily well-fibred sets, as in Lemma 2.27. □

These lemmas allow to generalize the proof in [Ple09a] that we can decide equality of well-fibred sets contained in each other. One might say that the countable infinite sets are the only problem in deciding equality of sets, and no problems appear when $\aleph_0$ is not contained in the counting polynomial of a set. Recall the total order "$\leq$" for polynomials in $\mathbb{Z}[\infty]$ defined before Proposition 2.10.

Theorem 2.29. *Let $V \subseteq W \subseteq \overline{F}^n$ be two well-fibred sets. Then, $c(V) \leq c(W)$ with equality if and only if $V = W$.*

Even in cases when $\aleph_0$ appears in the counting polynomial of two describable sets $V \subseteq W$ with algebraic counting polynomial $c(V)$ and $c(W)$, we can use the algebraic counting polynomial to prove that $V \neq W$. This is done using the following two estimations for the algebraic counting polynomial. First, any subset of $\overline{F}^1$ with a countably infinite complement can be enlarged to a set with finite complement. Thus, we say that the counting polynomial $\infty - \aleph_0$ is bounded from above by $\infty - k$ for all $k \in \mathbb{Z}_{\geq 0}$, and we write $\infty - \aleph_0 \prec \infty - k$. Second, any subset of $\overline{F}^1$ with a countably infinite complement can be shrunk to a finite set. Thus, we say that the counting polynomial $\infty - \aleph_0$ is bounded from below by k for all $k \in \mathbb{Z}_{\geq 0}$, and we write $k \prec \infty - \aleph_0$.

More formally, let $p(\aleph_0, \infty) \in \mathbb{Z}[\aleph_0, \infty]$ and $q(\infty) \in \mathbb{Z}[\infty]$. We write $p \prec q$ if $q(\infty) = p(\infty - k, \infty)$ and $p \succ q$ if $q(\infty) = p(k, \infty)$ for some $k \in \mathbb{Z}_{\geq 0}$.

Proposition 2.30. *Let $V_1 \subseteq V_2 \subseteq \overline{F}^n$ be to describable sets with counting polynomials $p_1(\aleph_0, \infty) := c(V_1)$ and $p_2(\aleph_0, \infty) := c(V_2)$. If there exist $q_1, q_2 \in \mathbb{Z}[\infty]$ with $p_1 \prec q_1 \lneqq q_2 \prec p_2$, then $V_1 \neq V_2$.*

The methods from this subsection easily allow to prove that all coefficients of the counting polynomial "above $\aleph_0$" are unique, and the problem from Remark 2.20 only affects the lower coefficients. More formally, let $p = \sum_{i=0}^{n} a_i \infty^i$ be an algebraic counting polynomial with coefficients $a_i \in \mathbb{Z}[\aleph_0]$ and let $0 \leq k < n$ be the highest index with $a_k \in \mathbb{Z}[\aleph_0] \setminus \mathbb{Z}$. Then, the coefficients a_j for $k < j \leq n$ are unique. Of course, this statement also holds for the counting sequence and the differential counting polynomial in the next section; however, it is tedious to state in these cases.

2.3 The Differential Counting Polynomial

> "In my opinion, a theory is the more valuable the more strongly it restricts possibilities, without coming into conflict with reality. It is like a wanted poster which is supposed to characterize a criminal; the more precisely it points him out the better."
>
> ALBERT EINSTEIN
> in [CE79, 8.12.1929]

Let F be a differential field of characteristic zero such that its field of constants is not countable (cf. Remark 2.18), $\overline{F}$ its algebraic closure, $<$ an orderly[7] ranking, $\Delta = \{\partial_1, \ldots, \partial_n\}$ a non-empty set of derivation operators, and $U = \{u^{(1)}, \ldots, u^{(m)}\}$ a non-empty set of differential indeterminates.

This section tries to describe (or to "count") the set of solutions of a system of differential equations, i.e., to assign a counting sequence and a differential counting polynomial. More specifically, to count the number of non-centered solutions (cf. Subsection 1.2.2), i.e., solutions in the set

$$E := \overline{F}[[z_1, \ldots, z_n]]^U \cong \bigoplus_{j=1}^{m} \overline{F}[[z_1, \ldots, z_n]] \cong F^{\{U\}_\Delta} \ .$$

This section succeeds in reducing the definition of the counting polynomial in the differential case to determining the algebraic counting polynomial of algebraic σ-systems. This approach is extended to formal power series solutions in Subsection 2.5.4.

Even though the counting sequence and the differential counting polynomial are non-unique in general, certain parts of them are well-defined. First if no $\aleph_0$ appears in the counting sequence or the differential counting polynomial, the they are unique; furthermore, they decide equality of solution sets contained in each other by Theorem 2.34. Second, the leading term (in the sense defined below) is connected to the differential dimension polynomial and thus unique by Theorem 2.36.

Determining the counting sequence or differential counting polynomial is not algorithmic (cf. Subsection 2.5.5), but many important special cases are either algorithmic or there are theoretical arguments that let us succeed (cf. Section 2.5).

2.3.1 Mixed Algebraic-Differential Systems

This subsection introduces systems that are hybrids of algebraic and differential systems, called algebraically restricted systems of differential equations. They combine differential equations with algebraic constraints for power series coefficients.

Consider the following set of indeterminates.

$$G := G(U, \Delta) := \left\{ g_{\mathbf{i}}^{(j)} \mid \mathbf{i} \in \mathbb{Z}_{\geq 0}^n, j \in \{1, \ldots, m\} \right\}$$

Call the polynomial ring $F[G]$ the **polynomial ring of indetermined power series coefficients**. Call the isomorphism

$$\rho : F\{U\} \xrightarrow{\sim} F[G] : u_{\mathbf{i}}^{(j)} \mapsto g_{\mathbf{i}}^{(j)}$$

[7] Example 1.84 and Theorem 2.36 demonstrate that this condition is necessary.

of F-algebras the **forgetful map**[8]. Extend this map to $\rho : F\{U\} \uplus F[G] \to F[G]$ via $Id_{F[G]}$ and to $\rho : (F\{U\} \uplus F[G])^{\{=,\neq\}} \to F[G]^{\{=,\neq\}}$ in the obvious way. Call the elements of $F[G]^{\{=\}}$ **power series coefficient equations** and the elements of $F[G]^{\{\neq\}}$ **power series coefficient inequations**.

Definition 2.31. Call a countable set $P \subset F\{U\}^{\{=\}} \uplus F[G]^{\{=,\neq\}}$ an **algebraically restricted σ-system of differential equations** if $P \cap \left(F\{U\}^{\{=\}} \uplus F[G]^{\{=\}}\right)$ is finite and an **algebraically restricted system of differential equations** if P is finite.

Now, we define non-centered solutions of algebraically restricted σ-systems of differential equations. Slightly generalize the definition of the algebraization isomorphism α and the evaluation map ϕ_e for $e \in E$ from Subsection 1.2.4 to be defined on power series coefficient equations and inequations. So, by abuse of notation, define

$$\alpha : E \to \overline{F}^{\{U\}_\Delta \uplus G} : \left(u^{(j)} \mapsto \sum_{\mathbf{i} \in \mathbb{Z}^n_{\geq 0}} a^{(j)}_{\mathbf{i}} \frac{z^{\mathbf{i}}}{\mathbf{i}!} \right) \mapsto \begin{cases} u^{(j)}_{\mathbf{i}} \mapsto a^{(j)}_{\mathbf{i}} \\ g^{(j)}_{\mathbf{i}} \mapsto a^{(j)}_{\mathbf{i}} \end{cases}$$

and

$$\phi_e : F\{U\} \uplus F[G] \to \overline{F} : \begin{cases} u^{(j)}_{\mathbf{i}} \mapsto \alpha(e)(u^{(j)}_{\mathbf{i}}) \\ g^{(j)}_{\mathbf{i}} \mapsto \alpha(e)(g^{(j)}_{\mathbf{i}}) \end{cases} .$$

A **non-centered solution** of $p_= \in F[G]^=$ or $p_{\neq} \in F[G]^{\neq}$ is an $e \in E$ with $\phi_e(p) = 0$ or $\phi_e(p) \neq 0$, respectively. Furthermore, $e \in E$ is called a non-centered solution of an algebraically restricted σ-system of differential equations P, if it is a non-centered solution of each element in P. The set of non-centered solutions of P is denoted by $\mathfrak{Sol}_E(P) \subseteq E$. The image of $\mathfrak{Sol}_E(P)$ under $E \twoheadrightarrow E/E_{>\ell}$, i.e., the set of non-centered solutions of P truncated at order ℓ, is denoted by $\mathfrak{Sol}_E(P)_{\leq \ell} \subseteq E/E_{>\ell}$.

2.3.2 Definition of the Differential Counting Polynomial

This subsection defines the counting sequence and the differential counting polynomial in the following way. Theorem 2.32 yields an algebraic Thomas σ-decomposition of an algebraically restricted system of differential equations. This theorem can be seen as a substitute for the Thomas decomposition, which does not exist anymore in this setup. For the σ-systems in this σ-decomposition, the algebraic counting polynomial (cf. Subsection 2.2.3) defines the counting sequence and the differential counting polynomial.

Theorem 2.32. *Let $P \subset F\{U\}^{\{=\}} \cup F[G]^{\{=,\neq\}}$ be an algebraically restricted system of differential equations. Let $\ell \in \mathbb{Z}_{\geq 0}$. There exists a countable set C of simple algebraic σ-systems in $F[G]_{\leq \ell}$ with*

$$\mathfrak{Sol}_E(P)_{\leq \ell} = \biguplus_{\widetilde{P} \in C} \mathfrak{Sol}_E(\widetilde{P})_{\leq \ell} .$$

The proof of this theorem successively turns differential equations in $F\{U\}^{\{=\}}$ into power series coefficient equations and inequations in $F[G]^{\{=,\neq\}}$. As a differential equation has infinitely many consequences for power series coefficients, this yields an infinite decomposition. We postpone the proof of this theorem to page 120 in the next section.

[8]It forgets the differential structure and forgetful functors are often *r*ight adjoints.

This theorem explains the necessity to define the algebraic counting polynomial for σ-systems, as the truncated solutions of differential equations can be described by algebraic σ-systems. Using the infinite decomposition, we can define differential versions of the counting polynomial.

Definition 2.33. Let P be an algebraically restricted system of differential equations. Let C_ℓ be a countable set of algebraic σ-systems with $\mathfrak{Sol}_E(P)_{\leq\ell} = \biguplus_{\widetilde{P}\in C_\ell} \mathfrak{Sol}_E(\widetilde{P})_{\leq\ell}$ from Theorem 2.32 for each $\ell \in \mathbb{Z}_{\geq 0}$.

(1) If the algebraic counting polynomial is defined for all C_ℓ, then define a **counting sequence** of P (or $\mathfrak{Sol}_E(P)$)

$$c(P) : \ell \mapsto c(C_\ell)$$

as element in $\mathbb{Z}[\infty, \aleph_0]^{\mathbb{Z}_{\geq 0}}$.

(2) Define an **ℓ-th differential counting polynomial** as the polynomial $c(P)(\ell) \in \mathbb{Z}[\infty, \aleph_0]$ for all $\ell \in \mathbb{Z}_{\geq 0}$.

(3) If there exists a polynomial

$$p \in \mathbb{Q}[\ell, \aleph_0, \infty, \infty^\ell, \infty^{\frac{\ell^2}{2!}}, \ldots, \infty^{\frac{\ell^n}{n!}}]$$

such that $c(P)(\ell) = p$ for ultimately all ℓ, then call p a **differential counting polynomial** of P and denote it by $\overline{c}(P)$.

If $I = \langle p_1, \ldots, p_k\rangle_\Delta$ is a radical differential ideal, then define $c(I) := c(\{p_1, \ldots, p_k\})$ and $\overline{c}(I) := \overline{c}(\{p_1, \ldots, p_k\})$.

Note that the definition of the counting sequence explicitly allows to prescribe initial conditions with power series coefficient equations and inequations. In contrast, differential inequations are not suitable to define a counting sequence (cf. Remark 1.49).

To simplify the notation, we speak of "the" counting sequence and "the" differential counting polynomial, even though they are not unique. Furthermore, we write ∞^{ℓ^2} instead of $(\infty^{\frac{\ell^2}{2!}})^2$ and use similar simplifications. The computation of examples is postponed after the development of suitable means in Subsection 2.5.1.

2.3.3 Equality of Sets and the Differential Counting Polynomial

For the application of the counting sequence and differential counting polynomial, we need statements that compare the counting sequence and differential counting polynomial for solution sets contained in each other. If no $\aleph_0$ appears, then the description of well-fibred sets from Subsection 2.2.4 allows a satisfying statement: the counting sequence and the differential counting polynomial are both strong enough to decide whether two sets of solutions contained in each other are equal. If $\aleph_0$ appears, then Remark 2.20 prevents such a strong statement. However, the counting sequence (and also the differential counting polynomial) still allows to prove that certain sets are different. This is stated formally in the following theorem and proposition, which are both a direct corollary of Subsection 2.2.4.

The statement of the next theorem uses the following inductively defined total order "$\leq$" for polynomials $p, q \in \mathbb{Q}[\ell, \infty, \infty^\ell, \infty^{\frac{\ell^2}{2!}}, \ldots, \infty^{\frac{\ell^n}{n!}}]$. First, $p \leq q$ if and only if $0 \leq q - p$. If $p \in \mathbb{Q}$, then "$\leq$" extends the natural order on $\mathbb{Q}$. If $p \notin \mathbb{Q}$, then $0 \leq p$ if and only if $0 \leq \operatorname{init}(p)$, for the algebraic ranking $\ell < \infty < \infty^\ell < \infty^{\frac{\ell^2}{2!}} < \ldots < \infty^{\frac{\ell^n}{n!}}$.

Theorem 2.34. *Let $P_1, P_2 \subset F\{U\}^{\{=\}} \cup F[G]^{\{=,\neq\}}$ be two algebraically restricted system of differential equations with $\mathfrak{Sol}_E(P_1) \subseteq \mathfrak{Sol}_E(P_2)$, such that the counting sequences $c(P_1)$ and $c(P_2)$ exist. Then:*

(1) If $c(P_1)(\ell) \in \mathbb{Z}[\infty]$ for all $\ell \in \mathbb{Z}_{\geq 0}$, then $c(P_1)$ is the unique[9] counting sequence.

(2) If $c(P_1)(\ell), c(P_2)(\ell) \in \mathbb{Z}[\infty]$ for all $\ell \in \mathbb{Z}_{\geq 0}$, then $c(P_1)(\ell) \leq c(P_2)(\ell)$ for all $\ell \in \mathbb{Z}_{\geq 0}$, and equality holds if and only if $\mathfrak{Sol}_E(P_1) = \mathfrak{Sol}_E(P_2)$.

Assume the differential counting polynomials $\overline{c}(P_1)$ and $\overline{c}(P_2)$ exist. Then:

(3) If $\overline{c}(P_1) \in \mathbb{Q}[\ell, \infty, \infty^{\ell}, \infty^{\frac{\ell^2}{2!}}, \ldots, \infty^{\frac{\ell^n}{n!}}]$, then $\overline{c}(P_1)$ is the unique differential counting polynomial.

(4) If $\overline{c}(P_1), \overline{c}(P_2) \in \mathbb{Q}[\ell, \infty, \infty^{\ell}, \infty^{\frac{\ell^2}{2!}}, \ldots, \infty^{\frac{\ell^n}{n!}}]$, then $\overline{c}(P_1) \leq \overline{c}(P_2)$, and equality holds if and only if $\mathfrak{Sol}_E(P_1) = \mathfrak{Sol}_E(P_2)$.

Remark 2.20 indicates that a stronger version of this theorem is unlikely. However, the estimation of algebraic counting polynomials from Proposition 2.30, which proves that two sets are not equal, generalizes to the differential case. The definition of the estimation $\prec$ is given before Proposition 2.30.

Proposition 2.35. *Let $P_1, P_2 \subset F\{U\}^{\{=\}} \cup F[G]^{\{=,\neq\}}$ be two algebraically restricted system of differential equations with $\mathfrak{Sol}_E(P_1) \subseteq \mathfrak{Sol}_E(P_2)$ such that the counting sequences $c(P_1)$ and $c(P_2)$ exist. If there exist an $\ell \in \mathbb{Z}_{\geq 0}$ and $q_1, q_2 \in \mathbb{Z}[\infty]$ with $c(P_1)(\ell) \prec q_1 \lneqq q_2 \prec c(P_2)(\ell)$, then $\mathfrak{Sol}_E(P_1) \neq \mathfrak{Sol}_E(P_2)$.*

2.3.4 Comparison to the Differential Dimension Polynomial

The counting sequence and the differential counting polynomial are connected to the differential dimension polynomial. This implies that certain parts of the counting sequence and the differential counting polynomial are unique, even though they are not unique when $\aleph_0$ appears in them (cf. Remark 2.20 and Theorem 2.34).

Under the assumptions of the following theorem, both the ℓ-th differential counting polynomial and the differential counting polynomial have an element in $\mathbb{Z}_{\geq 1}$ as leading coefficient, i.e., every such polynomial has a **leading term**

$$\lambda_{c(I)}(\ell) := a(\ell) \cdot \infty^{f(\ell)} \text{ for some } a : \mathbb{Z}_{\geq 0} \to \mathbb{Z}_{\geq 1} \text{ and } f : \mathbb{Z}_{\geq 0} \to \mathbb{Z}_{\geq 0} ,$$

when considered as polynomial in the indeterminate ∞ resp. the indeterminates $\infty^{\frac{\ell^i}{i!}}$ for $0 \leq i \leq n$ and coefficients in $\mathbb{Z}[\aleph_0]$ resp. $\mathbb{Q}[\aleph_0, \ell]$.

Theorem 2.36. *Let $I := \mathcal{I}(S)$ the differential ideal associated to a simple differential system S. Let Ω_I be the differential dimension function, and ω_I be the differential dimension polynomial. If a counting sequence $c(I)$ of I exists, then for the leading terms of the ℓ-th differential counting polynomial the following holds*

$$\lambda_{c(I)}(\ell) = a(\ell) \cdot \infty^{\Omega_I(\ell)} , \qquad \text{where } a(\ell) = \prod_{\substack{p_= \in S^= \\ \operatorname{ord}(p) \leq \ell}} \operatorname{mdeg}(p) \in \mathbb{Z}_{\geq 1} .$$

If a differential counting polynomial $\overline{c}(I)$ of I exits, then

$$\lambda_{\overline{c}(I)} = a(\ell) \cdot \infty^{\omega_I(\ell)} , \qquad \text{where } a(\ell) = \prod_{p_= \in S^=} \operatorname{mdeg}(p) \in \mathbb{Z}_{\geq 1} .$$

[9] It is of course only unique for the fixed ranking, as indicated after Theorem 2.36.

The same holds for the counting sequence and differential counting polynomial of the simple system S.

We postpone the proof to the next section (page 122).

The counting sequence and the differential counting polynomial depend on the chosen orderly ranking (cf. Remark 1.76). Again, this is not a problem for comparing solution sets using Theorem 2.34 and Proposition 2.35, as all counting sequences or all differential counting polynomials only need to be computed with respect to the same ranking.

2.4 Proofs for the Differential Counting Polynomial

The goal of this section is to prove the two unproved theorems of the previous section.

The idea of the proof of Theorem 2.32 is to adapt the algebraic Thomas decomposition for a system of differential equations by treating the differential equations and all their iterated derivatives as algebraic equations. Furthermore, we allow finitely many power series coefficient equations and inequations. Of course, this is a decomposition of infinitely many equations in infinitely many indeterminates, so an algorithmic approach does not terminate. However, the algorithmic approach presented below produces "reasonable" simple algebraic systems at some step. In general, these "reasonable" systems still do not correctly characterize all truncated non-centered solutions up to order ℓ, but further steps only produce new inequations, whereas no new equations arise. In that sense, this decomposition "convergences" against the σ-systems needed for Theorem 2.32.

The proof of Theorem 2.36 builds on a structural statement about algebraic ideals associated to simple σ-systems, in particular, how the algebraic counting polynomial behaves under taking the Zariski closure. For the purpose of the ideal, one can ignore the countable set of inequations, as they play no role in defining the ideal.

Let F be a differential field of characteristic zero such that its field of constants is not countable, $\overline{F}$ its algebraic closure, $<$ an orderly ranking, $\Delta = \{\partial_1, \ldots, \partial_n\}$ a non-empty set of derivation operators, and $U = \{u^{(1)}, \ldots, u^{(m)}\}$ a non-empty set of differential indeterminates. The given orderly ranking $<$ on $F\{U\}$ induces an (algebraic) ranking on $F[G]$. Thereby, write $G = \{\overline{g_1}, \overline{g_2}, \ldots\}$ where the indeterminates $\overline{g_i}$ are defined by the total order $\overline{g_i} < \overline{g_{i+1}}$ induced by the ranking.

2.4.1 StrongReduce

This preparatory step for the proof introduces a stronger form of the reduction algorithm. This stronger reduction ensures that two properties are generically satisfied for a polynomial with respect to a simple algebraic system. First, the resulting polynomial is generically square-free and, second, prime relative to the equation of the same leader in the simple algebraic system, in case such a polynomial exists. To achieve this, it uses the splitting algorithms ResSplitDivide (cf. Algorithm 1.27) and ResSplitSquareFree (cf. Algorithm 1.28) as post-processing of the result of Reduce (cf. Algorithm 1.15).

Recall that the two algorithms ResSplitDivide and ResSplitSquareFree return two systems and a polynomial. Denote the latter polynomial by writing [3] behind the procedure names ResSplitDivide and ResSplitSquareFree.

For this subsection assume that σ-systems have a finite T-list as candidate simple system (allowing weak triangularity instead of triangularity) and a Q-list as queue (cf. Section 1.3). The formal definition of these lists is given below.

Algorithm 2.37 (StrongReduce).
Input: A system S and a polynomial $p \in R$ reduced with respect to S such that $(S_Q)_{<\mathrm{ld}(p)} = \emptyset$.
Output: A polynomial $q \in R$ with $\phi_{\mathbf{a}}(p) = 0$ if and only if $\phi_{\mathbf{a}}(q) = 0$ for each $\mathbf{a} \in \mathfrak{Sol}(S)$. Further properties of the output are given in Remark 2.38.
Algorithm:

1: $x \leftarrow \mathrm{ld}(p)$
2: $q \leftarrow p$
3: **for** $r \in S_x^{\neq}$ **do**
4: $\quad q \leftarrow \mathsf{ResSplitDivide}(S, q, r)[3]$
5: **end for**
6: $q \leftarrow \mathsf{ResSplitSquareFree}(S, q)[3]$
7: **return** q

This algorithm appears in two senses below. The first sense is a strict algorithmic sense as written here. In the second sense StrongReduce is interpreted rather as a function and not as an algorithm. Then, we can loosen the condition of S being a system and allow S to be a σ-system with countably many inequations. In this case, the **for**-loop in line 3 is formally infinite. However, at most $\mathrm{mdeg}(q)$ calls of ResSplitDivide in line 4 can change q, and we only perform these finitely many calls.

The following remark describes cases, where StrongReduce does not change the polynomial in its input. In a nutshell, this is the case if this polynomial is (a) generically squarefree on the solutions of the input system and (b) has generically no common divisor with the corresponding polynomial in the system.

Remark 2.38. Let S be a system and $p \in R$ a polynomial reduced with respect to S. Then, $\mathsf{StrongReduce}(S, p) = p$ if and only if both (a) $\mathsf{Reduce}(S_T, \mathrm{res}_0(p, \frac{\partial}{\partial x} p, x)) \neq 0$, and (b) if S_T has an equation of leader x, then $\mathsf{Reduce}(S_T, \mathrm{res}_0((S_T)_x, p, x)) \neq 0$.

In particular, the equality $\mathsf{StrongReduce}(S, p) = p$ holds in the following two scenarios. First, if S' is a system with S'_T having an equation of leader x and $q \in R$ reduced with respect to S', then this equality holds for S and p, where $(S, S_1, p) = \mathsf{ResSplitGCD}(S', q)$. Second, if S' is a system with S'_T having no an equation of leader x and $q \in R$ reduced with respect to S', then this equality holds for S and p, where $(S, S_1, p) = \mathsf{ResSplitSquareFree}(S', q)$. ◁

2.4.2 Algebraic Systems and Reduction

This subsection introduces the "data structure" which turns algebraically restricted systems of differential equations into algebraic systems. This is used both for the proof of Theorem 2.32 in this section and in the next section for examples (cf. Subsection 2.5.1).

This "data structure" associates the corresponding equation or set of inequations for each indeterminate by the allocation map β defined below. Both in the algebraic and differential algorithm in Section 1.3, the unique equation or inequation in the T-list with leader x was associated to the indeterminate x. The equations and inequation with an appropriate leader were created by reductions among the equations and inequations. In contrast, in this context, a differential equation cannot be reduced by an algebraic equation to yield an equation with appropriate leader. Thus, the association of a differential equation to an indeterminate is a process from a differential equation to an algebraic equation. This process begins with the pre-allocation map $\overline{\beta}$, which creates a suitable derivative of the differential equation. Then, the differential structure is removed by the forgetful map ρ (cf. Subsection 2.3.1). Finally, we are left with an algebraic equation, which can be manipulated by Reduce and StrongReduce. The image of the allocation map β is the result of this process.

An algebraically restricted σ-system of differential equations P has the subsets consisting of differential equations, power series coefficient equations, power series coefficient inequations, and power series coefficients restrictions, denoted by $P^{\partial,=} := P \cap F\{U\}^{\{=\}}$, $P^{a,=} := P \cap F[G]^{\{=\}}$, $P^{a,\neq} := P \cap F[G]^{\{\neq\}}$, and $P^{a} := P^{a,=} \cup P^{a,\neq}$, respectively.

Let P be an algebraically restricted σ-system of differential equations. Now, we define weakly triangular algebraic σ-systems P_i. (Thus, the reduction and splitting algorithms from Subsections 1.3.1, 2.4.1, and 1.3.2 also work for the case of algebraic σ-systems when setting $(P_i)_T := P_i$.) Define $P_0 := \emptyset$. Suppose inductively that P_{i-1} is a weakly triangular σ-system in $F[\overline{g_1}, \ldots, \overline{g_{i-1}}]$ for some $i \in \mathbb{Z}_{>0}$. Define P_i using the pre-allocation map

$$\overline{\beta} : G \to \mathbb{P}_1(\{P^{\partial,=}\}_\Delta) \uplus \mathbb{P}_1(P^{a,=}) \uplus \mathbb{P}(P^{a,\neq})$$

where $\mathbb{P}(A)$ denotes the power set of a set A and $\mathbb{P}_1(A)$ denotes its subset of sets of cardinality one. If $\overline{\beta}(\overline{g_i}) \subset P^a$ then let $P_i := P_{i-1} \cup \overline{\beta}(\overline{g_i})$ and if $\overline{\beta}(\overline{g_i}) \subset \{P^{\partial,=}\}_\Delta$ then let

$$P_i := P_{i-1} \cup \mathsf{StrongReduce}(P_{i-1}, \mathsf{Reduce}(P_{i-1}, \rho(\overline{\beta}(\overline{g_i})))) \ .$$

Assume that $\operatorname{ld}(P_i \setminus P_{i-1}) \subseteq \{\overline{g_i}\}$ so P_i is a weakly triangular σ-system in $F[\overline{g_1}, \ldots, \overline{g_i}]$.

Definition 2.39. Call a function $\beta : G \to \mathbb{P}_1(P^{a,=}) \uplus \mathbb{P}(P^{a,\neq})$ an **allocation map** if there exist $\overline{\beta}$ and P_i for all $i \in \mathbb{Z}_{\geq 1}$ as described above with $\beta(\overline{g_i}) = P_i \setminus P_{i-1}$. Call the map $\overline{\beta}$ the corresponding **pre-allocation map**. Call the corresponding weakly triangular algebraic σ-systems P_i the ***i*-th combined algebraic σ-system associated to P by** β.

Assume that all algebraically restricted σ-systems of differential equations have an allocation map. (If not explicitly specified otherwise, it is the empty set constantly.)

The following example demonstrates why StrongReduce is used.

Example 2.40 (cf. Example D.6)**.** Let $\Delta = \{\partial_t\}$ and $U = \{u\}$. Consider solutions[10] $u(t) = \sum_{i=0}^{\infty} g_i \frac{t^i}{i!}$ centered around zero of the differential equation $p := u_t^2 - 4u = 0$ such that the solution has a zero at the center of expansion, i.e., consider the algebraically restricted system of differential equations $P := \{(p)_=, (g_0)_=\}$.

Begin to construct a suitable pre-allocation map $\overline{\beta}$ and the corresponding allocation map β. For the first combined algebraic σ-system P_1 define $\overline{\beta}(g_0) := \{(g_0)_=\}$ and get $P_1 = \{(g_0)_=\}$. The only constraint for g_1 is given by p. Therefore, set $\overline{\beta}(g_1) := \{p_=\}$. For the corresponding value of the allocation map get $\rho(\overline{\beta}(g_1)) = \rho(p_=) = (g_1^2 - 4g_0)_=$. This equation is the square $(g_1^2)_=$ after being reduced modulo P_1. Only the application of ResSplitSquareFree in StrongReduce yields $\beta(g_1) = \{(g_1)_=\}$. ◁

The reduction with respect to algebraic systems easily carries over to algebraically restricted σ-system of differential equations: they can reduce elements in $F[G]$.

Algorithm 2.41 (Reduce)**.**
Input: An algebraically restricted σ-system of differential equations P with allocation map β, a polynomial $p \in F[G]$.
Output: A polynomial q with $\phi_e(p) = 0$ if and only if $\phi_e(q) = 0$ for each $e \in \mathfrak{Sol}(P)$.
Algorithm:

[10] Using above notation, $g_i = \overline{g_{i+1}}$.

1: $\overline{g_i} \leftarrow \mathrm{ld}(p)$. // *This defines* i
2: $P_i \leftarrow i$-th combined algebraic σ-system associated to P by β
3: **return** $\mathsf{Reduce}(P_i, p)$

For an algebraically restricted σ-system of differential equations the T-list, the candidate simple system, and Q-list, the queue, are defined similarly to those of algebraic systems in Section 1.3. Let P be an algebraically restricted σ-system of differential equations with allocation map β. Call the weakly triangular set $P_T = \bigcup_{i\in\mathbb{Z}_{\geq 1}} P_i$ the **T-list** of P, where P_i is the i-th combined algebraic system associated to P by β. The **Q-list** of P, i.e., the queue of unprocessed polynomials, is given by

$$P_Q := (P^a \setminus \mathrm{im}(\beta)) \cup \left\{ p \in \rho\left(\{P^{\partial,=}\}_\Delta\right) \middle| \mathsf{Reduce}(P,p) \neq 0 \right\} .$$

The second set in this union seems counterintuitive. It is needed, as differential equations can never be moved into the T-list, as a differential equation has *infinitely* many consequences. To prevent cluttering up the Q-list by superfluous constraints, the reduction to zero is used to decide whether the influence of *one* derivative of a differential equation is already included in the T-list. Note that both the T-list and the Q-list only contain equations and inequations in $F[G]$, but no differential equations.

The proof uses the set of solutions of P_T as superset of the set of solutions of P. It successively enlarges P_T such that $\mathfrak{Sol}_E(P_T)$ "converges" against $\mathfrak{Sol}_E(P)$.

2.4.3 An Infinite Decomposition

This subsection proves Theorem 2.32. The main tool is Construction 2.46 below. It is an infinite process for algebraically restricted *systems* of differential equations, similar to the algebraic Thomas decomposition of algebraic systems. As it might run infinitely long, it can only "converge" against the correct solution set. When computing the counting sequence and the differential counting polynomial in practice, this gives an approximation and often leads to a good guess for the correct answer. (Of course, one has to verify this guess.)

In general, the (pre) allocation maps can return sets of inequations. In this subsection these sets are always finite, and thus one can multiply these inequations. We use this to simplify the notation in this subsection and change Definition 2.39 in such a way that the (pre) allocation maps returns singletons.

We begin with a technical subalgorithm. It inserts a newly treated equation into the T-list by changing the pre-allocation map $\overline{\beta}$. In addition to a system, this algorithm gets two equations $p_=$ and $r_=$ as input. The idea behind these two equations is the following. The equation $r_=$ is the original equation and may be a differential equation. The power series coefficient equation $p_=$ is the result of applying reduction, gcd and square-free methods to $r_=$. This subalgorithm keeps track of $r_=$ to set the image of the pre-allocation map $\overline{\beta}$ to $r_=$.

Algorithm 2.42 ($\mathsf{InsertEquation}$).
Input:

- An algebraically restricted system of differential equations P' with allocation map $\beta_{P'}$,
- an equation $p_= \in F[G]^{\{=\}}$ with $\mathrm{ld}(p) = \overline{g_i}$, and
- an equation $r_= \in (F\{U\} \cup F[G])^{\{=\}}$ with $\rho(r_=) \in P_Q$

such that $\mathsf{StrongReduce}(P', \mathsf{Reduce}(P', \rho(r))) = p$.
Output: An algebraically restricted system of differential equations P with allocation map β_P with $\beta(\overline{g_i}) = p$, $\mathfrak{Sol}_E(P) = \mathfrak{Sol}_E(P')$ and $\mathsf{Reduce}(P, \rho(r)) = \mathsf{Reduce}(P, p) = 0$. In particular, $\mathsf{Reduce}(P, \rho(r))$ implies that $\rho(r)$ is removed from the Q-list of P.
Algorithm:

1: $P \leftarrow P'$.
2: **if** $r \in F[G]$ **then**
3:     **if** $p \neq r$ **then**
4:         $P^a \leftarrow (P^a \setminus \{r_=\}) \cup \{p_=\}$
5:     **end if**
6:     $\overline{\beta_P}(\overline{g_i}) \leftarrow p_=$
7: **else if** $r \in F\{U\}$ **then**
8:     **if** $p \neq \mathsf{Reduce}(P, \rho(r))$ **then**
9:         $P^a \leftarrow P^a \cup \{p_=\}$
10:         $\overline{\beta_P}(\overline{g_i}) \leftarrow p_=$
11:     **else**
12:         $\overline{\beta_P}(\overline{g_i}) \leftarrow r_=$
13:     **end if**
14: **end if**

Proof. First, show that $\beta(\overline{g_i}) = p$. In line 6 and line 10 the image of the pre-allocation map $\overline{\beta}$ is set to the equation $p_=$. In line 12 the image of the pre-allocation map $\overline{\beta}$ is set to the equation $r_=$. From the condition $\mathsf{StrongReduce}(P', \mathsf{Reduce}(P', \rho(r))) = p$ it follows that p lies in the image of the allocation map β.

Second, show that $\mathfrak{Sol}_E(P) = \mathfrak{Sol}_E(P')$. The substitution of $r_=$ by $p_=$ in line 4 does not change the set of solutions, since both appear as power series coefficient equations, and the algorithms Reduce and $\mathsf{StrongReduce}$, which descibe the relation between $r_=$ and $p_=$, do not change the set of solutions. Similarly, adding $p_=$ to the system in line 9 also leaves the set of solutions of the system unchanged, as the power series coefficient equation $p_=$ is just a consequence of the differential equation $r_=$; the equation $p_=$ is even equivalent to $\rho(r_=)$ on the set of solution.

The third point $\mathsf{Reduce}(P, \rho(r)) = \mathsf{Reduce}(P, p) = 0$ follows easily from $\beta(\overline{g_i}) = p$ and $\mathsf{StrongReduce}(P', \mathsf{Reduce}(P', \rho(r))) = p$. □

Remark 2.43. The following algorithm $\mathsf{InfiniteDecompose}$ sloppily uses the algorithms $\mathsf{InitSplit}$, $\mathsf{ResSplitGCD}$, $\mathsf{ResSplitSquareFree}$, and $\mathsf{ResSplitDivide}$ for algebraically restricted system of differential equations rather than for algebraic or differential systems. This is justified because all splittings are done with respect to power series equations and inequations in $F[G]$. More specific, splitting an algebraically restricted system of differential equations P with respect to a polynomial $p \in F[G]$ results in two algebraically restricted systems of differential equations P_1 and P_2 with $P_1^{a,\neq} = P^{a,\neq} \cup \{p_{\neq}\}$ and $P_2^{a,=} = P^{a,=} \cup \{p_=\}$. ◁

The selection strategy needs to be adapted to algebraically restricted systems of differential equations.

Definition 2.44. A **selection strategy** for algebraically restricted systems of differential equations is a map, which maps an algebraically restricted system of differential equations P with $P_Q \neq \emptyset$ to an element $q \in P_Q$, such that the following two properties are satisfied:

(1) If $\mathsf{Select}(P) = q$, then $\mathrm{ld}(\mathsf{Reduce}(P, P_Q)) \cap \{\overline{g_i} \in G \mid \overline{g_i} < \mathrm{ld}(\mathsf{Reduce}(P, q))\} = \emptyset$.

(2) If $\mathsf{Select}(P) = q_{\neq}$ is an inequation, then additionally $\mathrm{ld}(\mathsf{Reduce}(P, (P_Q)^{=})) \cap \{\overline{g_i} \in G \mid \overline{g_i} \leq \mathrm{ld}(\mathsf{Reduce}(P, q))\} = \emptyset$ holds.

Construction 2.46 may produce countably many systems. For "convergence", all of these systems need to be treated repeatedly. To achieve this, choose systems according to the following condition. Let $\mathbb{P}(A)$ denote the power set of a set A.

Definition 2.45 (Choose). A **choice** for algebraically restricted systems of differential equations is a map

$$\begin{aligned}\mathsf{Choose} : \mathbb{P}\left(\{P \mid P \text{ algebraically restricted system of differential equations}\}\right)\\ \longrightarrow \{P \mid P \text{ algebraically restricted system of differential equations}\} :\\ L \longmapsto P \in L\end{aligned}$$

with the property $\min(\mathrm{ld}(\mathsf{Choose}(L)_Q)) = \min(\mathrm{ld}(P'_Q)|P' \in L)$.

Construction 2.46 (InfiniteDecompose).
Input: An algebraically restricted system of differential equations P
Computation steps: They are printed on page 115.

Proof. We show that the input of each subalgorithm is sound. This is clear for the subalgorithms InitSplit, ResSplitGCD, ResSplitSquareFree, and ResSplitDivide. For the two calls of InsertEquation $p_=$ is reduced with respect to P, since q is reduced with respect to P, $\mathrm{ld}(p) = \mathrm{ld}(q)$, and $\mathrm{mdeg}(p) \leq \mathrm{mdeg}(q)$. At last, condition $\mathsf{StrongReduce}(P, q) = p$ for $q = \mathsf{Reduce}(P, \rho(r))$ follows from Remark 2.38. □

Note that a polynomial $p \in \{P^{\partial,=}\}_\Delta$ is removed from the Q-list by adding it (or a divisor of it) to the T-list. Thus, p reduces to zero and is no longer contained in the Q-list.

Note that we do not claim termination of this construction. However, now we show several properties of this construction, in particular that it produces the systems of the statement of Theorem 2.32.

The proof of the first loop invariant of the correctness proof of the algorithm Decompose (cf. page 40) can almost verbatim be used to prove the following lemma.

Lemma 2.47. *In Construction 2.46*

$$\mathfrak{Sol}_E(P') = \biguplus_{P \in L} \mathfrak{Sol}_E(P)$$

after each while loop.

Lemma 2.48. *Let P be an algebraically restricted system of differential equations in L in Construction 2.46 and $\overline{g_i} \in G$. Then, P_T is triangular, $\phi_{<\overline{g_i},\mathbf{a}}(p)$ is square-free, and $\phi_{\mathbf{a}}(\mathrm{init}(p)) \neq 0$ for all $p \in P_T$ with $\mathrm{ld}(p) = \overline{g_i}$ and all $\mathbf{a} \in \mathfrak{Sol}((P_T)_{<\overline{g_i}} \cup (P_Q)_{<\overline{g_i}})$.*

Before giving the proof, which is similar to the second loop invariant of the correctness proof of Decompose (cf. page 40), an easy corollary springs to mind.

Corollary 2.49. *Let P be an algebraically restricted system of differential equations in L in Construction 2.46 and $\overline{g_i} \in G$. If $(P_Q)_{\leq\overline{g_i}} = \emptyset$, then $(P_T)_{\leq\overline{g_i}}$ is a simple algebraic system.*

Construction 2.46 (InfiniteDecompose)

$L \leftarrow \{P'\}$
while $|L| > 0$ **do**
$P \leftarrow \mathsf{Choose}(L)$; $L \leftarrow L \setminus \{P\}$
$r \leftarrow \mathsf{Select}(P)$; $q \leftarrow \mathsf{Reduce}(P, \rho(r))$; $x \leftarrow \mathrm{ld}(q)$
if $q \notin \{c_= \mid c \in F \setminus \{0\}\}$[a] **then**
if $x \neq 1$ **then**
if q is an equation **then**
if $\beta_P(x)$ is an equation **then**
if $\mathsf{Reduce}(P_T, \mathrm{res}_0(\beta_P(x), q, x)) = 0$ **then**
$(P, P_1, p) \leftarrow \mathsf{ResSplitGCD}(P, q)$; $L \leftarrow L \cup \{P_1\}$
$P \leftarrow \mathsf{InsertEquation}(P, p_=, r_=)$
else
$P^{a,=} \leftarrow P^{a,=} \cup \{\mathrm{res}_0(\beta_P(x), q, x)_=\}$
end if
else
$(P, P_2) \leftarrow \mathsf{InitSplit}(P, q)$; $L \leftarrow L \cup \{P_2\}$
$(P, P_3, p) \leftarrow \mathsf{ResSplitSquareFree}\,(P, q)$; $L \leftarrow L \cup \{P_3\}$
$P \leftarrow \mathsf{InsertEquation}(P, p_=, r_=)$
end if
else if q is an inequation **then**
if $\beta_P(x)$ is an equation **then**
$(P, P_4, p) \leftarrow \mathsf{ResSplitDivide}\,(P, \beta_P(x), q)$; $L \leftarrow L \cup \{P_4\}$
$P^{a,=} \leftarrow P^{a,=} \cup \{p_=\}$; $\overline{\beta_P}(x) \leftarrow \{p_=\}$
else
$(P, P_5) \leftarrow \mathsf{InitSplit}(P, q)$; $L \leftarrow L \cup \{P_5\}$
$(P, P_6, p) \leftarrow \mathsf{ResSplitSquareFree}\,(P, q)$; $L \leftarrow L \cup \{P_6\}$
if $\beta_P(x)$ is an inequation **then**
$(P, P_7, r) \leftarrow \mathsf{ResSplitDivide}\,(P, \beta_P(x), p)$; $L \leftarrow L \cup \{P_7\}$
$\beta_P(x) \leftarrow (r \cdot p)_{\neq}$
else if $\beta_P(x)$ is empty **then**
$\beta_P(x) \leftarrow p_{\neq}$
end if
end if
end if
end if
$L \leftarrow L \cup \{P\}$
end if
end while

[a] $q \neq 0$ is not possible because of the definition of P_Q.

Proof of Lemma 2.48. One easily checks that all steps in the algorithm allow only one polynomial $(P_T)_{\overline{g_i}}$ in P_T for each leader $\overline{g_i}$, thus triangularity obviously holds.

At the beginning of Construction 2.46 the statement holds, because $P_T = \emptyset$ for the input system P. So assume that the condition holds at the beginning of the main loop. Show that all polynomials added to the image of the allocation map β, and thus to P_T, have non-zero initial and are square-free. For $\mathfrak{Sol}((P_T)_{<\overline{g_i}} \cup (P_Q)_{<\overline{g_i}}) = \emptyset$, the statement is trivially true. So, let $\mathbf{a} \in \mathfrak{Sol}((P_T)_{<\overline{g_i}} \cup (P_Q)_{<\overline{g_i}})$.

For the equation $p_=$ added as conditional gcd of $(P_T)_{\overline{g_i}}$ and q in line 11, $\phi_{<\overline{g_i},\mathbf{a}}(p)$ is a divisor of $\phi_{<\overline{g_i},\mathbf{a}}((P_T)_{\overline{g_i}})$. As $\phi_{<\overline{g_i},\mathbf{a}}((P_T)_{\overline{g_i}})$ is square-free by assumption, so is $\phi_{<\overline{g_i},\mathbf{a}}(p)$. The inequation added to P in ResSplitGCD is the initial of $p_=$.

The equation $p_=$ inserted into P_T in line 18 and the inequation $p_{\neq}$ inserted in line 31 are square-free due to ResSplitSquareFree, and their initials are non-zero as p is either identical to q, or it is a pseudo quotient of q by $\mathrm{SPRS}_i\left(q, \frac{\partial}{\partial \overline{g_i}} q, \overline{g_i}\right)$ for some $i > 0$. On the one hand, if p equals q, the call of InitSplit for q ensures a non-zero initial for p. On the other hand, the polynomial $\mathrm{SPRS}_i\left(q, \frac{\partial}{\partial \overline{g_i}} q, \overline{g_i}\right)$ has initial $\mathrm{res}_i\left(q, \frac{\partial}{\partial \overline{g_i}} q, \overline{g_i}\right)$, which is added as an inequation by ResSplitSquareFree.

The equation $p_=$ that replaces the old equation $(P_T)_{\overline{g_i}}$ in line 23 is the quotient of $(P_T)_{\overline{g_i}}$ by an inequation. It is square-free, because $\phi_{<\overline{g_i},\mathbf{a}}(p)$ is a divisor of $\phi_{<\overline{g_i},\mathbf{a}}((P_T)_{\overline{g_i}})$, which is square-free by assumption. Again, p is either identical to $(P_T)_{\overline{g_i}}$ or a pseudo quotient of $(P_T)_{\overline{g_i}}$ by $\mathrm{SPRS}_i\left((P_T)_{\overline{g_i}}, q, \overline{g_i}\right)$ for some $i > 0$ and, using the same arguments as in the last paragraph, the initial of p does not vanish.

Finally, consider the inequation $(r \cdot p)_{\neq}$ added in line 29 as a least common multiple of $((P_T)_{\overline{g_i}})_{\neq}$ and $p_{\neq}$. The inequation $\phi_{<\overline{g_i},\mathbf{a}}(p)$ is square-free and has a non-vanishing initial for the same reasons as before. Due to $\phi_{<\overline{g_i},\mathbf{a}}(r) \sim \frac{\phi_{<\overline{g_i},\mathbf{a}}((P_T)_{\overline{g_i}})}{\gcd(\phi_{<\overline{g_i},\mathbf{a}}((P_T)_{\overline{g_i}}),\phi_{<\overline{g_i},\mathbf{a}}(p))}$, the polynomials $\phi_{<\overline{g_i},\mathbf{a}}(r)$ and $\phi_{<\overline{g_i},\mathbf{a}}(p)$ have no common divisors. As $\phi_{<\overline{g_i},\mathbf{a}}(r)$ divides $\phi_{<\overline{g_i},\mathbf{a}}((P_T)_{\overline{g_i}})$, using the same arguments as before, $\phi_{<\overline{g_i},\mathbf{a}}(r)$ is square-free and has a non-vanishing initial. This completes the proof. □

The following lemmas are a first step towards a formal statements of the form "all systems and all constraints in the systems are treated at some point". For their formulation we use the following language. In Construction 2.46, call the systems $P_1, \ldots, P_7$ and the system P added to L in line 36 the **children** of a system P chosen in line 3. The latter system P added to L in line 36 is also called the **heir** of the system P chosen in line 3. Similarly, define a **descendent** as an element in the transitive hull of children and a **successor** as an element in the transitive hull of heir.

Lemma 2.50. *Consider a chain $P = P^{(1)}, P^{(2)}, \ldots$ of algebraically restricted system of differential equations, such that $P^{(j+1)}$ is a child of $P^{(j)}$. Let $\overline{g_i} \in G$. Then there is a $k \in \mathbb{Z}_{\geq 2}$ such that $P_Q^{(k)} \cap F[\overline{g_1}, \ldots, \overline{g_i}]^{\{=,\neq\}} = \emptyset$.*

Proof. The proof is similar to the termination of Decompose (cf. page 42). Define $\prec$ as the composite order $[\prec_1, \prec_2, \prec_3, \prec_4]$ of the four orders defined below. (It depends on $\overline{g_i}$ from the statement of the lemma.) The $\prec_j$ are well-founded (the proof is the same as in Definition and Remark 1.35), and thus $\prec$ is. Let P, P' be algebraically restricted systems of differential equations.

(1) For $j = 1, \ldots, i$ define $\prec_{1,\overline{g_j}}$ by $P \prec_{1,\overline{g_j}} P'$ if and only if $\mathrm{mdeg}\left((P_T)^{=}_{\overline{g_j}}\right) < \mathrm{mdeg}\left((P'_T)^{=}_{\overline{g_j}}\right)$, with $\mathrm{mdeg}\left((P_T)^{=}_{\overline{g_j}}\right) := \infty$ if $(P_T)^{=}_{\overline{g_j}}$ is empty. Define the composite order $\prec_1$ as $[\prec_{1,\overline{g_1}}, \ldots, \prec_{1,\overline{g_i}}]$.

(2) Define the map μ from the set of algebraically restricted systems of differential equations to $\{1, \overline{g_1}, \dots, \overline{g_i}, \overline{g_\infty}\}$, where $\mu(P)$ is minimal such that there exists an equation $p \in (P_Q)^{=}_{\mu(S)}$ with $\mathsf{Reduce}(P, p) \neq 0$, or $\mu(S) = \overline{g_\infty}$ if no such equation exists. Then, $P \prec_2 P'$ if and only if $\mu(P) < \mu(P')$ with $1 < \overline{g_j}$ and $\overline{g_j} < \overline{g_\infty}$ for $1 \leq j \leq i$.

(3) $P \prec_3 P'$ if and only if there is $p_{\neq} \in F[\overline{g_1}, \dots, \overline{g_i}]^{\neq}$ and a finite (possibly empty) set $K \subset F[\overline{g_1}, \dots, \overline{g_i}]^{\neq}$ with $\mathrm{ld}(q) < \mathrm{ld}(p) \; \forall\, q \in K$ such that $P_Q^{a,\neq} \uplus \{p_{\neq}\} = (P')_Q^{a,\neq} \uplus K$ holds.

(4) $P \prec_4 P'$ if and only if $|\rho(P_Q) \cap F[\overline{g_1}, \dots, \overline{g_i}]| < \left|\rho(P'_Q) \cap F[\overline{g_1}, \dots, \overline{g_i}]\right|$.

Tacitly use the fact that reduction never makes polynomials bigger in the sense of Remark 1.17.(3). Again, for $j = 1, \dots, 4$ use the notation $P \not\precsim_j P'$ if neither $P \prec_j P'$ nor $P' \prec_j P$ holds.

Denote the system chosen from L in line 4 by $\widehat{P}$ and the system added to L in line 36 by P. Let q be the element selected from and reduced with respect to $\widehat{P}$ in line 4, and x its leader. Prove that the children $P, P_1, \dots, P_7$ of $\widehat{P}$ are $\prec$-smaller than $\widehat{P}$. Note, that $P^{(i+1)}$ is generated from $P^{(i)}$ as one of these children. As $\prec$ is well-founded, this means that $\rho(P_Q) \cap F[\overline{g_1}, \dots, \overline{g_i}]$ after finitely many steps by order $\prec_4$. Since $x > g_i$ implies the claim by the axiom (1) from the definition of Select, assume that $x \leq g_i$.

For $j = 1, \dots, 7$, $((P_j)_T)^{=} = (\widehat{P}_T)^{=}$, and thus $P_j \not\precsim_1 \widehat{P}$. The properties of Select in Definition 2.44 directly require that there is no equation in $(\widehat{P}_Q)^{=}$ with a leader smaller than x. However, the equation added to the system P_j returned from $\mathsf{InitSplit}$ is the initial of q, which has a leader smaller than x and does not reduce to 0 (cf. Remark 1.17.(2)). Furthermore, the equations added in one of the subalgorithms based on $\mathsf{ResSplit}$ have a leader smaller than x and do not reduce to 0. In each case $P_j \prec_2 \widehat{P}$ is proved.

It remains to show $P \prec \widehat{P}$. If q is reduced to $0_{=}$, then it is omitted from P_Q, and so $P \prec_4 \widehat{P}$. As the system is otherwise unchanged, $P \not\precsim_j \widehat{P}, 1 \leq j \leq 3$, and therefore $P \prec \widehat{P}$ holds. If q is reduced to $c_{\neq}$ for some $c \in F \setminus \{0\}$, then $P \prec_3 \widehat{P}$ and $P \not\precsim_j \widehat{P}, 1 \leq j \leq 2$, since the only change was the removal of an inequation from $P^{a,\neq}$. Otherwise, one of the following cases occurs:

Lines 10-11 set $\beta_P(x)$ to $p_{=}$ of smaller degree than $\beta_{\widehat{P}}(x)$ and 15-18 add $\beta_P(x)$ as a new equation. In both cases $P \prec_1 \widehat{P}$.

In line 13, $P_T = \widehat{P}_T$ implies $P \not\precsim_1 \widehat{P}$. The polynomial q is chosen according to Select (cf. Definition 2.44.(1)), which implies $(\widehat{P}_Q)^{=}_{<x} = \emptyset$ and $(P_Q)^{=}_{<x} = \{\mathrm{res}_0(\beta_P(x), q, x)_{=}\}$. Line 9 ensures $\mathsf{Reduce}(P, \mathrm{res}_0(\beta_P(x), q, x)) \neq 0$ and, thus, $P \prec_2 \widehat{P}$ follows.

Consider lines 22-23. If the degree of $\beta_P(x)$ is smaller than the degree of $\beta_{\widehat{P}}(x)$, then $P \prec_1 \widehat{P}$. In case the degree doesn't change, $P \not\precsim_2 \widehat{P}$ and $(P_Q)^{=} = (\widehat{P}_Q)^{=}$ guarantees $P \not\precsim_1 \widehat{P}$. However, q is removed from P_Q and replaced by an inequation with smaller leader, which implies $P \prec_3 \widehat{P}$.

In lines 24-32, obviously $P \not\precsim_j \widehat{P}, 1 \leq j \leq 2$. As before, q is removed from P_Q and replaced by an inequation of smaller leader, which once more implies $P \prec_3 \widehat{P}$. □

Lemma 2.51. *In Construction 2.46 each system in L will be chosen after a finite number of steps.*

Proof. Let $P' \in L$ and $\overline{g_i} = \min(\mathrm{ld}(P'_Q))$. The map Choose ensures that the algorithms treat a system with a polynomial of minimal leader in its Q-list. Lemma 2.50 implies that $P_Q \cap F[\overline{g_1}, \ldots, \overline{g_i}]^{\{=,\neq\}} = \emptyset$ for all $P \in L \setminus \{P'\}$ after a finite number of steps. At that point, P' will be chosen. □

Lemma 2.52. *Let P' be an algebraically restricted system of differential equations and $p \in (P')_Q$. Then there is a number $k \in \mathbb{Z}_{\geq 0}$ such that each descendent of P' has selected p (via* Select*) after k runs of the while loop in Construction 2.46.*

Proof. This follows directly from Lemma 2.50 and Lemma 2.51 □

Proposition 2.53. *Let P' be an algebraically restricted system of differential equations. Then, for every $e \in E \setminus \mathfrak{Sol}_E(P')$ there exists an $k \in \mathbb{Z}_{>0}$ such that after k steps of the while loop in Construction 2.46 this element e is not contained in $\mathfrak{Sol}_E(P_T)$ for all $P \in L$.*

Proof. As $e \notin \mathfrak{Sol}_E(P')$ there exists a constraint in the system that does not have e as a solution, i.e., there is an $p \in (P')^{a,\neq}$ with $\phi_e(p) = 0$, there is a $p \in (P')^{a,=}$ with $\phi_e(p) \neq 0$, or there is a $p \in \rho(\{(P')^{\partial,=}\}_\Delta)$ with $\phi_e(p) \neq 0$. By Lemma 2.52 the constraint is selected after a finite number of steps in each descendent of P'. □

The "convergence" of Construction 2.46 is shown in two steps. The first step shows that after finitely many steps no new equations of the given order ℓ arise. The second step looks at inequations.

Let P be an algebraically restricted system of differential equations with T-list P_T and $i \in \mathbb{Z}_{\geq 1}$. Let $q := \prod_{p \in (P_T)^{=}_{\leq \overline{g_i}}} \mathrm{init}(p) \in F[\overline{g_1}, \ldots, \overline{g_i}]$. Call the ideal

$$\begin{aligned}\mathcal{I}_{T,\leq\overline{g_i}}(P) &:= \langle (P_T)^{=}_{\leq\overline{g_i}} \rangle : q^\infty \\ &= \left\{ p \in F[\overline{g_1}, \ldots, \overline{g_i}] \middle| q^r \cdot p \in \langle (P_T)^{=}_{\leq\overline{g_i}} \rangle \text{ for some } r \in \mathbb{Z}_{\geq 0} \right\}\end{aligned}$$

in $F[\overline{g_1}, \ldots, \overline{g_i}]$ the **ideal associated to the T-list of P up to $\overline{g_i}$**. The next goal is to describe how these ideals approximate a differential ideal.

Lemma 2.54. *Let $P' \subset F\{U\}^=$ be an algebraically restricted system of differential equations and P a descendent of P'. Then, $\mathcal{I}_{T,\leq\overline{g_i}}(P') \subseteq \mathcal{I}_{T,\leq\overline{g_i}}(P)$ for all $\overline{g_i} \in G$.*

Proof. It suffices to consider the case when P is a child of P'. Adding new equations to P'_T increases the ideal and adding an inequation to P'_T does not change the ideal. Furthermore, the two cases when changing an existing equation, i.e., when computing the gcd of two equations or dividing an equation by an inequation, replace the equation by a divisor modulo the lower equation in P'_T. □

Lemma 2.55. *Let $P' = (P')^{\partial,=}$ be a system of differential equations, viewed as an algebraically restricted system of differential equations. If Construction 2.46 is started with P', then*

$$\bigcap_{P \in L} \mathcal{I}_{T,\leq\overline{g_i}}(P) \subseteq \rho(\sqrt{\langle (P')^{\partial,=} \rangle_\Delta}) \cap F[\overline{g_1}, \ldots, \overline{g_i}]$$

at all steps and for all $\overline{g_i} \in G$.

Proof. Obviously, $\mathfrak{Sol}_E(\mathcal{I}_{T,\leq\overline{g_i}}(P)) \supseteq \mathfrak{Sol}_E(P)$ for all $P \in L$, and thus

$$\bigcup_{P\in L} \mathfrak{Sol}_E(\mathcal{I}_{T,\leq\overline{g_i}}(P)) \supseteq \biguplus_{P\in L} \mathfrak{Sol}_E(P) = \mathfrak{Sol}_E(P') ,$$

where the last equality is from Lemma 2.47. Applying the vanishing ideal operator $\mathcal{I}$ and making use of the inclusion reverting bijection from Corollary 1.67 results in

$$\mathcal{I}(\bigcup_{P\in L} \mathfrak{Sol}_E(\mathcal{I}_{T,\leq\overline{g_i}}(P))) = \bigcap_{P\in L} \mathcal{I}(\mathfrak{Sol}_E(\mathcal{I}_{T,\leq\overline{g_i}}(P))) \subseteq \mathcal{I}(\mathfrak{Sol}_E(P'))$$

Then, $\mathcal{I}_{T,\leq\overline{g_i}}(P) \subseteq \mathcal{I}(\mathfrak{Sol}_E(\mathcal{I}_{T,\leq\overline{g_i}}(P)))$ and by the Nullstellensatz for non-centered solutions (cf. Theorem 1.65 and Corollary 1.67) $\sqrt{\langle (P')^{\partial,=}\rangle_\Delta} = \mathcal{I}(\mathfrak{Sol}_E(P'))$. □

Lemma 2.56. *Let $P' \subset F\{U\}^=$ be an algebraically restricted system of differential equations. Then, for every $\overline{g_i} \in G$ there is an $k \in \mathbb{Z}_{>0}$ such that Construction 2.46 started with P' results in*

$$\mathcal{I}_{F[G]}(\mathfrak{Sol}_E(P')) \cap F[\overline{g_1}, \ldots, \overline{g_i}] \subseteq \mathcal{I}_{T,\leq\overline{g_i}}(P)$$

after k steps of the while loop for all descendents $P \in L$ of P'.

Proof. This is a claim about the polynomial ring $R := F[\overline{g_1}, \ldots, \overline{g_i}]$ in finitely many variables. In particular, R is NOETHERian and its ideals have a primary decomposition.

By Lemma 2.50 the lower part of the Q-list $(P_Q)_{\leq\overline{g_i}}$ of all descendents P of P' is empty after a finite number of steps. At that point, by Corollary 2.49 and Proposition 1.62 the ideal $\mathcal{I}_{T,\leq\overline{g_i}}(P)$ is radical. By Lemma 2.54 the ideals $\mathcal{I}_{T,\leq\overline{g_i}}(P)$ increase when going to a child of a system. Thus, is suffices to consider only descendents P of P' with $(P_Q)_{\leq\overline{g_i}} = \emptyset$.

Let P be any descendent of P' with $(P_Q)_{\leq\overline{g_i}} = \emptyset$ and $\mathcal{I}_{T,\leq\overline{g_i}}(P) = \bigcap_{i=1}^h \mathfrak{p}_i$ the prime decomposition of the radical ideal $\mathcal{I}_{T,\leq\overline{g_i}}(P)$. Show that $J := \mathcal{I}_{F[G]}(\mathfrak{Sol}_E(P')) \cap R \subseteq \mathfrak{p}_i$ for all $1 \leq i \leq h$, perhaps after substituting P by a descendent. Assume on the contrary that $J \not\subseteq \mathfrak{p}_i$ for an $1 \leq i \leq h$. By the Nullstellensatz, there exists an $e \in \mathfrak{Sol}_E(\mathfrak{p}_i) \setminus \mathfrak{Sol}_E(J)$, as both ideals are radical. As $\mathfrak{Sol}_E((P_T)_{\leq\overline{g_i}}) \cap \mathfrak{Sol}_E(\mathfrak{p}_i)$ is dense in $\mathfrak{Sol}_E(\mathfrak{p}_i)$ (cf. Proposition 1.62), there is even an $e \in (\mathfrak{Sol}_E((P_T)_{\leq\overline{g_i}}) \cap \mathfrak{Sol}_E(\mathfrak{p}_i)) \setminus \mathfrak{Sol}_E(J)$. By Propositon 2.53 all descendents of P will not have e as a solution after a certain number of steps. At that point, the prime component $\mathfrak{p}_i$ is removed from the decomposition or replaced by larger components. As the ring is NOETHERian, prime components can only be removed a finite number of times until all components contain J. □

Proposition 2.57. *Let $P' \subset F\{U\}^=$ be an algebraically restricted system of differential equations. Then, for every $\overline{g_i} \in G$ and $R := F[\overline{g_1}, \ldots, \overline{g_i}]$ there is an $k \in \mathbb{Z}_{>0}$ such that after k steps of the while loop of Construction 2.46*

$$\mathcal{I}_{F[G]}(\mathfrak{Sol}_E(P')) \cap R = \bigcap_{P\in L} \mathcal{I}_{T,\leq\overline{g_i}}(P) .$$

Proof. The inclusion "$\supseteq$" is clear, since the ideal $\mathcal{I}_{F[G]}(\mathfrak{Sol}_E(P')) \cap R$ contains by definition all polynomials in R that all solutions of P' fullfill as equations, and the polynomials in $\bigcap_{P\in L} \mathcal{I}_{T,\leq\overline{g_i}}(P)$ are fullfilled as equations by all solutions of P'. The inclusion "$\subseteq$" follows from Lemma 2.56. □

Inconsistent systems, and only those, lead to termination of Construction 2.46.

Corollary 2.58. *For a system $P \subset F\{U\}^=$ of differential equations with $\mathfrak{Sol}_E(P) = \emptyset$ the while loop in Construction 2.46 terminates without system, i.e., $L = \emptyset$.*

The last ingredient of the proof of Theorem 2.32 is the comprehensive THOMAS decomposition, a stronger form of a THOMAS decomposition which is also disjoint after certain projections. Let $\pi_i : \overline{F}^n \to \overline{F}^i : (a_1, \ldots, a_n) \mapsto (a_1, \ldots, a_i)$ the projections for $1 \leq i \leq n$ from Remark 2.6. Let $\{S_1, \ldots, S_k\}$ be a set of algebraic systems with disjoint solutions sets. Call $\{S_1, \ldots, S_k\}$ **comprehensive** with respect to y_l, $1 \leq l \leq n$, if

$$\pi_l(\mathfrak{Sol}(S_i)) \cap \pi_l(\mathfrak{Sol}(S_j)) \in \{\emptyset, \pi_l(\mathfrak{Sol}(S_j))\}$$

for all $1 \leq i, j \leq k$. Using the constructions from Proposition 1.34 it is theoretically easy, but computationally hard, to compute a comprehensive decomposition. Similar definitions exists for triangular chains [CGL+07].

Proof of Theorem 2.32. Start Construction 2.46 with P. Let $\overline{g}_i$ be the largest element in G such that the corresponding differential variable has order ℓ.

Without loss of generality assume that during Construction 2.46 all combined algebraic systems are comprehensive with respect to $\overline{g_i}$. To keep the language understandable, several systems having the same projection onto the lower i variables are grouped together and referred to as *one system*. This is justified, as the main interest of the theorem lies in this projection.

According to Proposition 2.57 there is a finite number k of steps of the while loop in Construction 2.46 such that

$$\mathcal{I}_{F[G]}(\mathfrak{Sol}_E(P)) \cap F[\overline{g_1}, \ldots, \overline{g_i}] = \bigcap_{P' \in L} \mathcal{I}_{T, \leq \overline{g_i}}(P') \ .$$

As $\mathcal{I}_{F[G]}(\mathfrak{Sol}_E(P)) \cap F[\overline{g_1}, \ldots, \overline{g_i}]$ is a radical ideal in a NOETHERian ring, it has a prime decomposition into finitely many prime ideals. At this number k of steps of the while loop, there are systems P' in L such that $\mathcal{I}_{T, \leq \overline{g_i}}(P')$ is the intersection of a subset of the above prime ideals. By increasing the number k of steps of the while loop, one may assume that the ideals of these systems never split in further steps of the while loop in Construction 2.46. Let P' be one of these systems.

Let P'' be the heir of P', in particular the solutions sets of P' and P'' have the same ZARISKI closure. Then Proposition 1.107 is applicable to the combined algebraic systems $(P')_i$ and $(P'')_i$ associated to P' and P'', as both systems have the same ideal, and thus their number of equations is identical by Theorem 1.94. Proposition 1.107 then states that not only the number of equations in $(P')_i$ and $(P'')_i$ is identical, but also their leaders and degrees. Inductively, the successors of P' share the same ideal $\mathcal{I}_{T, \leq \overline{g_i}}(P')$ associated to the T-list up to $\overline{g_i}$.

So all successors P''' of P' share the same set of equations in their combined algebraic systems $(P''')_i$, but possibly have more inequations. Thus, the system

$$\bigcup_{P''' \text{ successor of } P'} (P''')_i$$

is an algebraic σ-system.

This results in a finite set of algebraic σ-systems having truncated solutions that are dense in the truncated solutions of P. The complement of this dense set is described by a countable set of algebraically restricted systems of differential equations. Continue with these systems inductively. The ideals of these systems are stricly lager than the previous ideals. In particular, each chain of children in the "genealogical tree" of systems has finite depth[11], since the polynomial ring $F[\overline{g_1}, \ldots, \overline{g_i}]$ is NOETHERian. Hence, the number of algebraic σ-systems remains countable.

The algebraic σ-systems resulting this process are simple by Corollary 2.49. □

2.4.4 Ideals and Inequations

This subsection explains how "tweaking" the inequations of a simple algebraic system (including changing the solution set) yields insights into ideals and algebraic counting polynomials of simple (σ-)systems. In particular, the leading coefficient of the algebraic counting polynomial is fixed under certain permutations of the indeterminates. These statements about leading terms of algebraic counting polynomials prove Theorem 2.36.

The following obvious lemma is the basis for the results of this subsection.

Lemma 2.59. *Let S be a simple algebraic system in $R = F[y_1, \ldots, y_n]$ and $q \in S$ an equation or inequation with $\mathrm{ld}(q) = y_{i+1}$. If y_i does not appear in q, then S is also simple with respect to the ranking $y_1 < \ldots < y_{i-1} < y_{i+1} < y_i < y_{i+2} < \ldots < y_n$ and the algebraic counting polynomial of S is the same for both rankings.*

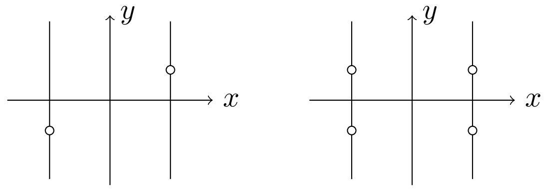
The assumptions of Lemma 2.59 are rarely satisfied. However, we demonstrate that removing a certain subset of lower dimension from the set of solutions assures these assumptions if the system S has an equation with leader y_i.

Example 2.60. Let $R = \mathbb{Q}[x, y]$ with $x < y$ and $S = \{p := x^2 - 1 = 0, q(x, y) := 2y - x \neq 0\}$. Let ξ_1 and ξ_2 be the two zeros of p. Consider

$$q(\xi_1, y) \cdot q(\xi_2, y) = 4y^2 - 2(\xi_1 + \xi_2)y + \xi_1\xi_2 \; .$$

Here, replacing the elementary symmetric polynomials in the ξ_i by the coefficients of p yields $4y^2 - 1$. The system $S' := \{p = 0, 4y^2 - 1 \neq 0\}$ is still simple and apart from a set of lower dimension has the same solution set as S (cf. Figure 2.4). Furthermore, S' is also simple for the ranking $y < x$ by Lemma 2.59. The algebraic counting polynomials for the systems are $c(S) = 2\infty - 2$ and $c(S') = 2\infty - 4$. ◁

Figure 2.4: The solutions of S in Example 2.60 on the left and of S' on the right.



A generalisation of this example is the following lemma.

Lemma 2.61. *Let S be a simple algebraic system in $R = F[y_1, \ldots, y_n]$, $p_= \in S^=$ an equation, and $q_{\neq} \in S^{\neq}$ an inequation with $\mathrm{ld}(p) = x < \mathrm{ld}(q) = z$. There is an inequation q' of degree $\deg_z(q') = \deg_z(q) \cdot \deg_x(p)$ with x not actually appearing in q' such that $S' := (S \cup \{q'_{\neq}\}) \setminus \{q_{\neq}\}$ is still simple. In particular, $\mathcal{I}(S') = \mathcal{I}(S)$.*

[11] However, this tree has countably infinite breadth, in general.

Proof. Let $d := \deg_x(p)$. Take $q'' := \prod_{k=1}^{d} q_{|x=\xi_k}$ for indeterminates ξ_k. Replacing the l-th symmtric polynomial $e_l(\xi_1,\ldots,\xi_d)$ of degree l in q'' by the coefficient of x^{d-l} in $p_=$ (seen as polynomial in x) leads to a polynomial q' with the claimed properties. □

Lemma 2.62. *Let S be a simple algebraic system in $R = F[y_1,\ldots,y_n]$. Let $X := \mathrm{ld}(S^=)$ and $Y := \{y_1,\ldots,y_n\} \setminus X$. Let c be the algebraic counting polynomial with respect to the ranking $y_1 < \ldots < y_n$. Let c' be the algebraic counting polynomial with respect to the ranking $Y < X$ such that the variables within X and Y are ordered by the previous ranking. Then the leading coefficients of $c(\mathfrak{Sol}(S))$ and $c'(\mathfrak{Sol}(S))$ coincide.*

Proof. Use Lemma 2.61 to replace each inequation with an inequation not involving leaders of lower ranking equations. This changes the degree of inequations, but does not change the leading coefficient of the algebraic counting polynomial. Now, use Lemma 2.59 to change the ranking such that all inequations have lower leaders than all equations. The system remains simple with the same algebraic counting polynomial. □

Lemma 2.63. *Let $S \subset \overline{F}[y_1,\ldots,y_n]$ be a simple algebraic σ-system. Then, both algebraic counting polynomials $c(\mathfrak{Sol}(S))$ of $\mathfrak{Sol}(S)$ and $c(\overline{\mathfrak{Sol}(S)})$ of the* Zariski *closure $\overline{\mathfrak{Sol}(S)}$ of $\mathfrak{Sol}(S)$ in $\overline{F}^n$ have the same degree and the same leading coefficient when considered as polynomial in the indeterminate ∞.*

Proof. The claim about the degree follows directly from Proposition 2.23, which equates the dimension with the degree of the algebraic counting polynomial. Show the claim about the leading coefficient by induction on the number n of indeterminates. For shorter notation write $T := \mathfrak{Sol}(S)$ and $\overline{T}$ for its Zariski closure.

The claim is clear for $n = 1$. If $|T|$ is finite, then $T = \overline{T}$ and $c(T) = |T| = c(\overline{T})$. Otherwise, $c(\overline{T}) = \infty$ and $c(T) \in \{\infty - \aleph_0 + a, \infty - b \mid a \in \mathbb{Z}, b \in \mathbb{Z}_{\geq 0}\}$.

Assume that the claim is shown for $n-1$. By Lemma 2.62 assume without loss of generality that $(S_{y_n})_=$ is an equation. (Lemma 2.62 does not apply when $\overline{T} = \overline{F}^n$; however, this case is trivial.) Let $\pi_{n-1} : \overline{F}^n \to \overline{F}^{n-1}$ be the projection associated to the ranking (cf. Remark 2.6). Then, $\pi_{n-1}(T) \subseteq \pi_{n-1}(\overline{T}) \subseteq \overline{\pi_{n-1}(T)}$, where $\overline{\pi_{n-1}(T)}$ is the Zariski closure of both $\pi_{n-1}(T)$ and $\pi_{n-1}(\overline{T})$. Let a be the leading coefficient of $c(\pi_{n-1}(T))$. By the induction hypothesis, a is also the leading coefficient of $c(\pi_{n-1}(\overline{T}))$ and $c(\overline{\pi_{n-1}(T)})$.

By Definition 2.19.(4), the leading coefficient of $c(T)$ is $a \cdot \deg_{y_n}(S_{y_n})$. Show that this is also the leading coefficient of $c(\overline{T})$. Therefore, assume without loss of generality that S is a system, i.e., a finite set, by removing inequations from S such that it remains simple, which does not change the degree and leading coefficient of the algebraic counting polynomial. Under this assumption the claim is clear, as a dense open set of $\overline{T}$ is a $\deg_{y_n}(S_{y_n})$-cover of a dense open set of $\pi_{n-1}(\overline{T})$. (The exceptional sets are of lower dimension and so their algebraic counting polynomial has a lower degree by Proposition 2.23.) □

Proof of Theorem 2.36. By Lemma 2.63 assume without loss of generality that the set of solutions $\mathfrak{Sol}_E(I)_{\leq \ell}$ up to order ℓ is constructible (and not just describable). Now, the claim follows directly from the definition of the differential dimension function $\Omega_I : \ell \mapsto \dim(F\{U\}_{\leq \ell}/I_{\leq \ell})$ and that the dimension coincides with the degree of the algebraic counting polynomial (cf. Proposition 2.23). The formula for $a(\ell)$ follows from the proof of Lemma 2.63.

The claim for the differential counting polynomial follows, as the differential dimension polynomial ω_I ultimately coincides with Ω_I.

By Proposition 1.66, the solution set $\mathfrak{Sol}_E(S)$ of S has the solution set $\mathfrak{Sol}_E(I)$ of I as Kolchin closure. In particular, the truncated solutions of $\mathfrak{Sol}_E(S)_{\leq \ell}$ and $\mathfrak{Sol}_E(I)_{\leq \ell}$ have the same Zariski closure. Thus, the claim for $c(S)$ follows from Lemma 2.63. $\square$

2.5 Examples of Counting Polynomials

> "To many, mathematics is a collection of theorems. For me, mathematics is a collection of examples; a theorem is a statement about a collection of examples and the purpose of proving theorems is to classify and explain the examples…"
>
> John Conway
> in [Con81, v]

In this section we compute counting sequences and differential counting polynomials. In general, there cannot be an algorithm that decides the existence of formal power series solutions (cf. Subsection 2.5.5). Thus, we can at best hope for tricks that determine the counting sequence and the differential counting polynomial for many classes of examples. This section introduces enumerable systems, for which the counting sequences can easily be defined and read off, and decomposes the set of solutions of differential equations disjointly into enumerable systems for some important classes of differential equations.

A first class of examples consists of simple differential systems that do not involve inequations. This is a vast class of examples, which includes systems of linear differential equations and most systems of semilinear differential equations "from nature". The second class consists of first order ordinary differential equations of main degree one.

Up to that point, all examples are treated using non-centered solutions; then Subsection 2.5.4 describes how to deal with variable coefficients and how to consider formal or convergent power series solutions. In this context, several examples of unexpected behavior are treated, including examples which show that countable infinite "exceptional sets" appear.

Let F be a differential field of characteristic zero such that its field of constants is not countable, $\overline{F}$ its algebraic closure, $<$ an orderly ranking, $\Delta = \{\partial_1, \ldots, \partial_n\}$ a non-empty set of derivation operators, and $U = \{u^{(1)}, \ldots, u^{(m)}\}$ a non-empty set of differential indeterminates.

2.5.1 Enumerable systems

This subsection introduces enumerable systems, a special form of algebraically restricted systems of differential equations that allows to read off the counting sequence, as these systems are simple and make all algebraic and differential constraints obvious.

Recall from Definition 2.39 the definition of the allocation map β and the corresponding i-th combined algebraic σ-system P_i associated to an algebraically restricted σ-systems of differential equations P by β. Stripped of the technicalities, β assigns an equation or a set of inequations to each variable in the polynomial ring $F[G]$ of indetermined power series coefficients. Combining the equations and inequations assigned to the lowest ranking i variable yields P_i.

Definition 2.64. Let P be algebraically restricted σ-systems of differential equations together with an allocation map β. Call P an **enumerable system**[12] if

(1) (**simplicity**) all combined algebraic systems P_i associated to P by β are simple,

(2) (**algebraic constraints**) $P^{a,=} \uplus P^{a,\neq} \subseteq P_T$, and

[12] strictly speaking, enumerable systems are not systems, but σ-systems.

(3) (**differential constraints/passivity**) $\mathsf{Reduce}(P, p) = 0$ for all $p \in \rho(\langle P^{\partial,=}\rangle_\Delta)$, where ρ is the forgetful map that turns a differential equation into an algebraic equation (cf. Subsection 2.3.1).

The following proposition and theorem state that an enumerable system is well-suited for describing its set of solutions.

Proposition 2.65. *Let P be an enumerable system with allocation map β and P_i the combined algebraic systems associated to P by β for all $i \in \mathbb{Z}_{\geq 1}$. Then,*

$$\mathfrak{Sol}_E(P) = \bigcap_{i=1}^{\infty} \mathfrak{Sol}_E(P_i) \ .$$

Before giving the proof, we present a theorem that is a direct corollary of this proposition.

Theorem 2.66. *Let P be an enumerable system with allocation map β and P_i the combined algebraic systems associated to P by β. Let $i_\ell \in \mathbb{Z}_{\geq 0}$ such that g_{i_ℓ} is the highest ranking variable in G of order ℓ for each $\ell \in \mathbb{Z}_{\geq 0}$. Then,*

$$\mathfrak{Sol}_E(P)_{\leq \ell} = \mathfrak{Sol}_E(P_{i_\ell})_{\leq \ell} \ .$$

In particular, the counting sequence $c(P)$ of P is given by

$$c(P) : \mathbb{Z}_{\geq 0} \to \mathbb{Z}[\infty, \aleph_0] : \ell \mapsto c(P_{i_\ell}) \ ,$$

where the algebraic counting polynomials $c(P_{i_\ell})$ can be defined by Lemma 2.24, as the P_{i_ℓ} are simple algebraic σ-systems in $F[\overline{g_1}, \ldots, \overline{g_{i_\ell}}]$.

This theorem describes the counting sequence for a single enumerable system. In general, a system of differential equations or an algebraically restricted system of differential equations needs to be decomposed into enumerable systems.

Proof of Proposition 2.65. Let $e \in \mathfrak{Sol}_E(P)$. Show that $e \in \mathfrak{Sol}_E(P_i)$ for all $i \in \mathbb{Z}_{\geq 1}$ by induction on i. For $i = 1$ the claim is clear. So assume that $e \in \mathfrak{Sol}(P_{i-1})$. If $(P_i)_{g_i}$ is empty or comes from an element in P^a, then there is nothing to show. So let $(P_i)_{g_i} = \mathsf{StrongReduce}(P_{i-1}, \mathsf{Reduce}(P_{i-1}, \rho(p)))$ for a derivative p of an element in $P^{\partial,=}$. Then, $\phi_e(\rho((P_i)_{g_i})) = 0$ if and only if $\phi_e((P_i)_{g_i}) = 0$ for all $e \in E$, as $\phi_e = \phi_e \circ \rho$ follows directly from the definitions. The algorithms StrongReduce and Reduce do not change the set of solutions. The claim follows by induction.

Let $e \in \mathfrak{Sol}_E(P_i)$ for all i. It is clear that $e \in \mathfrak{Sol}_E(P^a)$ from the condition of algebraic constraints in the definition of enumerable systems. Use the passivity of enumerable systems for proving that $e \in \mathfrak{Sol}_E(P^{\partial,=})$: Let $p \in \langle P^{\partial,=}\rangle_\Delta$. As $\mathsf{Reduce}(P_i, p) = 0$ for some i there are $q_1, \ldots, q_k, q \in F[G]$ and $p_1, \ldots, p_k \in P_i^=$ such that $q\rho(p) - \sum_{j=1}^{k} q_j p_j = 0$. Now $\phi_e(p_j) = 0$ for all j and $\phi_e(q) \neq 0$ imply $\phi_e(p) = 0$. □

The following example demonstrates that enumerable systems can be useful to determine the counting sequence.

Example 2.67. Consider the differential equation $p := u_{2,0}^2 + u_{0,2} + u_{0,1} + u_{1,0}$ over the differential field $F = \mathbb{C}$ for $U = \{u\}$ and $\Delta = \{\partial_x, \partial_y\}$ with respect to the degree reverse lexicographical ranking. As seen in Example 1.1, Maple [map] suggests

$$L_1 := \left\{ f_1(x) + f_2(y) \middle| \left(\partial_x^2 f_1(x)\right)^2 = b_1 - \partial_x f_1(x), \partial_y^2 f_2(y) = -b_1 - \partial_y f_2(y), b_1 \in \mathbb{C} \right\}$$

as the solution set of $S := \{p = 0\}$, or, with the help of the THOMAS decomposition,

$$\begin{aligned} L_2 :=& \Big\{ -\frac{1}{12}x^3 + \frac{1}{2}b_1x^2 + (b_2 - b_1^2)x - b_2y + b_3 - b_4e^{-y} + b_5 \Big| b_1, b_2, b_3, b_4, b_5 \in \mathbb{C} \Big\} \\ & \uplus \Big\{ b_1(x + y + 1) - b_2e^{-y} + b_3(x - y) + b_4 \Big| b_1, b_2, b_3, b_4 \in \mathbb{C} \Big\} . \end{aligned}$$

The question remains whether any of these two sets of solutions is complete. This question can be decided by comparing the counting sequence of the system $S = \{p = 0\}$ with the counting sequences of the sets L_1 and L_2.

To compute the counting sequence of $S = \{p = 0\}$, split this system into the two systems $S_1 := \{p = 0, q := g_{0,2} + g_{1,0} + g_{0,1} \neq 0\}$ and $S_2 := \{p = 0, q = 0\}$. The system S_1 is enumerable with the pre-allocation map $\overline{\beta_1}$ mapping $g_{i+2,j}$ to $\{(\partial_x^i \partial_y^j p)_=\}$ for $i, j \in \mathbb{Z}_{\geq 0}$, $g_{0,2}$ to $\{q_{\neq}\}$, and to the empty set otherwise. In system S_2 the power series coefficient equation $q = 0$ is equivalent to $g_{2,0} = 0$. Using $g_{2,0} = 0$ instead of $q = 0$, S_2 is enumerable by the pre-allocation map $\overline{\beta_2}$, which maps $g_{i,j+2}$ to $\{(\partial_x^i \partial_y^j p)_=\}$ for $i, j \in \mathbb{Z}_{\geq 0}$, $g_{2,0}$ to $\{(g_{2,0})_=\}$, and to the empty set otherwise. Here, the leader of $\rho(\partial_x^i \partial_y^j p) = 2g_{2,0}g_{i+2,j} + g_{i,j+2} + lot$, where lot stand for term of order at most $i+j+1$, is $g_{i,j+2}$, since $2g_{2,0}g_{i+2,j}$ vanishes due to the equation $(g_{2,0})_=$ for all $(i, j) \in \mathbb{Z}^2_{\geq 0} \setminus \{(0, 0)\}$. Thus, the counting sequences of these systems are:

$$c(S_1)(\ell) = \begin{cases} 0 \mapsto \infty, \\ 1 \mapsto \infty^3, \\ \ell \mapsto 2\infty^{2\ell}(\infty - 1), \quad \ell \geq 2 \end{cases}$$

$$c(S_2)(\ell) = \begin{cases} 0 \mapsto \infty, \\ 1 \mapsto \infty^3, \\ \ell \mapsto \infty^{2\ell}, \quad \ell \geq 2 . \end{cases}$$

As the systems $(S_1)_{\leq 1}$ and $(S_2)_{\leq 1}$ have equal solution sets, and all algebraic simple system up to order $\ell \geq 2$ associated to these two systems are disjoint, the counting sequence of S is

$$c(S)(\ell) = \begin{cases} 0 \mapsto \infty, \\ 1 \mapsto \infty^3, \\ \ell \mapsto 2\infty^{2\ell+1} - \infty^{2\ell}, \quad \ell \geq 2 . \end{cases}$$

The solution set L_1 results from an unsuccessful application of the separation of variables and describes a set of solutions of S with counting sequence $c(L_1)(\ell) = 2\infty^4$ for ℓ large enough. The counting sequence of L_2 is $c(L_2)(\ell) = \infty^5 + \infty^4$ for ℓ large enough. Both these counting sequences of solution sets are tiny in comparison of the counting sequence of S. Thus, neither L_1 nor L_2 captures the complete solution set of S. However, it is not clear how many of the missing solutions can be described by elementary functions.

Of course, also the differential dimension polynomial implies that neither L_1 nor L_2 is the complete set of solutions of S, as a THOMAS decomposition of S consists of two simple differential systems with differential dimension polynomials $2\ell + 1$ and 4. $\triangleleft$

As seen in this example, the counting sequence of disjoint enumerable systems is not additive for lower orders. To add them, one has to check whether the corresponding combined algebraic σ-systems are disjoint.

A formal description of prolonging the system is helpful for examples. The idea is to replace a differential equation $p_=$ by its derivatives Δp and the algebraic equation $\rho(p)_=$. The following lemma ensures correctness and does not require a proof.

Lemma 2.68. *Let $p_= \in F\{U\}^{\{=\}}$ be a differential equation and $e \in E$. Then, $e \in \mathfrak{Sol}_E(p_=)$ if and only if $e \in \mathfrak{Sol}_E(\Delta p_=) \cap \mathfrak{Sol}_E(\rho(p_=))$. In particular, let P be an algebraically restricted system of differential equations and $p_= \in P^{\partial,=}$. Then,*

$$\mathfrak{Sol}_E(P) = \mathfrak{Sol}_E\left((P \setminus \{p_=\}) \cup \Delta p_= \cup \{\rho(p_=)\}\right) \ .$$

Algorithm 2.69 (SingleProlongation).
Input: An algebraically restricted system of differential equations P', a differential equation $p_= \in (P')^{\partial,=}$.
Output: An algebraically restricted system of differential equations P with $\mathfrak{Sol}_E(P') = \mathfrak{Sol}_E(P)$ and $P^{\partial,=} = (P')^{\partial,=} \setminus \{p_=\} \cup \{\Delta p_=\}$.
Algorithm:

$P := P'$;
$P^{\partial,=} := P^{\partial,=} \setminus \{p_=\} \cup \{\Delta p_=\}$;
$P^{a,=} := P^{a,=} \cup \{\rho(p_=)\}$;
return P;

All differential equations in an algebraically restricted system of differential equations can be prolonged collectively. Let P' be an algebraically restricted system of differential equations and $\ell \in \mathbb{Z}_{\geq 0}$. Call an algebraically restricted system of differential equations P with $\mathfrak{Sol}_E(P') = \mathfrak{Sol}_E(P)$ and $P^{\partial,=} \cap F\{U\}_{\leq \ell} = \emptyset$ a **prolongation** of P' up to order ℓ.

Algorithm 2.70 (Prolongation).
Input: An algebraically restricted system of differential equations P', a non-negative integer $\ell \in \mathbb{Z}_{\geq 0}$
Output: A prolongation P of P' up to order ℓ.
Algorithm:

$P := P'$;
while $P^{\partial,=} \cap F\{U\}_{\leq \ell} \neq \emptyset$ **do**
    Let $p_= \in P^{\partial,=} \cap F\{U\}_{\leq \ell}$;
    $P :=$ SingleProlongation$(P, p_=)$;
end while
return P;

2.5.2 Simple Systems without Inequations

Many important classes of systems of differential equations yield a decomposition into one simple differential system without inequation. These systems allow to compute the counting sequence and even the differential counting polynomial using the simple algebraic systems up to certain orders. The following lemma describes how to use the Janet cone decomposition to construct an allocation map, which makes such systems enumerable.

Lemma 2.71. *Let $P = P^{\partial,=} = \{p_1, \ldots, p_s\}$ be a simple differential system in $F\{U\}$ without inequations. Then, with a suitable allocation map, P is an enumerable system.*

Proof. First define the pre-allocation map $\overline{\beta}$. If $\overline{g_i} \in G$ is contained in the cone $\{\mathrm{ld}(p_j)\}_{\Delta(p_j,P)}$ for some $1 \leq j \leq s$, then $\overline{g_i} = \rho(\delta\, \mathrm{ld}(p_j))$ for some δ in the free commutative monoid $\mathrm{Mon}(\Delta_P(p_j))$ generated by the reductive derivations $\Delta_P(p_j)$ from the Janet cone decomposition. In this case define $\overline{\beta}(\overline{g_i}) := \delta p_j$. Otherwise, define $\overline{\beta}(\overline{g_i}) := \emptyset$. Denote by β the allocation map corresponding to $\overline{\beta}$.

Let $i \in \mathbb{Z}_{\geq 0}$. As usual, denote by P_i the combined algebraic systems associated to P by β and denote by $P_{\leq \overline{u_i}}$ the simple algebraic system up to $\overline{u_i}$ associated to S, where $\overline{u_i}$ is the i-th smallest differential variable with respect to the ranking $<$ in $\{U\}_\Delta$. Now, $P_i = \rho(P_{\leq \overline{u_i}})$. This follows directly from the construction of both sides, as the image of $\overline{\beta}$ intersected with $F[\overline{g_1}, \ldots, \overline{g_i}]$ equals P_i. As the $P_{\leq \overline{u_i}}$ are all simple (cf. Lemma 1.46), the simplicity condition (1) from Definition 2.64 is fulfilled.

The condition (2) of algebraic constraints from Definition 2.64 is trivially fulfilled, as $P^a = \emptyset$. The condition (3) of passivity from Definition 2.64 is fulfilled, as P is differentially passive. Refrain from spelling out the details, and refer to Lemma 1.47 or Proposition 2.65 for a similar proof. □

This lemma implies a closed formula for the differential counting polynomial of simple differential systems without inequations.

Theorem 2.72. *Let $P = P^{\partial,=} = \{p_1, \ldots, p_s\}$ be a simple differential system in $F\{U\}$ without inequations. Then, its counting sequence is*

$$c(P) = l \mapsto \prod_{\substack{1 \leq i \leq s \\ \operatorname{ord}(p_i) \leq \ell}} \operatorname{mdeg}(p_i) \cdot \infty^{\Omega_{\mathcal{I}(P)}(\ell)} ,$$

where $\Omega_{\mathcal{I}(P)}$ is the differential dimension function, and its differential counting polynomial is

$$\prod_{1 \leq i \leq s} \operatorname{mdeg}(p_i) \cdot \infty^{\omega_{\mathcal{I}(S)}(\ell)} ,$$

where $\omega_{\mathcal{I}(P)}$ is the differential dimension polynomial (cf. Theorem 1.74).

Proof. Lemma 2.71 implies that P is an enumerable system. The claim follows by spelling out Theorem 2.66 using the same combinatorial means as in Subsection 1.6.4. □

The following examples of systems of differential equations yield a THOMAS decomposition into simple differential systems (usually only a single one) without inequations. This is trivially the case for systems of linear differential equations. Another of these examples are **semilinear** systems $P = P^{\partial,=} \subset F\{U\}^{\{=\}}$ of differential equations, i.e., systems where all equations have an initial in F and are of main degree one. Even though pseudo reduction does not respect semilinearity, many examples of semilinear systems of differential equations stay semilinear during a THOMAS decomposition.

Example 2.73. The RICATTI equation $u_t - a(t)u^2 - b(t)u - c(t)$ is a semilinear first order differential equation. By Theorem 2.72 it has differential counting polynomial ∞. ◁

Example 2.74. Let $F = \mathbb{C}(x,t)$, $\Delta = \{\partial_t, \partial_x\}$, and $U = \{u\}$. The viscous (cf. Example 1.6) BURGERS' equation $u_{xx} - u_t - uu_x = 0$ has differential counting polynomial $\infty^{2\ell+1}$ by Theorem 2.72. ◁

Example 2.75. Consider the inviscid BURGERS' equation $p := u_t + uu_x$. For an orderly ranking with $u_t > u_x$ the equation is semilinear and by Theorem 2.72 the counting polynomial is $\infty^{\ell+1}$.

For a ranking with $u_x > u_t$ the differential counting polynomial is the same with a more involved proof. Look for a power series solution $\sum_{i,j=0}^{\infty} a_{i,j} \frac{t^i x^j}{i! j!}$. The system

$\{p = 0\}$ splits into $S_1 := \{p = 0, a_{0,0} \neq 0\}$ and $S_2 := \{p = 0, a_{0,0} = 0\}$. The first system S_1 has counting polynomial $(\infty - 1)\infty^\ell$. For the second system the leading term of $\rho(p) = a_{0,0}a_{0,1} + a_{1,0}$ is $a_{1,0}$ after applying the relation $a_{0,0} = 0$. Similarly, using the same relation, the leading term of $\rho(\partial_t^i \partial_x^j p)$ is $a_{i+1,j}$. Thus, there is a linear relation for all derivatives of u_t and the relation $a_{0,0}$. This yields differential counting polynomial ∞^ℓ for this system. The counting polynomials of these two systems add up to $\infty^{\ell+1}$.

One might expect a shock wave appearing for the second ranking. However, the approach presented here looks at germs of analytic solutions and cannot prescribe initial values at a point where the shock wave forms. Thus, it cannot capture shock waves. ◁

Example 2.76. Let $F = \mathbb{C}$, $\Delta = \{\partial_x, \partial_y, \partial_z, \partial_t\}$, $U = \{u, v, w, p\}$, and fix the degree-reverse lexicographical ranking. The system S of the incompressible Navier-Stokes equations is given by the following equations (cf. also Example 1.92).

$$\begin{aligned} u_t + u \cdot u_x + v \cdot u_y + w \cdot u_z + p_x - \big(\underline{u_{xx}} + u_{yy} + u_{zz}\big) &= 0, \\ v_t + u \cdot v_x + v \cdot v_y + w \cdot v_z + p_y - \big(\underline{v_{xx}} + v_{yy} + v_{zz}\big) &= 0, \\ w_t + u \cdot w_x + v \cdot w_y + w \cdot w_z + p_z - \big(\underline{w_{xx}} + w_{yy} + w_{zz}\big) &= 0, \\ \underline{u_x} + v_y + w_z &= 0 \end{aligned}$$

A differential Thomas decomposition for S is given by the one system where the Poisson pressure equation is added to S, i.e.

$$S \ \cup \ \left\{ \ 2 \cdot u_y \cdot v_x + 2 \cdot u_z \cdot w_x + 2 \cdot v_z \cdot w_y + u_x^2 + v_y^2 + w_z^2 + \underline{p_{xx}} + p_{yy} + p_{zz} = 0 \ \right\} \ .$$

In particular, the Thomas decomposition of S does not contain any inequation. The differential dimension function $\Omega_{\mathcal{I}(S)}$ is equal to the polynomial function $\omega_{\mathcal{I}(S)}(\ell) = \ell^3 + \frac{11}{2}\ell^2 + \frac{17}{2}\ell + 4$. By Theorem 2.72, the differential counting polynomial of the incompressible Navier-Stokes equations is

$$\overline{c}(S) = \infty^{\ell^3 + \frac{11}{2}\ell^2 + \frac{17}{2}\ell + 4} \ . \qquad ◁$$

Example 2.77. Chemical reactions are often described by the differential equations derived from the law of mass action. By this law, the rate of every (elementary) reaction is in proportion to the product of the concentrations of the reactants. For each system of reactions, this translates into a system of semilinear ordinary differential equations. These systems are modeled by a differential indeterminate for each chemical molecule involved and the differential equations are in bijection to the differential variables of order one (via the leader map ld). Thus, these systems are simple and Theorem 2.72 implies that their differential counting polynomial is ∞^m, where m is the number of molecules.

However, several of these differential equations additionally assume some fixed initial values, usually that certain concentrations are initially zero. These assumptions can be modeled as power series coefficient equations, which preserve countability of the system. Of course, this decreases the differential counting polynomial to ∞^{m-i} if i initial values are fixed.

For example, for the Michaelis-Menten kinetics

$$\frac{ds}{dt} = -k_1 es + k_{-1}c, \qquad \frac{de}{dt} = -k_1 es + (k_{-1} + k_2)c,$$
$$\frac{dc}{dt} = k_1 es - (k_{-1} + k_2)c, \qquad \frac{dp}{dt} = k_2 c$$

with unknown functions s, e, c, p and rate constants k_1, k_{-1}, k_2 one additionally assumes $c(0) = 0$ and $p(0) = 0$ [Mur02, §6.1]. Thus, the differential counting polynomial is $\infty^{4-2} = \infty^2$. Using a stoichiometric conservation law and that the last equation is uncoupled from the previous ones, the equations can be rewritten to

$$\frac{ds}{dt} = -k_1 e_0 s + (k_1 s + k_{-1})c, \qquad \frac{dc}{dt} = k_1 e_0 s - (k_1 s + k_{-1} + k_2)c$$

for a constant $e_0 = e(0)$ and the additional assumption $c(0) = 0$. The differential counting polynomial ∞^2 can also be seen in this rewritten form of these equations, when the implied equation $\frac{de_0}{dt} = 0$ is added to the system. ◁

Example 2.78. The ordinary simple differential system $\{u_t^2 - 1 = 0\}$ has counting polynomial 2∞. For any constant a_0 there are two solutions $u(t) = \pm t + a_0$. ◁

2.5.3 First Order ODEs of Main Degree 1

This subsection considers ordinary differential equations, i.e., $\Delta := \{\partial\}$, for a single differential indeterminate $U := \{u\}$.

Theorem 2.79. *Consider $\Delta := \{\partial\}$. Let $p := A(u)u_1 + B(u) \in F\{u\}$ for $A(u), B(u) \in F[u]$ with $A(u)$ not the zero polynomial. The differential counting polynomial of $P := \{p = 0\}$ is*

$$\overline{c}(P) = \infty - b + d + e\ .$$

Here $b \in \mathbb{Z}$ is the number of distinct zeros[13] *of $A(u)$, $d \in \mathbb{Z}$ is the number of distinct common zeros of $A(u)$ and $B(u)$, and $e \in \mathbb{Z}$ is the number of distinct common zeros of $A(u)$ and $B(u)$ that appear in $A(u)$ and $B(u)$ with the same multiplicity. The zeroth differential counting polynomial $c(P)(0)$ is $\infty - b + d$ and $\overline{c}(P) = c(P)(\ell)$ for all $\ell \geq 1$.*

We postpone the proof until the end of the section, and instead give an interpretation of this theorem and examples. Assume that $F = \mathbb{C}$ in the context of Theorem 2.79. Then, by Corollary 1.58, there are $\infty - b$ formal power series solutions that correspond to solutions with a zeroth coefficient that is not a zero of $A(u)$. Over $\mathbb{R}$ these solutions locally converge by the Picard-Lindelöf theorem. Let κ be a common zero of $A(u)$ and $B(u)$. Then the constant function $u(t) = \kappa$ is a solution, which can easily be seen by splitting of $u - \kappa$ from p. There are d of these solutions. The remaining e solutions can be interpreted over the fields $\mathbb{R}$ and $\mathbb{C}$. Let κ be a common root of $A(u)$ and $B(u)$ with the same multiplicity λ in both polynomials. The zeroth power series coefficient of such a solution is κ if $u - \kappa$ appears in $A(u)$ and $B(u)$ with the same multiplicity. Let $(u - \kappa)^\lambda$ be the corresponding factor of $A(u)$ and $B(u)$ and let $\overline{A}(u) := \frac{A(u)}{q(u)}$ and $\overline{B}(u) := \frac{B(u)}{q(u)}$. Let t_0 be the expansion point for the power series. Then,

$$\lim_{t\to t_0} u'(t) = \lim_{t\to t_0} \frac{B(t)}{A(t)} = \lim_{t\to t_0} \frac{\overline{B}(t)}{\overline{A}(t)}$$

is a well-defined non-zero value; it is the first power series coefficient. Hence, this power series solution is different from above d solutions, which are constant.

We look at examples of Theorem 2.79. All these examples have constant coefficients and by Corollary 1.58 the solutions can be interpreted as formal power series solutions.

[13] of course over the algebraic closure of F.

Example 2.80. Consider $uu_1 - 1$. According to Theorem 2.79, it has counting polynomial[14] $\infty - 1 + 0 + 0$. The solutions MAPLE's dsolve [map] returns are $\pm\sqrt{-2t + c_0}$, which seems to indicate $2\cdot(\infty-1)$ solutions. However, when expanding the power series $\pm\sqrt{-2t + c_0}$ around 0, it can be written as $\sqrt{c_0}\cdot q(\sqrt{c_0}^2, t)$ for a $q \in \mathbb{C}[\sqrt{c_0}^2, (\sqrt{c_0})^{-2}][[t]]$. The latter power series can be seen as power series with coefficients using a constant $\sqrt{c_0} \in \mathbb{C} \setminus \{0\}$. Similarly, using an ansatz directly from $uu_1 - 1$ to compute a formal power series solution yields the same power series.

In conclusion, c_0 seems to be the "right" parameter for giving a closed form solution, but the "wrong" parameter for a power series solution. ◁

Example 2.81. Consider $uu_1 - u$. According to Theorem 2.79, it has differential counting polynomial $\infty - 1 + 1 + 1$. Its solutions are $u(t) = 0$ and $u(t) = t + c_0$ for each $c_0 \in \mathbb{C}$. ◁

Example 2.82. Consider $u^2u_1 - u$. According to Theorem 2.79, it has differential counting polynomial $\infty - 1 + 1 + 0$. Its solutions are $u(t) = 0$ and the ones in (2.80). ◁

Example 2.83. Consider $u^2u_1 - u^2$. According to Theorem 2.79, it has differential counting polynomial $\infty - 1 + 1 + 1$. Its solutions are the same ones as in (2.81). ◁

Example 2.84. Consider $A(u) = u(u+2)(u+1) \in \mathbb{C}[u]$, $B(u) = u(u+2)(u-2) \in \mathbb{C}[u]$, and

$$p = A(u)u_1 + B(u) = u(u+2)(u+1)u_1 + u(u+2)(u-2) \in \mathbb{C}\{u\} \ .$$

By Theorem 2.79, the differential counting polynomial is $\overline{c}(\{p = 0\}) = \infty - 3 + 2 + 2 = \infty + 1$. Check this using the MAPLE command dsolve [map]; three (families of) solutions are returned:

$$\begin{aligned} u &= 0 \\ u &= -2 \\ u &= 3\,\mathrm{LambertW}\left(\frac{1}{3}c_0 \exp\left(-\frac{1}{3}t - \frac{2}{3}\right)\right) + 2 \end{aligned}$$

for a $c_0 \in \mathbb{C}$. Here LambertW denotes the "inverse" of $z \mapsto z\exp(z)$ [CGH+96]. This seems to indicate that there are $\infty+2$ solutions. However, not all $c_0 \in \mathbb{C}$ in the third family of solutions allow a power series solution at every base point. More precisely, a power series solution around $t_0 \in \mathbb{C}$ is possible if and only if $\mathrm{LambertW}\left(\frac{1}{3}c_0 \exp\left(-\frac{1}{3}t_0 - \frac{2}{3}\right)\right) \neq -1$. This holds if and only if $c_0 \neq -3\exp\left(\frac{1}{3}t_0 - \frac{1}{3}\right)$. Thus, when excluding this one solution from above $\infty + 2$ ones, there are only $\infty + 1$ left, as predicted. ◁

Proof of Theorem 2.79. Use the notation $G := \{g_i | i \in \mathbb{Z}_{\geq 0}\}$ for the indetermined power series coefficients and the forgetful map ρ, which maps u_i to g_i.

Decompose the set of solutions of the system

$$S := \{p := A(u)u_1 + B(u) = 0\}$$

[14] This example also shows that applying the inclusion-exclusion-principle to a Thomas decomposition does not allow counting. A differential Thomas decomposition of $uu_1 - 1 = 0$ yields $\{\{uu_1 - 1 = 0, u \neq 0\}\}$. By the inclusion-exclusion-principle applied to this system the set of solutions of the systems $\{uu_1 - 1 = 0\}$ need to be considered and the set of solutions of $\{uu_1 - 1 = 0, u = 0\}$ need to be removed. As $\{uu_1 - 1 = 0, u = 0\}$ has no solutions, the original problem needs to be solved.

into enumerable systems. System S splits into the two systems

$$T := \{p = A(u)u_1 + B(u) = 0, \widetilde{A}(g_0) \neq 0\}$$
$$S^{(1)} := \{p = A(u)u_1 + B(u) = 0, \widetilde{A}(g_0) = 0\}$$

where $\widetilde{A}(u)$ is the square-free part of $A(u)$. The following allocation map β_T for the system T turns it into an enumerable system.

$$\beta_T : G \to F[G]^{\{=,\neq\}}, i \mapsto \begin{cases} \widetilde{A}(g_0) \neq 0, & i = 0 \\ \rho\left(\partial^{i-1} p\right) = 0, & i \in \mathbb{Z}_{>0} \end{cases}.$$

Show that T with allocation map β_T is enumerable. First, note that β_T is its own pre-allocation map. The combined algebraic systems $T_1 = \{\widetilde{A}(g_0) \neq 0\}$ is simple, since $\widetilde{A}$ is a square-free univariate polynomial. The combined algebraic systems T_i for $i > 1$ are also simple, as they only additionally include $\rho\left(\{\partial^{i-1}p\}\right)$ as equations; these are of main degree one and the initial $\rho(A)(g_0)$ has the same zeros as the inequation $\widetilde{A}(g_0) \neq 0$, which is contained in T_i. The condition on algebraic constraints and passivity are trivial.

Now show that T has differential counting polynomial $\infty - b$. There is an equation of main degree one for all indeterminates except g_0. Furthermore, the system T has an inequation $\widetilde{A}(g_0)$ of degree b for the leader g_0. So the differential counting polynomial is $\infty - \deg(\widetilde{A}) = \infty - b$.

Rewriting system $S^{(1)}$ by prolongation up to order two yields

$$\mathsf{Prolongation}(S^{(1)}, 2) = \{ \quad \begin{aligned} \partial^2 p &= 0, \\ \widetilde{A}(g_0) &= 0, \\ B(g_0) &= 0, \\ (A'(g_0)g_1 + B'(g_0)) \cdot g_1 &= 0\} \end{aligned}$$

with $\partial^2 p = A(u)u_3 + (3A'(u)u_1 + B'(u))u_2 + A''(u)u_1^3 + B''(u)u_1^2$. Splitting this system with respect to g_1 leads to the following two systems.

$$S^{(1,1)} := \{ \quad \begin{aligned} \partial^2 p &= 0, \\ \widetilde{A}(g_0) &= 0, \\ B(g_0) &= 0, \\ g_1 &= 0\} \end{aligned}$$

$$S^{(1,2)} := \{ \quad \begin{aligned} \partial^2 p &= 0, \\ \widetilde{A}(g_0) &= 0, \\ B(g_0) &= 0, \\ A'(g_0)g_1 + B'(g_0) &= 0, \\ g_1 &\neq 0\} \end{aligned}$$

Lemma 2.86 shows that system $S^{(1,1)}$ is equivalent to the system $\{u_1 = 0, \widetilde{A}(g_0) = 0, B(g_0) = 0\}$. The latter system is again equivalent to $\{u_1 = 0, C(g_0) = 0\}$, where C is the square-free part of the gcd of A and B. This system has differential counting polynomial d, the number of distinct common zeros of $A(u)$ and $B(u)$. By Lemma 2.88

system $S^{(1,2)}$ has differential counting polynomial e. Summing up the three differential counting polynomials $\infty - b$, d, and e of the systems T, $S^{(1,1)}$, and $S^{(1,2)}$, respectively, implies the claim. □

Corollary 2.85. *In the context of Theorem 2.79, let F be a differential field of meromorphic functions over $\mathbb{C}$ and $\zeta \in \mathbb{C}$. Assume that ζ is regular (cf. Definition 1.51) with respect to $\{p = 0, A(u) \neq 0\}$. Then, the set of non-centered solutions in $\mathfrak{Sol}_E(\{p = 0\})$ that correspond to $\infty - b + d$ in the differential counting polynomial are mapped to convergent power series in $\mathfrak{Sol}_{\mathbb{C},\zeta}(\{p = 0\})$ by ψ_ζ if they do not have a pole in ζ.*

Proof. The image of $\mathfrak{Sol}_E(\{p = 0\})$ under ψ_ζ is contained in $\mathfrak{Sol}_{\mathbb{C},\zeta}(\{p = 0\})$ by Theorem 1.52. The convergence of the $\infty - b$ solutions from the system T follows from RIQUIER's Existence Theorem 1.60 applied to $\{p = 0, A(u) \neq 0\}$. The d solutions from the systems $S^{(1,1)}$ are constant. □

Prove the lemmas used in above proof of Theorem 2.79.

Lemma 2.86. *Let $p := A(u)u_1 + B(u) \in F\{U\}$ for $A(u), B(u) \in F[U]$ such that $A(u)$ is not the zero polynomial and $\widetilde{A}$ is the square-free part of A. The system $S^{(1,1)} := \{\partial^2 p = 0, \widetilde{A}(g_0) = 0, B(g_0) = 0, g_1 = 0\}$ is equivalent to the system $\{u_1 = 0, \widetilde{A}(g_0) = 0, B(g_0) = 0\}$.*

Proof. The prolongation $\mathsf{Prolongation}(S^{(1,1)}, 3)$ of $S^{(1,1)}$ includes the power series equation $B'(g_0) \cdot g_2 = 0$. This power series equation arises from $\rho(\partial^2 p)$ and the two relations $g_1 = 0$ and $\widetilde{A}(g_0) = 0$, where $\widetilde{A}(g_0) = 0$ implies $A(g_0) = 0$.

When splitting $\mathsf{Prolongation}(S^{(1,1)}, 3)$ with respect to g_2, the case of $g_2 \neq 0$ is inconsistent. This can be seen as in this case $B'(g_0)$ has to be zero. Then, another prolongation implies the power series equation $A'(g_0) = 0$ and successive further prolongations using $g_2 \neq 0$ imply the power series equations $B''(g_0) = 0$, $A''(g_0) = 0$, $B'''(g_0) = 0$ and so on. In particular, $(\partial^{(\deg(A))} A(u)) = 0$ is zero, but $(\partial^{(\deg(A))} A(u))$ is a non-zero constant. As $g_2 \neq 0$ yields a contradiction, system $S^{(1,1)}$ is equivalent to $S^{(1,1)} \cup \{g_2 = 0\}$.

In every k-th further prolongation, the power series equation $B'(g_0) \cdot g_{2+k} = 0$ appears. Setting $g_{2+k} \neq 0$ yields a similar contradiction as above. Thus, $S^{(1,1)}$ has the same set of solutions if the equations $g_i = 0$, $i \geq 2$, are added. The equation $g_1 = 0$ is already contained in $S^{(1,1)}$. The equations $g_i = 0$, $i \geq 1$, together are equivalent to $u_1 = 0$. Thus, $u_1 = 0$ can be added to $S^{(1,1)}$, which makes $\partial^2 p = 0$ and $g_1 = 0$ superfluous. □

The following formula is a generalization of the chain rule for the derivative.

Lemma 2.87 (FAÀ DI BRUNO's Formula, [Por01, §4.3])**.**

$$\frac{d^k}{dx^k} f(g(x)) = \sum_{\substack{(h_1,\ldots,h_k) \in \mathbb{Z}_{\geq 0}^k \\ 1 \cdot h_1 + \ldots + k \cdot h_k = k}} \frac{k!}{h_1!\, h_2! \, \ldots \, h_k!} \cdot f^{(h_1 + \ldots + h_k)}(g(x)) \cdot \prod_{j=1}^{k} \left(\frac{g^{(j)}(x)}{j!} \right)^{h_j}$$

Lemma 2.88. *Let $p := A(u)u_1 + B(u) \in F\{U\}$ for $A(u), B(u) \in F[U]$ such that $A(u)$ is not the zero polynomial and $\widetilde{A}$ the square-free part of A. The system $S^{(1,2)} := \{\partial^2 p = 0, \widetilde{A}(g_0) = 0, B(g_0) = 0, A'(g_0)g_1 + B'(g_0) = 0, g_1 \neq 0\}$ has differential counting polynomial $e \in \mathbb{Z}$, where e is the number of distinct common zeros of $A(u)$ and $B(u)$ that appear in $A(u)$ and $B(u)$ with the same multiplicity.*

Proof. Recognize $S^{(1,2)}$ as S^1 in the following family

$$S^k := \{ \quad \begin{aligned} \partial^{k+1}p &= 0, \\ \widetilde{A}(g_0) &= 0, \\ A^{(1)}(g_0) = \ldots = A^{(k-1)}(g_0) &= 0, \\ B^{(0)}(g_0) = \ldots = B^{(k-1)}(g_0) &= 0, \\ A^{(k)}(g_0)g_1 + B^{(k)}(g_0) &= 0, \\ g_1 &\neq 0\} \end{aligned}$$

of systems. Here,

$$\partial^{k+1}p = \sum_{i=0}^{k+1} \binom{k+1}{i} u_{k-i+2} \sum_{\substack{(h_1,\ldots,h_i)\in\mathbb{Z}^i_{\geq 0} \\ 1\cdot h_1+\ldots+i\cdot h_i=i}} \frac{i!}{h_1!\,h_2!\,\ldots\,h_i!} A^{(h_1+\ldots+h_i)}(u_0)\cdot\prod_{j=1}^{i}\left(\frac{u_j}{j!}\right)^{h_j}$$
$$+ \sum_{\substack{(h_1,\ldots,h_{k+1})\in\mathbb{Z}^{k+1}_{\geq 0} \\ 1\cdot h_1+\ldots+(k+1)\cdot h_{k+1}=k+1}} \frac{(k+1)!}{h_1!\,h_2!\,\ldots\,h_{k+1}!} B^{(h_1+\ldots+h_{k+1})}(u_0)\cdot\prod_{j=1}^{k+1}\left(\frac{u_j}{j!}\right)^{h_j}$$

by Faà Di Bruno's Formula (cf. Lemma 2.87). As $A^{(1)}(g_0) = \ldots = A^{(k-1)}(g_0) = B^{(0)}(g_0) = \ldots = B^{(k-1)}(g_0) = 0$ in S^k simply write

$$\begin{aligned} \partial^{k+1}p &= hot(u_{k+2},\ldots,u_0) \\ &\quad + \left(\left(\binom{k+1}{1} + \binom{k+1}{2}\right) A^{(k)}(u)u_1 + \binom{k+1}{2} B^{(k)}(u)\right) u_1^{k-1}u_2 \\ &\quad + lot(u_1,u) \\ &= hot(u_{k+2},\ldots,u_0) \\ &\quad + \left(\binom{k+2}{2} A^{(k)}(u)u_1 + \binom{k+1}{2} B^{(k)}(u)\right) u_1^{k-1}u_2 \\ &\quad + lot(u_1,u)\ , \end{aligned}$$

where $hot(u_{k+2},\ldots,u) \in F[u_{k+2},\ldots,u]$ represents terms vanishing after first applying the forgetful map ρ and afterwards reduction by the power series equations in S^k, and $lot(u_1,u) \in F[u_1,u_0]$ represents lower order terms, which only involve the differential variables u_1 and u_0. For $k = \min(\deg(A(u)),\deg(B(u))) + 1$ the system S^k is inconsistent, because at least one of the equations $A^{(k-1)}(g_0) = 0$ or $B^{(k-1)}(g_0) = 0$ has a constant, non-zero left hand side. Hence, for the remainder of this proof we assume $k \leq \min(\deg(A(u)),\deg(B(u)))$.

The initial of $\rho(\partial^{k+1}p)$ is $((\binom{k+2}{2}A^{(k)}(g_0)g_1 + (\binom{k+1}{2}B^{(k)}(g_0))g_1^{k-1}$ after reduction, and it is non-zero if and only if $B^{(k)}(g_0)$ is non-zero, because of the power series equation $A^{(k)}(g_0)g_1+B^{(k)}(g_0) = 0$. So split S^k into two systems with respect to whether $B^{(k)}(g_0)$ is zero or non-zero.

In the first system add the equation $B^{(k)}(g_0) = 0$ to S^k. Then the equation $A^{(k)}(g_0)g_1 + B^{(k)}(g_0) = 0$ and the inequation $g_1 \neq 0$ imply $A^{(k)}(g_0) = 0$. Using these new equations one easily sees that $\rho(\partial^{k+1}p)$ reduces to zero and, thus, $\partial^{k+1}p$ can be replaced by $\partial^{k+2}p$. This yields the system S^{k+1}.

Consider the second system into which the inequation $B^{(k)}(g_0) \neq 0$ is added. This inequation ensures that the initial $\left(\binom{k+2}{2}A^{(k)}(u)u_1 + \binom{k+1}{2}B^{(k)}(u)\right)u_1^{k-1}$ of the reduced form of $\rho(\partial^{k+1}p)$ is non-zero. The equation $A^{(k)}(g_0)g_1+B^{(k)}(g_0)=0$ implies $A^{(k)}(g_0)\neq 0$ from $B^{(k)}(g_0)\neq 0$.

Claim that the resulting system

$$T^k := \{ \quad \begin{aligned} \partial^{k+1}p &= 0,\\ \widetilde{A}(g_0) = A^{(1)}(g_0) = \ldots = A^{(k-1)}(g_0) &= 0,\\ B^{(0)}(g_0) = \ldots = B^{(k-1)}(g_0) &= 0,\\ A^{(k)}(g_0)g_1 + B^{(k)}(g_0) &= 0,\\ A^{(k)}(g_0) &\neq 0,\\ B^{(k)}(g_0) &\neq 0,\\ g_1 &\neq 0 \end{aligned} \quad \}$$

can be transformed into an enumerable one by a suitable allocation map and algebraic transformations for the univariate polynomials in g_0. Therefore, show that not only the coefficient of g_2 in $\rho(\partial^{k+1}p)$ does not vanish but also the coefficient of g_ℓ in $\rho(\partial^{k+\ell-1}p)$ for all $\ell > 2$. In

$$\begin{aligned} &\rho(\partial^{k+\ell-1}p)\\ &= \sum_{i=0}^{k+\ell-1}\binom{k+\ell-1}{i} g_{k+\ell-i} \sum_{\substack{(h_1,\ldots,h_i)\in\mathbb{Z}^i_{\geq 0}\\ 1\cdot h_1+\ldots+i\cdot h_i=i}} \frac{i!}{h_1!\,h_2!\,\ldots\,h_i!} A^{(h_1+\ldots+h_i)}(g_0)\cdot\prod_{j=1}^{i}\left(\frac{g_j}{j!}\right)^{h_j}\\ &+ \sum_{\substack{(h_1,\ldots,h_{k+\ell-1})\in\mathbb{Z}^{k+\ell-1}_{\geq 0}\\ 1\cdot h_1+\ldots+(k+\ell-1)\cdot h_{k+\ell-1}=k+\ell-1}} \frac{(k+\ell-1)!}{h_1!\,h_2!\,\ldots\,h_{k+\ell-1}!} B^{(h_1+\ldots+h_{k+\ell-1})}(g_0)\cdot\prod_{j=1}^{k+\ell-1}\left(\frac{g_j}{j!}\right)^{h_j} \end{aligned}$$

all terms including g_i for $i > \ell$ vanish because of $A^{(1)}(g_0) = \ldots = A^{(k-1)}(g_0) = B^{(0)}(g_0) = \ldots = B^{(k-1)}(g_0) = 0$. The coefficient of g_ℓ is

$$= \left(\left(\binom{k+\ell-1}{k} + \binom{k+\ell-1}{k-1}\right) A^{(k)}(g_0)g_1 + \binom{k+\ell-1}{\ell} B^{(k)}(g_0)\right) g_1^{k-1}$$

$$= \left(\binom{k+\ell}{\ell} A^{(k)}(g_0)g_1 + \binom{k+\ell-1}{\ell} B^{(k)}(g_0)\right) g_1^{k-1}$$

This term is non-zero, completely analogous to the coefficient of g_2.

Then the univariate polynomials in g_0 imply that there are exactly as many solutions for g_0 in T^k as the number of common zeros of $A(g_0)$ and $B(g_0)$ that appear with cardinality k in both polynomials. So the union of the sets of solutions of all T^k is the number of distinct common zeros of $A(u)$ and $B(u)$ that appear in $A(u)$ and $B(u)$ with the same multiplicity. This implies the claim for T^k. □

2.5.4 Counting of Formal and Convergent Power Series Solutions

The previous subsections considered non-centered solutions. This subsection transfers these previous results to formal and convergent power series solutions, and thus counts the set of Taylor polynomials.

To achieve this, one would formally need to adapt the proof of Theorem 2.32 to the context of formal power series solutions in Subsection 1.4.2. This proof is the same, even though certain terms vanish of the center of expansion [15]. On a dense subset of the complex n-space the infinite computation is exactly the same as the one in Theorem 2.32. In particular, for the important special case of constant coefficients, e.g., $F = \mathbb{C}$, the set of non-centered solutions is in bijection to the power series solutions (cf. Corollary 1.58). As there is nothing to prove, this subsection deals mostly with examples.

The convergence of "most" formal power series solutions is again given by Riquier's Existence Theorem 1.60.

The approach to formal power series solutions in Subsection 1.4.2 motivates the technical definitions needed for the examples. For this subsection, let $\mathbb{C}[G]$ be the polynomial ring of indetermined power series coefficients over $\mathbb{C}$, $\zeta = (\zeta_1, \ldots, \zeta_n) \in \mathbb{C}^n$ the center of expansion, F a field of meromorphic functions in n complex variables $y_1, \ldots, y_n$, and $\Delta = \{\partial_{y_1}, \ldots, \partial_{y_n}\}$.

We define power series solutions in the ring $\mathbb{C}[[y_1 - \zeta_1, \ldots, y_n - \zeta_n]]$ of power series centered around ζ for algebraically restricted systems of differential equations. As these solutions are already defined for differential equations in Subsection 1.4.2, we only need to define them for power series coefficient equations and inequations. Therefore, we extend the definition of the substitution homomorphism Φ_f of F-algebras, which evaluates differential variables at a formal power series $f \in \mathbb{C}[[y_1 - \zeta_1, \ldots, y_n - \zeta_n]]^U$ in a differentially compatible way, to also evaluate the algebraic variables in the ring $F[G]$ of indeterminate power series coefficients. However, these variables are evaluated by substituting them by one formal power series coefficient instead of an entire formal power series:

$$\Phi_f : \mathbb{C}[G] \to \mathbb{C}[[y_1 - \zeta_1, \ldots, y_n - \zeta_n]] : g^{(j)}_{\mathbf{i}} \mapsto f(u^{(j)})_{\mathbf{i}} \quad ,$$

where $f(u^{(j)})_{\mathbf{i}}$ is the coefficient of the monomial $(y_1 - \zeta_1)^{i_1} \ldots (y_n - \zeta_n)^{i_n}$ in $f(u^{(j)}) \in \mathbb{C}[[y_1 - \zeta_1, \ldots, y_n - \zeta_n]]$. A **formal power series solution around** ζ of $p_= \in \mathbb{C}[G]^=$ or $q_{\neq} \in \mathbb{C}[G]^{\neq}$ is an $f \in \mathbb{C}[[y_1 - \zeta_1, \ldots, y_n - \zeta_n]]^U$ with $\Phi_f(p) = 0$ or $\Phi_f(q) \neq 0$, respectively. Let P be an algebraically restricted σ-system of differential equations. Call such an f a formal power series solution around ζ of P if it is a solution of each element in P. Denote the set of formal power series solutions of P around ζ by $\mathfrak{Sol}_{\mathbb{C},\zeta}(P) \subseteq \mathbb{C}[[y_1 - \zeta_1, \ldots, y_n - \zeta_n]]^U$.

Counting the Taylor polynomials up to order ℓ requires the following notion of solutions. Let $\mathbb{C}[[y_1 - \zeta_1, \ldots, y_n - \zeta_n]]^U_{>\ell}$ be the $\mathbb{C}[[y_1 - \zeta_1, \ldots, y_n - \zeta_n]]$-submodule of $\mathbb{C}[[y_1 - \zeta_1, \ldots, y_n - \zeta_n]]^U$ generated by the $u^{(j)} \mapsto (y_1 - \zeta_1)^{\mathbf{i}_1} \ldots (y_n - \zeta_n)^{\mathbf{i}_n}$ for $\mathbf{i} \in \mathbb{Z}^n_{\geq 0}$ with $|\mathbf{i}| = \ell + 1$. Call the image $\mathfrak{Sol}_{\mathbb{C},\zeta}(P)_{\leq \ell}$ of $\mathfrak{Sol}_{\mathbb{C},\zeta}(P)$ under

$$\mathbb{C}[[y_1 - \zeta_1, \ldots, y_n - \zeta_n]]^U \twoheadrightarrow \mathbb{C}[[y_1 - \zeta_1, \ldots, y_n - \zeta_n]]^U / \mathbb{C}[[y_1 - \zeta_1, \ldots, y_n - \zeta_n]]^U_{>\ell} \ ,$$

the set of **formal power series solutions of P around ζ truncated at order ℓ**.

The definition of the counting series and the differential counting polynomial of power series solutions is similar to the definition of the differential counting polynomial

[15] Formally, the Nullstellensatz used in the proof of Lemma 2.55 is no longer applicable, but substituting the center of expansion into both sides preserves the inclusion claimed in this lemma.

of non-centered solutions in Definition 2.33. We only need to replace the solution sets E, $E_{>\ell}$, $\mathfrak{Sol}_E$, and $\mathfrak{Sol}_E(\ )_{\leq\ell}$ with $\mathbb{C}[[y_1-\zeta_1,\dots,y_n-\zeta_n]]^U$, $\mathbb{C}[[y_1-\zeta_1,\dots,y_n-\zeta_n]]^U_{>\ell}$, $\mathfrak{Sol}_{\mathbb{C},\zeta}$, and $\mathfrak{Sol}_{\mathbb{C},\zeta}(\ )_{\leq\ell}$, respectively.

For the examples in this section, redefine the forgetful map ρ such that it inserts ζ into functions in F in addition to forgetting the differential structure, i.e.,

$$\rho : F\{U\} \xrightarrow{\sim} \mathbb{C}[G] : \begin{cases} u_{\mathbf{i}}^{(j)} & \mapsto g_{\mathbf{i}}^{(j)} \\ y_i & \mapsto \zeta_i \end{cases} .$$

Extend it to $\rho : F\{U\} \cup \mathbb{C}[G] \to \mathbb{C}[G]$ via $Id_{\mathbb{C}[G]}$ and to $\rho : (F\{U\} \cup \mathbb{C}[G])^{\{=,\neq\}} \to \mathbb{C}[G]^{\{=,\neq\}}$ in the obvious way. Strictly speaking, this is a partial function defined on the elements without pole in ζ, but ρ is never applied to elements with a pole in ζ.

The rest of this subsection considers six examples. Begin with the Clairaut equations. They were among the first examples[16] in which the difference between singular and regular solutions was studied [Cla36] (cf. also [Inc44, 2.45] and Appendix D).

Example 2.89. Let $F = \mathbb{C}(t)$. Consider the Clairaut equation

$$P := \{u - t \cdot u_1 - f(u_1) = 0\}$$

with $f(u_1) = \sum_{i=0}^{\deg(f)} b_i u_1 \in \mathbb{C}[u_1]$ of degree at least 2. We study power series solutions of the form $u(t) = \sum_{i=0}^{\infty} g_i \frac{(t-t_0)^i}{i!}$ centered around $t_0 \in \mathbb{C}$. Claim: The differential counting polynomial for formal power series solutions is

$$\overline{c}(P) = \deg(f) \cdot \infty$$

at a generic center of expansion. More precisely, for each zeroth Taylor coefficient there are $\deg(f)$ first Taylor coefficients which yield a unique formal (and even convergent) power series solution. At special centers of expansion, further examined below for small degrees of f, the differential counting polynomial is smaller.

A Prolongation yields the system

$$\mathsf{Prolongation}(P,2) = \left\{u_2 \cdot (t + f'(u_1)) = 0, \quad g_0 - t_0 \cdot g_1 - f(g_1) = 0\right\}.$$

Splitting $\mathsf{Prolongation}(P,2)$ with respect to u_2 because of the factorized differential equation $u_2 \cdot (t + f'(u_1)) = 0$ yields two systems. The first system

$$S_1 := \{u_2 = 0, \quad g_0 - t \cdot g_1 - f(g_1) = 0\}$$

has general solutions in the sense of Appendix D, which are lines in this case. It has differential counting polynomial $\deg(f)\cdot\infty - \deg(f) + 1$ due to the Euler characteristic (cf. Corollary 2.16). The second system

$$S_2 := \left\{t + f'(u_1) = 0, \quad u_2 \neq 0, \quad g_0 - t_0 \cdot g_1 - f(g_1) = 0\right\}$$

contains the separant of the differential equation. Hence, the solutions of S_2 are singular solutions in the sense of Appendix D. A prolongation of S_2 yields

$$\mathsf{Prolongation}(S_2,2) = \{ \begin{aligned} u_2 \cdot f''(u_1) + 1 &= 0, \\ u_2 &\neq 0, \\ t_0 + f'(g_1) &= 0, \\ g_0 - t_0 \cdot g_1 - f(g_1) &= 0\} , \end{aligned}$$

[16] The first example was probably [Inc44, Appendix A.5] due to Taylor [Tay, Prop. VIII, Prob. V].

and $\rho(u_2 \cdot f''(u_1) + 1) = g_2 \cdot f''(g_1) + 1 = 0$ implies $f''(g_1) \neq 0$. Furthermore, $g_2 \neq 0$ holds and, in particular, the differential inequation $u_2 \neq 0$ is superfluous. So $\mathsf{Prolongation}(S_2, 2)$ is equivalent to the system

$$\left\{u_2 \cdot f''(u_1) + 1 = 0, \quad t_0 + f'(g_1) = 0, \quad g_0 - t_0 \cdot g_1 - f(g_1) = 0, \quad f''(g_1) \neq 0\right\}.$$

The initial of $\rho(\partial^i(u_2 \cdot f''(u_1)+1))$, $i \geq 0$ is $f''(g_1)$ and non-zero. Thus, the differential counting polynomial of this algebraically restricted system of differential equations is the same as the algebraic counting polynomial of the system $S_{alg} := \{t_0 + f'(g_1) = 0, g_0 - t_0 \cdot g_1 - f(g_1) = 0, f''(g_1) \neq 0\}$ in the indeterminates $g_1 > g_0$.

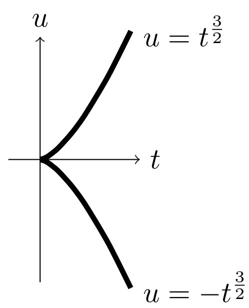
For generic values of t_0, the algebraic counting polynomial $c(S_{alg})$ is $\deg(f) - 1$. Namely, as the set of solutions is finite, the algebraic counting polynomial is independent of the ranking (cf. Proposition 2.12). For generic values of t_0, the subsystem $\{t_0 + f'(g_1) = 0, f''(g_1) \neq 0\} \subset S_{alg}$ has $\deg(f) - 1$ possible values for g_1 in a solutions. Then, the equation $g_0 - t_0 \cdot g_1 - f(g_1) = 0$ ensures that each of these solutions yields a unique value for g_0 in a solution. The behavior might be different for certain values of t_0, which depend on the coefficients b_i of f.

For $\deg(f) = 2$ a straight forward computation with the algebraic THOMAS decomposition shows that the system always has one solution. For $\deg(f) = 3$ the system has two or zero solutions. The case of zero solutions appears exactly when trying to expand the power series around the point $t_0 = \frac{b_2^2 - 3b_1b_3}{3b_3}$. This means that the singular solution does not have a formal power series centered around this particular point. For $\deg(f) = 4$ the situation is more complicated: there are either zero, one, or three solutions. First, there are zero solutions at the point $t_0 = \frac{b_3^3 - 16b_1b_4^2}{16b_4^2}$ if $8b_2b_4 - 3b_3^2 = 0$. Second, there is one solution at the two zeros of

$$\begin{aligned} 108b_4^2 \cdot t_0^2 + \left(216b_1b_4^2 - 108b_2b_3b_4 + 27b_3^3\right) \cdot t_0 \\ + 108b_1^2b_4^2 + 32b_2^3b_4 - 108b_1b_2b_3b_4 + 27b_1b_3^3 - 9b_2^2b_3^2 = 0 \end{aligned}$$

(seen as polynomial in t_0) if $8b_2b_4 - 3b_3^2 \neq 0$. In all other cases, there are three solutions.

Examples demonstrate why there are less solutions at certain points. If $f(u_1) = -\frac{4}{27}u_1^3$, then there are the two singular solutions $u(t) = \pm t^{\frac{3}{2}}$, neither of which can be expanded into a power series around their impasse singularity (or cusp) $t_0 = 0$ (cf. Proposition E.3). This can be seen in the (real) picture on the right. This special value for t_0 arises the following way. The singular solutions are determined by $\operatorname{sep}(p) = t + f'(u_1) = 3b_3u_1^2 + 2b_2u_1 + b_1 + t_0 = 0$. Trying to solve this equation for u_1 results in the discriminant $3b_3t_0 - b_2^2 + 3b_1b_3$ (of this equation w.r.t. u_1), which has aforementioned value for t_0 as solution.

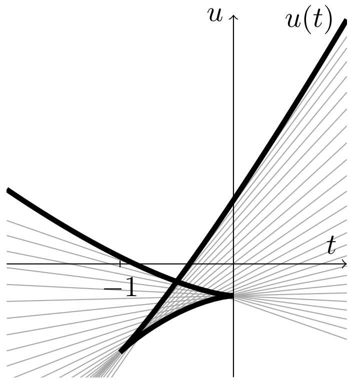


An example for the case of zero solutions for $\deg(f) = 4$ is $f(u_1) = \frac{27}{256}u_1^4$ at the point $t_0 = 0$. The three singular solutions are $u(t) = \zeta_3 t^{\frac{4}{3}}$, where ζ_3 is a (possibly trivial) third root of unity and have an impasse point at $t_0 = 0$.

An example for the case of one solution for $\deg(f) = 4$ is $f(u_1) = -\frac{1}{2}u_1^4 + u_1^3 - \frac{9}{32}$ at the points are $t_0 = 0$ and $t_0 = -1$. The three singular solutions are

$$\begin{aligned} u(t) &= \frac{96t^2 + (16z + 96)t + 3z^2 + 27}{32z} \quad \text{with} \\ z &= \zeta_3 \left(256t^3 + 272t^2 + 128t^4 + 144t + 27 + 64\sqrt{t^3(t+1)^3(1+2t)^2}\right) \end{aligned}$$

and again ζ_3 a (possibly trivial) third root of unity. Only the solution with $\zeta_3 = 1$ admits a power series solution around $t_0 = 0$ and $t_0 = -1$. The impasse points can be seen in the following diagram, where the singular solution is displayed in black and some regular solutions are displayed in light gray.



It is easy to establish convergence of the solutions. All regular solutions are lines. The singular solutions are all solutions of the simple differential system $\{t + f'(u_1) = 0\}$ and, thus, converge by RIQUIER's Theorem 1.60. ◁

In the second example demonstrates that certain formal power series solutions do not necessarily converge, when they are centered around a non-regular point. This shows that the hypothesis of RIQUIER's Existence Theorem 1.60 cannot be relaxed.

Example 2.90. Let $U := \{u\}$, $\Delta := \{\partial_t\}$ and $F := \mathbb{C}(t)$. Consider the differential equation $p := uu_2 - u_1 + t$. Claim: p has a unique formal power series solution centered around $t_0 = 0$ with zeroth power series coefficient 0, and this formal power series does not converge.

So consider the algebraically restricted system $\{p_=, g_0 = 0\}$ of differential equations. $\rho(p) = g_0g_2 - g_1 = 0$ implies $g_1 = 0$. Similarly, $\rho(\partial_t p) = 0$ implies $g_2 = 1$. For $k \geq 2$

$$\partial_t^k p = uu_{k+2} + (ku_1 - 1)u_{k+1} + \sum_{i=2}^{k} \binom{k}{i} u_i u_{k+2-i} \ .$$

Applying ρ and using the relations $g_0 = g_1 = 0$ results in

$$g_{k+1} = \sum_{i=2}^{k} \binom{k}{i} g_i g_{k+2-i} \ .$$

This shows that there is a unique formal power series solution. Furthermore, this formula shows by a trivial induction that all coefficients are non-negative real numbers. We give an estimate for the $2k$-th coefficient.

$$\begin{aligned} g_{2k} &= \sum_{i=2}^{2k-1} \binom{2k-1}{i} g_i g_{2k+1-i} \\ &= \sum_{i=2}^{k} \binom{2k-1}{i} g_i g_{2k+1-i} + \sum_{i=k+1}^{2k-1} \binom{2k-1}{i} g_i g_{2k+1-i} \\ &= \sum_{i=2}^{k} \left(\binom{2k-1}{i} + \binom{2k-1}{2k+1-i} \right) g_i g_{2k+1-i} \end{aligned}$$

Taking only the summand for $i = 2$ results in the following bound.

$$\begin{aligned}&\geq \left(\binom{2k-1}{2} + \binom{2k-1}{2k-1}\right) g_2 g_{2k-1} \\ &= \left(2k^2 - 3k + 2\right) g_{2k-1}\end{aligned}$$

The same estimation also implies $g_{2k+1} \geq (2k^2 - k + 1)g_{2k}$. For proving that the formal power series does not converge, apply the ratio test.

$$\liminf_{k\to\infty} \left| \frac{\frac{g_k}{k!}}{\frac{g_{k-1}}{k-1!}} \right| = \liminf_{k\to\infty} \frac{g_k}{k \cdot g_{k-1}} \geq \liminf_{k\to\infty} \frac{2\left(\frac{k}{2}\right)^2 + \mathcal{O}(k)}{k} = \infty$$

More generally a straight forward computation using the techniques in this section yields the differential counting polynomial for $\{p = 0\}$. The counting sequence is

$$\ell \mapsto \begin{cases} \infty^2 - \infty, & \ell \geq 1 \\ \infty, & \ell = 0 \end{cases}$$

around each center $t_0 \in \{\frac{1}{k} \mid k \in \mathbb{Z}_{\geq 0}\}$, and

$$\ell \mapsto \begin{cases} \infty^2 - \infty + 1, & \ell \geq 1 \\ \infty, & \ell = 0 \end{cases}$$

around each center t_0 for $t_0 \in \mathbb{C} \setminus \{\frac{1}{k} \mid k \in \mathbb{Z}_{\geq 0}\}$. ◁

The third example gives a more formal treatment of the "sphere equation" from Example 2.5 in the overview section, but lacks the geometric intuition.

Example 2.91. Consider $U = \{u\}$, $\Delta = \{\partial_t\}$, $F = \mathbb{C}(t)$, and the differential equation $p = u_1^2 + u^2 + t^2 - 1 = 0$. Denote by $\sum_{i=0}^{\infty} g_i \frac{(t-t_0)^i}{i!}$ the formal power series for u centered around $t_0 \in \mathbb{C}$.

It is clear that adding $g_0^2 + t_0^2 - 1 \neq 0$ to $\{p = 0\}$ yields the enumerable system $\{p = 0, g_0^2 + t_0^2 - 1 \neq 0\}$ for $t_0^2 - 1 \neq 0$ and $\{p = 0, g_0 \neq 0\}$ for $t_0^2 - 1 = 0$. These systems have the counting sequence

$$\ell \mapsto \begin{cases} 2\infty - 4, & \ell \geq 1 \\ \infty - 2, & \ell = 0 \end{cases}$$

and

$$\ell \mapsto \begin{cases} 2\infty - 2, & \ell \geq 1 \\ \infty - 1, & \ell = 0 \end{cases},$$

respectively.

Adding the complementary constraint $g_0^2 + t_0^2 - 1 = 0$ yields an inconsistent system for $t_0 \neq 0$ and the following system for $t_0 = 0$ after three prolongations.

$$\{ \quad \begin{aligned} u_1u_5 + 4u_2u_4 + 3u_3^2 + uu_4 + 4u_1u_3 + 3u_2^2 &= 0, \\ g_3 &= 0, \\ g_2^2 + g_0g_2 + 1 &= 0, \\ g_1 &= 0, \\ g_0^2 - 1 &= 0 \end{aligned} \quad \}$$

This system is enumerable, as the k-th prolongation of $u_1u_5 + 4u_2u_4 + 3u_3^2 + uu_4 + 4u_1u_3 + 3u_2^2$ has the highest ranking term $((4+k)g_2 + g_0)g_{4+k}$ after application of the forgetful map ρ and using the relation $g_1 = 0$. In particular, this relation has a non-zero initial and is square-free. Thus, for $t_0 = 0$ there are four additional formal power series solutions.

MAPLE's dsolve [map] finds no solutions for this differential equation. ◁

The fourth examples shows that differential counting polynomials can depend on the order ℓ.

Example 2.92. Consider $U = \{u, v\}$, $\Delta = \{\partial_t\}$ and $F = \mathbb{C}$ with the orderly ranking with $u > v$. Let $p := vu_1 - u$ and

$$S := \{p = 0\} \qquad (S)$$

Claim:

$$\bar{c}(S) = c(S)(\ell) = \infty^{\ell+2} - \infty^{\ell+1} + (\ell+1)\infty^{\ell} - \ell\infty^{\ell-1}$$

for all $\ell \geq 1$.

Corollary 1.58 gives a bijection between formal power series solutions and non-centered solutions independent of the chosen center, because of the constant coefficients in this example. Thus, make the ansatz $u(t) = \sum_{i=0}^{\infty} a_i \frac{t^i}{i!}$ and $v(t) = \sum_{i=0}^{\infty} b_i \frac{t^i}{i!}$ for formal power series solutions centered around zero to compute the counting sequence. We use the forgetful map

$$\rho : \mathbb{C}\{U\} \to \mathbb{C}[a_i, b_i | i \in \mathbb{Z}_{\geq 0}] : u_i \mapsto a_i, v_i \mapsto b_i \ .$$

It is clear that adding $b_0 \neq 0$ to S makes the system

$$T := \{p = 0, b_0 \neq 0\} \qquad (T)$$

enumerable. It has the counting sequence $c(T) : \ell \mapsto (\infty - 1)\infty^{\ell+1}$.

The complementary system $\{p = 0, b_0 = 0\}$ prolongs to the system

$$S_1 := \{ \quad \partial_t p = vu_2 + (v_1 - 1)u_1 = 0, \quad a_0 = 0, \quad b_0 = 0 \quad \} , \qquad (S_1)$$

which is part of the family

$$S_k := \{ \quad \partial_t^k p = vu_{k+1} + (kv_1 - 1)u_k + \sum_{i=2}^{k} \binom{k}{i} v_i u_{k+1-i} = 0, \quad a_0 = \ldots = a_{k-1} = 0, \quad b_0 = 0, \quad \prod_{i=1}^{k-1}(ib_1 - 1) \neq 0 \quad \} \qquad (S_k)$$

of systems. Consider the initial of the equation $\rho(\partial_t^k p)$. This equation yields $(kb_1 - 1)a_k$ after reduction in S_k and thus has initial $(kb_1 - 1)$. Adding $(kb_1 - 1) \neq 0$ to S_k, to make sure that the initial is non-zero, and prolonging $\partial_t^k p$ results in the system S_{k+1}. Complementary, adding $(kb_1 - 1) = 0$ to S_k and prolonging $\partial_t^k p$ yields the system

$$T_k := \{ \quad \partial_t^{k+1} p = vu_{k+2} + ((k+1)v_1 - 1)u_{k+1} + \sum_{i=2}^{k+1} \binom{k+1}{i} v_i u_{k+2-i} = 0, \quad a_0 = \ldots = a_{k-1} = 0, \quad b_0 = kb_1 - 1 = 0 \quad \} . \qquad (T_k)$$

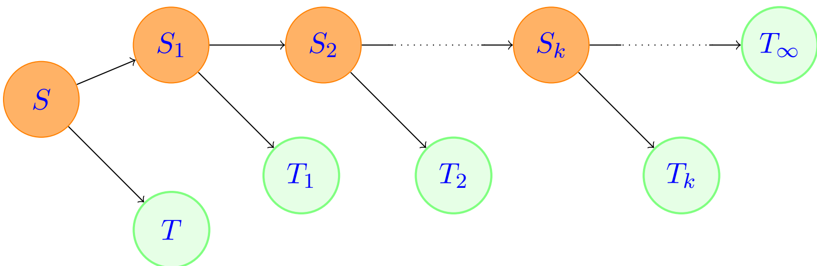
Note that the inequations from S_k are superfluous in T_k because of the equation $kb_1 - 1 = 0$. Furthermore, the equation $\rho(\partial_t^{k+1+j} p)$ reduces to $\frac{1}{k} a_{k+1+j} + \binom{k+1+j}{2} b_2 a_{k+j}$ in the context of T_k for all $j \in \mathbb{Z}_{\geq 0}$. In particular, this reduced form has the leader a_{k+1+j} for all $j \in \mathbb{Z}_{\geq 0}$ and there is no constraint for a_k. This family of systems has the following counting sequence.

$$c(T_k) : \ell \mapsto \begin{cases} \infty^{\ell}, & \ell \geq k \\ \infty^{\ell-1}, & 1 \leq \ell < k \\ 1, & \ell = 0 \end{cases}$$

We study the remaining system $T_\infty := \bigcup_{i=1}^{\infty} S_i$. The equations $a_k = 0$ for all $k \in \mathbb{Z}_{\geq 0}$ yield the differential equation $u = 0$ and also make the differential equation p superfluous. Furthermore, b_1 is not allowed to be of the form $\frac{1}{k}$ for any $k \in \mathbb{Z}_{\geq 1}$. We denote this informally by writing $\prod_{i=1}^{\infty} kb_1 - 1 \neq 0$, which represents the infinite set of all inequations $kb_1 - 1 \neq 0$ for $i \in \mathbb{Z}_{\geq 1}$. Summing up, the following system describes these remaining set of solutions.

$$T_\infty := \{ \quad u = 0, \quad b_0 = 0, \quad \prod_{i=1}^{\infty} ib_1 - 1 \neq 0 \quad \} \tag{T_∞}$$

The following diagram visualizes the splittings. Here, dark orange nodes represent unfinished systems and light green nodes represent enumerable systems.



We discuss the counting sequence. For order $\ell = 0$ all special cases are identical $\{a_0 = b_0 = 0\}$ and have algebraic counting polynomial 1. They are disjoint with T, which has counting polynomial $\infty^2 - \infty$. Thus, the differential counting polynomial is $\infty^2 - \infty + 1$ for $\ell = 0$.

Assume that $\ell \geq 1$. To get the ℓ-th differential counting polynomial of the union of the sets of solutions of special case systems T_∞ and T_k, $k \geq 1$, we apply Lemma 2.25, where $\phi_{\leq a_0,(0,0)}((T_\infty)_{\leq \ell})$ plays the role of T_0 and $\phi_{\leq a_0,(0,0)}((T_k)_{\leq \ell})$ plays the role of T_k, $k \geq 1$. To apply Lemma 2.25 we need to ensure its hypothesis, i.e., check whether several properties are satisfied. The partition property of Lemma 2.25.(1) is easily verified. The existence of the algebraic counting polynomials for Lemma 2.25.(4) and the finiteness of the systems $\phi_{\leq a_0,(0,0)}((T_k)_{\leq \ell})$ for Lemma 2.25.(2) have already been shown above. For Lemma 2.25.(3) note that the algebraic counting polynomial is different depending on whether b_1 is in $\left\{ \frac{1}{k} \middle| k \in \mathbb{Z}_{\geq 0} \right\}$ or not; in the first case, the algebraic counting polynomial is ∞^{ℓ} for $\ell \geq k$ large enough and $\infty^{\ell-1}$ for $\ell < k$, and in the second case the algebraic counting polynomial is $\infty^{\ell-1}$ for each value of b_1. Thus, Lemma 2.25 can be applied and yields

$$\begin{aligned} & c\left(\mathfrak{Sol}_{\mathbb{C}^{2\ell}}(\phi_{\leq a_0,(0,0)}((T_\infty)_{\leq \ell})) \cup \bigcup_{k=1}^{\infty} \mathfrak{Sol}_{\mathbb{C}^{2\ell}}((\phi_{\leq a_0,(0,0)}(T_k)_{\leq \ell}))\right) \\ & = (\infty - \ell) \cdot c(\phi_{\leq b_1,(0,0,\overline{b_1})}(T_\infty))(\ell) + \sum_{j=1}^{\ell} c(\phi_{\leq a_0,(0,0)}(T_\infty))(\ell) \\ & = (\infty - \ell) \cdot \infty^{\ell-1} + \sum_{j=1}^{\ell} \infty^{\ell} \\ & = (\ell+1)\infty^{\ell} - \ell\infty^{\ell-1} , \end{aligned}$$

where $\overline{b_1} \in \mathbb{C} \setminus \{\frac{1}{k} | k \in \mathbb{Z}_{\geq 0}\}$. As there is only one choice for the solutions of b_0 and a_0,

$$c(\mathfrak{Sol}_{\mathbb{C}^{2\ell+2}}((T_\infty)_{\leq \ell}) \cup \bigcup_{k=1}^{\infty} \mathfrak{Sol}_{\mathbb{C}^{2\ell+2}}((T_k)_{\leq \ell})) = (\ell+1)\infty^{\ell} - \ell\infty^{\ell-1}$$

Add the counting polynomial $(\infty - 1)\infty^{\ell+1}$ of the generic system T to the combined differential counting polynomial of the special cases. This results in the counting sequence

$$c(S) = l \mapsto \begin{cases} \infty^{\ell+2} - \infty^{\ell+1} + (\ell+1)\infty^{\ell} - \ell\infty^{\ell-1}, & \ell \geq 1 \\ \infty^2 - \infty + 1, & \ell = 0 \end{cases}$$

of S. See Example E.8 for an explanation of this counting sequence using the VESSIOT theory.

RIQUIER's Existence Theorem 1.60 implies the convergence for the formal power series solutions of system T for analytical initial conditions. System T_∞ gives the zero power series for u, which converges, and only restricts the choice for the first two power series coefficients of v, hence v can be chosen to converge or diverge. The solutions of the systems T_k can diverge even for analytical initial conditions. Consider for example system T_1 and prescribe $b_0 = 0, b_1 = 1, b_2 = 1, b_i = 0$ for all $i \geq 3$. Then, by the ratio test the radius of convergence of the solution for u is zero:

$$\left|\frac{a_{k+1}}{(k+1)a_k}\right| = \frac{k-1}{k} \left|\frac{\sum_{i=2}^{k} \binom{k}{i} \frac{b_{i+1}}{i+1} a_{k+1-i}}{\sum_{i=2}^{k} \binom{k}{i} b_i a_{k+1-i}} + \frac{k}{2} b_2\right| = \frac{k-1}{2} \longrightarrow \infty, k \to \infty$$

However, by a similar computation, the analytical initial condition $b_0 = 0, b_1 = 1, b_2 = 0, b_i = i!$, for $i \geq 3$, implies that the radius of convergence of u is 1.

Compare the set of solutions described here with the one found by MAPLE. Therefore, consider real (instead of complex) formal and convergent power series solutions centered around zero. This is no substantial restriction, as real initial conditions lead to real power series solutions above. MAPLE's dsolve [map] returns an arbitrary $v(t)$ and

$$u(t) = c \cdot e^{\int_0^t \frac{1}{v(h)} \mathrm{d}h}$$

for a constant c. This set of solutions depend on $\ell + 2$ (seemingly arbitrary) constants up to order ℓ, where $\ell + 1$ of those come from $v(t)$. However, the zeroth power series coefficient of $v(t)$ cannot be zero, as otherwise the integral does not exist and this is not a formal (or convergent) power series solution; in particular not all of the $\ell+2$ constants are arbitrary. Thus, MAPLE's dsolve only finds $\infty^{\ell+2} - \infty^{\ell+1}$ solutions in order ℓ. In particular, a subset with counting sequence $\ell \mapsto (\ell+1)\infty^{\ell} - \ell\infty^{\ell-1}$ of the solutions is not found (cf. Theorem 2.34). As seen above, some of these solutions are (convergent) analytical solutions.

The differential dimension polynomial only shows that there are $\ell + 2$ arbitrary parameters for a solution, so it can not account for the missing solutions. ◁

The fifth example demonstrates that there are systems with the following peculiar behavior. For a power series coefficient of order one any value can be chosen except for the countable set $\{\frac{1}{k} \mid k \in \mathbb{Z}_{\geq 1}\}$. This countable exceptional set yields $\aleph_0$ in the differential counting polynomial of the system.

Example 2.93. Consider $U = \{u, v\}$, $\Delta = \{\partial_t\}$ and $F = \mathbb{C}(t)$ with the orderly ranking with $u > v$. Let $p := vu_1 - u + \frac{1}{t}$ and

$$S := \{p = 0, v_2 = 0\} \tag{S}$$

S has no solutions centered around 0, so let $t_0 \in \mathbb{C} \setminus \{0\}$. Claim:

$$\overline{c}(S) = c(S)(\ell) = \infty^3 - \infty^2 + \infty - \aleph_0$$

for all $\ell \geq 1$, and every of these solutions yields a locally convergent formal power series solution centered around t_0.

The computations in this example are independent of the base point $t_0 \neq 0$ and show that the evaluation $\psi_{t_0} : E \mapsto \mathbb{C}[[y_1 - \zeta_1, \ldots, y_n - \zeta_n]]^U \cup \{\infty\}$ induces a bijection between the set of non-centered solutions and the set of formal power series solutions centered around t_0. Thus, compute the differential counting polynomial using the formal power series ansatz $u(t) = \sum_{i=0}^{\infty} a_i \frac{(t-t_0)^i}{i!}$ and $v(t) = \sum_{i=0}^{\infty} b_i \frac{(t-t_0)^i}{i!}$ and the forgetful map

$$\rho : \mathbb{C}[t, t^{-1}]\{U\} \to \mathbb{C}[a_i, b_i | i \in \mathbb{Z}_{\geq 0}] : u_i \mapsto a_i, v_i \mapsto b_i, t \mapsto t_0 \ .$$

It is clear that adding $b_0 \neq 0$ to S results in the enumerable system

$$T := \{p = 0, v_2 = 0, b_0 \neq 0\} \tag{T}$$

with ℓ-th differential counting polynomial $c(T)(\ell) = \infty^3 - \infty^2$ for every order $\ell \geq 1$.

The complementary system $\{p = 0,\ v_2 = 0,\ b_0 = 0\}$ prolongs to the system

$$S_1 := \{ \quad \partial_t p = vu_2 + (v_1 - 1)u_1 - \frac{1}{t^2} = 0, \quad v_2 = 0, \quad a_0 - \frac{1}{t} = 0, \quad b_0 = 0 \quad \} . \tag{S_1}$$

It is part of the following family of systems.

$$S_k := \{ \quad q_k := vu_{k+1} + (kv_1 - 1)u_k + (-1)^k \frac{k!}{t^{k+1}} = 0, \quad v_2 = 0, \quad (ib_1 - 1)a_i + (-1)^i \frac{i!}{t^{i+1}} = 0 \quad \forall\ 0 \leq i < k, \quad b_0 = 0, \quad \prod_{i=1}^{k-1}(ib_1 - 1) \neq 0 \quad \} \tag{S_k}$$

Here q_k results from differential reduction by v_2 of $\partial_t^k p$. After application of ρ and reduction with elements in S_k the differential equations q_k yield $(kb_1-1)a_k+(-1)^k\frac{k!}{t^{k+1}}$. Adding $(kb_1-1)\neq 0$ to S_k, to ensure a non-zero initial, and prolonging q_k, which after reduction by v_2 results in q_{k+1}, yields the system S_{k+1}. Complementary, when adding $kb_1-1=0$ to S_k the system is inconsistent. This can be seen by reducing $\partial_t q_k$ by v_2, which again results in q_{k+1}. Then

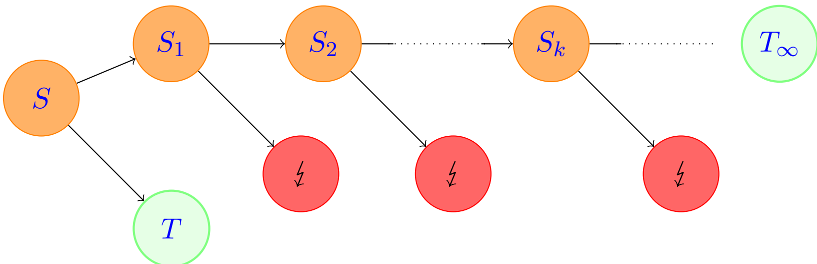
$$\rho(q_{k+1}) = b_0 a_{k+2} + (kb_1-1)a_{k+1} + (-1)^{k+1}\frac{(k+1)!}{t^{k+2}} = 0$$

yields the contradiction $(-1)^{k+1}\frac{(k+1)!}{t^{k+2}}=0$ by using the relations $b_0=0$ and $kb_1-1=0$.

Study the remaining system $T_\infty := \bigcup_{i=1}^\infty S_i$. The equations $(kb_1-1)a_k+(-1)^k\frac{k!}{t^{k+1}}=0$ for all $k\in\mathbb{Z}_{\geq 0}$ imply p and make it superfluous. Furthermore, b_1 is not allowed to be of the form $\frac{1}{k}$ for any $k\in\mathbb{Z}_{\geq 1}$. Denote this informally by $\prod_{i=1}^\infty(kb_1-1)\neq 0$. This results in the following system.

$$T_\infty := \left\{ \begin{aligned} v_2 &= 0, \\ (kb_1-1)a_k+(-1)^k\frac{k!}{t^{k+1}} &= 0 \quad \forall\, k\in\mathbb{Z}_{\geq 0}, \\ b_0 &= 0, \\ \textstyle\prod_{k=1}^\infty(kb_1-1) &\neq 0 \end{aligned} \right\} \qquad (T_\infty)$$

The following short diagram visualizes the splittings with dark orange for unfinished systems, light green for enumerable systems, and dark red systems with a lightning for inconsistent systems.



For order $\ell=0$ the system T_∞ has one solution $\{a_0=\frac{1}{t_0}, b_0=0\}$ and has differential counting polynomial 1. It is disjoint with T, which has differential counting polynomial $\infty^2-\infty$. Thus, the zeroth differential counting polynomial is $\infty^2-\infty+1$ for $\ell=0$. Now assume $\ell\geq 1$. The only choice in the special case system T_∞ is for b_1 and it may be chosen freely in $\mathbb{C}\setminus\left\{\frac{1}{k}\middle| k\in\mathbb{Z}_{\geq 1}\right\}$. Thus, $c(T_\infty)=\infty-\aleph_0$. Thus, the counting sequence of S is

$$c(S) = l \mapsto \begin{cases} \infty^3-\infty^2+\infty-\aleph_0, & \ell\geq 1 \\ \infty^2-\infty+1, & \ell = 0 \end{cases},$$

and this is explained in Example E.7 by the Vessiot theory.

All formal power series solutions of this example converge. Riquier's Existence Theorem 1.60 implies this for the ones of system T. For system T_∞ the solutions of v are lines and the ratio test shows that the radius of convergence for the formal power series solutions of u is $|t_0|$:

$$\left|\frac{a_{k+1}}{(k+1)a_k}\right| = \left|\frac{kb_1-1}{(k+1)b_1-1}\right|\cdot\left|\frac{1}{t_0}\right| \longrightarrow \left|\frac{1}{t_0}\right|, k\to\infty \qquad \triangleleft$$

The sixth example deals with partial differential equations. In contrast to the ordinary examples before, this requires a technical treatment to ensure passivity.

Example 2.94. Consider the system $S := \{p_=, q_=\}$ of the differential equations

$$p := v \cdot u_x - y \cdot u \qquad\qquad q := v_y + x \cdot u$$

for $U = \{u, v\}$, $\Delta = \{\partial_x, \partial_y\}$, and $F = \mathbb{C}(x, y)$. Make the ansatz

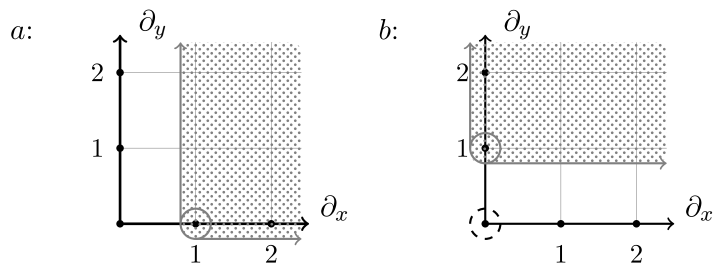
$$u(x,y) = \sum_{i,j\in\mathbb{Z}_{\geq 0}} a_{i,j} \frac{(x-x_0)^i (y-y_0)^j}{i!j!} \in \mathbb{C}[[x-x_0, y-y_0]]$$
$$v(x,y) = \sum_{i,j\in\mathbb{Z}_{\geq 0}} b_{i,j} \frac{(x-x_0)^i (y-y_0)^j}{i!j!} \in \mathbb{C}[[x-x_0, y-y_0]]$$

for formal power series solutions of the system S expanded around $(x_0, y_0) \in \mathbb{C}^2$ and determine the differential counting polynomial of this set of solutions. Let $(x_0, y_0) \in \mathbb{C}^2$ with the assumption $x_0 \neq 0$ or $y_0 \neq 0$. Fix the degree-reverse lexicographical ranking, so the induced ranking on $G = \{a_{i,j}, b_{i,j} \mid i, j \in \mathbb{Z}_{\geq 0}\}$ begins with $b_{0,0} < a_{0,0} < b_{0,1} < a_{0,1} < b_{1,0} < a_{1,0} < b_{0,2}$. The forgetful map $\rho : \mathbb{C}(x, y)\{u, v\} \to \mathbb{C}[G]$ substitutes x, y, $\partial_x^i \partial_y^j u$, and $\partial_x^i \partial_y^j v$ by x_0, y_0, $a_{i,j}$, and $b_{i,j}$, respectively.

The equation $q = v_y + x \cdot u$ is semilinear. Thus, for $i, j \in \mathbb{Z}_{\geq 0}$ the power series coefficients $b_{i,j+1}$ are determined by the equations $\rho(\partial_x^i \partial_y^j q)$ dependent on the coefficients of lower order. The highest ranking indeterminate in $\rho\left(\partial_x^i \partial_y^j p\right)$ is $a_{i+1,j}$ occurring in the term $b_{0,0} \cdot a_{i+1,j}$, which might vanish for $b_{0,0} = 0$. Split the system into a favorable system with the $b_{0,0} \neq 0$ and one with $b_{0,0} = 0$. In the favorable system

$$T := \{ \quad p = v \cdot \underline{u_x} - y \cdot u = 0, \quad q = \underline{v_y} + x \cdot u = 0, \quad b_{0,0} \neq 0 \quad \}, \tag{T}$$

given $a_{0,i} \in \mathbb{C}$ for $i \in \mathbb{Z}_{\geq 0}$, $b_{0,0} \in \mathbb{C} \setminus \{0\}$, and $b_{i,0} \in \mathbb{C}$ for $i \in \mathbb{Z}_{\geq 1}$, there is a unique formal power series solution. Picture this using the following diagram.



All power series coefficients marked by gray dots are uniquely determined, once the lower coefficients are chosen. The one coefficient $b_{0,0}$, marked by a dashed circle, can be chosen almost arbitrarily, only constrained by an inequation of degree one. The other coefficients that are not marked, i.e., $a_{0,i}$ and $b_{i+1,0}$ for all $i \in \mathbb{Z}_{\geq 0}$, can be chosen arbitrarily. With this description, one easily defines an allocation map β which makes T an enumerable system. The corresponding counting sequence for this system is $c(T) : \ell \mapsto (\infty - 1) \cdot \infty^{2\ell+1}$.

Counting the set of solutions of the system with $b_{0,0} = 0$ is harder. The rest of this example looks for the highest differential variable in a derivative $\rho(\partial_x^i \partial_y^j p)$ of p such that its initial is not implied zero. Consider

$$S' := \{ \quad p = v \cdot u_x - y \cdot u = 0, \quad q = v_y + x \cdot u = 0, \quad b_{0,0} = 0 \quad \} . \tag{S'}$$

Then $\rho(p) = b_{0,0}a_{1,0} - y_0 a_{0,0} = 0$, $b_{0,0} = 0$, and $y_0 \neq 0$ imply $a_{0,0} = 0$. The system

$$\mathsf{SingleProlongation}(S', p) = \{ \quad \partial_x p = \underset{\sim}{v \cdot u_{xx}} + (v_x - y) \cdot u_x = 0, \quad \partial_y p = \underset{\sim}{v \cdot u_{xy}} + \underset{\sim}{x \cdot u \cdot u_x} - y \cdot u_y - \underset{\sim}{u} = 0, \quad q = \underline{v_y} + \underset{\sim}{x \cdot u} = 0, \quad b_{0,0} = a_{0,0} = 0 \quad \}$$

implies $a_{0,i} = 0$, $a_{1,i} = 0$, $b_{0,i+1} = 0$, and $b_{1,i+1} = 0$ for all $i \in \mathbb{Z}_{\geq 1}$ as consequences from Lemma 2.95, and an algebraic THOMAS decomposition of $\{\rho(q) = 0, \rho(\partial_x q) = 0, \rho(p) = 0, \rho(\partial_x p) = 0, \rho(\partial_x \partial_y p) = 0, b_{0,0} = 0\}$ yields $x_0 a_{1,0}^2 + a_{1,0} = a_{1,0}(x_0 a_{1,0} + 1) = 0$ as a consequence. (The terms that vanish after application of ρ are underwaved, e.g., the term $v \cdot u_{xx}$ in $\mathsf{SingleProlongation}(S', p)$ maps to $b_{0,0} \cdot a_{2,0}$ and vanishes because of $b_{0,0} = 0$.) Thus, rewrite the system as

$$S'' := \{ \quad \partial_x p = \underset{\sim}{v \cdot u_{xx}} + (v_x - y) \cdot u_x = 0, \quad q = \underline{v_y} + \underset{\sim}{x \cdot u} = 0, \quad a_{0,i} = b_{0,i} = a_{1,i+1} = b_{1,i+2} = 0, \quad i \geq 0, \quad a_{1,0} \cdot (x_0 a_{1,0} + 1) = 0 \quad \} . \tag{S''}$$

In S'' all equations of the form $\rho(\partial_y^i p)$ reduce to zero, so one only needs to consider $\partial_x p$ and all its derivatives. Obviously, the two cases $a_{1,0} = 0$ and $x_0 a_{1,0} + 1 = 0$ are disjoint. By Lemma 2.96 the case $a_{1,0} = 0$ yields the system

$$T' := \{ \quad u = 0, \quad v_y = 0, \quad b_{0,0} = 0 \quad \} . \tag{T'}$$

This system has the counting sequence $c(T') : \ell \mapsto \infty^\ell$. By Lemma 2.97 the case $x_0 a_{1,0} + 1 = 0$ yields the system

$$T'' := \{ \quad \partial_x^2 p = \underset{\sim}{v \cdot u_{xxx}} + (2v_x - y) \cdot \underline{u_{xx}} + u_x v_{xx} = 0, \quad \partial_x^2 q = \underline{v_{xxy}} + x \cdot u_{xx} + 2u_x = 0, \quad a_{0,i} = b_{0,i} = a_{1,i+1} = b_{1,i+2} = 0, \quad i \geq 0, \quad b_{1,0} - y_0 = 0, \quad b_{1,1} - 1 = 0, \quad x_0 a_{1,0} + 1 = 0, \quad \} . \tag{T''}$$

Here, $\rho(\partial_x^{i+2}\partial_y^j p)$ and $\rho(\partial_x^{i+2}\partial_y^j q)$ have the leaders $a_{i+2,j}$ and $b_{i+2,j+1}$ after application of ρ. The initial of $a_{i+2,j}$ is 1 and the initial of $b_{i+2,j+1}$ is y_0. This system has the counting sequence $c(T'') : \ell \mapsto \infty^{\ell-1}$.

Next, we count the union of the sets of solutions of the three systems T, T', and T''. The system $T_{\leq 0}$ is disjoint with both $T'_{\leq 0}$ and $T''_{\leq 0}$, but the systems $T'_{\leq 0}$ and $T''_{\leq 0}$ have identical solutions. Thus, $c(S)(0) = c(T)(0) + c(T')(0) = c(T)(0) + c(T'')(0) = \infty^2 - \infty + 1$. For order $\ell \geq 1$ these systems are disjoint, and adding the corresponding polynomials yields

$$\begin{aligned} c(S)(\ell) &= c(T) + c(T') + c(T'') \\ &= (\infty - 1) \cdot \infty^{2\ell+1} + \infty^{\ell} + \infty^{\ell-1} \\ &= \infty^{2\ell+2} - \infty^{2\ell+1} + \infty^{\ell} + \infty^{\ell-1} . \end{aligned}$$

In comparison, MAPLE's pdsolve [map] yields the solution set where u is the zero function and v is an arbitrary function depending on only x (and not y). This solution set has the counting sequence $\ell \mapsto \infty^{\ell+1}$, much less than $\ell \mapsto \infty^{2\ell+2} - \infty^{2\ell+1} + \infty^{\ell} + \infty^{\ell-1}$. ◁

Lemma 2.95. *In the context of Example 2.94, the system* SingleProlongation(S', p) *implies the algebraic constraints for power series coefficients* $a_{0,i} = 0$, $a_{1,i} = 0$, $b_{0,i+1} = 0$, *and* $b_{1,i+1} = 0$ *for all* $i \in \mathbb{Z}_{\geq 1}$ *as consequences.*

Proof. For $i = 1$ this follows from an algebraic THOMAS decomposition of $\{b_{0,0} = 0, \rho(q) = 0, \rho(\partial_x q) = 0, \rho(\partial_y q) = 0, \rho(\partial_x \partial_y q) = 0, \rho(p) = 0, \rho(\partial_x p) = 0, \rho(\partial_y p) = 0, \rho(\partial_x \partial_y p) = 0, \rho(\partial_x \partial_y^2 p) = 0\}$.

Assume the claim holds for all j smaller i. Show that it holds for i in four steps.

First, consider ρ applied to $\partial_y^i p = \sum_{j=0}^{i} \binom{i}{j} \underset{\sim}{v_{y^j} u_{xy^{i-j}}} - y u_{y^i} - \underset{\sim}{u_{y^{i-1}}}$. By induction the $\rho(v_{y^j})$ and $\rho(u_{y^{i-1}})$ reduce to zero. Now $y_0 \neq 0$ implies $a_{0,i} = \rho(u_{y^i}) = 0$.

Second, consider $\rho(\partial_y^i q = v_{y^{i+1}} + x \cdot u_{y^i})$. This equation implies $b_{0,i+1} = 0$ using the equation $a_{0,i} = 0$.

Third, a case distinction shows $a_{1,i} = 0$. Consider

$$\begin{aligned} \partial_y^i \partial_x p &= \partial_y^i \left(v u_{xx} + v_x u_x - y u_x \right) \\ &= \sum_{j=0}^{i} \binom{i}{j} v_{y^{i-j}} u_{x^2 y^j} + \sum_{j=0}^{i} \binom{i}{j} v_{xy^{i-j}} u_{xy^j} - y u_{xy^i} - i u_{xy^{i-1}} \\ &= \sum_{j=0}^{i} \binom{i}{j} \underset{\sim}{v_{y^{i-j}} u_{x^2 y^j}} + \sum_{j=0}^{i-1} \binom{i}{j} \underset{\sim}{v_{xy^{i-j}} u_{xy^j}} + \binom{i}{i} v_x u_{xy^i} - y u_{xy^i} - i \underset{\sim}{u_{xy^{i-1}}} . \end{aligned}$$

When applying ρ all terms but $b_{1,0} a_{1,i} - y_0 a_{1,i} = (b_{1,0} - y_0) a_{1,i}$ vanish. For the initial $b_{1,0} - y_0 \neq 0$ the claim $a_{1,i} = 0$ holds. So assume $b_{1,0} = y_0$. Consider

$$\begin{aligned} \partial_y^{i+1} \partial_x p &= \partial_y^{i+1} \left(v u_{xx} + v_x u_x - y u_x \right) \\ &= \sum_{j=0}^{i+1} \binom{i+1}{j} v_{y^{i+1-j}} u_{x^2 y^j} + \sum_{j=0}^{i+1} \binom{i+1}{j} v_{xy^{i+1-j}} u_{xy^j} - y u_{xy^{i+1}} - (i+1) u_{xy^i} \end{aligned}$$

Reorganize the sums to see the terms that vanish after an application of ρ.

$$\begin{aligned} &= \sum_{j=0}^{i+1} \binom{i+1}{j} \underset{\sim}{v_{y^{i+1-j}} u_{x^2 y^j}} + \sum_{j=1}^{i-1} \binom{i+1}{j} \underset{\sim}{v_{xy^{i+1-j}} u_{xy^j}} \\ &\quad + \binom{i+1}{0} v_{xy^{i+1}} u_x + \binom{i+1}{i} v_{xy} u_{xy^i} \\ &\quad + \underset{\sim}{\left(\binom{i+1}{i+1} v_x u_{xy^{i+1}} - y u_{xy^{i+1}} \right)} - (i+1) u_{xy^i} . \end{aligned}$$

An application of ρ leaves

$$\begin{aligned}(i+1)b_{1,1}a_{1,i} - (i+1)a_{1,i} + a_{1,0}b_{1,i+1} &= ((i+1)b_{1,1} - (i+1))a_{1,i} + a_{1,0}b_{1,i+1} \\ &= -(i+1)(x_0 a_{1,0}+1)a_{1,i} + a_{1,0}b_{1,i+1} \ .\end{aligned}$$

It has already been shown that $a_{1,0}(x_0 a_{1,0}+1) = 0$. On the one hand, if $a_{1,0} = 0$ the claim follows directly. On the other hand, $a_{1,0} = -\frac{1}{x_0}$ implies $b_{1,i+1} = 0$; substituting this and $a_{0,i} = 0$ into $\rho(\partial_x \partial_y^i q) = \rho(v_{xy^{i+1}} + u_{y^i} + x \cdot u_{xy^i}) = b_{1,i+1} + x_0 a_{1,i} + a_{0,i}$ implies the claim, as $x_0 \neq 0$.

Fourth, if $b_{1,i+1} = 0$ is not shown then consider $\partial_x \partial_y^i q = v_{xy^{i+1}} + u_{y^i} + x \cdot u_{xy^i}$. As $a_{0,i} = 0$ and $a_{1,i} = 0$ by assumption $\rho(\partial_x \partial_y^i q)$ reduces to $b_{1,i+1} = 0$. □

Lemma 2.96. *In the context of Example 2.94, adding $a_{1,0} = 0$ to the system (S'') results in the system $\{u = 0, v_y = 0, b_{0,0} = 0\}$.*

Proof. First observe that $b_{1,1} = 0$ follows from reducing $\rho(\partial_x q)$ by $a_{0,0} = a_{1,0} = 0$.

The statement $u = 0$ is equivalent to $a_{i,j} = 0$ for all $i, j \in \mathbb{Z}_{\geq 0}$. Show the latter one by an induction over i. Note that $a_{i,j} = 0$ for all $j \in \mathbb{Z}_{\geq 0}$ and $0 \leq i \leq 1$. Assume that the claim holds for all values lower than i and consider

$$\partial_y^j \partial_x^i p = \partial_y^j \left(\underset{\sim}{v u_{x^{i+1}}} + (iv_x - y)u_{x^i} + \sum_{k=2}^{i} \binom{i}{k} \underset{\sim}{v_{x^k} u_{x^{i+1-k}}} \right)$$

For $k \geq 2$ by the induction hypothesis for all $j \geq 0$ both $\rho(\partial_y^j (v_{x^k} u_{x^{i+1-k}}))$ and $\rho(\partial_y^j (v u_{x^{i+1}})$ reduce to zero. So it suffices to consider

$$\partial_y^j \left((iv_x - y)u_{x^i}\right) = (iv_x - y)u_{x^i y^j} + (i\underset{\sim}{v_{xy}} - 1)u_{x^i y^{j-1}} + \sum_{k=2}^{j} \binom{j}{k} \underset{\sim}{i v_{xy^k} u_{x^i y^{j-k}}} \ .$$

By $b_{1,k} = 0$ for all $k \geq 2$ the sum vanishes by an application of ρ. If $(ib_{1,0} - y_0) \neq 0$, then $a_{i,j} = 0$ by induction on j. If $(ib_{1,0} - y_0) = 0$, then $\partial_y^{j+1} \partial_x^i p$ implies $a_{i,j} = 0$.

Now, $v_y = q - x \cdot u = 0$ follows directly from $u = 0$. This proof "used" all derivatives of p and q in the sense that all their derivatives reduce to zero after evaluation. □

Lemma 2.97. *In the context of Example 2.94, adding $x_0 a_{1,0} + 1 = 0$ to the system S'' yields the system*

$$T'' := \left\{ \begin{aligned} \partial_x^2 p = \quad & \underset{\sim}{v \cdot u_{xxx}} + (2v_x - y) \cdot \underline{u_{xx}} + u_x v_{xx} = 0, \\ \partial_x^2 q = \quad & \underline{v_{xxy}} + x \cdot u_{xx} + 2u_x = 0, \\ & a_{0,i} = b_{0,i} = a_{1,i+1} = b_{1,i+2} = 0, \quad i \geq 0, \\ & b_{1,0} - y_0 = 0, \\ & b_{1,1} - 1 = 0, \\ & x_0 a_{1,0} + 1 = 0 \end{aligned} \right\} .$$

Here, $\rho(\partial_x^{i+2} \partial_y^j p)$ and $\rho(\partial_x^{i+2} \partial_y^j q)$ have leader $a_{i+2,j}$ and $b_{i+2,j+1}$ after application of ρ.

Proof. The consequences $b_{1,0} - y_0 = 0$ and $b_{1,1} - 1 = 0$ follow from $\rho(\partial_x p)$ and $\rho(\partial_x \partial_y p)$ and substitution of known relations into them. After that it is clear that all derivatives of $\rho(\partial_x^i \partial_y^j p)$ and $\rho(\partial_x^i \partial_y^j q)$ with $0 \leq i \leq 1$ and $j \in \mathbb{Z}_{\geq 0}$ reduce to zero.

The claim about leader of derivatives of $\rho(\partial_x^2 q)$ is clear. It remains to be shown for $\partial_x^2 p$. The two leading terms of $\partial_x^{i+2}\partial_y^j p$ are $vu_{x^{i+3}} + ((i+2)v_x - y)u_{x^i y^j}$. The first of these terms vanishes after application of ρ due to $b_{0,0} = 0$. The second term is mapped to $((i+2)b_{1,0} - y_0)a_{i,j}$ by ρ, which is equivalent to $(i+1)y_0 a_{i,j}$, since $b_{1,0} - y_0 = 0$. Thus, $a_{i,j}$ has a non-zero initial and the claim is shown. □

2.5.5 Counting is not Algorithmic

This subsection gives a short overview over results of Denef and Lipshitz, who have shown that in general the decision whether a system has formal power series solutions is undecidable. In particular, this shows that it is impossible to count the number of formal power series solutions algorithmically in general.

Theorem 2.98 ([DL84, 4.11])**.** *Let $n \geq 9$. There does not exist an algorithm to decide the following: Does a single partial differential equation with variable coefficients for one unknown function u given as input have a formal power series solution in $\mathbb{C}[[y_1, \ldots, y_n]]$.*

Proof. Consider $u = \sum_{\mathbf{i}\in\mathbb{Z}_{\geq 0}} a_{\mathbf{i}} \cdot y_1^{i_1} \ldots y_n^{i_n} \in \mathbb{C}[[y_1, \ldots, y_n]]$ for solutions of the following differential equations. For each $p \in \mathbb{Z}[z_1, \ldots, z_n]$ use the Euler operator to get

$$p(y_1\partial_1, \ldots, y_n\partial_n)u = \sum_{\mathbf{i}\in\mathbb{Z}_{\geq 0}} p(i_1, \ldots, i_n) \cdot a_{\mathbf{i}} \cdot y_1^{i_1} \ldots y_n^{i_n} \ .$$

Thus, the differential equation

$$p(y_1\partial_1, \ldots, y_n\partial_n)u = \sum_{\mathbf{i}\in\mathbb{Z}_{\geq 0}} 1 \cdot y_1^{i_1} \ldots y_n^{i_n}$$

has a solution if and only if $a_{\mathbf{i}}$ can be chosen as $p(i_1, \ldots, i_n)^{-1}$ for all $\mathbf{i} \in \mathbb{Z}_{\geq 0}^n$. This is possible if and only if the Diophantine equation $p(i_1, \ldots, i_n)$ has no natural solution $\mathbf{i} \in \mathbb{Z}_{\geq 0}^n$. The latter problem is undecidable for $n \geq 9$ [Mat77]. □

Theorem 2.99. *There exists a system of linear partial differential equations over $\mathbb{C}(y_1, \ldots, y_n)\{u\}$ having a formal power series solution in $\mathbb{Q}[[y_1, \ldots, y_n]]$, but no computable power series solution*[17]*.*

Again, in the proof (cf. [DL84, 4.12]) the Euler operator $p(y_1\partial_1, \ldots, y_n\partial_n)$ is used to get polynomials in integers as coefficients in power series.

For other solution sets there exist algorithms. For example in [GS91] a set of generalized formal power series is introduced, i.e. formal power series with real exponents such that the exponents converge to $-\infty$. It is possible to count the number of these solutions up to some "order" such that these solutions extend to all orders, using a Newton polygon method. For systems of ordinary differential equations in $\mathbb{Q}[t]\{U\}$ there exists an algorithm to decide whether such a system has a formal power series solution in $\mathbb{C}[[t]]$ or $\mathbb{R}[[t]]$ [DL84, Theorem 3.1]. However, this algorithm does not seem to be capable of counting the number of solutions. This is due to showing that any regular point in an irreducible variety leads to a solution and leaving the question open for singular points.

[17] I.e., no formal power series solution $u = \sum_{\mathbf{i}\in\mathbb{Z}_{\geq 0}} a_{\mathbf{i}} \cdot y_1^{i_1} \ldots y_n^{i_n}$ exists such that there is a recursive function $f : \mathbb{Z}_{\geq 0}^n \to \mathbb{Q}$ with $f(\mathbf{i}) = a_{\mathbf{i}}$.

Appendix A

Differential Elimination

> My aim in this is to show that the celestial machine is to be likened not to a divine organism but rather to a clockwork [...], insofar as nearly all the manifold movements are carried out by means of a single, quite simple magnetic force [...].
>
> Johannes Kepler
> in a letter to Herwart von Hohenburg, as quoted in [MAKA09]

> I now demonstrate the frame of the System of the World.
>
> Sir Isaac Newton
> in Principia ("De mundi systemate"), translation [NM03]

> Kepler and Newton represent a critical transition in human history, the discovery that fairly simple mathematical laws pervade all of Nature; that the same rules apply on Earth as in the skies; and that there is a resonance between the way we think and the way the world works.
>
> Carl Sagan
> in [Sag80]

This appendix treats differential elimination theory and uses the Thomas decomposition as algorithmic tool. The case of elimination for ordinary differential equations has been treated first in [Rit50, Chapter V] and was extended to the case of partial differential equations in [Sei56]. Both these approaches give a characteristic set of the elimination ideal and are algorithmic in the sense that they give the reduction as decision method whether a polynomial lies in that ideal. By a change of ranking, the elimination usually can be speeded up [BLMM10]. Elimination has many applications; among them is system theory, which is sketched below. Other applications lie in automatic theorem proving (see [Wan95] and the references therein) and in biology and chemistry (see [BLLM11] and the references therein). This appendix applies the implementation of the THOMAS decomposition to elimination. Therefore, it uses results about elimination ideals from [Rob12]. The disjointness of the THOMAS decomposition allows additional applications than the previously mentioned classical approaches to elimination.

Let F be a differential field of characteristic zero, $\Delta = \{\partial_1, \dots, \partial_n\}$ a non-empty set of derivation operators, and $U = \{u^{(1)}, \dots, u^{(m)}\}$ a non-empty set of differential indeterminates.

Elimination uses block rankings and elimination rankings (cf. Subsection 1.2.3). Fix a block ranking $B_1 \ll \dots \ll B_k$ for a partition $U = \biguplus_{i=1}^{k} B_i$ of the set of differential indeterminates. If $B_1, \dots, B_i \subseteq U$, write $F\{B_1, \dots, B_i\}$ for the differential polynomial ring $F\{\bigcup_{i=1}^{k} B_i\}$. Let $B \subseteq U$ and I a differential ideal in $F\{U\}$. Then $I \cap F\{B\}$ is called the **elimination ideal** of I with respect to B. The next statements show how to compute elimination ideals.

Proposition A.1 ([Rob12, 3.1.36]). *Let S be a simple differential system over $F\{U\}$ with respect to a block ranking $B_1 \ll \dots \ll B_k$ and $1 \le i \le k$. Then*

$$\mathcal{I}(S) \cap F\{B_1, \dots, B_i\} = \mathcal{I}_{F\{B_1,\dots,B_i\}}\left(S \cap F\{B_1, \dots, B_i\}^{\{=,\neq\}}\right) .$$

Corollary A.2 ([Rob12, 3.1.37]). *Let S be a (not necessarily simple) differential system over $F\{U\}$, and let $S_1, \dots, S_\ell$ be a THOMAS decomposition of S with respect to a block ranking $B_1 \ll \dots \ll B_k$. Then for every $1 \le i \le k$*

$$\mathcal{I}(S) \cap F\{B_1, \dots, B_i\} = \bigcap_{j=1}^{\ell} \mathcal{I}_{F\{B_1,\dots,B_i\}}\left(S_j \cap F\{B_1, \dots, B_i\}^{\{=,\neq\}}\right) .$$

Eliminations ideals can also be computed using characteristic set methods or the ROSENFELD-GRÖBNER algorithm. The THOMAS decomposition sets itself apart since simple differential system describe the projected solution set and not its KOLCHIN closure. Recall the definition of the set $E := \overline{F}[[z_1, \dots, z_n]]^U$ of non-centered solutions from Subsection 1.2.4. Denote the restricted non-centered solution set by

$$E^{(i)} := \overline{F}[[z_1, \dots, z_n]]^{\bigcup_{j=1}^{i} B_i} ,$$

in particular $E^{(k)} = E$. For differential systems S in $F\{B_1, \dots, B_i\}$ denote the solution set in $E^{(i)}$ by $\mathfrak{Sol}_{E^{(i)}}(S)$.

Remark 1.10 implies the property for any simple differential system S over $F\{U\}$ with respect to a block ranking. For all $1 \le i \le j \le k$

$$\mathrm{re}_{j,i}(\mathfrak{Sol}_{E^{(j)}}(S)) = \mathfrak{Sol}_{E^{(i)}}(S \cap F\{B_1, \dots, B_i\}) ,$$

where $\mathrm{re}_{j,i}$ denotes the restriction of $E^{(j)}$ to $E^{(i)}$.

As a demonstration, these elimination methods allow a comparison of the laws of planetary motions from KEPLER and NEWTON. Similar but less detailed computations in [Wu91] and [Wan95, §5, Example2] show that these laws are generically equivalent. The THOMAS decomposition gives a more detailed description due to its disjointness. In particular, this example shows that the solutions of KEPLER's laws are a subset of the solutions of NEWTON's laws, and that the complements of the solutions of KEPLER's laws in the solutions of NEWTON's laws consist of parabolas (and complex solutions).

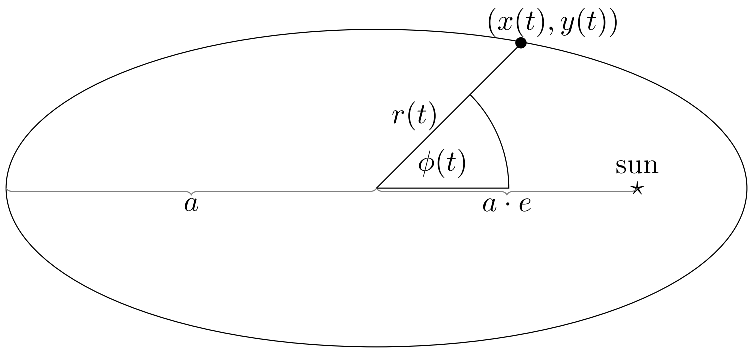
Example A.3. The laws of planetary motion by KEPLER are:

- Each planet describes an ellipse with the sun at one focus.
- The radius vector from the sun to a planet sweeps out equal area in equal time.

Newton derived the following laws:

- The acceleration of any planet is inversely proportional to the square of the distance from the sun to the planet.
- The acceleration vector of any planet is directed to the sun.

This example considers the motion of a planet around the sun. Assign the coordinates $(0,0)$ to the sun. The planet has the coordinates $x(t)$, $y(t)$ in dependence of the time t. However, the computations are easier in polar coordinates $r(t) = \sqrt{(x(t))^2 + (y(t))^2}$ and $\phi(t) = \arctan\left(\frac{y(t)}{x(t)}\right)$. Note that $x(t) = r\cos(\phi(t))$ and $y(t) = r\sin(\phi(t))$.



First we show how to derive differential equations for movement on an ellipse with eccentricity e, semimajor axis a, and where $\phi(t) = 0$ in the perihelion. The relation between r and ϕ is given by $r(t) = \frac{a(-e^2+1)}{1+e\cos(\phi(t))}$. Remark 1.43 and Remark 1.2 allow to model this equation with $U = \{a, cosphi, e, \phi, r, sinphi\}$ with the extra relations $cosphi^2 + sinphi^2 = 1$, $\partial_t cosphi = -sinphi \cdot \partial_t\phi$, $\partial_t sinphi = cosphi \cdot \partial_t\phi$, $\partial_t a = 0$, $\partial_t e = 0$.

```
restart;
with(DifferentialThomas):
L:=[
   r[0]*(1+e[0]*cosphi[0])-a[0]*(1-e[0]^2),
   cosphi[0]^2+sinphi[0]^2-1,
   cosphi[1]+sinphi[0]*phi[1],
   sinphi[1]-cosphi[0]*phi[1],
   a[1],e[1]
]:
```

For the exclusion of the trivial cases where both celestial bodies are at the same spot we add $r \neq 0$, and to prevent that the orbital speed is zero we add $\partial_t\phi \neq 0$. The following two procedures extract the equations and inequations only involving r and ϕ from a system.

```
Projection_r_phi_equations:=proc(system)
   return remove(
      b->has(b,a) or has(b,cosphi) or has(b,p)
                        or has(b,e) or has(b,sinphi),
      DifferentialSystemEquations(system)
   ):
end proc:
```

```
Projection_r_phi_inequations:=proc(system)
   return remove(
      b->has(b,a) or has(b,cosphi) or has(b,p)
                  or has(b,e) or has(b,sinphi),
      DifferentialSystemInequations(system)
   ):
end proc:
```

A block ranking with $a, e, cosphi, sinphi \gg r, \phi$ yields the relations between r and ϕ.

```
ivar:=[t]:
dvar:=[[a,e,cosphi,sinphi],[r,phi]]:
ComputeRanking(ivar,dvar):
res_K1:=DifferentialThomasDecomposition(L,[r[0],phi[1]]);
```

$$res\_K1 := [DifferentialSystem, DifferentialSystem]$$

The second system describes the case when the ellipse is a circle, as restricting to r and ϕ yields a constant radius.

```
K1_2:=Projection_r_phi_equations(res_K1[2]):
K1_2_Ineq:=Projection_r_phi_inequations(res_K1[2]):
[op(map(a->a=0,JetList2Diff(K1_2))),
op(map(a->a<>0,JetList2Diff(K1_2_Ineq)))];
```

$$[\tfrac{d}{dt}r(t) = 0, r(t) \neq 0, \tfrac{d}{dt}\phi(t) \neq 0]$$

The first system descibes the generic case of an ellipse that is not a circle.

```
K1_1:=Projection_r_phi_equations(res_K1[1]):
K1_1_Ineq:=Projection_r_phi_inequations(res_K1[1]):
res_K1:=[
   op(DifferentialThomasDecomposition(K1_1,K1_1_Ineq)),
   op(DifferentialThomasDecomposition(K1_2,K1_2_Ineq))];
```

$$res\_K1 := [DifferentialSystem, DifferentialSystem]$$

The second law of KEPLER yields $\partial_t\left(r^2\partial_t\phi\right) = 0$ (cf. [NS92, A.3.3.12]).

```
K2:=PartialDerivative(r[0]^2*phi[1],t);
```

$$K2 := 2\, r_1\phi_1 r_0 + \phi_2 {r_0}^2$$

Consider NEWTON's laws. They imply that the acceleration of the planet is given by $\sqrt{\left(\partial_t^2 x\right)^2 + \left(\partial_t y\right)^2} = \sqrt{\left(\partial_t^2\left(r\ cosphi\right)\right)^2 + \left(\partial_t^2\left(r\ sinphi\right)\right)^2}$ and that multiplication by r^2 yields a constant. Thus, $r^4 \cdot \left((\partial_t^2(r\,cosphi))^2 + (\partial_t^2(r\,sinphi))^2\right)$ is constant, as the square of a constant is again constant. A value is a constant if its derivative is zero, and this yields $\partial_t^2\left(r^4 \cdot \left((\partial_t^2(r\,cosphi))^2 + (\partial_t^2(r\,sinphi))^2\right)\right) = 0$. Again, eliminate *cosphi* and *sinphi* from this equation and exclude trivial cases where $r = 0$, $\partial_t\phi = 0$ and the acceleration is zero.

```
ivar:=[t]:
dvar:=[[cosphi,sinphi],[r,phi]]:
ComputeRanking(ivar,dvar):
L:=[
   PartialDerivative(
      r[0]^4*(PartialDerivative(r[0]*cosphi[0],t,t)^2
      +PartialDerivative(r[0]*sinphi[0],t,t)^2),t),
   cosphi[0]^2+sinphi[0]^2-1,
   cosphi[1]+sinphi[0]*phi[1],
   sinphi[1]-cosphi[0]*phi[1]
]:
res_N1:=DifferentialThomasDecomposition(L,[r[0],phi[1],
   PartialDerivative(r[0]*cosphi[0],t,t)^2
   +PartialDerivative(r[0]*sinphi[0],t,t)^2]);
```

$$res\_N1 := [DifferentialSystem, DifferentialSystem, DifferentialSystem]$$

This yields three systems for NEWTON's first law.

```
N1_1:=Projection_r_phi_equations(res_N1[1]):
N1_1_Ineq:=Projection_r_phi_inequations(res_N1[1]):
N1_2:=Projection_r_phi_equations(res_N1[2]):
N1_2_Ineq:=Projection_r_phi_inequations(res_N1[2]):
N1_3:=Projection_r_phi_equations(res_N1[3]):
N1_3_Ineq:=Projection_r_phi_inequations(res_N1[3]):
```

The second law of NEWTON states that the acceleration orthogonal to the line through sun and planet is zero, i.e., $\partial_t (x\partial_t y - y\partial_t x) = 0$ holds. An easy calculation using the relation $x(t) = r(t)\cos(\phi(t))$ shows that this condition is equivalent to KEPLER's second law $\partial_t \left(r^2 \partial_t \phi\right) = 0$.

```
N2:=K2;
```

$$N2 := 2\, r_1 \phi_1 r_0 + \phi_2 {r_0}^2$$

Compute the systems that intersect the sets of solutions of the first and second law of KEPLER

```
dvar2:=[r,phi]:
ComputeRanking(ivar,dvar2);
res_K:=map(RemoveSuperfluousInequations,
   [op(DifferentialThomasDecomposition([op(K1_1),K2],K1_1_Ineq)),
    op(DifferentialThomasDecomposition([op(K1_2),K2],K1_2_Ineq))]);
```

$$res\_K := [DifferentialSystem, DifferentialSystem]$$

and of the first and second law of NEWTON.

```
res_N:=[
   op(DifferentialThomasDecomposition([op(N1_1),N2],N1_1_Ineq)),
   op(DifferentialThomasDecomposition([op(N1_2),N2],N1_2_Ineq)),
   op(DifferentialThomasDecomposition([op(N1_3),N2],N1_3_Ineq))];
```

$$res\_N := [DifferentialSystem]$$

The intersection of the solutions of KEPLER's laws and NEWTON's laws is equal to KEPLER's laws.

```
res_Intersect:=IntersectDecompositions(res_K,res_N);
```

$$res\_Intersect := [DifferentialSystem, DifferentialSystem]$$

```
evalb(
   DifferentialSystemEquations(res_K[1])
   =DifferentialSystemEquations(res_Intersect[1])),
evalb(
   DifferentialSystemInequations(res_K[1])
   =DifferentialSystemInequations(res_Intersect[1]));
```

$$true, true$$

```
evalb(
   DifferentialSystemEquations(res_K[2])
   =DifferentialSystemEquations(res_Intersect[2])),
evalb(
   DifferentialSystemInequations(res_K[2])
   =DifferentialSystemInequations(res_Intersect[2]));
```

$$true, true$$

Consider trajectories which are solutions to NEWTON's laws and not to KEPLER's laws. Compute a decomposition of this set of solutions.

```
ComplementOfDecomposition(res_K):
res_N_minus_K:=IntersectDecompositions(%,res_N);
```

$$res\_N\_minus\_K := [DifferentialSystem, DifferentialSystem]$$

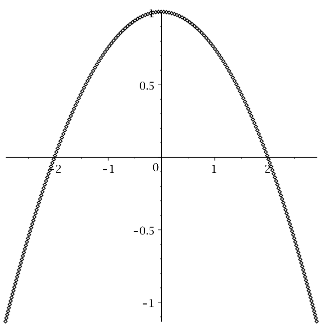
The second of these systems is physically not feasible, as solving $\phi(t)$ for $r(t)$ yields purely imaginary angles $\phi(t)$.

```
ComputeRanking([t],[[phi],[r]]);
res2:=DifferentialThomasDecomposition(
   DifferentialSystemEquations(res_N_minus_K[2]),
   DifferentialSystemInequations(res_N_minus_K[2])):
solve(
   JetList2Diff(DifferentialSystemEquations(res2[1])[1]),
   diff(phi(t),t));
```

$$\frac{i\frac{d^2}{dt^2}r(t)}{\frac{d}{dt}r(t)}, \frac{-i\frac{d^2}{dt^2}r(t)}{\frac{d}{dt}r(t)}$$

Some numerical solutions of the first systems lead one to belief that its solution set of the first of these systems consists of parabolas.

```
lsg:=dsolve(
   [op(JetList2Diff(DifferentialSystemEquations(res_N_minus_K[1])))
   ,phi(0)=0,D(phi)(0)=1,r(0)=1,D(r)(0)=0]
   ,numeric):
plots[pointplot](
   map(a->[sin(a[1])*a[2],cos(a[1])*a[2]],
   map(t->[rhs(lsg(t/20)[2]),rhs(lsg(t/20)[4])],[$-100..100])));
```



All parabolas are characterized by the equation $r(t)\,(1+\cos(\phi(t)))-p=0$ for a constant p (cf. [NS92, A.3.2.29]).

```
L:=[
   r[0]*(1+cosphi[0])-p[0],
   cosphi[0]^2+sinphi[0]^2-1,
   cosphi[1]+sinphi[0]*phi[1],
   sinphi[1]-cosphi[0]*phi[1],
   p[1]
]:
dvar:=[[cosphi,sinphi,p],[r,phi]]:
ComputeRanking(ivar,dvar):
res_P:=DifferentialThomasDecomposition(L,[phi[1],r[0]]);
```

$$res\_P := [DifferentialSystem]$$

```
P:=Projection_r_phi_equations(res_P[1]):
P_Ineq:=Projection_r_phi_inequations(res_P[1]):
```

The following system has all solutions from Newton that are parabolas and not solutions from Kepler.

```
dvar:=[r,phi]:
ComputeRanking(ivar,dvar):
res_P:=map(RemoveSuperfluousInequations,
   DifferentialThomasDecomposition(P,P_Ineq)):
```

```
res_P_intersect_N_minus_K
   :=IntersectDecompositions(res_P,res_N_minus_K);
```

$$res\_P\_intersect\_N\_minus\_K := [DifferentialSystem]$$

All physically possible solutions from NEWTON that were not solutions from KEPLER are parabolas.

```
evalb(
   DifferentialSystemEquations(res_P_intersect_N_minus_K[1])
   =DifferentialSystemEquations(res_N_minus_K[1])),
evalb(DifferentialSystemInequations(
   res_P_intersect_N_minus_K[1])
   =DifferentialSystemInequations(res_N_minus_K[1]));
```

$$true, true$$

This shows that all solutions of the first system of the equations that satisfied NEWTON's laws but not KEPLER's laws are parabolas. Furthermore, none of KEPLER's solutions is a parabola. This is not clear in advance, as the parabolas might safisfy the differential equations for ellipses.

```
IntersectDecompositions(res_K,res_P);
```

$$[]$$

To summarize this example, the equations of NEWTON imply those of KEPLER, but have the parabolas (and complex solutions) that do not occur in KEPLER's laws. Furthermore, KEPLER's equations also have hyperbolas as solutions, since hyperbolas share their characterizing differential equations with the ellipses. ◁

Now, we demonstrate elimination on examples in system theory, in particular how to determine whether indeterminates are observable or flat output. Therefore, we adapt well-known concepts of nonlinear control theory to the framework of the differential THOMAS decomposition and demonstrates them on an example. This is joint work with DANIEL ROBERTZ and published in [LHR13].

Differential algebra was first used for control theory in [Fli89] and brought into an algorithmic form in [Dio91, Dio92]. For a modern treatment, including the notion of flatness, see [LHR13, Gla90, Dio92, FG93, FLMR95, Pom01] and the references therein.

Assume that a (nonlinear) control system is given by a differential system S over $F\{U\}$. As usual, we make no a priori distinction between input, output, state variables, etc. Let $x \in U$ and $Y \subseteq U \setminus \{x\}$. Then x is **observable with respect to** Y in S if there exists $p \in \mathcal{I}(S) \setminus \{0\}$ such that $p \in F\{Y\}[x]$ is a polynomial in x (not involving any proper derivative of x) with coefficients in $F\{Y\}$ such that neither its leading coefficient nor $\frac{\partial p}{\partial x}$ is contained in $\mathcal{I}(S)$. Corollary A.2 implies a method to decide observability for certain *simple* differential systems.

Corollary A.4. *Let $x \in U$ and $Y \subseteq U \setminus \{x\}$ and let S be simple with respect to a block ranking satisfying $U \setminus (Y \cup \{x\}) \gg \{x\} \gg Y$. Then x is observable with respect to Y in S if and only if $S^= \cap F\{Y\}[x] \neq \emptyset$. If these two equivalent statements hold, then the p from the definition can be taken as the unique $p \in S^= \cap F\{Y\}[x]$ with $\mathrm{ld}(p) = x$.*

Let $Y \subseteq U$. Then Y is called a **flat output** of S if $\mathcal{I}(S) \cap F\{Y\} = \{0\}$, and every $x \in U \setminus Y$ is observable with respect to Y. The control system given by S is said to be **flat** if a flat output exists. Deciding whether a given nonlinear control system is flat is a difficult problem in general. However, flatness of a subset of the differential indeterminates is decidable by Corollary A.2:

Corollary A.5. *Let $Y \subseteq U$, and let S be simple with respect to a block ranking satisfying $(U \setminus Y) \gg Y$. Then Y is a flat output of S if and only if $S^= \cap F\{Y\} = \emptyset$, and the order of the leader of each equation in $S^=$ is zero.*

More generally, if S is not simple, the computation of a differential THOMAS decomposition of S with respect to a block ranking satisfying $U \setminus Y \gg Y$ might allow to decide whether Y is a flat output. Then Y is a flat output of S if (but not necessarily "only if") it is a flat output of every system S_i of a THOMAS decomposition of S.

Example A.6. Consider the model of a continuous stirred-tank reactor taken from [KS72]. This model describes a tank with a material, dissolved of concentration c. Due to stirring, assume this concentration to be constant everywhere in the tank. Two input feeds with flow rates F_1 and F_2 feed this material into the tank with constant concentrations c_1 and c_2, respectively. There exists an outward flow with a flow rate proportional to the square root of the volume V of liquid in the tank. The system is modeled by the following two differential equations for an experimental constant k

$$\dot{V}(t) = F_1(t) + F_2(t) - k\sqrt{V(t)}$$
$$\overset{\cdot}{\overline{c(t)\,V(t)}} = c_1\,F_1(t) + c_2\,F_2(t) - c(t)\,k\sqrt{V(t)}\ .$$

The properties of the system depend on the constants c_1 and c_2. To allow case distinctions for these constants use Remark 1.2 and model these constants as functions $c_1(t)$ and $c_2(t)$ satisfying $\dot{c}_1(t) = 0$ and $\dot{c}_2(t) = 0$. We introduce a new differential indeterminate for the square root $\sqrt{V(t)}$, and substitute $V(t)$ by $\sqrt{V(t)}^2$ following Remark 1.43. We assume $c_1(t) \neq 0$, $c_2(t) \neq 0$, and $V(t) \neq 0$ to exclude trivial cases. Compute a THOMAS decomposition of the system using a ranking with $\{F_1, F_2\} \gg \{\sqrt{V}, c\} \gg \{c_1, c_2\}$.

```
ivar:=[t]:
dvar:=[[F1,F2],[sV,c],[c1,c2]]:
ComputeRanking(ivar,dvar);
L:=[ 2*sV[1]*sV[0]-F1[0]-F2[0]+k*sV[0],
     c[1]*sV[0]^2-c2[0]*F2[0]+c[0]*k*sV[0]
      -c1[0]*F1[0]+2*c[0]*sV[1]*sV[0],
     c1[1], c2[1]]:
res:=DifferentialThomasDecomposition(L,[sV[0],c1[0],c2[0]]);
```

$$res := [\mathit{DifferentialSystem}, \mathit{DifferentialSystem}, \mathit{DifferentialSystem}]$$

The decomposition consists of three simple differential systems. Print the first one.

```
subs(sV(t)=sqrt(V(t)),PrettyPrintDifferentialSystem(res[1]));
```

$$\Big[\ (c_2(t) - c_1(t))\,\underline{F_1(t)} + \left(\frac{d}{dt}c(t)\right)\left(\sqrt{V(t)}\right)^2 + (c(t) - c_2(t))\left(2\,\frac{d}{dt}\sqrt{V(t)} + k\right)\sqrt{V(t)} = 0, \tag{A.1}$$

$$(c_1(t) - c_2(t))\,\underline{F_2(t)} + \left(\frac{d}{dt}c(t)\right)\left(\sqrt{V(t)}\right)^2 + (c(t) - c_1(t))\left(2\,\frac{d}{dt}\sqrt{V(t)} + k\right)\sqrt{V(t)} = 0, \tag{A.2}$$

$$\underline{\frac{d}{dt}c_1(t)} = 0,\ \underline{\frac{d}{dt}c_2(t)} = 0, \tag{A.3}$$

$$\sqrt{V(t)} \neq 0,\ c_1(t) - c_2(t) \neq 0.$$

$$c_2(t) \neq 0,\ c_1(t) \neq 0\ \Big]$$

The equations (A.1) and (A.2) allow to solve for $F_1(t)$ and $F_2(t)$ given any $c(t)$ and $V(t)$. Thus, consider $c(t)$ and $V(t)$ a flat output of the system under the additional condition $c_1 - c_2 \neq 0$ on the constants. Note that the two equations $\dot{c}_1(t) = 0$ and $\dot{c}_2(t) = 0$ in (A.3) just model the parameters c_1 and c_2 as constants.

The other two systems of this decomposition include the condition $c_1 = c_2$. This condition prohibits to control the concentration in the tank as both input feeds are equivalent. In particular, these systems do not admit $c(t)$ and $V(t)$ as a flat output.

For the observability of $\sqrt{V(t)}$ we choose a ranking with $\{\sqrt{V}\} \gg \{c, F_1, F_2\} \gg \{c_1, c_2\}$. A Thomas decomposition with this ranking consists of seven systems:

```
ivar:=[t]:
dvar:=[[sV],[c,F1,F2],[c1,c2]]:
ComputeRanking(ivar,dvar);
res:=DifferentialThomasDecomposition(L,[sV[0],c1[0],c2[0]]);
```

$res := [DifferentialSystem, DifferentialSystem, DifferentialSystem,$
$DifferentialSystem, DifferentialSystem, DifferentialSystem, DifferentialSystem]$

In the first two systems an equation with $\sqrt{V(t)}$ as leader appears, and thus $\sqrt{V(t)}$ is observable. For the first system the condition on the parameters for observability is

$$(c(t) - c_1)F_1(t) + (c(t) - c_2)F_2(t) \neq 0.$$

The second system is not physically feasible as it involves negative input feeds due to $F_2(t) \neq 0$ and $F_1(t) = -F_2(t)$.

The other five systems include an equation with $\frac{d}{dt}\sqrt{V(t)}$ as leader and thus $\sqrt{V(t)}$ is not observable: In the second system the concentrations $c(t)$, c_1, and c_2 are equal and constant. In the third system one input feed is zero and the concentration in the tank is equal to the concentration in the other input feed. The remaining two systems are not physically feasible due to negative values. $\triangleleft$

Appendix B

JANET Decomposition of the Complement

Let $\Delta = \{\partial_1, \ldots, \partial_n\}$ and $U = \{u^{(1)}, \ldots, u^{(m)}\}$ be non-empty sets of derivation operators and differential indeterminates, respectively.

Similar to the JANET decomposition of a set of differential variables closed under the action of Δ, the complement of such a set allows a decomposition into cones.

Algorithm B.1 (JanetComplement).
Input: A finite set $W \subset \{U\}_\Delta$ of differential variables, a set $\Delta' \subseteq \Delta$ of the derivations, and a set $V \subset \{U\}_\Delta$ satisfying $\{W\}_{\Delta'} \subseteq \{V\}_{\Delta'}$ and $\{v\}_{\Delta'} \cap \{v'\}_{\Delta'} = \emptyset$ for all distinct $v, v' \in V$.
Output: A cone decomposition of $\{V\}_{\Delta'} \setminus \{W\}_{\Delta'}$.
Algorithm: The algorithm is printed on page 162.

If JanetComplement is applied to (W, Δ, U), then it results in a cone decomposition of $\{U\}_\Delta \setminus \{W\}_\Delta$, i.e. the complement of the set $\{W\}_\Delta$ in $\{U\}_\Delta$.

Proof. The termination of JanetComplement is clear, since each recursive call diminishes the set of derivations by one.

It is easy to see in lines 3 and 18 that the input of JanetComplement satisfies the input specifications.

The cone decomposition can be done independently for all cones $\{v\}_{\Delta'}$, $v \in V$. This implies correctness of line 3.

The base case of the recursion in line 12 is trivially correct since $v \in W$ by the input specification $\{W\}_{\Delta'} \subset \{V\}_{\Delta'}$.

For the correctness of the recursion in line 18 in connection with the replacement in line 20 show disjointness and that the resulting cones yield $\{v\}_{\Delta'} \setminus \{W\}_{\Delta'}$. Assume inductively that JanetComplement is correct for any input with second argument of cardinality smaller than $|\Delta'|$. The cones in $\bigcup_{i=0}^{d} C_i$ in line 18 are mutually disjoint. First, they are disjoint in each C_i by induction hypothesis, and second, the apexes of the cones of different C_i have different order in ∂_k and no cone has ∂_k as reductive prolongation. The replacement in line 20 does not change the disjointness of the cones since only ∂_k is added as reductive prolongation to the cones with highest order in ∂_k, i.e. the ones in C_d. At last, the cones in C_i form a partition of

$$\overline{C_i} := \left\{\partial_k^{i-e} v\right\}_{(\Delta' \setminus \{\partial_k\})} \setminus \left\{ \bigcup_{j=e}^{i} \left\{ \partial_k^{i-j} w \,\middle|\, w \in W, \operatorname{ord}_k w = j \right\} \right\}_{(\Delta' \setminus \{\partial_k\})}$$

Algorithm B.1 (JanetComplement)

1: **if** $|V| > 1$ **then**
2:     // *Consider base variables in V independently*
3:     **return** $\bigcup_{v \in V} \mathsf{JanetComplement}(\{w \in W | w \in \{v\}_{\Delta'}\}, \Delta', \{v\})$
4: **end if**
5: **if** $|V| = 0$ **then**
6:     **return** $\emptyset$
7: **end if**
8: Let v be the unique element in V
9: **if** $W = \emptyset$ **then**
10:     **return** $\{(v, \Delta')\}$ // *The complement equals the full cone*
11: **else if** $|\Delta'| = 0$ **then**
12:     **return** $\emptyset$ // *Base case of the recursion: $W = \{v\}$*
13: **else**
14:     Let k be the unique element in $\{\, i \,|\, \partial_i \in \Delta', i \geq j \ \forall \partial_j \in \Delta' \,\}$
15:     $d \leftarrow \max\{\operatorname{ord}_k w \,|\, w \in W\}$
16:     $e \leftarrow \operatorname{ord}_k v$
17:     **for** $i = e, \ldots, d$ **do**
18:         $C_i \leftarrow \mathsf{JanetComplement}\left(\bigcup_{j=e}^{i} \left\{ \partial_k^{i-j} w \,\middle|\, w \in W, \operatorname{ord}_k w = j \right\}, \Delta' \setminus \{\partial_k\}, \{\partial_k^{i-e} v\} \right)$
19:     **end for**
20:     Replace each $(c, \Delta'') \in C_d$ with $(c, \Delta'' \cup \{\partial_k\})$
21:     **return** $\bigcup_{i=0}^{d} C_i$
22: **end if**

after line 18 by induction hypothesis. By construction $\bigcup_{i=e}^{d} \overline{C_i}$ is the set $(\{v\}_{\Delta'} \setminus \{W\}_{\Delta'})$ intersected with the set of $\left\{ u_{\mathbf{i}}^{(j)} \in \{U\}_\Delta \,\middle|\, \mathbf{i}_k \leq d \right\}$. The replacement in line 20 ensures

$$\{v\}_{\Delta'} \setminus \{W\}_{\Delta'} = \bigcup_{(c, \Delta'') \in \bigcup_{i=e}^{d} C_i} \{c\}_{\Delta''}$$

because

$$(\{v\}_{\Delta'} \setminus \{W\}_{\Delta'}) \cap \left\{ u_{\mathbf{i}}^{(j)} \in \{U\}_\Delta \,\middle|\, \mathbf{i}_k = l \right\} = \partial_k^{l-d} \left((\{v\}_{\Delta'} \setminus \{W\}_{\Delta'}) \cap \left\{ u_{\mathbf{i}}^{(j)} \in \{U\}_\Delta \,\middle|\, \mathbf{i}_k = d \right\} \right)$$

for $l > d$. □

Appendix C

Estimates for the Dimension Polynomial

Given a system of differential equations, there are some a-priori estimates on the differential dimension polynomial. This appendix gives a short overview over the literature. For a more detailed treatment and open problems see [KLMP99, Sections 5.6, 5.8].

Let F be a differential field of characteristic zero, $<$ an orderly ranking, $\Delta = \{\partial_1, \ldots, \partial_n\}$ be a non-empty set of derivation operators, and $U = \{u^{(1)}, \ldots, u^{(m)}\}$ be a non-empty set of differential indeterminates.

Proposition C.1 ([Rit32])**.** *Let $S = S^{=}$ be a system of ordinary differential equations over $U = \{u^{(1)}, \ldots, u^{(m)}\}$ such that S does not contain derivatives of $u^{(i)}$ of order greater than b_i for $1 \leq i \leq m$. Let S' be simple differential system in a* Thomas *decomposition of S with $\mathcal{I}(S')$ prime. If $\omega_{\mathcal{I}(S')}(\ell)$ is constant, then $\omega_{\mathcal{I}(S')}(\ell) \leq b_1 + \ldots + b_m$.*

Kolchin generalized Ritt's result to partial differential equations.

Theorem C.2 ([KLMP99, Theorem 5.6.5])**.** *Let $S = S^{=}$ be a system of differential equations over $U = \{u^{(1)}, \ldots, u^{(m)}\}$. Let $\partial \in \Delta$ and assume that S does not contain derivatives of $u^{(i)}$ of order in ∂ greater than b_i for $1 \leq i \leq m$. Let S' be a simple differential system in a* Thomas *decomposition of S with $\mathcal{I}(S')$ prime. If the differential type of $\omega_{\mathcal{I}(S')}(\ell)$ is $m-1$, then the typical dimension does not exceed $b_1 + \ldots + b_m$.*

The next theorem due to Johnson solves the Janet conjecture (cf. [Jan21]). However, it is conjectured that this theorem also holds for the nonlinear case.

Theorem C.3 ([Joh78])**.** *Let $S = S^{=}$ be a system of m* linear *differential equations over $U = \{u^{(1)}, \ldots, u^{(m)}\}$. Let S' be the simple differential system of a* Thomas *decomposition of S. If the differential type of $\omega_{\mathcal{I}(S')}(\ell)$ is less than $m-1$, then $\omega_{\mathcal{I}(S')}(\ell) = 0$, and there exists at most one solution of S.*

Theorem C.4 ([KLMP99, Theorem 5.6.7])**.** *Let $S = S^{=}$ be a system of* linear *differential equations over one differential indeterminate $U = \{u\}$ and $b_1 \geq b_2$ the two highest orders of equations in S. If the differential type of $\omega_{\mathcal{I}(S')}(\ell)$ is $m-2$, then the typical dimension does not exceed $b_1 b_2$.*

The Jacobi conjectures generalize Theorem C.2. It is conjectured that they are true without the extra assumptions.

Theorem C.5 (Weak Jacobi bound, [Jac09])**.** *Let $p_1, \ldots, p_m \in I$, where I is a differential prime ideal in $F\{u^{(1)}, \ldots, u^{(m)}\}$. Let $\omega_I(\ell) = \sum_{i=0}^{n} a_i \binom{\ell+i}{\ell}$ be the dimension* *polynomial of I and let $\gamma_{i,j}$ be the highest order of $u^{(i)}$ appearing in p_j or 0 if $u^{(i)}$ does not appear in p_j, $1 \leq i,j \leq m$. If $a_n = 0$, then*

$$a_{n-1} \leq \max_{\rho \in S_n} \sum_{i=1}^{n} \gamma_{i,\rho(i)} \ ,$$

under the extra assumption $n = |\Delta| = 1$ and all p_i are of main degree one and have initial 1.

Theorem C.6 (Strong Jacobi bound). *Let $p_1, \ldots, p_m \in I$, where I is a differential prime ideal in $F\{u^{(1)}, \ldots, u^{(m)}\}$. Let $\omega_I(\ell) = \sum_{i=0}^{n} a_i \binom{\ell+i}{\ell}$ be the dimension polynomial of I and let $\gamma_{i,j}$ be the highest order of $u^{(i)}$ appearing in p_j or $-\infty$ if $u^{(i)}$ does not appear in p_j, $1 \leq i,j \leq m$. If $a_n = 0$, then*

$$a_{n-1} \leq \max_{\rho \in S_n} \sum_{i=1}^{n} \gamma_{i,\rho(i)} \ ,$$

under any one of the extra assumptions:

(1) All p_i are linear ([Rit35]).

(2) $m = |U| \leq 2$ ([Rit35]).

(3) $n = |\Delta| = 1$ and all p_i are of order[1] 1 ([Lan70]).

(4) The p_i are independent over I ([KMP08], also for the definition of independent).

For the case of more equations than differential indeterminates see [Tom76], where the linear case and the case of $|U| \leq 2$ are solved.

[1]Every system is equivalent to a first order one; this equivalence might increase the bound.

Appendix D

Prime Decomposition

> [A] process is obtained which, if carried sufficiently far, will actually produce the irreducible systems. Unfortunately, there is nothing in this process which informs one, at any point, as to whether or not the process has had its desired effect.
>
> RITT
> in [Rit32, Introduction]

> [The problem] seems to be very far from a solution.
>
> KOLCHIN
> in [Kol73, §IV.9]

The proof of the differential dimension polynomial Section 1.7 includes statements about prime decompositions of radical algebraic and differential ideals. This appendix summarizes these results and complements them with some additional statements.

Theorem 1.94 implies that the associated primes of an ideal $\mathcal{I}(S)$ associated to a simple algebraic system S are equidimensional. Corollary 1.100 states that the indeterminates that do not show up as leaders of equations are a transcendence basis, and by Lemma D.3 below this transcendence basis satisfies a minimality condition, which is induces by the ranking. These results transfer to the differential case by Lemma 1.93.

Proposition 1.68 implies that $\mathcal{I}(S) = \bigcap_{i=1}^{k} \mathcal{I}(S_i)$ for both an algebraic or a differential THOMAS decomposition $S_1, \ldots, S_k$ of an algebraic[1] resp. differential system S. If S is simple, then a subset C of a THOMAS decomposition realizes this intersection by Proposition D.1 below. This subset is characterized by the leaders of the equations.

This appendix also summarizes results in the context of the RITT problem, which is a famous open problem in differential algebra: computing a minimal prime decomposition.

Let F be a field resp. differential field of characteristic zero and $R := F[y_1, \ldots, y_n]$ resp. $R := F\{U\}$ for a non-empty set of derivation operators $\Delta = \{\partial_1, \ldots, \partial_n\}$ and a non-empty set of differential indeterminates $U = \{u^{(1)}, \ldots, u^{(m)}\}$.

[1] This result is only cited for the differential case. The source proves it for both cases.

Proposition D.1. *Let S be a simple system and $S_1, \dots, S_k$ a* THOMAS *decomposition of $\mathcal{I}(S)$ or $\mathfrak{Sol}(S)$ resp. $\mathfrak{Sol}_E(S)$. Let $C := \{S_i \mid 1 \le i \le \ell, \mathrm{ld}(S_i^=) = \mathrm{ld}(S^=)\}$ and call the elements of C the* ***constituents*** *of the* THOMAS *decomposition $S_1, \dots, S_k$. Then,*

$$\mathcal{I}(S) = \bigcap_{S' \in C} \mathcal{I}(S') \ .$$

Furthermore, the sets of associated primes of the ideals in C are pairwise disjoint, and

$$\prod_{x \in \mathrm{ld}(S^=)} \deg_x(S_x) = \sum_{S' \in C} \prod_{x \in \mathrm{ld}(S^=)} \deg_x((S')_x) \ .$$

This proposition implies a sufficient criterion for algebraic and differential prime ideals: If S is a simple system with $\mathrm{mdeg}(p_=) = 1$ for all $p_= \in S^=$, then $\mathcal{I}(S)$ is prime.

The following lemma is used to prove Proposition D.1. It describes the splitting of one simple *algebraic* system into two systems and yields the necessary structural information about splitting an ideal associated to a simple algebraic system into two such ideals.

Lemma D.2. *Let S, S_1, S_2 be simple algebraic systems in $R = \overline{F}[y_1, \dots, y_n]$ with*

(i) $\mathcal{I}(S) = \mathcal{I}(S_1) \cap \mathcal{I}(S_2)$,

(ii) $\mathfrak{Sol}(S_1) \cap \mathfrak{Sol}(S_2) = \emptyset$, *and*

(iii) $X := \mathrm{ld}(S^=) = \mathrm{ld}(S_1^=) = \mathrm{ld}(S_2^=)$.

Then there exists an $x \in X$ with

(1) $\deg_x(S_x) = \deg_x((S_1)_x) + \deg_x((S_2)_x)$ *and*

(2) $\deg_z(S_z) = \deg_z((S_1)_z) = \deg_z((S_2)_z)$ *for all $z \in X \setminus \{x\}$.*

Proof. We prove in two steps that we can without loss of generality assume that $X = \{y_1, \dots, y_n\}$. First, using Lemma 2.61, we can assume without loss of generality that $\{y_1, \dots, y_n\} \setminus X < X$, as this process does not change the degrees of equations, the ideals, and disjointness. Second, we can replace $\overline{F}$ by the algebraic closure of $\overline{F}(\{y_1, \dots, y_n\} \setminus X)$ and remove the inequations from the simple algebraic systems. All associated primes have the set $\{y_1, \dots, y_n\} \setminus X$ as transcendence basis (cf. Corollary 1.100), and thus the images of these ideals in the localization are still associated primes.

This assumption implies that the ideals are zero-dimensional. Thus, the associated primes are in bijection to the set of solutions of the systems, and $\mathfrak{Sol}(S_1) \uplus \mathfrak{Sol}(S_2) = \mathfrak{Sol}(S)$. Furthermore, the rank of the locally free module $\overline{F}[y_1, \dots, y_n]/\mathcal{I}(S)$ over $\overline{F}[y_1, \dots, y_{n-1}]/\mathcal{I}(S_{<y_n})$ is the cardinality of the fibers of the projections $\pi_{n-1} : \overline{F}^n \to \overline{F}^{n-1}$ restricted to the set of solutions of $S_{<y_n}$.

There is a smallest ranking variable $x = y_k \in X$ with $\deg_x((S_1)_x) \neq \deg_x(S_x)$. Otherwise, $\mathfrak{Sol}(S) = \mathfrak{Sol}(S_1)$ by Proposition 2.10.(2), and thus $\mathfrak{Sol}(S_2) = \emptyset$, which contradicts the existence of solutions from Remark 1.10. By our assumption on X, $\mathcal{I}((S_1)_{<x}) = \mathcal{I}(S_{<x})$, as for indeterminates ranking lower than x there are equal degrees in both simple algebraic systems and thus equal algebraic counting polynomials. Furthermore, also $\deg_z((S_2)_z) = \deg_z(S_z)$ for all $z < x$ holds, as otherwise the fibers would not have equal cardinality. Thus, also $\mathcal{I}((S_2)_{<x}) = \mathcal{I}(S_{<x})$. For the fibers of the projection $\overline{F}^i \to \overline{F}^{i-1}$ to have the same cardinality, the equality $\deg_x(S_x) = \deg_x((S_1)_x) + \deg_x((S_2)_x)$ is necessary. This proves (1).

The proof of (2) is elementary. Let $a := \prod_{j=1}^{k-1} \deg_{y_j}(S_{y_j}) = \prod_{j=1}^{k-1} \deg_{y_j}((S_1)_{y_j}) = \prod_{j=1}^{k-1} \deg_{y_j}((S_2)_{y_j})$, $b^{(\ell)} := \prod_{j=k+1}^{\ell} \deg_{y_j}(S_{y_j})$, $b_i^{(\ell)} := \prod_{j=k+1}^{\ell} \deg_{y_j}((S_i)_{y_j})$, $d_i := \deg_x((S_i)_x)$, and $d := \deg_x(S_x) = d_1 + d_2$ for all $k < \ell \leq n$ and $1 \leq i \leq 2$. These values are all greater zero. Furthermore, $b^{(\ell)} \geq b_1^{(\ell)}, b_2^{(\ell)}$ for all $k < \ell \leq n$, as otherwise the fibers would not have equal cardinality. Then,

$$
\begin{aligned}
& & a b_1^{(\ell)} d_1 + a b_2^{(\ell)} d_2 &= a b^{(\ell)} d \\
&\Rightarrow & b_1^{(\ell)} d_1 + b_2^{(\ell)} d_2 &= b^{(\ell)} (d_1 + d_2) \\
&\Rightarrow & \underbrace{(b^{(\ell)} - b_1^{(\ell)})}_{\geq 0} \underbrace{d_1}_{>0} + \underbrace{(b^{(\ell)} - b_2^{(\ell)})}_{\geq 0} \underbrace{d_2}_{>0} &= 0 \\
&\Rightarrow & b_1^{(\ell)} = b_2^{(\ell)} &= b^{(\ell)} .
\end{aligned}
$$

In particular, $\deg_y(S_y) = \deg_y((S_1)_y) = \deg_y((S_2)_y)$ for all other $x < y = y_\ell \in X$. □

The following lemma gives a minimality condition for the transcendence basis in Corollary 1.100. Consider the following partial order on subsets of cardinality k of the set of indeterminates induced by the ranking: Replacing an indeterminate by a higher ranking one makes a set larger.

Lemma D.3. *Let S be a simple algebraic system in $R := F[y_1, \ldots, y_n]$. The transcendence basis $\{y_1, \ldots, y_n\} \setminus \operatorname{ld}(S^=)$ from Corollary 1.100 is smaller (with respect to preceding partial order) than any transcendence basis consisting of indeterminates.*

Proof. Denote the transcendence basis $\{y_1, \ldots, y_n\} \setminus \operatorname{ld}(S^=)$ of $R/\mathcal{I}(S)$ by $\{w_1, \ldots, w_k\}$ with $w_i < w_j$ for $1 \leq i < j \leq k$. Assume that $W' := \{w_1, \ldots, w_{i-1}, w_i', w_{i+1}, \ldots, w_k\}$ is a further transcendence basis modulo $\mathcal{I}(S)$ for some variable $w_i' < w_i$. By Corollary 1.100, the ideal $\mathcal{I}(S_{\leq w_i})$ has transcendence basis $\{w_1, \ldots, w_j\}$ for some $j < i$. In particular, w_i' is algebraically dependent on $\{w_1, \ldots, w_j\}$ modulo $\mathcal{I}(S_{\leq w_i})$ and thus modulo $\mathcal{I}(S)$. This contradicts W' being a transcendence basis. □

Proof of Proposition D.1. Proposition 1.62 implies $\mathcal{I}(S) = \bigcap_{i=1}^{k} \mathcal{I}(S_i)$. Together, the equidimensionality of ideals associated to simple algebraic systems (cf. Theorem 1.94) and the minimality of this transcendence basis (cf. Lemma D.3) imply that all systems not in C are embedded components in this intersection. The pairwise disjointness of sets of associated primes follows from the disjointness of a Thomas decomposition, and the formulas about degrees follows from applying Lemma D.2 iteratively.

For the differential version use that any differential decomposition induces an algebraic decomposition of the simple algebraic system $S_{\leq \ell}$ up to order ℓ associated to S. And use Proposition 1.66, the differential variant of Proposition 1.62. □

Finding a minimal prime decomposition of a radical differential ideal is related to finding the singular solutions[2]. Now, we present structure theorems of Ritt about minimal prime decompositions of *one* differential equation. Then it formulates the still unsolved Ritt problem: algorithmically finding a minimal prime decomposition of a radical differential ideal.

Theorem D.4 (Component Theorem, [Rit45, §6], [Rit50, III.§1], [Kol73, IV.§14])**.** *Let $\langle p \rangle_\Delta \subset F\{U\}$ be a differential ideal generated by $p \in F\{U\} \setminus F$. All prime components of*

[2]Ritt gave the first formalized definition of singular solutions of differential equations (cf. [Rit30], [Rit32, II.§19], [Rit36], and [Rit50, II.§20]).

this ideal are given by differential ideals of the form $\langle q\rangle_\Delta : \mathrm{sep}(q)^\infty$ *for some* $q \in F\{U\}$. *If* p *is algebraically irreducible and of order at least one, then there is exactly one prime component of* $\langle p\rangle_\Delta$ *that does not contain* $\mathrm{sep}(p)$.

The solutions of the one prime component not containing $\mathrm{sep}(p)$ are called **general solutions**. The solutions of $\langle p\rangle_\Delta$ that vanish on all separants of p are called **singular solutions**. The non-singular solutions are a subset of the general solutions; in particular, there can be general solutions which are singular. Under the assumption of the Component Theorem, every component contains the general solutions of a single differential polynomial. From this, the Low Power Theorem gives a minimal decomposition of the solution set of a single differential polynomial into its prime components. This approach is algorithmic [Rit36, Hub99].

Theorem D.5 (Low Power Theorem, [Rit36, §5], [Lev45], [Rit50, III.§2], [Kol73, IV.§15])**.** *Let* $p \in F\{U\} \setminus F$, $q \in F\{U\}$, *and* $I := \langle p\rangle_\Delta \subset F\{U\}$. *Write*[3] $cp = r \in F\{q\}(:= F[\mathrm{Mon}(\Delta)q])$ *such that neither the coefficients of* r *nor* c *are contained in* $\langle q\rangle_\Delta : \mathrm{sep}(q)^\infty$. *The differential ideal* $\langle q\rangle_\Delta : \mathrm{sep}(q)^\infty$ *is a prime component of* I *if and only if there is a term* $c_\lambda q^\lambda$ *with* $c_\lambda \in F$ *free of proper derivatives of* q *having lower degree (considered as a polynomial in* $F\{q\}$*) than all other terms in* r.

For a field of complex meromorphic functions, there are theorems that relate the analytic behavior of a singular solution of a single algebraically irreducible differential equation to the relation of its component to the general component. The solutions of the general component that vanish on at least one separant are approximated as a limit[4] of general solutions that do not vanish on this separant. The singular solutions in separate components usually show a behavior enveloping the general solutions [Rit41, Rit46]; the author does not know of a general theorem in this direction.

Example D.6 ([Rit50, II.§4, II.§19])**.** Let $F = \mathbb{C}$, $U = \{u\}$ and $\Delta = \{\partial_t\}$. Consider the differential equations $p_1 := u_1^2 - 4u = 0$ and $p_2 = u_1^2 - 4u^3 = 0$. Both equations have the solutions of $u = 0$ as singular solutions. For the first equation p_1 the singular solutions are a separate component apart from the general solution, by the Low Power Theorem. The general solutions are the solutions of $\langle p_1\rangle_\Delta : u^\infty$ and contain no singular solutions. For the second equation p_2 the decomposition into prime components leads a single prime component by the Low Power Theorem, and thus the singular solutions are a subset of the general solutions. In particular, $\langle p_2\rangle_\Delta : u^\infty = \langle p_2\rangle_\Delta$. In the first example the singular solutions envelop the non-singular solutions. In contrast, in the second example the singular solution can be approximated locally by a non-singular solution. ◁

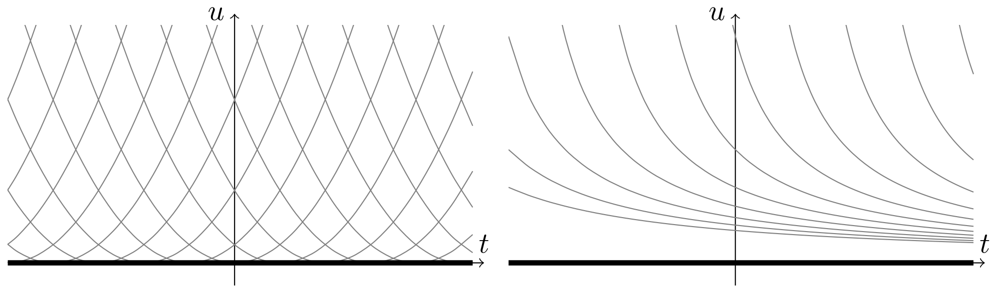
Studying singular solutions of systems with more differential equations is involved, and there is no comprehensive theory about the minimal prime decomposition of a radical differential ideal. Even though a prime decomposition is possible (cf. [Rit50, IX.§25] or [GKO08]), there is no known algorithmic way to detect inclusion of prime ideals. This problem is known as the Ritt problem and has several equivalent formulations.

Theorem D.7 ([GKO08])**.** *Assume that one can factorize univariate polynomials over the computable differential field* F. *The following algorithmic problem can be reduced to each other, i.e., an algorithm solution for one provides an algorithmic solution for all.*

[3]This representation, called preparation congruence, is in general not unique.

[4]this is made precise by the term "adherence" [Rit50, VI.§2] (cf. also [Rit32, IV.§64] and [Rit38b, IV])

Figure D.1: Solutions for p_1 (left) and p_2 (right) in Example D.6



(1) Given a characteristic set of a prime differential ideal, find a set of its generators.

(2) Given the characteristic sets of two prime differential ideals I_1 and I_2, determine whether $I_1 \subseteq I_2$.

(3) Compute a non-redundant *prime decomposition of a radical ideal.*

(4) Given a radical differential ideal by a set of generators, decide whether it is prime.

(5) Given a radical differential ideal by a set of generators, compute any *prime decomposition where the components are given by generators.*

(6) Given a radical differential ideal by a set of generators, determine whether a polynomial is a zero-divisor modulo that ideal.

Call the minimal bound k with $I = \langle I_{\leq k} \rangle_\Delta$ the **saturation index** of the differential ideal I. If we can compute a saturation index k of a radical differential ideal I given by a characteristic set or a simple differential system S, then we can solve item (1) by the following process. Compute all derivatives up to order k of the equations in S and saturate the ideal generated by these derivatives by their initials and separants. A generating set of this algebraic ideal is a generating set of the differential ideal. Thus, it is desirable to compute the saturation index, but in general it seems hard to do so. We ease the notation and define the saturation index of a simple differential system S to be the saturation index of $\mathcal{I}(S)$.

Appendix E

VESSIOT Theory

> One great advantage of geometry lies precisely in the fact that the senses can come to the assistance of the intellect, and help to determine the road to be followed, and many minds prefer to reduce the problems of analysis to geometric form.
>
> HENRI POINCARÉ
> in [Poi14]

This appendix is part of joint work with WERNER SEILER.

In Chapter 2 we have seen that a promising ansatz for a formal power series solution might fail to yield a formal power series solution. The goal of this appendix is to sketch the VESSIOT theory, which provides a language and geometric insight why this can happen. Disregarding this additional geometric insight and taking a purely computational standpoint, the VESSIOT theory is equivalent for finding power series solutions to the approach in Chapter 2.

The previous chapters used systems of equations and inequations to describe differential equations. Now, we exchange this algebraic perspective for a geometric perspective by using HILBERT's Nullstellensatz to look at the solutions of these systems in the affine space of TAYLOR coefficients (the jet space). This yields a variety, which admits an important additional structure: the VESSIOT distribution.

For example, consider the approach of the differential dimension polynomial. Given an ideal $I \subseteq F\{U\}$ associated to a simple differential system, the differential dimension polynomial is defined by the dimensions of the algebraic ideals $I \cap F\{U\}_{\leq \ell}$ for each $\ell \in \mathbb{Z}_{\geq 0}$. Looking at these algebraic ideals "throws away" the differential structure, and thus one is only able to capture the generic behavior of solutions.

The VESSIOT theory reconstructs the differential structure on $I \cap F\{U\}_{\leq \ell}$ using the VESSIOT distribution on the variety of $I \cap F\{U\}_{\leq \ell}$. This distribution specifies the "directions" any point on this variety can move tangentially to yield a solution. The behavior of this distribution at a point provides information on whether this point is suitable for a formal power series solutions. In particular, the VESSIOT distribution gives an interpretation for the non-existence of certain power series solutions and for the countably many "holes" in Example 2.93. Thus, understanding and computing these singularities is the focus of this appendix.

This appendix begins with defining the VESSIOT distribution and the types of singular points. The combination of both the algebraic and the differential THOMAS decomposition yields an algorithmic approach for detecting and distinguishing the different kinds of geometric singularities of solutions of a system of differential equations. Then, we discuss how geometric singularities of solutions behave under prolongations and thereby allow to recognize points which do not extend to formal power series solutions. Finally, this is applied to explain unexpected behaviors in the differential counting polynomial from Examples 2.92 and 2.93.

This appendix omits to specify small neighborhoods as domains of definition and uses a global notation; however, all statements in this appendix are exclusively local.

E.1 Geometric Singularities

We follow the description of the VESSIOT theory in [Sei10, Pom78], the historical reference is [Ves24].

The setup of the VESSIOT theory is the affine space with coordinates for both the center of expansion and the power series coefficients. More formally, the VESSIOT theory considers a jet bundle $J_\ell\pi$ of finite order ℓ. Its construction starts with $\mathcal{E} = \mathbb{C}^n \times \mathbb{C}^m$, where the independent variables $y_1, \ldots, y_n$ are an affine coordinate system on the base space $\mathcal{Y} = \mathbb{C}^n$, and the dependent variables $U = \{u^{(1)}, \ldots, u^{(m)}\}$ are an affine coordinate system of the fiber $\mathbb{C}^m$. Denote by π the natural projection on the first factor of $\mathcal{E}$. The jet bundle $J_\ell\pi$ of order ℓ is constructed from $\mathcal{E}$ by building the CARTESIAN product with the affine space having the differential variables of order 1 to ℓ as an affine coordinate system. There are natural projections $\pi^\ell_{\ell'} : J_\ell\pi \twoheadrightarrow J_{\ell'}\pi$ for $\ell' \leq \ell$. For convenience, identify $\mathcal{E} = J_0\pi$. In addition, the jet bundle $J_\ell\pi$ is fibred over the base space $\mathcal{Y}$ by the canonical projection $\pi^\ell : J_\ell\pi \to \mathcal{Y}$.

In the VESSIOT theory, we can introduce equations and inequations for the base space $\mathcal{Y}$; this is in contrast to differential algebra, which allows invertible "coordinates" of the base space $\mathcal{Y}$ in the differential field $F = \mathbb{C}(y_1, \ldots, y_n)$. Our approach, in contrast to the standard VESSIOT theory, uses complex instead of real coordinates, which allows an algorithmic treatment and a better comparison with the counting sequence, as HILBERT's Nullstellensatz is applicable.

Instead of differential systems or algebraically restricted systems of differential equations, we consider a geometric equivalent of these systems. A **jet variety** of order ℓ is a subvariety $\mathcal{R}_\ell$ of $J_\ell\pi$ such that $\pi^\ell|_{\mathcal{R}_\ell} : \mathcal{R}_\ell \to \mathcal{Y}$ is dominant. They arise for example in the following two cases. For a radical differential ideal I in $\mathbb{C}(y_1, \ldots, y_n)\{U\}$ define the **jet variety $\mathcal{R}_\ell(I)$ associated to I** as the vanishing set of $I \cap \mathbb{C}[y_1, \ldots, y_n]\{U\}_{\leq \ell}$. For a simple differential system S over $\mathbb{C}(y_1, \ldots, y_n)\{U\}$ define the **jet variety $\mathcal{R}_\ell(S)$ associated to S** as $\mathcal{R}_\ell(\mathcal{I}(S))$.

We give the classical definition of solutions in the jet language. This allows to motivate the VESSIOT distribution. Locally, an analytic section $\sigma : \mathcal{Y} \to \mathcal{E}$ with $\pi \circ \sigma = \mathrm{id}_{\mathcal{Y}}$ can be given as $\sigma(y_1, \ldots, y_n) = (y_1, \ldots, y_n, s(y_1, \ldots, y_n))$ with a holomorphic function $s : \mathbb{C}^n \to \mathbb{C}^m$. Such a section $\sigma : \mathcal{Y} \to \mathcal{E}$ can be prolonged, which yields a section of the jet bundle $j_\ell\sigma : \mathcal{Y} \to J_\ell\pi$, locally defined by adding all derivatives of the function s up to order ℓ, i.e.,

$$j_\ell\sigma(y_1, \ldots, y_n) = (y_1, \ldots, y_n, s_{\mathbf{i}}(y_1, \ldots, y_n) \mid \mathbf{i} \in \mathbb{Z}^n_{\geq 0}, |\mathbf{i}| \leq \ell) .$$

A **(strong/classical) solution** of a jet variety $\mathcal{R}_\ell \subseteq J_\ell\pi$ is an (analytic) section $\sigma : \mathcal{Y} \to \mathcal{E}$ such that $\operatorname{im} j_\ell\sigma \subseteq \mathcal{R}_\ell$.

The jet bundle $J_\ell\pi$ has a differential structure. This structure is captured by the

contact distribution $\mathcal{C}_\ell$, generated by the following linear independent vector fields[1]:

$$C_i^{(\ell)} = \partial_{y_i} + \sum_{\substack{\mathbf{i}\in\mathbb{Z}^n_{\geq 0}\\ 0\leq|\mathbf{i}|<\ell}} \sum_{j=1}^{n} u^{(j)}_{\mathbf{i}+e_i}\partial_{u^{(j)}_{\mathbf{i}}}, \qquad 1 \leq i \leq n$$

$$C_j^{\mathbf{i}} = \partial_{u^{(j)}_{\mathbf{i}}}, \qquad \mathbf{i} \in \mathbb{Z}^n_{\geq 0}, |\mathbf{i}| = \ell, 1 \leq j \leq m$$

The integral manifolds of the contact distribution are those coming from prolonged functions, i.e., a section $\gamma : \mathcal{Y} \to J_\ell\pi$ of the ℓ-th jet bundle is of the form $\gamma = j_\ell\sigma$ for a section $\sigma : \mathcal{Y} \to \mathcal{E}$, if and only if $T(\operatorname{im}\gamma) \subseteq \mathcal{C}_\ell$, where T denotes the tangent space. The first n fields $C_i^{(\ell)}$ are transversal to the fibration of $\pi^\ell : J_\ell\pi \to \mathcal{Y}$ and describe the "movement" of a function along the base space, and the fields $C_j^{\mathbf{i}}$ span the vertical space for the fibration $\pi^\ell_{\ell-1} : J_\ell\pi \twoheadrightarrow J_{\ell-1}\pi$.

The contact distribution induces the differential structure on a jet variety. Let $\sigma : \mathcal{Y} \to \mathcal{E}$ be a strong solution of a jet variety $\mathcal{R}_\ell \subseteq J_\ell\pi$. Then, by definition, $\operatorname{im} j_\ell\sigma \subseteq \mathcal{R}_\ell$; hence $T_\xi(\operatorname{im} j_\ell\sigma) \subseteq T_\xi\mathcal{R}_\ell$ for any point $\xi \in \operatorname{im} j_\ell\sigma$. Furthermore, for any prolonged section $T_\xi(\operatorname{im} j_\ell\sigma) \subseteq \mathcal{C}_\ell|_\xi$. Combine these two restrictions to the **Vessiot space** $\mathcal{V}_\xi[\mathcal{R}_\ell]$ of the jet variety $\mathcal{R}_\ell \subseteq J_\ell\pi$ at a point $\xi \in \mathcal{R}_\ell$. It is the linear space $\mathcal{V}_\xi[\mathcal{R}_\ell] = T_\xi\mathcal{R}_\ell \cap \mathcal{C}_\ell|_\xi$. The family of all Vessiot spaces is the **Vessiot distribution** denoted by $\mathcal{V}[\mathcal{R}_\ell]$.

In general, the behavior of the Vessiot spaces, including their dimensions, can change strongly from one point to another. However, there is the following result about generic uniformity. The points where this generic uniformity does not hold yield the singular points, which are important for the study of power series solutions. The constructive part of the classical proof of the generic uniformity is sketched, as it explains how the Vessiot spaces can be computed at smooth points and thus is the basis for our algorithmic approach to singularities below.

Proposition E.1. *The* Vessiot *spaces* $\mathcal{V}[\mathcal{R}_\ell]$ *define a smooth distribution of constant rank on a* Zariski *open subset of a jet variety* $\mathcal{R}_\ell$*.*

Proof. We restrict to smooth points $\xi \in \mathcal{R}_\ell$ in order to deal with a manifold. Let

$$\mathbf{v} = \sum_{i=1}^{n} a^i C_i^{(\ell)}|_\xi + \sum_{\substack{\mathbf{i}\in\mathbb{Z}^n_{\geq 0}\\ |\mathbf{i}|=\ell}} \sum_{j=1}^{m} b^j_{\mathbf{i}} C^{\mathbf{i}}_j|_\xi \tag{E.1}$$

be an arbitrary vector in $\mathcal{V}_\xi[\mathcal{R}_\ell]$ with coefficients $a^i, b^j_{\mathbf{i}} \in \mathbb{C}$. Such a vector is tangential to $\mathcal{R}_\ell$, if and only if it satisfies in addition $d(p)|_\xi(\mathbf{v}) = 0$ for all polynomial functions $p : J_\ell\pi \to \mathbb{C}$ having the jet variety $\mathcal{R}_\ell$ contained in the zero set. Hence, obtain the following linear system for the coefficients a^i and b^α_μ of $\mathbf{v}$.

$$\sum_{i=1}^{n} C_i^{(\ell)}(p)(\xi)a^i + \sum_{\substack{\mathbf{i}\in\mathbb{Z}^n_{\geq 0}\\ |\mathbf{i}|=\ell}} \sum_{j=1}^{m} C^{\mathbf{i}}_j|_\xi(p)(\xi) b^j_{\mathbf{i}} = 0 \tag{E.2}$$

The behavior of (E.2) can vary for different $\xi \in \mathcal{R}_\ell$. However, the set of solutions of (E.2) is smooth outside of a Zariski closed set, and, by enlarging this closed set, one can additionally assume that the dimension remains constant on it. □

[1]Note the difference between the vector field ∂_{y_i} and the derivation $\partial_i \in \Delta$.

A strong solution σ prolongs to a section $j_\ell\sigma$ of the jet bundle $J_\ell\pi$ with image in $\mathcal{R}_\ell$. We use the property that such a prolongation "moves along" the VESSIOT spaces to define a generalization of solutions. These are sections that allows us to talk about an "ansatz, that unexpectedly does not yield a power series solution" below. A **geometric solution** of the jet variety $\mathcal{R}_\ell$ is an n-dimensional submanifold $\mathcal{N} \subseteq \mathcal{R}_\ell$ such that $T\mathcal{N} \subseteq \mathcal{V}[\mathcal{R}_\ell]|_{\mathcal{N}}$. Any strong solution $\sigma : \mathcal{Y} \to \mathcal{E}$ automatically prolongs to the geometric solution $\operatorname{im} j_\ell\sigma$. However, a geometric solution does not necessarily project to a strong solution (cf. Lemma E.5).

A comparison of the behavior of differential equations and jet varieties in higher order is interesting, as not foreseeable constraints for a power series solution can appear in higher order and prevent the existence of formal power series solutions. This can be described by the prolongation and projection relating equations of different orders. Let $\mathcal{R}_\ell \subseteq J_\ell\pi$ a jet variety. Its (first) **prolongation** $\mathcal{R}_{\ell+1} \subseteq J_{\ell+1}\pi$ is obtained by adding all formal derivatives of the equations describing $\mathcal{R}_\ell$. Higher prolongations $\mathcal{R}_{\ell+r} \subseteq J_{\ell+r}\pi$ with $r > 1$ are defined by iteration. For small ℓ and a simple differential system S the prolongation of $\mathcal{R}_\ell(S)$ does not necessarily equal $\mathcal{R}_{\ell+1}(S)$. (However, equality holds if ℓ is at least the saturation index of $\mathcal{I}(S)$ as defined in Appendix D.) The **projection** of $\mathcal{R}_\ell$ to $J_k\pi$, $k \leq \ell$, is defined as $\pi^\ell_k(\mathcal{R}_\ell) \subseteq J_k\pi$.

Usually, prolongations and projections are used to ensure that all differential consequences are included in $\mathcal{R}_\ell$, i.e., to ensure formal integrability of $\mathcal{R}_\ell$. However, a jet variety $\mathcal{R}_\ell(I)$ coming from a differential ideal I is always formally integrable, and thus we avoid the problem of formal integrability in our setup.

Remark E.2. For the geometric intuition, compare the linear system (E.2) with the prolongation of a differential equation $p_= \in F\{U\}^{\{=\}}$ of order $\operatorname{ord}(p) = \ell$. The derivative $\partial_i p$ can be expressed using the contact fields as

$$\partial_i p = C_i^{(\ell)}(p) + \sum_{|\mu|=\ell} \sum_{\alpha} C^\mu_\alpha(p) u^\alpha_{\mu+1_i} ,$$

where $1_i \in \mathbb{Z}^n_{\geq 0}$ is the vector with i-th entry 1 and the other entries are zero. We see that the linear system (E.2) is a homogenized form of the linear system determining the TAYLOR coefficients of order $\ell + 1$. In particular, one expects to find solutions for the linear system (E.2) which do not yield new TAYLOR coefficients in order $\ell + 1$ when the coefficient of $C_i^{(\ell)}(p)$ can only be chosen to be zero (cf. Lemma E.5 for a formal statement). Geometrically, this means that the VESSIOT distribution has no n-dimensional transversal summand. This observation is the motivation for the following definition of singular points. ◁

The different kinds of geometric singularities provide the geometric intuition why a certain ansatz of a power series solution breaks down at a certain order. We define them via direct sum decompositions of the VESSIOT distribution into a transversal summand and the symbol space. Let $\mathcal{R}_\ell \subseteq J_\ell\pi$ be a jet variety. The **(geometric) symbol space** $\mathcal{N}_{\ell,\xi} \subseteq \mathcal{V}_\xi[\mathcal{R}_\ell]$ of $\mathcal{R}_\ell$ at a point $\xi \in \mathcal{R}_\ell$ consists of all tangent vectors in $T_\xi\mathcal{R}_\ell$ which are vertical for the fibration $\pi^\ell_{\ell-1}$. As in the proof of Proposition E.1, the symbol space is the solution space of a linear system of equations. We call a smooth point $\xi \in \mathcal{R}_\ell$

(i) **regular** if there exists an open neighborhood $\xi \in \mathcal{U} \subseteq \mathcal{R}_\ell$ such that the VESSIOT distribution $\mathcal{V}[\mathcal{R}_\ell]$ is of constant dimension on $\mathcal{U}$ and can be decomposed as $\mathcal{V}[\mathcal{R}_\ell] = \mathcal{N}_\ell \oplus \mathcal{H}$ with a transversal, n-dimensional distribution $\mathcal{H} \subseteq T\mathcal{U}$;

(ii) **regular singular** if there exists an open neighborhood $\xi \in \mathcal{U} \subseteq \mathcal{R}_\ell$ such that the VESSIOT distribution $\mathcal{V}[\mathcal{R}_\ell]$ has constant dimension on $\mathcal{U}$ but at the point ξ no n-dimensional complement to the symbol $\mathcal{N}_\ell$ exists, i.e., $\dim \mathcal{V}_\xi[\mathcal{R}_\ell] - \dim \mathcal{N}_\ell|_\xi < n$;

(iii) **irregular singular** if the VESSIOT distribution $\mathcal{V}[\mathcal{R}_\ell]$ has no constant dimension on every open neighborhood $\xi \in \mathcal{U} \subseteq \mathcal{R}_\ell$.

An irregular singularity $\xi \in \mathcal{R}_\ell$ is called **purely irregular** if an n-dimensional complement to the symbol $\mathcal{N}_\ell$ exists, i.e. $\dim \mathcal{V}_\xi[\mathcal{R}_\ell] - \dim \mathcal{N}_\ell|_\xi = n$. We call all singular points in (ii) and (iii) a **geometric singularity**. (This definition is independent on the choice of EUCLIDian or ZARISKI topology.)

Jet varieties might have non-geometric singularities, in particular algebraic singularities in the set $\mathcal{R}_\ell$ and singular solutions. For the sketchy treatment of the VESSIOT theory in this appendix we can ignore these singularities.

Regular singular points warrant at least a cursory explanation and some geometric intuition. For one ordinary differential equations of order one in the complex setting think of them as branch points of the RIEMANN surface of a germ of a solution. Consider for example the (rescaled) simple fold differential equation $\frac{4}{9}(u'(z))^2 - z = 0$ (cf. Example E.4). Its solutions are $\pm z^{\frac{3}{2}} + a$ for each $a \in \mathbb{C}$. Look at $z^{\frac{3}{2}}$ and its analytic continuation $-z^{\frac{3}{2}}$. Their common branch point $z = 0$ is a regular singular point in the differential equation. In this case the two branches yield a well-defined limit for the function value and first derivative in the branch point, however not for higher derivatives.

Real numbers allow another comprehensible description for regular singular points of ordinary differential equations. All previous definitions are valid for the real numbers instead of complex numbers. These behavior described in the following proposition is plotted in Figure E.1 and Figure E.2 on pages 178 and 180.

Proposition E.3. *Let $\mathcal{R}_\ell$ be an ordinary*[2] *jet variety over the real numbers such that everywhere $\dim \mathcal{V}[\mathcal{R}_\ell] = 1$. If $\xi \in \mathcal{R}_\ell$ is a regular point, then there exists a unique strong solution σ with $\xi \in \operatorname{im} j_\ell\sigma$. If $\xi \in \mathcal{R}_\ell$ is a regular singular point, then one of the following two possibilities appears. Either two strong solutions σ_1, σ_2 with $\xi \in \operatorname{im} j_\ell\sigma_i$ exist (which both either end or start in $\pi^\ell(\xi)$); in this case call ξ or $\pi_0^\ell(\xi)$ an **impasse point** (or **cusp**). Or there exists only one strong solution σ such that $j_\ell\sigma$ passes through ξ and its $(\ell+1)$-th derivative blows up at $\pi_0^\ell(\xi)$.*

Proof. Any one-dimensional distribution allows integral curves, e.g., by a special case of the FROBENIUS theorem. This integral curve is a smooth one-dimensional geometric solution σ_ℓ. Around any regular point this geometric solution projects onto the graph of a strong solution σ.

Assume that in an open simply connected neighborhood of ξ the Vessiot distribution $\mathcal{V}[\mathcal{R}_\ell]$ is generated by a vector field X. If ξ is a regular singular point, then X_ξ is vertical to π^ℓ. In particular, its ∂_t-component vanishes, where t is the (only) independent variable. The behavior of the projected geometric solution $\pi_0^\ell(\sigma_\ell)$ depends on whether or not the ∂_t-component changes its sign at ξ. If the sign changes, then $\pi_0^\ell(\sigma_\ell)$ has two branches corresponding to two strong solutions which both either begin or end at $\pi_0^\ell(\xi)$. Otherwise, the projected geometric solution $\pi_0^\ell(\sigma_\ell)$ is still the graph of a strong solution σ, but Remark E.2 implies that the $(\ell+1)$-th derivative of σ at $\pi_0^\ell(\xi)$ is infinite. □

The definition of geometric singularities is rather involved, compared with classical definitions of singularities of solutions of differential equations. This complication comes

[2] I.e., $|\Delta| = 1$.

from our more general setup where the “correct dimensions” are only known by a comparison with a neighborhood. For systems of finite type[3], [KS12] clarifies the “correct dimension” of $\mathcal{V}[\mathcal{R}_\ell]$. For jet varieties associated to a simple differential system S the constituents from Proposition D.1 describe the generic behavior and yield the “correct dimension” of $\mathcal{V}[\mathcal{R}_\ell]$. This is used in the next section to give an algorithm that detects geometric singularities.

E.2 Detection of Geometric Singularities

A combination of both the algebraic and differential THOMAS decomposition can detect geometric singularities. The differential THOMAS decomposition yields differential simple systems to describe the “correct dimension” of the VESSIOT distribution leading to regular points, and the algebraic THOMAS decomposition classifies the points of the jet variety with respect to these dimensions. For the sake of brevity, we refrain from giving a formal algorithm and only scetch the approach.

On the polynomial ring $F\{U\}_{\leq\ell}$ assume the algebraic ranking induced by the orderly differential ranking on $F\{U\}$. For simplicity, let $F = \mathbb{C}(y_1, \dots, y_n)$ with $\partial_i y_j = 1$ if $i = j$ and zero otherwise.

Assume that one is interested in finding the geometric singularities in order ℓ of a set of differential equations. By a differential THOMAS decomposition, split this set of differential equations into simple differential systems. Consider each of these systems S independently. However, instead of a simple differential system S, we work with the differential ideal $\mathcal{I}(S)$ associated to S. This has the minor drawback that the decomposition is no longer disjoint and a point might appear twice[4].

GRÖBNER basis methods and Lemma 1.93 can compute generators $p_1 \dots, p_k$ of the algebraic ideal $\mathcal{I}(S)_{\leq\ell}$. For these[5] p_i create the corresponding equations for the VESSIOT distribution as in the linear system (E.2) in Proposition E.1. These equations are homogeneous and linear in new indeterminates a^i and $b^j_{\mathbf{i}}$ for $1 \leq i \leq n$, $1 \leq j \leq m$, and $\mathbf{i} \in \mathbb{Z}^n_{\geq 0}$ with $|\mathbf{i}| = \ell$. In the following always assume that the $b^j_{\mathbf{i}}$ rank higher than the a^i, which rank higher than the differential variables. Additionally, assume that all involved polynomials are cleared of denominators involving $y_1, \dots, y_n$. Thus, these can also be considered as algebraic indeterminates; rank the y_i lower than all other indeterminates.

Apply the algebraic THOMAS decomposition to the union of the generators p_i of $\mathcal{I}(S)_{\leq\ell}$ as equations and the equations from the linear system (E.2). This is a potentially expensive computation over the polynomial ring

$$(\mathbb{C}[y_1, \dots, y_n]\{U\}_{\leq\ell})\,[a^1, \dots, a^n][b^j_{\mathbf{i}} \mid 1 \leq j \leq m, \mathbf{i} \in \mathbb{Z}^n_{\geq 0}, |\mathbf{i}| = \ell]\ .$$

The homogeneity of the equations from the linear system (E.2) implies that this decomposition is disjoint when projected down to $\mathbb{C}[y_1, \dots, y_n]\{U\}_{\leq\ell}$, i.e., comprehensive. In particular, this projection is an algebraic THOMAS decomposition[6] of the truncated differential ideal $\mathcal{I}(S)_{\leq\ell}$, and the results of Proposition D.1 apply. In particular, constituents (cf. Proposition D.1) among the projected components stand out when looking at the leaders of their equations. The solutions of all other projected systems are contained

[3] I.e., the dimension polynomial is finite for all components

[4] The classification of a point depends on the simple system it is compared to.

[5] To compute the VESSIOT distribution it suffices to consider those p_i of highest order ℓ.

[6] Strictly, this is only true if the y_i are invertible again, and all systems involving an equation with leader y_i are thrown away.

in the ZARISKI closure of these constituents and these inclusions can be determined by GRÖBNER basis methods.

The type of singular point (if any) is now characterized by the fibration of $\pi^{\ell}_{\ell-1}$ in the following way. In the original (non-projected) systems resulting from the algebraic THOMAS decomposition, all polynomials involving the indeterminates a^i and $b^j_{\mathbf{i}}$ are linear, homogeneous, and equations[7]. For a system to correspond to regular points, it is necessary that no equation having leader a^i exists, as otherwise in the VESSIOT space any transversal complement of the symbol space has its dimension decreased by one. This criterion is sufficient if additionally the geometric symbol space has the same dimension as the geometric symbol space of the constituents[8]. A system corresponds to a regular singular point, if the drop in dimension of any transversal part is compensated by the vertical subspace, i.e., if the number of equations in a^i and $b^j_{\mathbf{i}}$ combined is the same as in the neighboring constituent. The other systems correspond to irregular singular points; among those, the systems with no constraint on the a^i describe purely irregular singular points.

Example E.4. We demonstrate the algorithm on a conjectured classification of the local normal forms of scalar first-order ordinary differential equations in [Dar75].

(1) **simple fold** $t = (u')^2$

(2) $u = \frac{1}{2}\big((u')^2 + \chi t^2)\big)$ with three subcases depending on the value of χ:

 (a) **folded saddle** $\chi < 0$
 (b) **folded knot** $0 < \chi < \frac{1}{4}$
 (c) **folded spiral** $\chi > \frac{1}{4}$

(3) **elliptic gather** $t = (u')^3 - uu'$

(4) **hyperbolic gather** $t = (u')^3 + uu'$

Study the cases (mainly) in order $\ell = 1$.

For the simple fold (cf. Figure E.1) the above approach yields two systems:

$$\begin{array}{lrrll} \{ & -a + 2u_t \cdot b = 0, & u_t^2 - t = 0, & t \neq 0 & \} \\ \{ & a = 0, & u_t = 0, & t = 0 & \} \end{array}$$

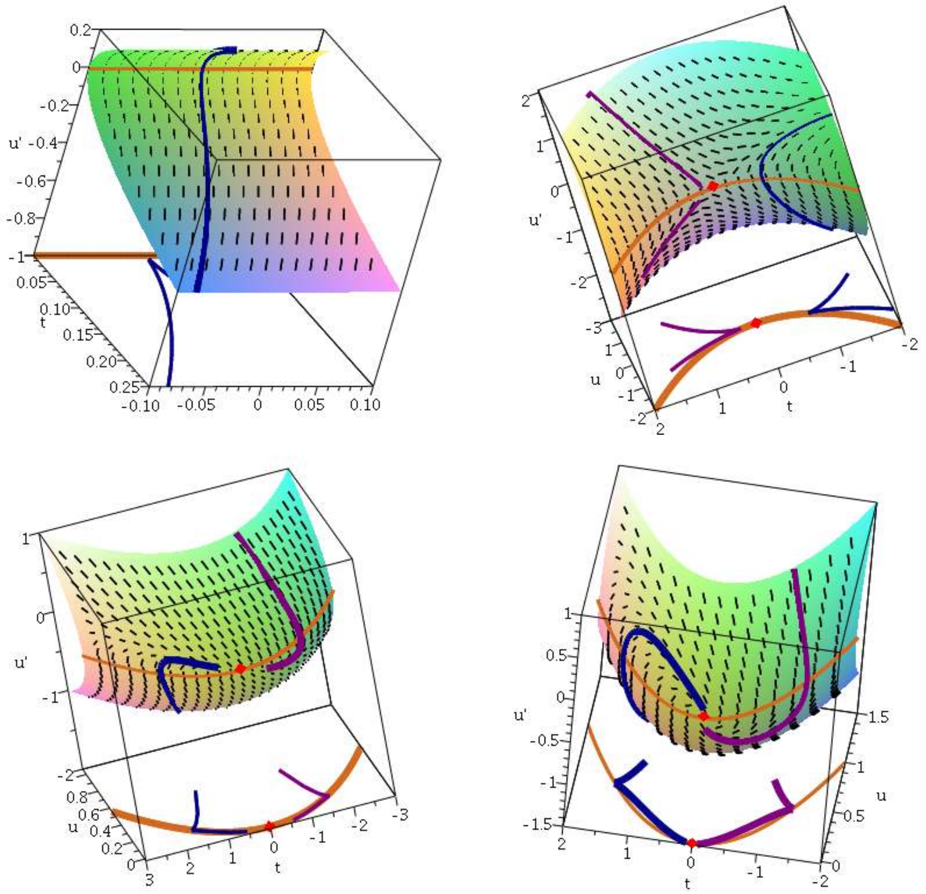
Choosing real values for t and u yields real values for u_t; furthermore, for each of these possibilities the pair (a, b) can also be chosen to be in $\mathbb{R}^2$. The first system describes regular points and the second system describes regular singular points. For each order $\ell > 1$ there is only one system, whose solutions project down to those of the first of the above two systems. It is a general phenomenon that regular points prolong to higher orders and regular singular points do not (cf. Theorem E.6).

The three cases in (2) suffer under using the complex numbers: there is no $<$-relation on $\mathbb{C}$ to distinguish values of χ. However, the three subcases of folded saddle, knot, and spiral can actually be treated as one system. The above approach yields the following

[7] Assume a reasonable algebraic THOMAS decomposition, as the one presented in Subsection 1.3.3, i.e., that no unnecessary splittings are performed.

[8] This dimension is equal for all of constituents by Proposition D.1 and complementary to the number of equations a leader $b^j_{\mathbf{i}}$. In this sense, the constituents describe the “correct dimensions”.

Figure E.1: These four plots show the simple fold (upper left), folded saddle ($\chi = -1$, upper right), the folded knot ($\chi = \frac{1}{8}$, lower left), and the folded spiral ($\chi = \frac{1}{2}$, lower right). The VESSIOT spaces are plotted by thin black dashes and in all four cases the singular points lie in the $u' = 0$-plane, plotted by a brown line. Additionally, geometric solutions are plotted in blue and purple. Both the singular curve and the geometric solutions are projected to a plane below the plot. In the latter three plots, the irregular singular points at $t = u = u' = 0$ are marked by a red point.



three cases assuming that $\chi \neq 0$ and $\chi \neq \frac{1}{4}$, where $p = u_t^2 + \chi t^2 - 2u$.

$$
\begin{array}{lrrrrr}
\{ & (\ldots)\cdot a + (\ldots)\cdot b = 0, & p = 0, & 2u - \chi t^2 \neq 0 & & \} \\
\{ & & u_t = 0, & u = 0, & t = 0 & \} \\
\{ & a = 0, & u_t = 0, & 2u - \chi t^2 = 0, & t \neq 0 & \}
\end{array}
$$

Again, real choices for lower ranking indeterminates lead to real solutions for higher ones, and in particular the computation can be interpreted over the real numbers. The first system is the only regular system. The second system is purely irregular singular, and for order $\ell = 2$ it prolongs[9] to another purely irregular singular system with $u_{tt}^2 - u_{tt} + \chi = 0$ and a regular singular system with $u_{tt}^2 - u_{tt} + \chi \neq 0$. The third system is regular singular and again does not prolong to higher order.

[9] We have not formally defined prolongation for systems with inequations. One needs to prolong the ZARISKI closure of this system and add the inequations.

Elliptic (3) and hyperbolic (4) gather show the same behavior up to signs.

$$
\begin{array}{lrrrrl}
\{ & (\ldots)\cdot b+(\ldots)\cdot a=0, & u_t^3\mp uu_t-t=0, & 4u^3\mp 27t^2\neq 0, & t\neq 0 & \} \\
\{ & (\ldots)\cdot b+(\ldots)\cdot a=0, & u_t^3\mp uu_t=0, & u\neq 0, & t=0 & \} \\
\{ & (\ldots)\cdot b+(\ldots)\cdot a=0, & uu_t\mp 3t=0, & 4u^3\mp 27t^2=0, & t\neq 0 & \} \\
\{ & & 2u_t\mp t=0, & u+3=0, & t^2\pm 4=0 & \} \\
\{ & a=0, & u_t=0, & u=0, & t=0 & \} \\
\{ & a=0, & 2uu_t\pm 3t=0, & 4u^3\mp 27t^2=0, & t^3\pm 4t\neq 0 & \} \\
\{ & a=0, & 2uu_t\pm 3t=0, & u^2-3u+9=0, & t^2\pm 4=0 & \}
\end{array}
$$

The first three systems are regular, and the first system is a constituent; all these three systems prolong to regular cases when repeating the computation for order $\ell=2$, however they split into more cases. The fourth system is purely irregular singular; it prolongs to a regular singular system (with the additional restriction $2u_{tt}^2\mp u_{tt}\neq 0$) and another purely irregular singular system (with the complementary additional restriction $2u_{tt}^2\mp u_{tt}=0$) in order $\ell=2$. The last three systems are regular singular, and thus they do not prolong to order $\ell=2$. The difference of both cases can be seen at the plots (cf. Figure E.2). In the case of the elliptic gather the impasse singularities point to the origin, whereas in the case of the hyperbolic gather the impasse singularities point away from the origin.

The computations performed in this example seem infeasible in order $\ell=3$. ◁

Naive numerical methods fail when integrating over impasse point or points where a derivative blows up. The plots of the curves in the previous example are constructed by integration in the jet space, where no singularity exists at regular singular points. Then the solution curve can be projected down to the t-u-plane.

E.3 Singularities and Counting Polynomials

This section describes the phenomena appearing in the counting sequence and the differential counting polynomial using geometric singularities. It first gives an intuitive overview on how the different kinds of singular points affect the existence of power series solutions. Then it casts the geometric intuition into formal statements and gives proofs. This allows to discuss the surprising examples of counting sequences and differential counting polynomials.

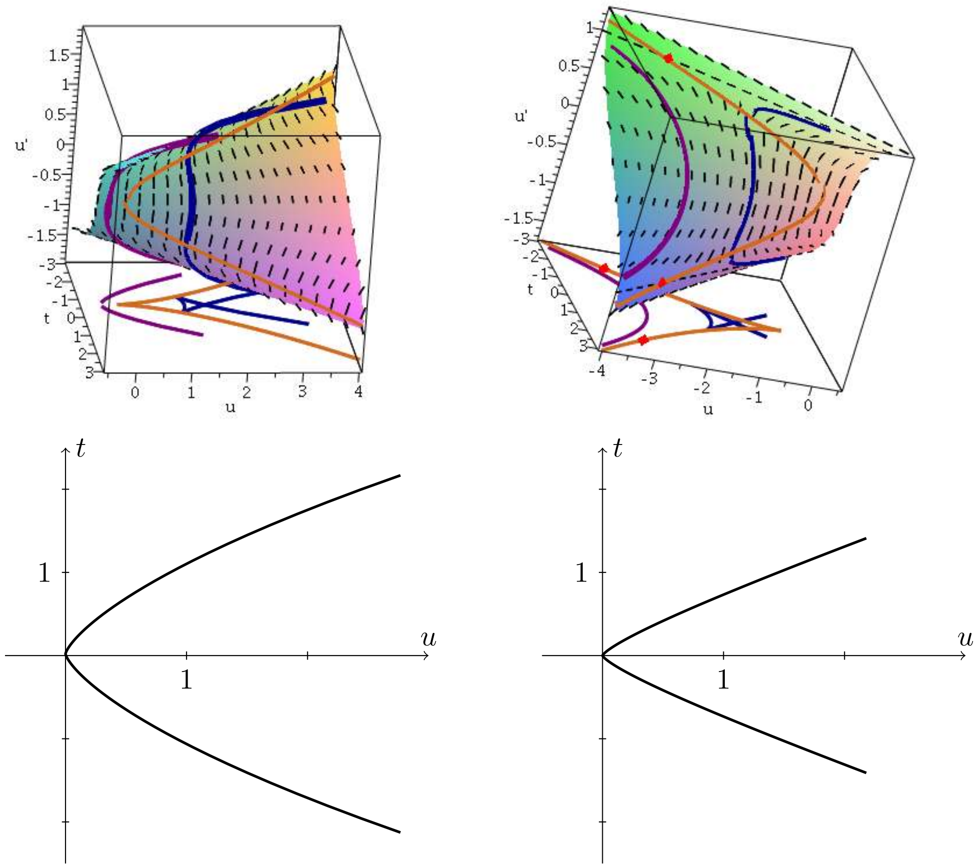
This informal discussion assumes that the jet varieties $\mathcal{R}_\ell$ are given by a differential ideal I and that ℓ is large, i.e., at least the saturation index[10] of I, which is defined as the minimal bound k with $I=\langle I_{\leq k}\rangle_\Delta$ (cf. Theorem D.7 and the text after the theorem).

A formal power series solution coming from a point $\xi_\ell\in\mathcal{R}_\ell$ exists if $(\pi^\ell_{\ell+1})^{-1}(\{\xi_\ell\})$ is non-empty, one of the elements in this fiber has a non-empty fiber under $\pi^{\ell+1}_{\ell+2}$, and so on. Thus, the fibrations given by the $\pi^\ell_{\ell+1}$ are important. We say that $\xi_{\ell+1}\in\mathcal{R}_{\ell+1}$ **lies above** $\xi_\ell\in\mathcal{R}_\ell$ and that $\xi_{\ell+1}$ **restricts to** ξ_ℓ if $\pi^\ell_{\ell+1}(\xi_{\ell+1})=\xi_\ell$. A jet variety $\mathcal{R}_{\ell+1}$ lies above another jet variety $\mathcal{R}'_\ell$ if each point of $\mathcal{R}_{\ell+1}$ lies above a point in $\mathcal{R}'_\ell$; in this case we also say that $\mathcal{R}_{\ell+1}$ restricts to $\mathcal{R}'_\ell$.

In a prolongation there is a point lying above a regular point, and all of these are again regular (cf. Theorem E.6). In particular, any regular point admits a formal

[10] The saturation index seems hard to compute due to the Ritt problem. Thus, the assumption that ℓ is above the saturation index of I is not easily verified.

Figure E.2: This figure shows the elliptic gather in the two left plots and hyperbolic gather in the two right plots. In the two upper plots, the Vessiot spaces are plotted by black lines, the singularities are given by a curve plotted in brown, two geometric solutions are plotted in blue and purple, everything is projected down to the u-t-plane, and irregular singular points are given by a red point, as in Figure E.1. The two lower plots show the projections to the t-u-axis of the geometric solutions through the point $(t, u, u_t) = (0, 0, 0)$; here the second derivative is infinite.



power series solution. The regular formal power series solutions (cf. Theorem 1.52) are examples of such regular points and it should be no surprise that the solutions with analytical initial conditions admit a positive radius of convergence (cf. Riquier's Existence Theorem 1.60).

There are no points lying above a regular singular point and, thus, they do not yield a formal power series solution (cf. Lemma E.5). For ordinary jet varieties there is a descent understanding of geometric solutions at regular singular points (cf. Proposition E.3).

With these two cases of regular points and regular singular points under control, we turn to the interesting case of irregular singular points, which show a multitude of behavior. The behavior in the fiber over an irregular singular point is not determined by the irregular singular point[11]. The following gives an overview about possible behaviors, but cannot give an algorithm to distinguish these cases. Purely irregular singular points are the main interest, as these are the only singular points where formal power series solution exist (cf. Lemma E.5). Above the saturation index, all points lying above a

[11] Note that the proof of Theorem 2.98 shows the algorithmic undecidability of existence of formal power series solutions at an irregular singular point.

purely irregular singular point are singular and all singular points lie above a purely irregular singular point. Usually, most singular points that lie above a purely irregular singular point are regular singular, and only few are purely irregular; in particular, one expects few formal power series solutions at singular points.

For simplification we restrict to the case of a jet variety $\mathcal{R}_\ell(S)$ associated to a simple differential system S; the results hold in general. For small ℓ and a simple differential system S the prolongation of $\mathcal{R}_\ell(S)$ does not necessarily equal $\mathcal{R}_{\ell+1}(S)$. However, equality holds for all ℓ at least the saturation index of $\mathcal{I}(S)$. In that case, the simple differential system does not result in a new equation in order $\ell+1$ which is not a derivative of an equation in order ℓ. This allows to predict the behavior of a jet variety in the next higher order[12].

Lemma E.5. *Let $\mathcal{R}_\ell(S) \subseteq J_\ell\pi$ be a jet variety associated to a simple differential system S such that $\mathcal{I}(S) = \langle \mathcal{I}(S)_{\leq \ell}\rangle_\Delta$ (i.e., ℓ is at least the saturation index of S), and let $\xi \in \mathcal{R}_\ell(S)$ be an arbitrary point. The prolonged equation $\mathcal{R}_{\ell+1}(S)$ contains points lying above ξ if and only if the* Vessiot *distribution $\mathcal{V}[\mathcal{R}_\ell(S)]$ contains an n-dimensional subdistribution transversal with respect to $\pi_\ell^{\ell+1}$. For the "only if" part the assumption the ℓ is at least the saturation index is superfluous.*

Proof. The proof follows by a comparison of the equations for the prolongation and the Vessiot distribution. Let $\mathcal{R}_\ell(S)$ be described by the polynomial equations $p_1 = 0, \dots, p_t = 0$. Due to the assumption on the saturation index, the prolonged equation $\mathcal{R}_{\ell+1}(S)$ can be described by augmenting the original system with the nt equations

$$C_i^{(\ell)}(p_k) + \sum_{\substack{\mathbf{i}\in\mathbb{Z}^n_{\geq 0}\\ |\mathbf{i}|=\ell}} \sum_{j=1}^{m} u^{(j)}_{\mathbf{i}+e_i} C_j^{\mathbf{i}}(p_k) = 0\,, \quad 1 \leq k \leq t\,, \quad 1 \leq i \leq n\,. \tag{E.3}$$

This is the same formula as ansatz (E.1), with a^i replaced by 1 and $b^j_{\mathbf{i}}$ replaced by $u^{(j)}_{\mathbf{i}+i}$. Thus, (E.3) has a solution if (E.1) has a solution with all a^i arbitrary. This is the case if the Vessiot space at ξ contains an n-dimensional transversal subdistribution. □

It follows that such an n-dimensional transversal subdistribution exists in only two cases: at regular points and at purely irregular singular points. In particular, the only singular points that can admit formal power series solutions are purely irregular.

Now, discuss the relationship between regular and singular points of a jet variety $\mathcal{R}_\ell$ and of its prolongation $\mathcal{R}_{\ell+1}$.

Theorem E.6. *Let $\mathcal{R}_\ell(S) \subseteq J_\ell\pi$ be a jet variety associated to a simple differential system S such that $\mathcal{I}(S) = \langle \mathcal{I}(S)_{\leq \ell}\rangle_\Delta$ (i.e., ℓ is at least the saturation index of S). Let $\xi_{\ell+1} \in \mathcal{R}_{\ell+1}(S)$ and $\xi_\ell := \pi_\ell^{\ell+1}(\xi_{\ell+1}) \in \mathcal{R}_\ell(S)$. Then $\xi_{\ell+1}$ is singular if and only if ξ_ℓ is purely irregular singular, and $\xi_{\ell+1}$ is regular if and only if ξ_ℓ is regular.*

Proof. Singular points are points where the vertical subspace of the Vessiot space have a higher dimension than neighboring points. The vertical subspace of the Vessiot space is characterized by linear equations; more specifically by the Jacobian of the equations of the jet variety with respect to the ℓ-th order differential variables. The Jacobian of a derivative of an equation with respect to the $(\ell+1)$-th order differential variables

[12] The behavior can be different for ℓ smaller than the saturation index of S. Then, due to new equations, singular points can appear above regular points, e.g., no singular points exist in order zero, but they may exist in order one for ordinary differential equations of order one.

has the same entries by an easy calculation. (No additional equations appear due to the assumption on the saturation index. In the case of ordinary differential equations the matrices are identical, in the partial case the entries appear multiple times.) In particular, a drop of the rank appears for order $\ell + 1$ exactly at the points where it appears for order ℓ.

If ξ_ℓ is singular, then Lemma E.5 implies that ξ_ℓ is purely irregular singular. □

Example E.7. Continue Example 2.93, the example with differential counting polynomial $\infty^3 - \infty^2 + \infty - \aleph_0$. The goal is to throw some light on this differential counting polynomial using the VESSIOT theory. Hence, consider $U = \{u, v\}$, $\Delta = \{\partial_t\}$ and $F = \mathbb{C}(t)$. Let $p := vu_1 - u + \frac{1}{t}$ and $S := \{p = 0, v_2 = 0\}$. A differential THOMAS decomposition results in the following two simple differential systems.

$$S' := \{ \quad p = 0, \quad v_2 = 0, \quad v \neq 0 \quad \} \quad \text{and}$$
$$\{ \quad u - \tfrac{1}{t} = 0, \quad v = 0 \quad \}$$

For our consideration the second system is superfluous, as it only has one solution. Thus, perform a decomposition of the first system in the sense of Section E.2 for different orders ℓ. All computations are parallel to Example 2.93 and hence omitted.

Each order $\ell \geq 1$ gives a regular system which is the prolongation of the regular system of the lower order. These systems have the same set of solutions as system T in Example 2.93, and consist of the differential equations of S, their derivatives, and the inequations $v \neq 0$ and $t \neq 0$.

In addition, for each order $\ell \geq 1$ there are three singular systems, $S_{\mathrm{irreg},\ell}$, $S_{\mathrm{reg1},\ell}$, and $S_{\mathrm{reg2},\ell}$. The set of solutions of these three singular systems restricts to those of system $S_{\mathrm{irreg},\ell-1}$ (if $\ell \geq 2$). The system $S_{\mathrm{irreg},\ell}$ describes purely irregular singular points:

$$S_{\mathrm{irreg},\ell} := \{ \quad \begin{array}{rl} t^{k+1}(kv_1 - 1)u_k + (-1)^{k+1}k! = 0, & 1 \leq k \leq \ell, \\ v = u - \frac{1}{t} = v_k = 0, & 2 \leq k \leq \ell, \\ \prod_{k=1}^{\ell}(kv_1 - 1) \neq 0, & \\ t \neq 0 & \end{array} \quad \}$$

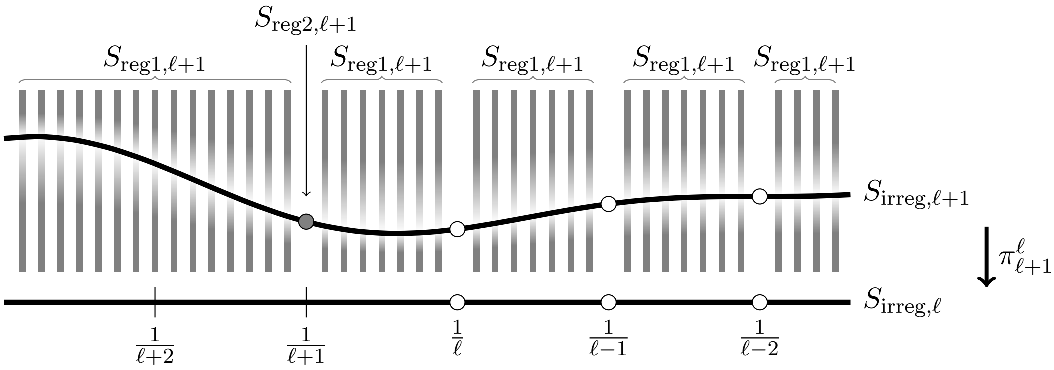
This system describes the same solutions as the systems S_k in Example 2.93. (Here, $t \neq 0$ is included in the system instead of being assumed beforehand.) The other two of these systems describe regular singular points:

$$S_{\mathrm{reg1},\ell} := \{ \quad \begin{array}{rl} t^{\ell+1}(\ell v_1 - 1)u_\ell + (-1)^{\ell+1}\ell! \neq 0, & \\ t^{k+1}(kv_1 - 1)u_k + (-1)^{k+1}k! = 0, & 1 \leq k < \ell, \\ u - \frac{1}{t} = v = v_k = 0, & 2 \leq k \leq \ell, \\ \prod_{k=1}^{\ell}(kv_1 - 1) \neq 0, & \\ t \neq 0 & \end{array} \quad \}$$

$$S_{\mathrm{reg2},\ell} := \{ \quad \begin{array}{rl} t^{k+1}(k - \ell)u_k + (-1)^{k+1}\ell \cdot k! = 0, & 1 \leq k \leq \ell, \\ v_k = 0, & 2 \leq k \leq \ell, \\ \ell v_1 - 1 = u - \frac{1}{t} = v = 0, & \\ t \neq 0 & \end{array} \quad \}$$

In particular, these two systems do not have formal power series solutions. Thus, the only formal power series solutions of S are the ones in the regular system and the solutions in the intersection of all purely irregular singular points.

We schematically picture the behavior of these singular points over a non-zero value for t. The irregular singular points in any order ℓ are a one-fold cover of the v_1-line except for the finite set $\{\frac{1}{\ell}, \frac{1}{\ell-1}, \dots, \frac{1}{2}, \frac{1}{1}\}$. All singular points in order $\ell+1$ lie above one of these irregular singular points. The fiber of $\pi^\ell_{\ell+1}$ over the irregular singular points with $v_1 = \frac{1}{\ell+1}$ consists of one regular singular point, found in the system $S_{\mathrm{reg2},\ell+1}$; in particular, over this singular point no formal power series solution exists. The fiber of all other irregular singular points consists of one irregular singular point from system $S_{\mathrm{irreg},\ell+1}$ and a one-parametric family of regular singular points from system $S_{\mathrm{reg1},\ell+1}$. When restricting to the real picture, one can check that all regular singular points are impasse points and do not yield ℓ-times differentiable solutions (cf. Proposition E.3).



◁

Example E.8. This is an explanation of the differential equation $p := vu_1 - u$ with differential counting polynomial $\infty^{\ell+2} - \infty^{\ell+1} + (\ell+1)\infty^\ell - \ell\infty^{\ell-1}$. Hence, consider $U = \{u, v\}$, $\Delta = \{\partial_t\}$ and $F = \mathbb{C}$. All computations are parallel to Example 2.92 and thus omitted. The decomposition of the system $\{p = 0\}$ with respect to geometric singularities, as explained in Section E.2, yields a linear relation between the number of systems and the order.

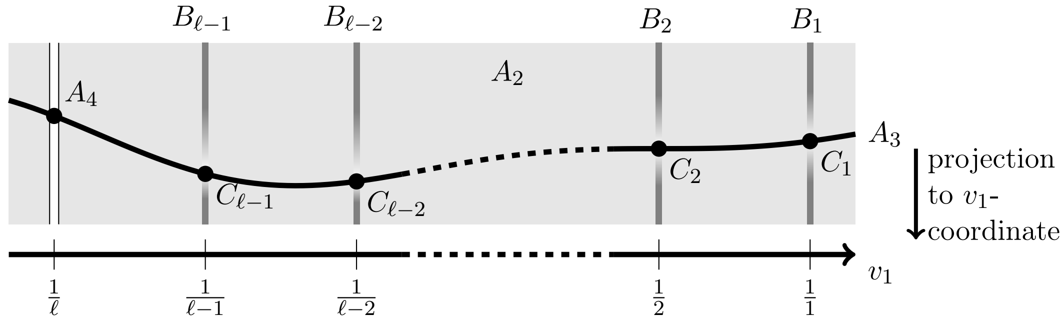
For each order $\ell \geq 1$ a decomposition as in Section E.2 yields $2\ell + 2$ systems.

Call the first of these systems A_1. It consists of regular points, which lie above those of the system A_1 in order $\ell - 1$. (When talking about projections tacitly assume $\ell \geq 2$.) It corresponds to system T from Example 2.92 and has counting sequence $\ell \mapsto (\infty - 1)\infty^{\ell+1}$. This system has all other systems in its closure.

Call the second system A_2. It is regular singular and includes the inequation $\prod_{i=1}^{\ell}(\ell v_1 - 1) \neq 0$. The third and fourth system, called A_3 and A_4, are both purely irregular singular and lie in the closure of A_2. Both of these systems lie above the system A_3 from lower order $\ell - 1$. The system A_3 includes the inequation $\prod_{i=1}^{\ell}(\ell v_1 - 1) \neq 0$ and A_4 includes the equation $\ell v_1 - 1 = 0$.

The remaining $2\ell-2$ systems appear in pairs (B_k, C_k) and both include the equation $kv_1 - 1 = 0$, for all $1 \leq k \leq \ell - 1$. The system B_k is regular singular. The system C_k is purely irregular singular, lies in the closure of B_k, corresponds to the system T_k from Example 2.92, and has the differential counting polynomial ∞^ℓ. The systems B_k and C_k for $1 \leq k \leq \ell - 2$ lie above the system to C_k from lower order $\ell - 1$; the systems $B_{\ell-1}$ and $C_{\ell-1}$ lie above the system A_4 from lower order $\ell - 1$.

The relation of the singular systems can be seen in the following schematic diagram. The purely irregular singular systems A_3, A_4, and C_k are colored in black, the regular singular systems A_2 and B_k are colored in gray. Contrary to the diagram, A_2 only contains A_3 and A_4 in its closure, but its closure intersects all systems B_k and C_k. The fibers of the projection to the v_1-axis are not necessarily one-dimensional.



Look at the purely irregular systems to explain the coefficient ℓ of the "singular part" of the differential counting polynomial. This coefficient stems from the fact that the algebraic counting polynomials of the fibers of the projection to v_1 have different algebraic counting polynomials. The algebraic counting polynomial is ∞^ℓ in case of a fiber given by a system C_k or A_4. The algebraic counting polynomial is $\infty^{\ell-1}$ in case of a fiber given by the system A_3. The number of the systems C_k increases with the order ℓ, and thus the coefficient of ∞^ℓ in the algebraic counting polynomial increases, and the coefficient of $\infty^{\ell-1}$ decreases. In summary, up to order ℓ there are

$$\underbrace{(\infty-\ell)}_{\#\text{ fibers } A_3}\cdot\underbrace{\infty^{\ell-1}}_{\text{fiber } A_3}+\underbrace{1}_{\#\text{ fibers } A_4}\cdot\underbrace{\infty^{\ell}}_{\text{fiber } A_4}+\underbrace{(\ell-1)}_{\#\text{ fibers } C_k}\cdot\underbrace{\infty^{\ell}}_{\text{fiber } C_k}=(\ell+1)\infty^\ell-\ell\infty^{\ell-1}$$

distinguishable formal power series solutions stemming from singular points. ◁

Bibliography

[AH05] J. Apel and R. Hemmecke. Detecting unnecessary reductions in an involutive basis computation. *J. Symbolic Comput.*, 40(4-5):1131–1149, 2005. 55

[Arn88] V. I. Arnol′d. *Geometrical methods in the theory of ordinary differential equations*, volume 250 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, New York, second edition, 1988. Translated from the Russian by Joseph Szücs. 5

[Bar01] M. Barakat. `jets`. A MAPLE-package for formal differential geometry. In *Computer algebra in scientific computing (Konstanz, 2001)*, pages 1–12. Springer, Berlin, 2001. 50

[BC99] A. Buium and P. J. Cassidy. Differential algebraic geometry and differential algebraic groups: from algebraic differential equations to diophantine geometry. *[Kol99]*, pages 567–636, 1999. 7, 19, 67, 71

[Ber96] D. Bertrand. Book Review: Lectures on diffential galois theory. *Bull. Amer. Math. Soc. (N.S.)*, 33(2):289–294, 1996. 21

[BGLHR10] T. Bächler, V. P. Gerdt, M. Lange-Hegermann, and D. Robertz. Thomas decomposition of algebraic and differential systems. In *Proceedings of the 12th international conference on Computer algebra in scientific computing*, Springer Lecture Notes in Computer Science Volume 6244, pages 31–54, 2010. (`arXiv:1008.3767`). 26, 30

[BGLHR12] T. Bächler, V. P. Gerdt, M. Lange-Hegermann, and D. Robertz. Algorithmic Thomas decomposition of algebraic and differential systems. *J. Symbolic Comput.*, 47(10):1233–1266, 2012. (`arXiv:1108.0817`). 7, 30, 33, 35, 36, 55

[BH04] F. Boulier and E. Hubert. *DIFFALG: description, help pages and examples of use*, 1996-2004. Symbolic Computation Group, University of Waterloo, Ontario, Canada (`http://www-sop.inria.fr/members/Evelyne.Hubert/diffalg/`). 55

[BL07] F. Boulier and F. Lemaire. A computer scientist point of view on Hilbert's differential theorem of zeros. `http://hal.archives-ouvertes.fr/hal-00170091`, 2007. 63

[BLH12] Thomas Bächler and Markus Lange-Hegermann. *AlgebraicThomas and DifferentialThomas: Thomas Decomposition for algebraic and differential*

systems, 2008-2012.
(http://wwwb.math.rwth-aachen.de/thomasdecomposition/). 7, 53

[BLLM11] F. Boulier, M. Lefranc, F. Lemaire, and P. Morant. Model reduction of chemical reaction systems using elimination. *Math. Comput. Sci.*, 5(3):289–301, 2011. 152

[BLMM10] F. Boulier, F. Lemaire, and M. Moreno Maza. Computing differential characteristic sets by change of ordering. *J. Symbolic Comput.*, 45(1):124–149, 2010. 151

[BLOP95] F. Boulier, D. Lazard, F. Ollivier, and M. Petitot. Representation for the radical of a finitely generated differential ideal. In *ISSAC'95: Proceedings of the 1995 International Symposium on Symbolic and Algebraic Computation*, pages 158–166, New York, NY, USA, 1995. ACM Press. (http://hal.archives-ouvertes.fr/hal-00138020). 7, 45, 56

[BLOP09] F. Boulier, D. Lazard, F. Ollivier, and M. Petitot. Computing representations for radicals of finitely generated differential ideals. *Appl. Algebra Engrg. Comm. Comput.*, 20(1):73–121, 2009. 6, 7, 28, 45, 55, 56

[Bou09] F. Boulier. *BLAD: Bibliothéques Lilloises d'Algébre Différentielle*, 2004-2009. (http://www.lifl.fr/~boulier/BLAD/). 56

[BP] T. Bächler and W. Plesken. Counting polynomials for linear codes, hyperplane arrangements, and matroids. *Accepted for publication in Documenta Mathematica*. 97

[BR78] G. Birkhoff and G. Rota. *Ordinary differential equations*. John Wiley & Sons, New York-Chichester-Brisbane, third edition, 1978. 64

[Car31] É. Cartan. Sur la théorie des systèmes en involution et ses applications à la relativité. *Bulletin de la Société Mathématique de France*, 59:88–118, 1931. 6

[CE79] É. Cartan and A. Einstein. *Letters on absolute parallelism, 1929–1932*. Princeton University Press, Princeton, N.J., 1979. Original text with English translation by Jules Leroy and Jim Ritter, Edited by Robert Debever. 6, 70, 75, 105

[CGH+96] R. M. Corless, G. H. Gonnet, D. E. G. Hare, D. J. Jeffrey, and D. E. Knuth. On the Lambert W function. *Adv. Comput. Math.*, 5(4):329–359, 1996. 131

[CGL+07] C. Chen, O. Golubitsky, F. Lemaire, M. Moreno Maza, and W. Pan. Comprehensive triangular decomposition. In Victor G. Ganzha, Ernst W. Mayr, and Evgenii V. Vorozhtsov, editors, *CASC*, volume 4770 of *Lecture Notes in Computer Science*, pages 73–101. Springer, 2007. 120

[Chy98] F. Chyzak. *Fonctions holonomes en calcul formel*. PhD thesis, Ecole Polytechnique, France, 1998. 43

[Cim07] I. Cimrák. A survey on the numerics and computations for the landau-lifshitz equation of micromagnetism. *Archives of Computational Methods in Engineering*, 15(3):1–37, 2007. 50

[Cla36] A. C. Clairaut. Solution de plusieurs problemes où il s'agit de trouver des courbes dont la propriété consiste dans une certaine relation entre leurs branches, exprimée par une équation donnée. *Histoire de l'Acadèmie royale des sciences*, (1):196–215, 1736. 137

[CLO92] D. Cox, J. Little, and D. O'Shea. *Ideals, varieties, and algorithms*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1992. An introduction to computational algebraic geometry and commutative algebra. 45, 48

[Con81] J. B. Conway. *Subnormal Operators*. Research Notes in Mathematics. Pitman Advanced Pub. Program, 1981. 124

[Cou95] S. C. Coutinho. *A primer of algebraic D-modules*, volume 33 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1995. 73

[CQR04] F. Chyzak, A. Quadrat, and D. Robertz. OreModules: A symbolic package for the study of multidimensional linear systems. In *Proceedings MTNS, Belgium*. 2004. 43

[CQR07] F. Chyzak, A. Quadrat, and D. Robertz. OreModules: a symbolic package for the study of multidimensional linear systems. In *Applications of time delay systems*, volume 352 of *Lecture Notes in Control and Inform. Sci.*, pages 233–264. Springer, Berlin, 2007. (http://wwwb.math.rwth-aachen.de/OreModules). 43

[CS98] F. Chyzak and B. Salvy. Non-commutative elimination in Ore algebras proves multivariate identities. *J. Symbolic Comput.*, 26(2):187–227, 1998. 43

[CS99] M. Caboara and M. Silvestri. Classification of compatible module orderings. *J. Pure Appl. Algebra*, 142(1):13–24, 1999. 26

[CTR08] E. S. Cheb-Terrab and A. D. Roche. Hypergeometric solutions for third order linear odes, 2008. (arXiv:0803.3474). 5

[CTvB95] E. S. Cheb-Terrab and K. von Bülow. A computational approach for the analytical solving of partial differential equations. *Computer Physics Communications*, 90(1):102 – 116, 1995. 5

[Dar75] L. Dara. Singularités génériques des équations différentielles multiformes. *Bol. Soc. Brasil. Mat.*, 6(2):95–128, 1975. 177

[Dio91] S. Diop. Elimination in control theory. *Math. Control Signals Systems*, 4(1):17–32, 1991. 157

[Dio92] S. Diop. Differential-algebraic decision methods and some applications to system theory. *Theoret. Comput. Sci.*, 98(1):137–161, 1992. Second Workshop on Algebraic and Computer-theoretic Aspects of Formal Power Series (Paris, 1990). 157

[DL84] J. Denef and L. Lipshitz. Power series solutions of algebraic differential equations. *Math. Ann.*, 267(2):213–238, 1984. 9, 150

[Doe09] C. Doench. Bivariate difference-differential dimension polynomials and their computation in Maple. Technical Report 09-19, RISC Report Series, University of Linz, Austria, 2009. 71

[Ein53a] A. Einstein. *Appendix II of "The meaning of relativity, 4th ed."*. Princeton University Press, N. J., 1953. in [Ein53b]. 6, 57, 78

[Ein53b] A. Einstein. *The meaning of relativity*. Princeton University Press, Princeton, N. J., 1953. 4th ed. 188

[Ein53c] A. Einstein. *Supplement to Appendix II of "The meaning of relativity, 4th ed."*. Princeton University Press, N. J., 1953. 78

[Eis95] D. Eisenbud. *Commutative algebra*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995. With a view toward algebraic geometry. 67, 80, 82

[FG93] M. Fliess and S. T. Glad. An algebraic approach to linear and nonlinear control. In *Essays on control: perspectives in the theory and its applications (Groningen, 1993)*, volume 14 of *Progr. Systems Control Theory*, pages 223–265. Birkhäuser Boston, Boston, MA, 1993. 157

[Fli89] M. Fliess. Automatique et corps différentiels. *Forum Math.*, 1(3):227–238, 1989. 157

[FLMR95] M. Fliess, J. Lévine, P. Martin, and P. Rouchon. Flatness and defect of non-linear systems: introductory theory and examples. *Internat. J. Control*, 61(6):1327–1361, 1995. 157

[Ful93] William Fulton. *Introduction to toric varieties*, volume 131 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1993. The William H. Roever Lectures in Geometry. 98

[GB98a] V. P. Gerdt and Y. A. Blinkov. Involutive bases of polynomial ideals. *Math. Comput. Simulation*, 45(5-6):519–541, 1998. Simplification of systems of algebraic and differential equations with applications. 25, 27, 48, 55

[GB98b] V. P. Gerdt and Y. A. Blinkov. Minimal involutive bases. *Math. Comput. Simulation*, 45(5-6):543–560, 1998. Simplification of systems of algebraic and differential equations with applications. 29, 30

[Ger99] V. P. Gerdt. Completion of linear differential systems to involution. In *Computer algebra in scientific computing—CASC'99 (Munich)*, pages 115–137. Springer, Berlin, 1999. 26

[Ger02] V. P. Gerdt. On an algorithmic optimization in the computation of involutive bases. *Programming and Computer Software*, 28(2):62–65, 2002. 47

[Ger05] V. P. Gerdt. Involutive algorithms for computing Gröbner bases. In *Computational commutative and non-commutative algebraic geometry*, volume 196 of *NATO Sci. Ser. III Comput. Syst. Sci.*, pages 199–225. IOS, Amsterdam, 2005. 25, 27, 55

[Ger08] V. P. Gerdt. On decomposition of algebraic PDE systems into simple subsystems. *Acta Appl. Math.*, 101(1-3):39–51, 2008. 7, 30

[Ger09] V. P. Gerdt. Algebraically simple involutive differential systems and Cauchy problem. *Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI)*, 373(Teoriya Predstavlenii, Dinamicheskie Sistemy, Kombinatornye Metody. XVII):94–103, 347, 2009. 64

[GKO08] O. D. Golubitsky, M. V. Kondratieva, and A. I. Ovchinnikov. On the generalized Ritt problem as a computational problem. *Fundam. Prikl. Mat.*, 14(4):109–120, 2008. 168

[GKOS09] O. Golubitsky, M. Kondratieva, A. Ovchinnikov, and A. Szanto. A bound for orders in differential Nullstellensatz. *J. Algebra*, 322(11):3852–3877, 2009. 54

[Gla90] S. T. Glad. Differential algebraic modelling of nonlinear systems. In *Realization and modelling in system theory (Amsterdam, 1989)*, volume 3 of *Progr. Systems Control Theory*, pages 97–105. Birkhäuser Boston, Boston, MA, 1990. 157

[GMO91] G. Gallo, B. Mishra, and F. Ollivier. Some constructions in rings of differential polynomials. In *Applied algebra, algebraic algorithms and error-correcting codes (New Orleans, LA, 1991)*, volume 539 of *Lecture Notes in Comput. Sci.*, pages 171–182. Springer, Berlin, 1991. 67

[GP08] G. Greuel and G. Pfister. *A* **Singular** *introduction to commutative algebra*. Springer, Berlin, extended edition, 2008. With contributions by Olaf Bachmann, Christoph Lossen and Hans Schönemann, With 1 CD-ROM (Windows, Macintosh and UNIX). 73

[GS91] D. Yu. Grigor′ev and M. F. Singer. Solving ordinary differential equations in terms of series with real exponents. *Trans. Amer. Math. Soc.*, 327(1):329–351, 1991. 150

[GY06] V. P. Gerdt and D. A. Yanovich. Investigation of the effectiveness of involutive criteria for computing polynomial Janet bases. *Programming and Computer Software*, 32(3):134–138, 2006. 55

[GYB01] V. P. Gerdt, D. A. Yanovich, and Y. A. Blinkov. Fast search for the Janet divisor. *Programming and Computer Software*, 27(1):22–24, 2001. 27

[Hab48] W. Habicht. Eine Verallgemeinerung des Sturmschen Wurzelzählverfahrens. *Comment. Math. Helv.*, 21:99–116, 1948. 33

[Had53] J. Hadamard. *Lectures on Cauchy's problem in linear partial differential equations*. Dover Publications, New York, 1953. 57

[HLR03] E. Hubert and N. Le Roux. Computing power series solutions of a nonlinear PDE system. In *Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation*, pages 148–155 (electronic), New York, 2003. ACM. 63

[Hoe77] C. Hoenselaers. The "strength" of a system of differential equations. *Progr. Theoret. Phys.*, 58(4):1185–1190, 1977. 78

[Hub99] E. Hubert. Essential components of an algebraic differential equation. *J. Symbolic Comput.*, 28(4-5):657–680, 1999. Differential algebra and differential equations. 168

[Hub00] E. Hubert. Factorization-free decomposition algorithms in differential algebra. *J. Symbolic Comput.*, 29(4-5):641–662, 2000. Symbolic computation in algebra, analysis, and geometry (Berkeley, CA, 1998). 6

[Hub03a] E. Hubert. Notes on triangular sets and triangulation-decomposition algorithms. I. Polynomial systems. In *Symbolic and numerical scientific computation (Hagenberg, 2001)*, volume 2630 of *Lecture Notes in Comput. Sci.*, pages 1–39. Springer, Berlin, 2003. 66, 81, 82

[Hub03b] E. Hubert. Notes on triangular sets and triangulation-decomposition algorithms. II. Differential systems. In *Symbolic and numerical scientific computation (Hagenberg, 2001)*, volume 2630 of *Lecture Notes in Comput. Sci.*, pages 40–87. Springer, Berlin, 2003. 45

[Inc44] E. L. Ince. *Ordinary Differential Equations.* Dover Publications, New York, 1944. 137

[Jac69] C. G. J. Jacobi. *Gesammelte Werke. Bände I–VIII.* Herausgegeben auf Veranlassung der Königlich Preussischen Akademie der Wissenschaften. Zweite Ausgabe. Chelsea Publishing Co., New York, 1969. 190

[Jac09] C. G. J. Jacobi. Looking for the order of a system of arbitrary ordinary differential equations. De investigando ordine systematis æquationibus differentialium vulgarium cujuscunque. *Appl. Algebra Engrg. Comm. Comput.*, 20(1):7–32, 2009. Translated from the Latin manuscript by François Ollivier, Edited by S. Cohn and C. W. Borchardt; see also [Jac69, Band V, p. 191-216]. 163

[Jan21] M. Janet. Sur les systemes aux dérivées partielles comprenant autant d'équations qui de fonctiones inconnues. *Acad. Sci. Paris*, 172:1637–1639, 1921. 7, 163

[Jan29] M. Janet. *Leçons sur les systèmes d'équations aux dérivées partielles.* Cahiers Scientifiques IV. Gauthiers-Villars, Paris, 1929. 7, 25

[Joh69a] J. Johnson. Differential dimension polynomials and a fundamental theorem on differential modules. *Amer. J. Math.*, 91:239–248, 1969. 70

[Joh69b] J. Johnson. A notion of Krull dimension for differential rings. *Comment. Math. Helv.*, 44:207–216, 1969. 79

[Joh78] J. Johnson. Systems of n partial differential equations in n unknown functions: the conjecture of M. Janet. *Trans. Amer. Math. Soc.* **242**, pages 329–334, 1978. 163

[Kap57] I. Kaplansky. *An introduction to differential algebra.* Actualités scientifiques et industrielles. Hermann, 1957. 21

[KB70] D. E. Knuth and P. B. Bendix. Simple word problems in universal algebras. In *Computational Problems in Abstract Algebra (Proc. Conf., Oxford, 1967)*, pages 263–297. Pergamon, Oxford, 1970. 14

[KLMP99] M. V. Kondratieva, A. B. Levin, A. V. Mikhalev, and E. V. Pankratiev. *Differential and difference dimension polynomials*, volume 461 of *Mathematics and its Applications*. Kluwer Academic Publishers, Dordrecht, 1999. 71, 78, 80, 163

[KMP08] M. V. Kondratieva, A. V. Mikhalev, and E. V. Pankratiev. Jacobi's bound for systems of algebraic differential equations. *Fundam. Prikl. Mat.*, 14(4):151–166, 2008. 164

[Kol64] E. R. Kolchin. The notion of dimension in the theory of algebraic differential equations. *Bull. Amer. Math. Soc.*, 70:570–573, 1964. 6, 70

[Kol73] E. R. Kolchin. *Differential algebra and algebraic groups*. Academic Press, New York, 1973. Pure and Applied Mathematics, Vol. 54. 29, 45, 55, 67, 68, 71, 73, 84, 165, 167, 168

[Kol99] E. R. Kolchin. *Selected works of Ellis Kolchin with commentary*. American Mathematical Society, Providence, RI, 1999. Commentaries by Armand Borel, Michael F. Singer, Bruno Poizat, Alexandru Buium and Phyllis J. Cassidy, edited and with a preface by Hyman Bass, Buium and Cassidy. 185

[KRMS98] Abdelilah Kandri Rody, Hamid Maârouf, and Mohamed Ssafini. Triviality and dimension of a system of algebraic differential equations. *J. Automat. Reason.*, 20(3):365–385, 1998. 56

[KS72] H. Kwakernaak and R. Sivan. *Linear optimal control systems*. Wiley-Interscience [John Wiley & Sons], New York, 1972. 158

[KS12] U. Kant and W.M. Seiler. Singularities in the geometric theory of differential equations. In W. Feng, Z. Feng, M. Grasselli, X. Lu, S. Siegmund, and J. Voigt, editors, *Dynamical Systems, Differential Equations and Applications (Proc. 8th AIMS Conference, Dresden 2010)*, volume 2, pages 784–793. AIMS, 2012. 93, 176

[Lan70] B. A. Lando. Jacobi's bound for the order of systems of first order differential equations. *Trans. Amer. Math. Soc.*, 152:119–135, 1970. 164

[Lev45] H. Levi. The low power theorem for partial differential polynomials. *Ann. of Math. (2)*, 46:113–119, 1945. 168

[Lev10] A. Levin. Dimension polynomials of intermediate fields and Krull-type dimension of finitely generated differential field extensions. *Math. Comput. Sci.*, 4(2-3):143–150, 2010. 71

[Lew57] H. Lewy. An example of a smooth linear partial differential equation without solution. *Ann. of Math. (2)*, 66:155–158, 1957. 6

[LHR13] M. Lange-Hegermann and D. Robertz. Thomas decomposition of parametric nonlinear control systems. In *proceedings of the IFAC Joint conference*, pages 296–301, 2013. (`arXiv:1212.0377`). 30, 157

[Lie67] S. Lie. *Differentialgleichungen*. Chelsea Publishing Series. Chelsea Publ., 1967. 95

[LMMX05] F. Lemaire, M. Moreno Maza, and Y. Xie. The RegularChains library in Maple. *SIGSAM Bull.*, 39(3):96–97, 2005. 55

[LS03] Viktor Levandovskyy and Hans Schönemann. PLURAL—a computer algebra system for noncommutative polynomial algebras. In *Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation*, pages 176–183 (electronic), New York, 2003. ACM. 43

[MAKA09] T. McGrew, M. Alspector-Kelly, and F. Allhoff. *The philosophy of science: an historical anthology*. Blackwell philosophy anthologies. Wiley-Blackwell, 2009. 151

[map] Maple 17.00. Maplesoft, a division of Waterloo Maple Inc., Waterloo, Ontario. 15, 19, 53, 55, 72, 125, 131, 141, 143, 148

[Mar74] K. H. Mariwalla. Applications of the concept of strength of a system of partial differential equations. *J. Mathematical Phys.*, 15:468–473, 1974. 78

[Mar11] M. A. Marco-Buzunáriz. A polynomial generalization of the Euler characteristic for algebraic sets. *ArXiv e-prints*, November 2011. 98

[Mat77] Ju. V. Matijasevič. Primes are enumerated by a polynomial in 10 variables. *Zap. Naučn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI)*, 68:62–82, 144–145, 1977. Theoretical applications of the methods of mathematical logic, II. 150

[Mat87] N. F. J. Matthews. On the strength of Maxwell's equations. *J. Math. Phys.*, 28(4):810–814, 1987. 78

[Mat92] N. F. J. Matthews. The strength of Einstein's equations. *Gen. Relativity Gravitation*, 24(1):17–33, 1992. 78

[Mis93] B. Mishra. *Algorithmic algebra*. Texts and Monographs in Computer Science. Springer-Verlag, New York, 1993. 33

[MM99] M. Moreno Maza. On triangular decompositions of algebraic varieties. Technical report, presented at the MEGA-2000 Conference, 1999. 30

[Mül07] F. Müller. Hopf bifurcation in landau-lifshitz-gilbert dynamics with a spin torque. 2007. Matheon preprint, `http://nbn-resolving.de/urn:nbn:de:0296-matheon-4022`. 49, 50

[Mur02] J. D. Murray. *Mathematical biology. I*, volume 17 of *Interdisciplinary Applied Mathematics*. Springer-Verlag, New York, third edition, 2002. An introduction. 130

[NM03] I. Newton and A. Motte. *Sir Isaac Newton's Mathematical Principles of Natural Philosophy and His System of the World*. Kessinger Publishing, 2003. Translation by Motte, A. 151

[NS92] W. Neutsch and K. Scherer. *Celestial mechanics*. Bibliographisches Institut, Mannheim, 1992. An introduction to classical and contemporary methods. 154, 156

[P97] A. Péladan. *Tests effectifs de nullité dans les extensions d'anneaux différentiels*. PhD thesis, École Polytechnique, 1997. 60

[PER81] Marian Boykan Pour-El and Ian Richards. The wave equation with computable initial data such that its unique solution is not computable. *Adv. in Math.*, 39(3):215–239, 1981. 9

[Ple09a] W. Plesken. Counting solutions of polynomial systems via iterated fibrations. *Arch. Math. (Basel)*, 92(1):44–56, 2009. 8, 23, 96, 97, 103

[Ple09b] W. Plesken. Gauss-Bruhat decomposition as an example of Thomas decomposition. *Arch. Math. (Basel)*, 92(2):111–118, 2009. 8

[Poi14] H. Poincaré. *Science and Method*. 1914. 171

[Pom78] J.-F. Pommaret. *Systems of partial differential equations and Lie pseudogroups*, volume 14 of *Mathematics and its Applications*. Gordon & Breach Science Publishers, New York, 1978. With a preface by André Lichnerowicz. 172

[Pom94] J.-F. Pommaret. *Partial differential equations and group theory*, volume 293 of *Mathematics and its Applications*. Kluwer Academic Publishers Group, Dordrecht, 1994. New perspectives for applications. 76

[Pom01] J.-F. Pommaret. *Partial differential control theory*, volume 530 of *Mathematics and its Applications*. Kluwer Academic Publishers Group, Dordrecht, 2001. Vol. I. Mathematical tools; Vol. II. Control systems, With a foreword by Jan C. Willems. 157

[Por01] I. R. Porteous. *Geometric differentiation*. Cambridge University Press, Cambridge, second edition, 2001. For the intelligence of curves and surfaces. 133

[PR05] W. Plesken and D. Robertz. Janet's approach to presentations and resolutions for polynomials and linear PDEs. *Arch. Math. (Basel)*, 84(1):22–37, 2005. 61

[Rab60] M. O. Rabin. Computable algebra, general theory and theory of computable fields. *Trans. Amer. Math. Soc.*, 95:341–360, 1960. 30

[Rau34] H. W. Raudenbush, Jr. Ideal theory and algebraic differential equations. *Trans. Amer. Math. Soc.*, 36(2):361–368, 1934. 68

[Riq93] C. Riquier. De l'existence des intégrales dans un système différentiel quelconque (suite et fin). *Ann. Sci. École Norm. Sup. (3)*, 10:167–181, 1893. 7

[Riq10] C. Riquier. *Les systèmes d'équations aux dérivées partielles*. Gauthiers-Villars, Paris, 1910. 64

[Rit30] J. F. Ritt. Manifolds of functions defined by systems of algebraic differential equations. *Trans. Amer. Math. Soc.*, 32(4):569–599, 1930. 167

[Rit32] J. F. Ritt. *Differential Equations from the Algebraic Standpoint*. American Mathematical Society, 1932. 68, 163, 165, 167, 168

[Rit35] J. F. Ritt. Jacobi's problem on the order of a system of differential equations. *Ann. of Math. (2)*, 36(2):303–312, 1935. 164

[Rit36] J. F. Ritt. On the singular solutions of algebraic differential equations. *Ann. of Math. (2)*, 37(3):552–617, 1936. 167, 168

[Rit38a] J. F. Ritt. Algebraic aspects of the theory of differential equations. *Semicentennial Addresses of the American Mathematical Society*, II:35–55, 1938. 66

[Rit38b] J. F. Ritt. On Certain Points in the Theory of Algebraic Differential Equations. *Amer. J. Math.*, 60(1):1–43, 1938. 168

[Rit41] J. F. Ritt. Complete difference ideals. *Amer. J. Math.*, 63:681–690, 1941. 168

[Rit45] J. F. Ritt. On the manifold of partial differential polynomials. *Ann. of Math. (2)*, 46:102–112, 1945. 167

[Rit46] J. F. Ritt. On the singular solutions of certain differential equations of the second order. *Proc. Nat. Acad. Sci. U. S. A.*, 32:255–258, 1946. 168

[Rit50] J. F. Ritt. *Differential Algebra*. American Mathematical Society Colloquium Publications, Vol. XXXIII. American Mathematical Society, New York, N. Y., 1950. 7, 56, 64, 151, 167, 168

[Rob85] L. Robbiano. Term orderings on the polynomial ring. In *EUROCAL '85, Vol. 2 (Linz, 1985)*, volume 204 of *Lecture Notes in Comput. Sci.*, pages 513–517. Springer, Berlin, 1985. 26

[Rob06] D. Robertz. *Formal Computational Methods for Control Theory*. PhD thesis, RWTH Aachen, Germany, June 2006. This thesis is available at `http://darwin.bth.rwth-aachen.de/opus/volltexte/2006/1586`. 43

[Rob07] D. Robertz. Janet bases and applications. In *Gröbner bases in symbolic analysis*, volume 2 of *Radon Ser. Comput. Appl. Math.*, pages 139–168. Walter de Gruyter, Berlin, 2007. 43

[Rob12] D. Robertz. Formal Algorithmic Elimination for PDEs. June 2012. Habilitationsschrift, accepted by the Faculty of Mathematics, Computer Science and Natural Sciences, RWTH Aachen University, 2012. 30, 43, 61, 66, 67, 68, 69, 73, 80, 152

[Ros59] A. Rosenfeld. Specializations in differential algebra. *Trans. Amer. Math. Soc.*, 90:394–407, 1959. 7, 45, 56

[RR97] C. J. Rust and G. J. Reid. Rankings of partial derivatives. In *Proceedings of the 1997 international symposium on Symbolic and algebraic computation*, ISSAC '97, pages 9–16, New York, NY, USA, 1997. ACM. 26

[Sag80] C. Sagan. *Cosmos*. Cosmos (Television program). Random House Publishing Group, 1980. 151

[Sch75] B. F. Schutz. On the strength of a system of partial differential equations. *J. Mathematical Phys.*, 16:855–856, 1975. 78

[Sei56] A. Seidenberg. An elimination theory for differential algebra. *Univ. California Publ. Math. (N.S.)*, 3:31–65, 1956. 7, 151

[Sei58] A. Seidenberg. Abstract differential algebra and the analytic case. *Proc. Amer. Math. Soc.*, 9:159–164, 1958. 60

[Sei69] A. Seidenberg. Abstract differential algebra and the analytic case II. *Proc. Amer. Math. Soc.*, 23:689–691, 1969. 60

[Sei94] W. M. Seiler. On the arbitrariness of the general solution of an involutive partial differential equation. *J. Math. Phys.*, 35(1):486–498, 1994. 77, 78

[Sei95] W. M. Seiler. Arbitrariness of the general solution and symmetries. *Acta Appl. Math.*, 41(1-3):311–322, 1995. Geometric and algebraic structures in differential equations. 78

[Sei10] W. M. Seiler. *Involution*, volume 24 of *Algorithms and Computation in Mathematics*. Springer-Verlag, Berlin, 2010. The formal theory of differential equations and its applications in computer algebra. 25, 26, 76, 78, 172

[Spa81] E. H. Spanier. *Algebraic topology*. Springer-Verlag, New York, 1981. Corrected reprint. 98

[Sué91] M. Sué. Involutive systems of differential equations: Einstein's strength versus Cartan's degré d'arbitraire. *J. Math. Phys.*, 32(2):392–399, 1991. 78

[Tay] B. Taylor. Methodus incrementorum directa & inversa. Translation of [Tay17] by Ian Bruce (`http://www.17centurymaths.com/contents/taylorscontents.html`). 137

[Tay17] B. Taylor. *Methodus Incrementorum Directa & Inversa*. Inny, 1717. 195

[Tho34] J. M. Thomas. Riquier's existence theorems. *Ann. of Math. (2)*, 35(2):306–311, 1934. 64

[Tho37] J. M. Thomas. *Differential Systems*. AMS Colloquium Publications vol XXI, 1937. 7, 21, 23, 55

[Tho40] J. M. Thomas. Orderly differential systems. *Duke Math. J.*, 7:249–290, 1940. 7, 64

[Tho62] J. M. Thomas. *Systems and Roots*. The William Byrd Press, INC, Richmond Virginia, 1962. 7, 23, 55

[Tho29] J. M. Thomas. Riquier's existence theorems. *Ann. of Math. (2)*, 30(1-4):285–310, 1928/29. 64

[Tom76] Tomasovic. *A Generalized Jacobi Conjecture for Arbitrary Systems of Algebraic Differential Equations*. PhD thesis, Columbia University, 1976. 164

[Tre94] Ar. Tresse. Sur les invariants différentiels des groupes continus de transformations. *Acta Math.*, 18(1):1–3, 1894. 7

[Ves24] E. Vessiot. Sur une théorie nouvelle des problèmes généraux d'intégration. *S. M. F. Bull.*, 52:336–395, 1924. 172

[Wan95] D. Wang. A method for proving theorems in differential geometry and mechanics. *J.UCS*, 1(9):658–673, 1995. 151, 152

[Wan98] D. Wang. Decomposing polynomial systems into simple systems. *J. Symbolic Comput.*, 25(3):295–314, 1998. 7, 23, 30, 33

[Wan03] D. Wang. *ϵpsilon: description, help pages and examples of use*, 2003. (http://www-spiral.lip6.fr/~wang/epsilon/). 55

[Wei] Z. Weinersmith. Saturday morning breakfast cereal. webcomic. www.smbc-comics.com/. 30

[Wei87] V. Weispfenning. Admissible orders and linear forms. *SIGSAM Bull.*, 21(2):16–18, May 1987. 26

[Wu91] W.-T. Wu. Mechanical theorem proving of differential geometries and some of its applications in mechanics. *J. Automat. Reason.*, 7(2):171–191, 1991. 152

[Yap00] C. K. Yap. *Fundamental problems of algorithmic algebra*. Oxford University Press, New York, 2000. 33

Index

Symbols