JOHANNES KEPLER
UNIVERSITÄT LINZ

Eingereicht von
Yi Zhang

Angefertigt am
Institute for Algebra

Betreuer und
Erstbeurteiler
Prof. Dr. Manuel Kauers

Zweitbeurteiler
Prof. Dr. Ziming Li

Mitbetreuung
Prof. Dr. Ziming Li

November 2016

Univariate Contraction and Multivariate Desingularization of Ore Ideals

Dissertation
zur Erlangung des akademischen Grades
Doktor der Naturwissenschaften
im Doktoratsstudium
Naturwissenschaften

JOHANNES KEPLER
UNIVERSITÄT LINZ
Altenbergerstraße 69
4040 Linz, Österreich
www.jku.at
DVR 0093696

Eidesstattliche Erklärung

Ich erkläre an Eides statt, dass ich die vorliegende Dissertation selbstständig und ohne fremde Hilfe verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt bzw. die wörtlich oder sinngemäß entnommenen Stellen als solche kenntlich gemacht habe.

Die vorliegende Dissertation ist mit dem elektronisch übermittelten Textdokument identisch.

Linz, November 2016

Yi Zhang

Kurzzusammenfassung

Gewöhnliche Lineare Differential- (und Differenzen-) Operatoren mit polynomiellen Koeffizienten sind eine bekannte algebraische Abstraktion zur Darstellung von D-finiten Funktionen (bzw. P-finiten Folgen). Sie bilden den Ore-Ring $\mathbb{K}(x)[\partial]$, wobei $\mathbb{K}$ der Konstantenkörper ist. Es sei angenommen, dass $\mathbb{K}$ der Quotientenkörper eines Hauptidealrings R ist. Der Ring $R[x][\partial]$ besteht aus den Elementen von $\mathbb{K}(x)[\partial]$ "ohne Nenner".

Ein gegebenes $L \in \mathbb{K}(x)[\partial]$ erzeugt ein Linksideal I in $\mathbb{K}(x)[\partial]$. Wir nennen $I \cap R[x][\partial]$ die univariate Kontraktion des Ore-Ideals I. Kontraktionsalgorithmus für L.

Wenn L ein gewöhnlicher linearer Differential- oder Differenzenoperator ist, entwickeln wir einen Kontraktionsalgorithmus für L, indem wir desingularisierte Operatoren verwenden, wie sie von Chen, Jaroschek, Kauers und Singer vorgeschlagen wurden. Wenn L ein gewöhnlicher Differentialoperator ist und $R = \mathbb{K}$, dann ist unser Algorithmus elementarer als bekannte Algorithmen. In anderen Flällen sind unsere Resultate neu.

Wir schlagen den Begriff des vollständig desingularisierten Operators vor, untersuchen ihre Eigenschaften, und entwickeln einen Algorithmus zu deren Berechnung. Vollständig desingularisierte Operatoren haben interessante Anwendungen wie die Zertifizierung ganzzahliger Folgen und die Überprüfung von Spezialfällen einer Vermutung von Krattenthaler.

Ein D-finites System ist eine endliche Menge von homogenen linearen partiellen Differentialgleichungen mit polynomiellen Koeffizienten in mehreren Variablen, deren Lösungsraum endliche Dimension hat. Für solche Systeme definieren wir den Begriff der Singularität anhand der in ihnen auftretenden Polynome. Wir zeigen, dass ein Punkt eine Singularität eines Systems ist, wenn es nicht eine Basis von Potenzreihenlösungen hat, deren Startterme bezüglich einer Termordnung kleinstmöglich sind. Als nächstes ist eine Singularität scheinbar, wenn das System eine volle Basis von Potenzreihenlösungen hat, deren Startterme nicht kleinstmöglich sind. Wir zeigen dann, dass scheinbare Singularitäten im multivariaten Fall genauso wie im univariaten Fall durch Hinzufügen geeigneter neuer Lösungen zum vorliegenden System entfernt werden können.

Abstract

Linear ordinary differential (difference) operators with polynomial coefficients form a common algebraic abstraction for representing D-finite functions (P-recursive sequences). They form the Ore ring $\mathbb{K}(x)[\partial]$, where $\mathbb{K}$ is the constant field. Suppose $\mathbb{K}$ is the quotient field of some principal ideal domain R. The ring $R[x][\partial]$ consists of elements in $\mathbb{K}(x)[\partial]$ without "denominator".

Given $L \in \mathbb{K}(x)[\partial]$, it generates a left ideal I in $\mathbb{K}(x)[\partial]$. We call $I \cap R[x][\partial]$ the univariate contraction of the Ore ideal I.

When L is a linear ordinary differential or difference operator, we design a contraction algorithm for L by using desingularized operators as proposed by Chen, Jaroschek, Kauers and Singer. When L is an ordinary differential operator and $R = \mathbb{K}$, our algorithm is more elementary than known algorithms. In other cases, our results are new.

We propose the notion of completely desingularized operators, study their properties, and design an algorithm for computing them. Completely desingularized operators have interesting applications such as certifying integer sequences and checking special cases of a conjecture of Krattenthaler.

A D-finite system is a finite set of linear homogeneous partial differential equations with polynomial coefficients in several variables, whose solution space is of finite dimension. For such systems, we define the notion of a singularity in terms of the polynomials appearing in them. We show that a point is a singularity of the system unless it admits a basis of power series solutions in which the starting monomials are as small as possible with respect to some term order. Then a singularity is apparent if the system admits a full basis of power series solutions, the starting terms of which are not as small as possible. We then prove that apparent singularities in the multivariate case can be removed like in the univariate case by adding suitable additional solutions to the system at hand.

Acknowledgements

As Socrates said, "Education is not the filling of a vessel, but the kinding of a flame". I would like to thank my supervisors Manuel Kauers and Ziming Li for guiding me to the research field of computer algebra and providing me the current Ph.D. topic. I am very grateful to Professor Manuel Kauers for initiating this research project, stimulating inspirational discussions, helping me revise papers, and sharing his immense knowledge in mathematics, programming and LaTeX. Besides, he also teaches me a lot about how to design slides and give a talk in an appropriate way. Professor Ziming Li influences me a lot for his rigorous and practical attitude towards both teaching and research, optimistic character for life, diligency and patience for supervising students. In particular, I learn a lot about how to write readable papers by working with him. Hereby, I would like to express my sincere gratitude again to both of them.

I would like to thank the following members in Research Institute for Symbolic Computation for their valuable help: Bruno Buchberger, Peter Paule, Franz Winkler, Jakob Ablinger, Johannes Middeke, Veronika Pillwein, Cristian-Silviu Radu, Tanja Gutenbrunner, Ilse Brandner-Foißner, Alexander Maletzky, Evans Doe Ocansey, Miriam Schussler, Liangjie Ye and Thieu Vo Ngoc. In particular, I thank Ralf Hemmecke for teaching me how to use the Ubuntu system. Special thanks go to Christoph Koutschan who helps me with `Mathematica` programming and provides me a postdoctoral position in his FWF-funded project "Algebraic Statistic and Symbolic Computation".

I would like to thank the following members in Institute for Algebra for their valuable help: Günter Pilz, Erhard Aichinger, Peter Fuchs, Peter Mayr, Markus Hetzmannseder, Carmen Schacherreiter, Markus Steidl, Rika Yatchak, Georg Regensburger, Clemens Raab, Hui Huang and Ronghua Wang.

I would like to thank the following members in Key Laboratory of Mathematics Mechanization for their valuable help: Wen-Tsun Wu and Xiaoshan Gao. In particular, I thank Shaoshi Chen for useful suggestions about my study and research, providing valuable information on literatures for revising my ISSAC paper.

I also want to acknowledge the financial support of the Austrian Science Fund FWF, namely the grant Y464-N18.

Last but not least, I want to thank my family for their support and understanding for both my life and study, which enable me to finish my Ph.D. thesis successfully. Thank you!

Contents

Chapter 1

Introduction

1.1 Background and motivation

D-finite functions play an important role in the part of computer algebra concerned with algorithms [25] for special functions. They are interesting in two aspects: On the one hand, they can be easily described by a finite amount of data, and efficient algorithms are available to do exact as well as approximate computation with them. On the other hand, they cover a lot of special functions which naturally appear in various different context, both within mathematics as well as applications, such as physics, engineering, statistics, combinatorics and so on. The notion was introduced by Stanley in 1980 [45]. The defining property of a D-finite function is that it satisfies a linear differential equation with polynomial coefficients. This differential equation, together with an appropriate number of initial terms, uniquely determines the function at hand. Investigation of singularities of a linear differential equation gives an opportunity to study singularities of D-finite functions without solving this equation.

There are various reasons why linear differential equations are easier than non-linear ones. One is of course that the solutions of linear differential equations form a vector space over the underlying field of constants. Another important feature concerns the singularities. While for a nonlinear differential equation the location of the singularities may depend continuously on the initial values, this is not possible for linear equations. Instead, a solution f of a differential equation

$$a_0(x)f(x) + \cdots + a_r(x)f^{(r)}(x) = 0,$$

where $a_0, \ldots, a_r$ are some analytic functions, can only have singularities at points $\xi \in \mathbb{C}$ with the property $a_r(\xi) = 0$. For example, x^{-1} is a solution of the equation $xf'(x) + f(x) = 0$, and the singularity at 0 is reflected by the root of the polynomial x in front of the term $f'(x)$ in the equation. Unfortunately, the converse is not true: there may be roots of the leading coefficient which do not indicate solutions that are singular there. For example, all the solutions of the equation $xf'(x) - 5f(x) = 0$ are constant multiples of x^5, and none of these functions is singular at 0.

In this thesis, we consider the case where $a_0, \ldots, a_r$ are polynomials and $a_r \neq 0$. In this case, a_r can have only finitely many roots. The roots of a_r are called the singularities of the equation. Those roots α of a_r such that the equation has no solution that is singular at α are called *apparent.* In other words, a root α of a_r is apparent if the equation admits r linearly independent formal power series solutions in $x - \alpha$. Deciding whether a singularity is apparent is therefore the same as checking whether the equation admits a fundamental system of formal power series solutions at this point. This can be done by inspecting the so-called *indicial polynomial* of the equation at α: if there exists a power series solution of the form $(x-\alpha)^\ell + \cdots$, then ℓ is the root of this polynomial.

When some singularity α of an ODE is apparent, then it is always possible to construct a second ODE whose solution space contains all the solutions of the first ODE, and which does not have α as a singularity. This process is called desingularization. The idea is easily explained. The key observation is that a point α is a singularity if and only if the indicial polynomial at α is different from $n(n-1)\cdots(n-r+1)$ or the ODE does not admits r linearly independent formal power series solutions in $x - \alpha$. As the indicial polynomial at an apparent singularity has only nonnegative integer roots, we can bring it into the required form by adding a finite number of new factors. Adding a factor $n - s$ to the indicial polynomial amounts to adding a solution of the form $(x-\alpha)^s + \cdots$ to the solution space, and this is an easy thing to do using well-known arithmetic of differential operators. See [1, 4, 11, 22, 23] for an expanded version of this argument and [1, 2] for analogous algorithms for recurrence equations.

We shall also consider the case of recurrence equations

$$a_0(n)f(n) + \cdots + a_r(n)f(n+r) = 0,$$

where again there is a strong connection between the roots of a_r and the singularities of a solution. As an example, consider the recurrence operator

$$L = (1+16n)^2\partial^2 - 32(7+16n)\partial - (1+n)(17+16n)^2,$$

which is taken from [1, Section 4.1]. Here, ∂ denotes the shift operator $f(n) \mapsto f(n+1)$. For any choice of two initial values $u_0, u_1 \in \mathbb{Q}$, there is a unique sequence $u\colon \mathbb{N} \to \mathbb{Q}$ with

$$u(0) = u_0,\ u(1) = u_1$$

and L applied to u gives the zero sequence. A priori, it is not obvious whether or not u is actually an integer sequence, if we choose u_0, u_1 from $\mathbb{Z}$, because the calculation of the $(n+2)$nd term from the earlier terms via the recurrence encoded by L requires a division by $(1+16n)^2$, which could introduce fractions. In order to show that this division never introduces a denominator, the authors of [1] note that every solution of L is also a solution of its left multiple

$$\begin{aligned} T &= \left(\frac{64}{(17+16n)^2}\partial + \frac{(23+16n)(25+16n)}{(17+16n)^2}\right) L \\ &= 64\partial^3 + (16n+23)(16n-7)\partial^2 - (576n+928)\partial \\ &\quad -(16n+23)(16n+25)(n+1). \end{aligned}$$

The operator T has the interesting property that the factor $(1+16n)^2$ has been "removed" from the leading coefficient. This is, however, not quite enough to complete the proof, because now a denominator could still arise from the division by 64 at each calculation of a new term via T. To complete the proof, Abramov, Barkatou and van Hoeij show that the potential denominators introduced by $(1+16n)^2$ and by 64, respectively, are in conflict with each other, and therefore no such denominators can occur at all.

The process of obtaining the operator T from L is also called desingularization, because there is a polynomial factor in the leading coefficient of L which does not appear in the leading coefficient of T. In the literature, there are some other applications of desingularization, such as extending P-recursive sequences [2] or explaining order-degree curve [10] for Ore operators.

In the example above, the price to be paid for the desingularization was a new constant factor 64 which appears in the leading coefficient of T but not in the original leading coefficient of L. Known algorithms for desingularization have two ways of thinking: (i) Literature [2, 1, 10, 11] achieve it by computing an appropriate left multiple of L, whose solution space in general strictly contains that of L. (ii) Paper [4] makes it through choosing an adequate gauge transformation. The solution space of the corresponding output is equivalent to that of L, and thus keeps the dimension invariant. However, all those results care only about the removal of polynomial factors without introducing new polynomial factors, but they do not consider the possible introduction of new constant factors. A contribution of the present thesis is a desingularization algorithm which minimizes, in a sense, also any constant factors introduced during the desingularization. For example, for the operator L above, our algorithm finds the alternative desingularization

$$\begin{aligned}\tilde{T} \;=\;& \partial^3 + \left(128n^3 - 104n^2 - 11n - 3\right)\partial^2 + \\ & \left(-256n^2 + 127n + 94\right)\partial - \\ & (128n^2 + 24n - 131)(1+n)^2,\end{aligned} \tag{1.1}$$

which immediately certifies the integrality of its solutions.

In more algebraic terms, we consider the following problem. Assume that L is an operator in $\mathbb{Z}[x][\partial]$, which is an Ore algebra (see Section 3.1 for definitions), we consider the left ideal $\langle L\rangle = \mathbb{Q}(x)[\partial]L$ generated by L in the extended algebra $\mathbb{Q}(x)[\partial]$. The univariate contraction of the Ore ideal $\langle L\rangle$ to $\mathbb{Z}[x][\partial]$ is defined as $\operatorname{Cont}(L) := \langle L\rangle \cap \mathbb{Z}[x][\partial]$. This is a left ideal of $\mathbb{Z}[x][\partial]$ which contains $\mathbb{Z}[x][\partial]L$, but in general more operators. Our goal is to compute a $\mathbb{Z}[x][\partial]$-basis of $\operatorname{Cont}(L)$. In the example above, such a basis is given by $\{L, \tilde{T}\}$ (see Example 3.3.11). The traditional desingularization problem corresponds to computing a basis of the $\mathbb{Q}[x][\partial]$-left ideal $\langle L\rangle \cap \mathbb{Q}[x][\partial]$.

The univariate contraction problem for Ore algebras $\mathbb{Q}[x][\partial]$ was proposed by Chyzak and Salvy [14, Section 4.3]. For the analogous problem in commutative polynomial rings, there is a standard solution via Gröbner bases [5, Section 8.7]. It reduces the contraction problem to a saturation problem. This reduction also works for the differential case, but in that case it is not so helpful because it is less obvious how to solve the saturation problem. In this case, the problem is also called the Weyl closure problem, which has important applications in non-commutative elimination and symbolic integration [7]. The Weyl closure of a left ideal in $\mathbb{K}(\mathbf{x})[\boldsymbol{\partial}]$ (see Section 4.1) is a differential analog of the radical of an ideal in the commutative polynomial ring $\mathbb{K}[\mathbf{x}]$. To be specific, assume that $G \subset \mathbb{K}[\mathbf{x}][\boldsymbol{\partial}]$ be a finite set such that $\mathbb{K}(\mathbf{x})[\boldsymbol{\partial}]G$ is D-finite and G is a Gröbner basis with respect to some term order. Set $f = \operatorname{lcm}(\operatorname{HC}(G_1), \ldots, \operatorname{HC}(G_k))$ and $\operatorname{Cont}(G) = \mathbb{K}(\mathbf{x})[\boldsymbol{\partial}]G \cap \mathbb{K}[\mathbf{x}][\boldsymbol{\partial}]$. Then

$$\operatorname{Cont}(G) = \{P \in \mathbb{K}[\mathbf{x}][\boldsymbol{\partial}] \mid f^s P \in \mathbb{K}(\mathbf{x})[\boldsymbol{\partial}]G \text{ for some } s \in \mathbb{N}\}.$$

Set

$$\operatorname{sol}(G) = \{v \in \mathbb{E} \mid P(v) = 0 \text{ for each } P \in \mathbb{K}(\mathbf{x})[\boldsymbol{\partial}]G\},$$

where $\mathbb{E}$ is a universal differential field extension [29, Section 7, page 133] of $\mathbb{K}(\mathbf{x})$. By [29, Proposition 2, Corollary 1, page 151–152],

$$\operatorname{Cont}(G) = \{P \in \mathbb{K}[\mathbf{x}][\boldsymbol{\partial}] \mid P(v) = 0 \text{ for each } v \in \operatorname{sol}(G)\}.$$

In the commutative case, Seidenberg's Lemma [5, Lemma 8.13] provides one method to compute the radical of a zero-dimensional ideal. One might expect that this result carries over to the differential setting. More precisely, assume that $G \subset \mathbb{K}[\mathbf{x}][\boldsymbol{\partial}]$ be a finite set such that $\mathbb{K}(\mathbf{x})[\boldsymbol{\partial}]G$ is D-finite and G is a Gröbner basis with respect to some term order. For each $i \in \{1, \ldots, n\}$, let $F_i \in \mathbb{K}[\mathbf{x}][\partial_i]$ be the generator of $\mathbb{K}(\mathbf{x})[\boldsymbol{\partial}]G \cap \mathbb{K}(\mathbf{x})[\partial_i]$, whose desingularized (see Definition 3.2.1) operator with minimal order is P_i. Then one might conjecture that

$$\operatorname{Cont}(G) = \mathbb{K}[\mathbf{x}][\boldsymbol{\partial}]G + \mathbb{K}[\mathbf{x}][\boldsymbol{\partial}]P_1 + \cdots + \mathbb{K}[\mathbf{x}][\boldsymbol{\partial}]P_n.$$

In the univariate case, this can be proven by Stafford Theorem ([34, page 1541] and [20]). However, it is no longer valid in the multivariate case. For example, consider the following Gröbner basis in $\mathbb{Q}(x, y)[\partial_x, \partial_y]$:

$$G = \{G_1, G_2\} = \{(x^2 - y^2)^2\partial_y - 2y, (x^2 - y^2)^2\partial_x + 2x\}.$$

Then $\mathbb{Q}(x, y)[\partial_x, \partial_y]G$ is D-finite. By computation, we find that G_1 and G_2 are desingularized operators of themselves with minimal orders, respectively. Using the Macaulay2 package `Dmodules` [19], we find that $\operatorname{Cont}(G) \neq \mathbb{Q}[x, y][\partial_x, \partial_y]G$. Instead, A solution for the Weyl closure problem was proposed by Tsai in [47] and his Ph.D. thesis [48], which involves homological algebra [21] and D-modules theory [15]. In the literature, we do not find any reference concerning the contraction problem of a difference or differential operator over $\mathbb{Z}[x][\partial]$.

Our work is based on desingularization for Ore operators by Chen, Jaroschek, Kauers and Singer in [10, 11]. In particular, the p-removing operator in [11, Lemma 4] provides us with a key to determine contraction ideals. In the shift case, they provide an upper bound for the order of a p-removing operator. This bound provides the termination of our algorithms concerning contraction ideals and completely desingularized operators. In the differential case, upper bounds for the order of a p-removing operator are given in [47, Algorithm 3.4] and [23, Lemma 4.3.12].

Another purpose of the present thesis is to generalize the two facts about apparent singularities sketched above to the multivariate setting. Instead of an ODE, we consider systems of PDEs known as D-finite systems. A D-finite system is a finite set of linear homogeneous partial differential equations with polynomial coefficients in several variables, whose solution space is of finite dimension. For such systems, we define the notion of a singularity in terms of the polynomials appearing in them (Def. 4.2.1). We show (Thm. 4.3.1) that a point is a singularity of the system unless it admits a basis of power series solutions in which the starting monomials are as small as possible with respect to some term order. Then a singularity is apparent if the system admits a full basis of power series solutions, the starting terms of which are not as small as possible. We then prove in Theorem 4.4.6 that apparent singularities in the multivariate case can be removed like in the univariate case by adding suitable additional solutions to the system at hand.

1.2 Contributions and outline

Based on ideas of [10, 11], we study the univariate contraction problem of Ore ideals. New results include:

(1) Theorem 3.2.3: characterize the connection between desingularized operators and contraction ideals.

(2) Algorithm 3.3.8: provide a method to determine the contraction ideal of a difference or differential operator.

(3) Introduce the notion of completely desingularized operators, give the connection between them and contraction ideals, and design an algorithm to compute them.

(4) Using completely desingularized operators, we study how to certify the integrality of a sequence and check special cases of a conjecture of Krattenthaler.

This work is published in ISSAC'16 [50].

Using Gröbner bases (Subsection 4.1.2) in the ring of linear partial differential operators, we generalize the desingularization technique for apparent singularities to the multivariate case. New results include:

(1) Theorem 4.3.1: characterize an ordinary point of a D-finite system by using its formal power series solutions.

(2) Theorem 4.4.6: describe a connection between apparent singularities and ordinary points.

(3) Algorithm 4.4.9 and Algorithm 4.4.12: we can remove and detect apparent singularities of a D-finite system in an algorithmic way.

The thesis is arranged as follows:

In Chapter 2, we consider Gröbner bases over the Ore algebra $R[\mathbf{x}][\boldsymbol{\partial}]$, where R is a principal ideal domain. In the commutative case, Gröbner bases over a principal ideal domain are introduced in [5, Section 10.1]. Our treatment is similar to that in the commutative case. Since we need to compute Gröbner bases over $R[\mathbf{x}][\partial]$ for determining contraction ideals, we generalize the theory in the commutative case to the Ore case. The results can be regarded as a minor supplement to known Gröbner bases theories.

In Chapter 3, we introduce the notion of desingularized operators and connect it with contraction ideals in Section 3.2. Next, we determine bases of contraction ideals in Section 3.3 and compute completely desingularized operators in Section 3.4. Finally, we present some interesting applications of completely desingularized operators, such as certifying integer sequences and checking special cases of Krattenthaler's conjecture.

In Chapter 4, we first define singularities and ordinary points of a D-finite system. Next, we characterize an ordinary point of such systems using its formal power series solutions. Finally, we describe the connection between ordinary points and apparent singularities, and use it to remove and detect apparent singularities in an algorithmic way.

Remark 1.2.1. *In this thesis, we use the calligraphic letter like $\mathcal{G}$ to denote Gröbner bases in the Ore algebra $R[\mathbf{x}][\boldsymbol{\partial}]$ (Section 2.1), the bold letter like $\mathbf{G}$ to denote Gröbner bases in the commutative polynomial ring $R[\mathbf{x}]$ (Section 2.1), and the usual letter like G to denote Gröbner bases in the ring of differential operators $\mathbb{K}(\mathbf{x})[\boldsymbol{\partial}]$ (Section 4.1), where R is a principal ideal domain and $\mathbb{K}$ is a field of characteristic zero.*

Chapter 2

Gröbner Bases of Ore Polynomials over a PID

In this chapter, we describe the notion of Gröbner bases and Buchberger's algorithm in the Ore algebra $R[\mathbf{x}][\boldsymbol{\partial}]$, where R is a principal ideal domain. It is based on [5, Section 10.1] and [37]. When $R = \mathbb{K}[t]$ with $\mathbb{K}$ being a field of characteristic zero, the notion of Gröbner bases and Buchberger's algorithm are available [28]. Furthermore, a corresponding implementation is available in [31]. Our motivation is to compute Gröbner bases over $R[\mathbf{x}][\boldsymbol{\partial}]$ for determining contraction ideals. For the more general cases, see [9] and [40, IV.46.13]. The reader who is familiar with Göbner bases may skip this chapter and proceed directly to the next one.

2.1 Ore algebras

In this section, we define Ore algebras that we are concerned with.

Let R be a principal ideal domain and n a nonnegative integer. Let $R[x_1, \ldots, x_n]$ be the ring of usual commutative polynomials over R. For brevity, we denote this ring by $R[\mathbf{x}]$. For each $i = 1, \ldots, n$, let σ_i be an R-automorphism of $R[\mathbf{x}]$ with the following properties:

(i) $\sigma_i(x_i) = \gamma_i x_i + \tau_i$ for some $\gamma_i, \tau_i \in R$ with γ_i being a unit in R,

(ii) $\sigma_i(x_j) = x_j$ for $j \neq i$.

Let δ_i be a σ_i-derivation on $R[\mathbf{x}]$, *i.e.*, an R-linear map satisfying the following three properties:

(i) $\delta_i(fg) = \sigma_i(f)\delta_i(g) + \delta_i(f)g \quad \text{for} \quad f, g \in R[\mathbf{x}]$,

(ii) $\delta_i(x_i)$ is a polynomial in $R[x_i]$ with degree less than or equal to 1,

(iii) $\delta_i(x_j) = 0$ for all $j \neq i$.

Then we have an Ore algebra

$$R[\mathbf{x}][\partial_1; \sigma_1, \delta_1] \cdots [\partial_n; \sigma_n, \delta_n]$$

of Ore polynomials [14], in which the addition is coefficientwise and the multiplication is defined by associativity via the commutation rules

(i) $\partial_i p = \sigma_i(p)\partial_i + \delta_i(p)$ for $p \in R[\mathbf{x}]$, $1 \leq i \leq n$,

(ii) $\partial_i \partial_j = \partial_j \partial_i$ for $1 \leq i, j \leq n$.

The ring $R[\mathbf{x}][\partial_1; \sigma_1, \delta_1] \cdots [\partial_n; \sigma_n, \delta_n]$ is abbreviated as $R[\mathbf{x}][\boldsymbol{\partial}]$ when σ_i and δ_i are clear from the context. According to [14], this is a (non-commutative) domain.

2.2 Terms and monomials

By a *term*, we mean a product $x_1^{\alpha_1} \cdots x_n^{\alpha_n} \partial_1^{\beta_1} \cdots \partial_n^{\beta_n}$ with $\alpha_i, \beta_j \in \mathbb{N}$, $1 \leq i, j \leq n$. For brevity, we set $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ and $\boldsymbol{\beta} = (\beta_1, \ldots, \beta_n)$. Then we may denote a term as $\mathbf{x}^{\boldsymbol{\alpha}} \boldsymbol{\partial}^{\boldsymbol{\beta}}$. By a *monomial*, we mean a product at, where a is a nonzero element of R, and t a term. Set T to be the set of all terms, and M the set of all monomials. Let $P \in R[\mathbf{x}][\boldsymbol{\partial}] \setminus \{0\}$. Since P is a sum of monomials, we denote the set of monomials in P by $\mathrm{M}(P)$. The set of corresponding terms is denoted by $\mathrm{T}(P)$.

Let $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \mathbb{N}^n$, we write $\boldsymbol{\alpha} \leq \boldsymbol{\beta}$ if $\alpha_i \leq \beta_i$ for all $1 \leq i \leq n$. Let $as, bt \in M$ with

$$s = \mathbf{x}^{\boldsymbol{\alpha}} \boldsymbol{\partial}^{\boldsymbol{\beta}}, t = \mathbf{x}^{\mathbf{u}} \boldsymbol{\partial}^{\mathbf{v}} \in T \quad \text{and} \quad a, b \in R.$$

We say that *as quasi-divides bt* if $a \mid b$ in R, $\boldsymbol{\alpha} \leq \mathbf{u}$ and $\boldsymbol{\beta} \leq \mathbf{v}$. In this case, we write $as \mid_q bt$. In other words, $s \mid t$ when we forget the commutation rules in $R[\mathbf{x}][\boldsymbol{\partial}]$.

Proposition 2.2.1. *Let S be a set of monomials in $R[\mathbf{x}][\boldsymbol{\partial}]$. Then S has a Dickson basis, i.e., there exists a finite subset N of S such that, for each $s \in S$, there exists $t \in N$ with $t \mid_q s$.*

Proof. We define the following map:

$$\begin{array}{cccc} \phi: & M & \longrightarrow & R \times \mathbb{N}^n \times \mathbb{N}^n \\ & a\mathbf{x}^{\boldsymbol{\alpha}} \boldsymbol{\partial}^{\boldsymbol{\beta}} & \mapsto & (a, \boldsymbol{\alpha}, \boldsymbol{\beta}). \end{array}$$

Obviously, ϕ is a bijection. Moreover, the quasi-divisibility relation in M corresponds to the following quasi-order in $R \times \mathbb{N}^n \times \mathbb{N}^n$:

$$(a_1, \boldsymbol{\alpha}_1, \boldsymbol{\beta}_1) \prec' (a_2, \boldsymbol{\alpha}_2, \boldsymbol{\beta}_2) \quad \text{if and only if} \quad a_1 \mid a_2, \ \boldsymbol{\alpha}_1 \leq \boldsymbol{\alpha}_2 \text{ and } \boldsymbol{\beta}_1 \leq \boldsymbol{\beta}_2,$$

where $(a_1, \boldsymbol{\alpha}_1, \boldsymbol{\beta}_1), (a_2, \boldsymbol{\alpha}_2, \boldsymbol{\beta}_2) \in R \times \mathbb{N}^n \times \mathbb{N}^n$. By [5, Proposition 4.49], $\phi(S)$ has a Dickson basis N' with respect to $\prec'$. Then $\phi^{-1}(N')$ is a Dickson basis of S. □

2.3 Term orders and monomial orders

In $R[\mathbf{x}][\boldsymbol{\partial}]$, a *term order* $\prec$ is a linear order on T that satisfies the following conditions:

(i) $1 \preceq t$ for each $t \in T$;

(ii) $\mathbf{x}^{\boldsymbol{\alpha}}\boldsymbol{\partial}^{\boldsymbol{\beta}} \prec \mathbf{x}^{\mathbf{a}}\boldsymbol{\partial}^{\mathbf{b}}$ implies $\mathbf{x}^{\boldsymbol{\alpha}+\mathbf{u}}\boldsymbol{\partial}^{\boldsymbol{\beta}+\mathbf{v}} \prec \mathbf{x}^{\mathbf{a}+\mathbf{u}}\boldsymbol{\partial}^{\mathbf{b}+\mathbf{v}}$ for each $(\mathbf{u}, \mathbf{v}) \in \mathbb{N}^n \times \mathbb{N}^n$;

A term order induces a partial order on M as follows:
For all $as, bt \in M$ with $s = \mathbf{x}^{\boldsymbol{\alpha}}\boldsymbol{\partial}^{\boldsymbol{\beta}}, t = \mathbf{x}^{\mathbf{u}}\boldsymbol{\partial}^{\mathbf{v}} \in T$ and $a, b \in R$,

$$as \prec bt \Longleftrightarrow s \prec t.$$

The induced order is called a *monomial order* on M.

Lemma 2.3.1. *Let $\prec$ be a monomial order on M. Then there is no strictly decreasing infinite sequence in M with respect to $\prec$.*

Proof. Suppose that

$$m_1, m_2, \ldots$$

is an infinite sequence in M with $m_i \succ m_{i+1}$ for all $i \in \mathbb{Z}^+$. By Proposition 2.2.1, there exists a finite number of monomials $m_{j_1}, \ldots, m_{j_k}$ such that, for all $i \in \mathbb{Z}^+$, there exists $\ell \in \{1, \ldots, k\}$ with $m_{j_\ell}|_q m_i$. Choose i to be greater than all the indices $j_1, \ldots, j_k$. Then m_{j_ℓ} cannot be higher than m_i, a contradiction. $\square$

Let $\prec$ be a monomial order on M, and $P \in R[\mathbf{x}][\boldsymbol{\partial}] \setminus \{0\}$. Then

$$P = c_1 t_1 + \cdots + c_\ell t_\ell,$$

where $c_1, \ldots, c_\ell \in R \setminus \{0\}$, and $t_1, \ldots, t_\ell$ are mutually distinct terms.

Assume that $t_1 \prec t_2 \prec \cdots \prec t_\ell$. Then t_ℓ, c_ℓ and $c_\ell t_\ell$ are called the *head term*, *head coefficient*, and *head monomial* of P, respectively. They are denoted by $\mathrm{HT}(P)$, $\mathrm{HC}(P)$ and $\mathrm{HM}(P)$, respectively.

Let $P, Q \in R[\mathbf{x}][\boldsymbol{\partial}]$. We say that $P, Q \in R[\mathbf{x}][\boldsymbol{\partial}]$ are *associated* to each other if there are unit elements $a, b \in R$ such that $aP = bQ$.

Proposition 2.3.2. *Let P and Q be two nonzero elements in $R[\mathbf{x}][\boldsymbol{\partial}]$. Then*

(i) $\mathrm{HT}(PQ) = \mathrm{HT}(\mathrm{HT}(P)\mathrm{HT}(Q))$*;*

(ii) $\mathrm{HC}(PQ)$ *and* $\mathrm{HC}(P)\mathrm{HC}(Q)$ *are associated;*

(iii) $\mathrm{HM}(PQ)$ *and* $\mathrm{HM}(\mathrm{HM}(P)\mathrm{HM}(Q))$ *are associated.*

Proof. Given $i \in \{1, \ldots, n\}$. By the definitions of σ_i, δ_i and the commutation rules in Section 2.1, we have

$$\partial_i x_i = \gamma_i(x_i \partial_i) + \tau_i \partial_i + a_i x_i + b_i,$$

where γ_i is a unit in R, and $\tau_i, a_i, b_i \in R$. Therefore, $\mathrm{HM}(\partial_i x_i) = \gamma_i x_i \partial_i$. A direct induction proves the proposition. $\square$

The following corollary is a step-stone for generalizing usual polynomial reductions to the Ore case.

Corollary 2.3.3. *Let $m_1, m_2 \in M$. If $m_1 \mid_q m_2$, then there exists $m_3 \in M$ such that*

$$m_2 = \mathrm{HM}(m_3 m_1).$$

Proof. Let $m_1 = a\mathbf{x}^{\boldsymbol{\alpha}}\boldsymbol{\beta}^{\boldsymbol{\beta}}, m_2 = b\mathbf{x}^{\mathbf{u}}\boldsymbol{\beta}^{\mathbf{v}}$ with $a, b \in R$, and $(\boldsymbol{\alpha}, \boldsymbol{\beta}), (\mathbf{u}, \mathbf{v}) \in \mathbb{N}^n \times \mathbb{N}^n$. Since $m_1 \mid_q m_2$, we have $a \mid b$, $\boldsymbol{\alpha} \leq \mathbf{u}$, $\boldsymbol{\beta} \leq \mathbf{v}$. Let $\mathbf{u}' = \mathbf{u} - \boldsymbol{\alpha}$, $\mathbf{v}' = \mathbf{v} - \boldsymbol{\beta}$. By item (iii) of the above proposition, there exists a unit γ in R such that

$$\mathrm{HM}(\mathbf{x}^{\mathbf{u}'}\boldsymbol{\partial}^{\mathbf{v}'}m_1) = \gamma a\mathbf{x}^{\mathbf{u}}\boldsymbol{\beta}^{\mathbf{v}}.$$

Since $\gamma a \mid b$, there exists $c \in R$ such that $c\gamma a = b$. Let $m_3 = c\mathbf{x}^{\mathbf{u}'}\boldsymbol{\partial}^{\mathbf{v}'}$, then

$$m_2 = \mathrm{HM}(m_3 m_1).$$

□

2.4 Reduction for Ore polynomials

In the sequel, we assume that $\prec$ is a term order on $R[\mathbf{x}][\boldsymbol{\partial}]$.

Definition 2.4.1. *Let $F, G, P \in R[\mathbf{x}][\boldsymbol{\partial}]$ with $FP \neq 0$, and let $\mathcal{P}$ be a subset of $R[\mathbf{x}][\boldsymbol{\partial}] \setminus \{0\}$. Then we say*

(i) F reduces to G modulo P by eliminating m *(notation $F \xrightarrow[P,m]{} G$), if there exists $m \in \mathrm{M}(F)$ with $\mathrm{HM}(P) \mid_q m$, and $G = F - m'P$, where m' is a monomial such that $\mathrm{HM}(m'P) = m$;*

(ii) F reduces to G modulo P *(notation $F \xrightarrow[P]{} G$), if $F \xrightarrow[P,m]{} G$ for some m in $\mathrm{M}(F)$;*

(iii) F reduces to G modulo $\mathcal{P}$ *(notation $F \xrightarrow[\mathcal{P}]{} G$), if $F \xrightarrow[P]{} G$ for some $P \in \mathcal{P}$;*

(iv) F *is* reducible modulo P *if there exists $G \in R[\mathbf{x}][\boldsymbol{\partial}]$ such that $F \xrightarrow[P]{} G$;*

(v) F *is* reducible modulo $\mathcal{P}$ *if there exists $G \in R[\mathbf{x}][\boldsymbol{\partial}]$ such that $F \xrightarrow[\mathcal{P}]{} G$.*

Remark 2.4.2. *The existence of m' in item (i) of the above definition is guaranteed by Corollary 2.3.3.*

If F is not reducible modulo P (modulo $\mathcal{P}$), then we say F is *in reduced form modulo P (modulo $\mathcal{P}$). A reduced form of F modulo $\mathcal{P}$* is an element $G \in R[\mathbf{x}][\boldsymbol{\partial}]$ that is in reduced form modulo $\mathcal{P}$ and satisfies

$$F \xrightarrow[\mathcal{P}]{*} G,$$

where $\xrightarrow[\mathcal{P}]{*}$ is the reflexive-transitive closure [5, Definition 4.71] of $\xrightarrow[\mathcal{P}]{}$. We call

$$F \xrightarrow[P,m]{} G$$

a *top-reduction* of F if $m = \mathrm{HM}(F)$; whenever a top-reduction of F exists (with $P \in \mathcal{P}$), we say that F is *top-reducible modulo P (modulo $\mathcal{P}$).*

Algorithm 2.4.3. *Given $F \in R[\mathbf{x}][\boldsymbol{\partial}]$ and $\mathcal{P} \subset R[\mathbf{x}][\boldsymbol{\partial}]$, compute a reduced form G of F modulo $\mathcal{P}$.*

```
G ← 0
L ← F
while L ≠ 0 do
    while L is top-reducible modulo 𝒫 do
        S ← L − m′P for some P ∈ 𝒫, m′ ∈ T with HM(m′P) = HM(L).
        L ← S
    end
    G ← G + HM(L)
    L ← L − HM(L)
end
```

The correctness of the above algorithm is evident.

Proof of the termination of Algorithm 2.4.3: Suppose Algorithm 2.4.3 does not terminate for some input F. Let $\{L_i\}_{i\in\mathbb{N}}$ be the operators that get assigned to L in the course of the algorithm. Then, $L_0 = F$. Moreover, the value of any L_{i+1} is either the case (i) $L_{i+1} = L_i - m'P$, for some $P \in \mathcal{P}, m' \in T$ with $\mathrm{HM}(m'P) = \mathrm{HM}(L_i)$ or it is the case (ii) $L_{i+1} = L_i - \mathrm{HM}(L_i)$. Therefore, we have $\mathrm{HT}(L_{i+1}) \prec \mathrm{HT}(L_i)$ for each $i \in \mathbb{N}$, i.e., $\{\mathrm{HT}(L_i)\}_{i\in\mathbb{N}}$ is a strictly decreasing sequence with respect to $\prec$, a contradiction to Lemma 2.3.1. □

2.5 Gröbner bases

As a matter of notation, if S is a subset of $R[\mathbf{x}][\boldsymbol{\partial}]$, we denote the left ideal generated by S in $R[\mathbf{x}][\boldsymbol{\partial}]$ as $R[\mathbf{x}][\boldsymbol{\partial}] \cdot S$. The set of head monomials of elements in S is denoted by $\mathrm{HM}(S)$.

Definition 2.5.1. *A finite set $\mathcal{G} \subset R[\mathbf{x}][\boldsymbol{\partial}]$ is called a* Gröbner basis *with respect to $\prec$ if for each monomial $u \in \mathrm{HM}(R[\mathbf{x}][\boldsymbol{\partial}] \cdot \mathcal{G})$ there exists $v \in \mathrm{HM}(\mathcal{G})$ such that $v \mid_q u$. If I is a left ideal of $R[\mathbf{x}][\boldsymbol{\partial}]$, then a* Gröbner basis of I *is a Gröbner basis that generates the left ideal I.*

Remark 2.5.2. *Note that $\mathcal{G} \subset R[\mathbf{x}][\boldsymbol{\partial}]$ is a Gröbner basis if and only if F is top-reducible modulo $\mathcal{G}$ for each $F \in R[\mathbf{x}][\boldsymbol{\partial}] \cdot \mathcal{G} \setminus \{0\}$.*

Proposition 2.5.3. *Let I be a left ideal of $R[\mathbf{x}][\boldsymbol{\partial}]$. Then I has a Gröbner basis.*

Proof. By Proposition 2.2.1, there exists a finite set N of $\mathrm{HM}(I)$ such that for each monomial $s \in \mathrm{HM}(I)$, there exists $t \in N$ such that $t \mid_q s$.

By the definition of N, it corresponds to a finite set $\mathcal{G} \subset I$ such that, for each $t \in N$, there exists an operator $P \in \mathcal{G}$ such that $\mathrm{HM}(P) = t$. Since $R[\mathbf{x}][\boldsymbol{\partial}] \cdot \mathcal{G} \subset I$, we have that $\mathcal{G}$ is a Gröbner basis by Definition 2.5.1.

Next, we prove that $\mathcal{G}$ generates I. For each $P \in I$, we have that $P \xrightarrow[\mathcal{G}]{*} Q$ by Algorithm 2.4.3 such that Q is a reduced form of P modulo $\mathcal{G}$. So,

$$Q = P - \sum_{G \in \mathcal{G}} V_G G$$

for some $V_G \in R[\mathbf{x}][\boldsymbol{\partial}]$. Thus, $Q \in I$. If Q is nonzero, then Q is top-reducible modulo $\mathcal{G}$, a contradiction. Consequently, $Q = 0$. $\square$

2.6 Standard representations of Ore polynomials

Let $F \in R[\mathbf{x}][\boldsymbol{\partial}] \setminus \{0\}$. *A standard representation* of F with respect to a finite set $\mathcal{P}$ of $R[\mathbf{x}][\boldsymbol{\partial}]$ is the following representation

$$F = \sum_{P \in \mathcal{P}} V_P P,$$

where $V_P \in R[\mathbf{x}][\boldsymbol{\partial}]$, such that $\mathrm{HT}(V_P P) \preceq \mathrm{HT}(F)$ or $V_P = 0$ for each $P \in \mathcal{P}$.

Lemma 2.6.1. *Let $\mathcal{P}$ be a finite subset of $R[\mathbf{x}][\boldsymbol{\partial}]$, F is a nonzero operator in $R[\mathbf{x}][\boldsymbol{\partial}]$, and assume that $F \xrightarrow[\mathcal{P}]{*} 0$. Then F has a stardard representation with respect to $\mathcal{P}$.*

Proof. Suppose that $F \in R[\mathbf{x}][\boldsymbol{\partial}] \setminus \{0\}$ such that $F \xrightarrow[\mathcal{P}]{*} 0$, but F does not have a standard representation. We may assume that F is minimal with this property in terms of the length [5, page 174] of the reduction chain. Since $F \xrightarrow[\mathcal{P}]{*} 0$, there exists $H \in R[\mathbf{x}][\boldsymbol{\partial}]$ with $F \xrightarrow[G]{} H$ for some $G \in \mathcal{P}$, say $H = F - mG$, where m is a monomial on $R[\mathbf{x}][\boldsymbol{\partial}]$. If $H = 0$, then $F = mG$ is a standard representation of F, a contradiction. Otherwise, H has a stardard representation

$$H = \sum_{i=1}^{k} V_i P_i$$

w.r.t. $\mathcal{P}$ by the minimality of F. Using the fact that $\mathrm{HT}(mG)$ is a term in F, it follows that

$$F = mG + \sum_{i=1}^{k} V_i P_i$$

is a stardard representation of F with respect to $\mathcal{P}$, a contradiction. $\square$

Assume that $\mathcal{G}$ is a Gröbner basis of a left ideal I of $R[\mathbf{x}][\boldsymbol{\partial}]$. By the argument in Proposition 2.5.3, for each element $F \in I$, we have that $F \xrightarrow[\mathcal{G}]{*} 0$. Thus, F has a standard representation with respect to $\mathcal{G}$ by the above lemma. However, the converse is not true. The next lemma shows that if we add one more condition then it can be a criterion for Gröbner bases.

To this end, we need one more notation. For $s, t \in T$ with $s = \mathbf{x}^{\boldsymbol{\alpha}}\boldsymbol{\partial}^{\boldsymbol{\beta}}$ and $t = \mathbf{x}^{\mathbf{u}}\boldsymbol{\partial}^{\mathbf{v}}$, we define the quasi least common multiple of s and t to be $\mathbf{x}^{\mathbf{e}}\boldsymbol{\partial}^{\mathbf{f}}$, where $e_i = \max(\alpha_i, u_i), f_i = \max(\beta_i, v_i)$ for $1 \leq i \leq n$, and denote it by $\operatorname{qlcm}(s,t)$. In other words, $\operatorname{qlcm}(s,t)$ is the least common multiple of s and t when they are treated as commutative terms.

Lemma 2.6.2. *Assume that $\mathcal{G}$ is a finite subset of $R[\mathbf{x}][\boldsymbol{\partial}]$ satisfying the following two conditions:*

(i) For all $G_1, G_2 \in \mathcal{G}$ there exists $H \in \mathcal{G}$ with

$$\operatorname{HT}(H) \mid_q \operatorname{qlcm}(\operatorname{HT}(G_1), \operatorname{HT}(G_2)) \quad \textit{and} \quad \operatorname{HC}(H) \mid \gcd(\operatorname{HC}(G_1), \operatorname{HC}(G_2)).$$

(ii) Every $F \in R[\mathbf{x}][\boldsymbol{\partial}] \cdot \mathcal{G}$ has a standard representation w.r.t. $\mathcal{G}$.

Then $\mathcal{G}$ is a Gröbner basis.

Proof. It suffices to prove that for all $F \in R[\mathbf{x}][\boldsymbol{\partial}] \cdot \mathcal{G} \setminus \{0\}$, F is top-reducible modulo $\mathcal{G}$. By condition (ii), we have

$$F = \sum_{i=1}^{k} V_i G_i$$

is a standard representation of F with respect to $\mathcal{G}$. Let $N \subset \{1, \ldots, k\}$ be the set of indices with the property that $\operatorname{HT}(F) = \operatorname{HT}(V_i G_i)$. Then

$$\operatorname{HM}(F) = \sum_{i \in N} \operatorname{HM}(V_i G_i),$$

and thus

$$\operatorname{qlcm}\{\operatorname{HT}(G_i) \mid i \in N\} \mid_q \operatorname{HT}(F), \quad \text{and} \quad \gcd\{\operatorname{HC}(G_i) \mid i \in N\} \mid \operatorname{HC}(F).$$

Note that the second divisibility relies on the fact that the two head coefficients

$$\operatorname{HC}(V_i G_i) \ \text{ and } \ \operatorname{HC}(V_i)\operatorname{HC}(G_i)$$

are associated, which is stated in Proposition 2.3.2. By condition (i) and a straightforward induction on the cardinality of N, there exists $H \in \mathcal{G}$ such that $\operatorname{HT}(H)$ quasi-divides the above quasi lcm, and $\operatorname{HC}(H)$ divides the gcd. We have

$$\operatorname{HM}(H) \mid_q \operatorname{HM}(F),$$

and thus F is top-reducible modulo $\mathcal{G}$. □

Remark 2.6.3. *When R is a field, the first condition in the above lemma is trivial, because the gcd of head coefficients is always one, and, therefore, H can be chosen to be either G_1 or G_2.*

2.7 Buchberger's criterion

Definition 2.7.1. *For $i = 1, 2$, consider $G_i \in R[\mathbf{x}][\boldsymbol{\partial}] \setminus \{0\}$ with $\mathrm{HC}(G_i) = a_i, \mathrm{HT}(G_i) = t_i$. Moreover, let $b_i \in R$ and $s_i \in T$ such that*

$$b_i a_i = \mathrm{lcm}(a_1, a_2) \quad \textit{and} \quad \mathrm{HT}(s_i t_i) = \mathrm{qlcm}(t_1, t_2).$$

By Proposition 2.3.2, there exists an invertible element $r_i \in R$ such that $\mathrm{HC}(s_i G_i) = r_i a_i$. Then the S-polynomial *of G_1 and G_2 is defined as*

$$\mathrm{spol}(G_1, G_2) = b_1 r_1^{-1} s_1 G_1 - b_2 r_2^{-1} s_2 G_2$$

Now let $c_1, c_2 \in R$ such that $\gcd(a_1, a_2) = c_1 a_1 + c_2 a_2$. Then we define the G-polynomial *of G_1 and G_2 with respect to c_1 and c_2 as*

$$\mathrm{gpol}_{(c_1,c_2)}(G_1, G_2) = c_1 r_1^{-1} s_1 G_1 + c_2 r_2^{-1} s_2 G_2.$$

Strictly speaking, S-polynomials are only defined up to multiplication by units. Nevertheless, there will be no harm in speaking of the S-polynomial. By contrast, the G-polynomial of $G_1, G_2 \in R[\mathbf{x}][\boldsymbol{\partial}]$ depends heavily on the choice of c_1 and c_2. We will from now on assume that for each pair $a_1, a_2 \in R \setminus \{0\}$, an arbitrary but fixed choice of a pair $c_1, c_2 \in R$ has been made such that $c_1 a_1 + c_2 a_2 = \gcd(a_1, a_2)$, and that G-polynomials are formed using this choice. The subscript (c_1, c_2) may then be suppressed.

Remark 2.7.2. *Note that condition (i) of Lemma 2.6.2 is equivalent to the G-polynomial of G_1 and G_2 being top-reducible modulo $\mathcal{G}$.*

The next theorem is a direct generalization of Buchberger's criterion [16, Page 85] in the commutative case.

Theorem 2.7.3. *Let $\mathcal{G}$ be a finite subset of $R[\mathbf{x}][\boldsymbol{\partial}]$. Assume that for each $G_1, G_2 \in \mathcal{G}$, the S-polynomial $\mathrm{spol}(G_1, G_2)$ is either equal to zero or has a standard representation with respect to $\mathcal{G}$, and $\mathrm{gpol}(G_1, G_2)$ is top-reducible modulo $\mathcal{G}$. Then every polynomial $F \in R[\mathbf{x}][\boldsymbol{\partial}] \cdot \mathcal{G}$ has a standard representation.*

Proof. Suppose that $F \in R[\mathbf{x}][\boldsymbol{\partial}] \cdot \mathcal{G} \setminus \{0\}$ does not have a standard representation with respect to $\mathcal{G}$. Let

$$F = \sum_{i=1}^{k} V_i G_i \tag{2.1}$$

with $V_i \in R[\mathbf{x}][\boldsymbol{\partial}]$ and $G_i \in \mathcal{G}$, $i = 1, \ldots, k$. We may assume that

$$s = \max\{\mathrm{HT}(V_i G_i) \mid 1 \leq i \leq k\}$$

is minimal among all such representations of F. Then $\mathrm{HT}(F) \prec s$. For a contradiction, we will produce a representation

$$F = \sum_{i=1}^{k'} V_i' G_i'$$

of the same kind such that $s' = \max\{\mathrm{HT}(V_i'G_i') \mid 1 \le i \le k'\} \prec s$. We proceed by induction on the number n_s of indices i with $s = \mathrm{HT}(V_iG_i)$.

First, $n_s = 1$ is impossible because $\mathrm{HT}(F) = s$ in this case. Let $n_s = 2$, without loss of generality, we may assume that $\mathrm{HT}(V_1G_1) = \mathrm{HT}(V_2G_2) = s$. This means that

$$s = \mathrm{HT}(t_1 \cdot \mathrm{HT}(G_1)) = \mathrm{HT}(t_2 \cdot \mathrm{HT}(G_2))$$

for some $t_1, t_2 \in T$. So, $\mathrm{qlcm}(\mathrm{HT}(G_1), \mathrm{HT}(G_2))$ quasi-divides s, say

$$s = \mathrm{HT}(u \cdot \mathrm{qlcm}(\mathrm{HT}(G_1), \mathrm{HT}(G_2)))$$

with $u \in T$. Since $n_s = 2$, we have $\mathrm{HM}(V_1G_1) + \mathrm{HM}(V_2G_2) = 0$, and so

$$a_1 \cdot \mathrm{HC}(G_1) = -a_2 \cdot \mathrm{HC}(G_2)$$

for some $a_1, a_2 \in R \setminus \{0\}$. Moreover, a_i and $\mathrm{HC}(V_i)$ are associated for $i = 1, 2$. It follows that there exists $a \in R \setminus \{0\}$ with

$$a \cdot \mathrm{lcm}(\mathrm{HC}(G_1), \mathrm{HC}(G_2)) = a_1 \cdot \mathrm{HC}(G_1) = -a_2 \cdot \mathrm{HC}(G_2)$$

and it is straightforward to see that

$$V_1G_1 + V_2G_2 = au \cdot \mathrm{spol}(G_1, G_2) + W,$$

where $W \in R[\mathbf{x}][\boldsymbol{\partial}]$ with $\mathrm{HT}(W) \prec s$. By assumption, $\mathrm{spol}(G_1, G_2) = 0$, or else it has a standard representation

$$\mathrm{spol}(G_1, G_2) = \sum_{i=1}^{k''} V_i''G_i''.$$

with respect to $\mathcal{G}$. Substituting $V_1G_1 + V_2G_2$ into (2.1), we obtain a representation

$$F = \sum_{i=3}^{k} V_iG_i + au \sum_{i=1}^{k''} V_i''G_i'' + W, \tag{2.2}$$

where the second sum is missing if the S-polynomial is zero. The maximum of the head terms occuring in the first sum is less than s by our assumption $n_s = 2$; the maximum s'' of the head terms in the second sum (if any) satisfies

$$s'' \prec \mathrm{HT}(u \cdot \mathrm{qlcm}(\mathrm{HT}(G_1), \mathrm{HT}(G_2))) = s.$$

Together, we see that the maximum s' of the head terms in the representation (2.2) satisfies $s' \prec s$, which means that (2.2) is the s'-representation that we were looking for.

Now let $n_s > 2$. Without loss of generality, we may again assume that

$$\mathrm{HT}(V_1G_1) = \mathrm{HT}(V_2G_2) = s.$$

Moreover, we have

$$\mathrm{HC}(V_1G_1) = a_1 \cdot \mathrm{HC}(G_1) \quad \text{and} \quad \mathrm{HC}(V_2G_2) = a_2 \cdot \mathrm{HC}(G_2) \tag{2.3}$$

where, as before, a_1 and a_2 are associated to the head coefficients of V_1 and V_2, respectively. Top-reducibility of $\mathrm{gpol}(G_1, G_2)$ modulo $\mathcal{G}$ means that there exists an element $H \in \mathcal{G}$ with

$$\mathrm{HT}(H) \mid_q \mathrm{lcm}(\mathrm{HT}(G_1), \mathrm{HT}(G_2)) \quad \text{and} \quad \mathrm{HC}(H) \mid \gcd(\mathrm{HC}(G_1), \mathrm{HC}(G_2)).$$

Since s quasi-divides both $\mathrm{HT}(G_1)$ and $\mathrm{HT}(G_2)$, we may conclude that $\mathrm{HT}(H)$ divides s, and (2.3) shows that

$$\mathrm{HC}(H) \mid \mathrm{HC}(V_1G_1) \quad \text{and} \quad \mathrm{HC}(H) \mid \mathrm{HC}(V_2G_2).$$

We can thus find a term $v \in T$, and $b_1, b_2 \in R$ such that

$$\mathrm{HM}(V_1G_1) = \mathrm{HM}(b_1 v \cdot \mathrm{HM}(H)) \quad \text{and} \quad \mathrm{HM}(V_2G_2) = \mathrm{HM}(b_2 v \cdot \mathrm{HM}(H)). \tag{2.4}$$

We can now modify our representation (2.1) as follows:

$$F = (V_1G_1 - b_1vH) + (V_2G_2 - b_2vH) + \left((b_1 + b_2)vH + \sum_{i=3}^{k} V_iG_i\right).$$

Equation (2.4) tells us that the head terms of sums in the first and second brackets are less than s. The number of summands with head term s in the third bracket is less than or equal to $1 + (n_s - 2) = n_s - 1$. By the induction hypothesis, we have

$$F = \sum_{i=1}^{k'} V_i' G_i'$$

with $s' = \max\{\mathrm{HT}(V_i'G_i') \mid 1 \leq i \leq k'\} \prec s$. $\square$

Corollary 2.7.4. *Let $\mathcal{G}$ be a finite subset of $R[\mathbf{x}][\boldsymbol{\partial}]$, and assume that for all $G_1, G_2 \in \mathcal{G}$,*

$$\mathrm{spol}(G_1, G_2) \xrightarrow[\mathcal{G}]{*} 0$$

and $\mathrm{gpol}(G_1, G_2)$ *is top-reducible modulo $\mathcal{G}$. Then $\mathcal{G}$ is a Gröbner basis.*

Proof. By Lemma 2.6.1, all nonzero S-polynomials have standard representations. By the above theorem, it follows that every $F \in R[\mathbf{x}][\boldsymbol{\partial}] \cdot \mathcal{G} \setminus \{0\}$ has a standard representation with respect to $\mathcal{G}$. As we have mentioned before, top-reducibility of $\mathrm{gpol}(G_1, G_2)$ modulo $\mathcal{G}$ means that condition (i) of Lemma 2.6.2 is satisfied. Hence, Lemma 2.6.2 and Remark 2.7.2 imply that $\mathcal{G}$ is a Gröbner basis. $\square$

2.8 Buchberger's algorithm

The following algorithm for the computation of Gröbner bases is a fairly obvious imitation of the classical Buchberger algorithm for the commutative case. It enlarges the input set by non-zero reduced forms of S-polynomials and G-polynomials until all S-polynomials reduce to zero and all G-polynomial are top-reducible.

Algorithm 2.8.1. *Given a finite subset $\mathcal{P} \subset R[\mathbf{x}][\boldsymbol{\partial}]$, compute a finite subset $\mathcal{G} \subset R[\mathbf{x}][\boldsymbol{\partial}]$ such that $\mathcal{G}$ is a Gröbner basis in $R[\mathbf{x}][\boldsymbol{\partial}]$ and $R[\mathbf{x}][\boldsymbol{\partial}] \cdot \mathcal{P} = R[\mathbf{x}][\boldsymbol{\partial}] \cdot \mathcal{G}$.*

$\mathcal{G} \leftarrow \mathcal{P}$
$B \leftarrow \{\{P_1, P_2\} \mid P_1, P_2 \in \mathcal{G}, P_1 \neq P_2\}$
$D \leftarrow \emptyset$
$C \leftarrow B$
while $B \neq \emptyset$ **do**
  while $C \neq \emptyset$ **do**
    select $\{P_1, P_2\}$ *from* C
    $C \leftarrow C \setminus \{\{P_1, P_2\}\}$
    if *there does not exist* $G \in \mathcal{G}$ *with* $\mathrm{HT}(G) \mid \mathrm{lcm}(\mathrm{HT}(P_1), \mathrm{HT}(P_2))$,
    $\mathrm{HC}(G) \mid \mathrm{HC}(P_1)$ *and* $\mathrm{HC}(G) \mid \mathrm{HC}(P_2)$ **then**
      $H \leftarrow \mathrm{gpol}(P_1, P_2)$
      $H_0 \leftarrow$ *a reduced form of* H *modulo* $\mathcal{G}$
      $D \leftarrow D \cup \{\{G, H_0\} \mid G \in \mathcal{G}\}$
      $\mathcal{G} \leftarrow \mathcal{G} \cup \{H_0\}$
    end
  end
  select $\{P_1, P_2\}$ *from* B
  $B \leftarrow B \setminus \{\{P_1, P_2\}\}$
  $H \leftarrow \mathrm{spol}(P_1, P_2)$
  $H_0 \leftarrow$ *a reduced form of* H *modulo* $\mathcal{G}$
  if $H_0 \neq 0$ **then**
    $D \leftarrow D \cup \{\{G, H_0\} \mid G \in \mathcal{G}\}$
    $\mathcal{G} \leftarrow \mathcal{G} \cup \{H_0\}$
    $B \leftarrow B \cup D$; $C \leftarrow D$; $D \leftarrow \emptyset$
  end
end

Theorem 2.8.2. *Let R be a computable PID [5, Definition 10.13] and assume that the term order $\prec$ is decidable [5, page 178]. Then the above algorithm computes, for every finite subset $\mathcal{P}$ of $R[\mathbf{x}][\boldsymbol{\partial}]$, a Gröbner basis $\mathcal{G}$ in $R[\mathbf{x}][\boldsymbol{\partial}]$ such that $R[\mathbf{x}][\boldsymbol{\partial}] \cdot \mathcal{G} = R[\mathbf{x}][\boldsymbol{\partial}] \cdot \mathcal{P}$.*

Proof. We first prove the termination of the above algorithm. Suppose that the algorithm does not terminate for input $\mathcal{P}$. Then there are infinitely many polynomials that get added to $\mathcal{G}$. Assume that they are added sequently as H_1, H_2, ... Then, we have an infinite sequence

$$\mathrm{HM}(H_1), \mathrm{HM}(H_2), \ldots.$$

Since each H_i is in reduced form modulo the $\mathcal{G}$ to which it will be added. It follows that

$$\mathrm{HM}(H_i) \nmid_q \mathrm{HM}(H_j)$$

for all $j > i$. By Proposition 2.2.1, there exists a finite set

$$D = \{\mathrm{HM}(H_{i_1}), \ldots, \mathrm{HM}(H_{i_\ell})\}$$

such that, for all $j \in \mathbb{Z}^+$, there exists $m \in D$ with $m \mid_q \mathrm{HM}(H_j)$. But this is impossible when j is greater than $i_1, \ldots, i_\ell$, a contradiction.

When the algorithm terminates, both B and C are empty. It follows that all the S-polynomials formed by elements in $\mathcal{G}$ reduce to zero modulo $\mathcal{G}$ and all the G-polynomials formed by elements in $\mathcal{G}$ are top-reducible. By Corollary 2.7.4, $\mathcal{G}$ is a Gröbner basis. It is evident that

$$R[\mathbf{x}][\boldsymbol{\partial}] \cdot \mathcal{P} = R[\mathbf{x}][\boldsymbol{\partial}] \cdot \mathcal{G}.$$

□

2.9 Elimination ideals

Let I be a left ideal in $R[\mathbf{x}][\boldsymbol{\partial}]$ and $\{U_1, \ldots, U_r\} \subset \{x_1, \ldots, x_n, \partial_1, \ldots, \partial_n\}$. We denote the two sets $\{U_1, \ldots, U_r\}$ and $\{x_1, \ldots, x_n, \partial_1, \ldots, \partial_n\}$ as $\{\mathbf{U}\}$ and $\{\mathbf{x}, \boldsymbol{\partial}\}$, respectively. It is evident to see that $I \cap R[\mathbf{U}]$ is a left ideal of the ring $R[\mathbf{U}]$. This ideal is called the *elimination ideal* of I with respect to $\{\mathbf{U}\}$, or $\mathbf{U}$ for short, and we will denote it by $I_{\mathbf{U}}$. As a matter of notation, we write $\mathrm{T}(\{\mathbf{U}\})$ or $\mathrm{T}(\mathbf{U})$ for the set of terms with respect to $\mathbf{U}$. Assume that a term order $\prec$ on T is given. We write $\{\mathbf{U}\} \prec \{\mathbf{x}, \boldsymbol{\partial}\} \setminus \{\mathbf{U}\}$ if for each $s \in \mathrm{T}(\mathbf{U})$ and $t \in \mathrm{T}(\{\mathbf{x}, \boldsymbol{\partial}\}) \setminus T(\mathbf{U})$, $s \prec t$. We can always find a decidable term order $\prec$ on T satisfying $\{\mathbf{U}\} \prec \{\mathbf{x}, \boldsymbol{\partial}\} \setminus \{\mathbf{U}\}$: just take for $\prec$ a lexicographical order where every variable in $\{\mathbf{U}\}$ is smaller than every one in $\{\mathbf{x}, \boldsymbol{\partial}\} \setminus \{\mathbf{U}\}$.

Lemma 2.9.1. *Assume that $\{\mathbf{U}\} \subset \{\mathbf{x}, \boldsymbol{\partial}\}$ and $\prec$ is a term order with $\{\mathbf{U}\} \prec \{\mathbf{x}, \boldsymbol{\partial}\} \setminus \{\mathbf{U}\}$. Then the following claims hold:*

(i) If $s \in \mathrm{T}$ and $t \in \mathrm{T}(\mathbf{U})$ with $s \prec t$, then $s \in \mathrm{T}(\mathbf{U})$.

(ii) If $F \in R[\mathbf{U}]$ and $P, G \in R[\mathbf{x}][\boldsymbol{\partial}]$ with $F \underset{P}{\longrightarrow} G$, then $P, G \in R[\mathbf{U}]$.

(iii) If $F \in R[\mathbf{U}]$ and $\mathcal{G} \subset R[\mathbf{x}][\boldsymbol{\partial}]$, then every reduced form of F modulo $\mathcal{G}$ lies in $R[\mathbf{U}]$.

Proof. (i) It follows from the definition of the term order $\prec$.

(ii) Since $\mathrm{HT}(P)$ divides some $t \in \mathrm{T}(F)$, we must have $\mathrm{HT}(P) \in \mathrm{T}(\mathbf{U})$. Thus, we have that $\mathrm{T}(P) \subset \mathrm{T}(\mathbf{U})$ by (i), *i.e.*, $P \in R[\mathbf{U}]$. It follows from the definition of reduction that $G \in R[\mathbf{U}]$. Claim (iii) can be derived from (ii) by induction on the length of reduction chains. □

The next proposition provides a method to compute elimination ideals.

Proposition 2.9.2. *Let I be a left ideal of $R[\mathbf{x}][\boldsymbol{\partial}]$ and $\{\mathbf{U}\} \subset \{\mathbf{x}, \boldsymbol{\partial}\}$. Assume that $\prec$ is a term order that satisfies $\{\mathbf{U}\} \prec \{\mathbf{x}, \boldsymbol{\partial}\} \setminus \{\mathbf{U}\}$, and $\mathcal{G}$ is Gröbner basis of I with respect to $\prec$. Then $\mathcal{G} \cap R[\mathbf{U}]$ is a Gröbner basis of the elimination ideal $I_{\mathbf{U}}$.*

Proof. Set $\mathcal{G}' = \mathcal{G} \cap R[\mathbf{U}]$. We show that every $0 \neq F \in I_{\mathbf{U}}$ is reducible modulo $\mathcal{G}'$. Let $0 \neq F \in I_{\mathbf{U}}$. Then $F \in I$, and thus F is reducible modulo $\mathcal{G}$, say $F \underset{G}{\longrightarrow} H$ with $G \in \mathcal{G}$. By Lemma 2.9.1 (ii), $G \in \mathcal{G}'$, and thus F is reducible modulo $\mathcal{G}'$. □

2.10 Saturation with respect to a constant

Let I be a left ideal in $R[\mathbf{x}][\boldsymbol{\partial}]$, and $c \in R$. The saturation of I with respect to c is defined as

$$I : c^\infty = \left\{ P \in R[\mathbf{x}][\boldsymbol{\partial}] \mid c^i P \in I \text{ for some } i \in \mathbb{N} \right\}.$$

Since c is a constant with respect to σ_i and δ_i for $i \in \{1, \ldots, n\}$, c is in the center of $R[\mathbf{x}][\boldsymbol{\partial}]$. It follows that the saturation $I : c^\infty$ is a left ideal in $R[\mathbf{x}][\boldsymbol{\partial}]$. A basis of the saturation ideal can be computed in the same way as in the commutative case.

To this end, we need to introduce some new indeterminates. Let σ_y be the identity map of $R[\mathbf{x}, y]$, where y is a new indeterminate. Let δ_y be the σ_y-derivation that maps everything in $R[\mathbf{x}, y]$ to zero. Then one can extend the ring $R[\mathbf{x}][\boldsymbol{\partial}]$ to $R[\mathbf{x}, y][\boldsymbol{\partial}, \partial_y]$. Moreover, $R[y][\partial_y]$ lies in the center of the extended ring. For $r \in R$, one can define an evaluation map

$$\begin{array}{cccc} \phi_r : & R[\mathbf{x}, y][\boldsymbol{\partial}, \partial_y] & \longrightarrow & R[\mathbf{x}][\boldsymbol{\partial}] \\ & \sum_{i=0}^{\ell} \sum_{j=0}^{m} f_{ij} y^i \partial_y^j & \mapsto & \sum_{i=0}^{\ell} f_{i0} r^i, \end{array}$$

where $f_{ij} \in R[\mathbf{x}][\boldsymbol{\partial}]$. Since $R[y][\partial_y]$ is contained in the center of $R[\mathbf{x}, y][\boldsymbol{\partial}, \partial_y]$, the map ϕ_r is a ring homomorphism.

Proposition 2.10.1. *Let I be a left ideal of $R[\mathbf{x}][\boldsymbol{\partial}]$ and c be a non-zero element in R. Assume that J is a left ideal*

$$R[\mathbf{x}, y][\boldsymbol{\partial}, \partial_y] \cdot (I \cup \{1 - cy\}),$$

Then $I : c^\infty = J \cap R[\mathbf{x}][\boldsymbol{\partial}]$.

Proof. Let $J_{\mathbf{x},\boldsymbol{\partial}} = J \cap R[\mathbf{x}][\boldsymbol{\partial}]$. If $G \in J_{\mathbf{x},\boldsymbol{\partial}}$, then

$$G = Q_1 P + Q_2(1 - cy) \tag{2.5}$$

with $Q_1, Q_2 \in R[\mathbf{x}, y][\boldsymbol{\partial}, \partial_y]$ and $P \in I$. Next, let us pass to the extended ring $Q_R[\mathbf{x}, y][\boldsymbol{\partial}, \partial_y]$ of $R[\mathbf{x}, y][\boldsymbol{\partial}, \partial_y]$, we may apply the evaluation homomorphism $\phi_{1/c}$ to (2.5) and then multiply the resulting equation by c^d, where $d = \deg_y(Q_1)$. We thus obtain $c^d G = QP$ with Q being in $R[\mathbf{x}][\boldsymbol{\partial}]$. Consequently, $J_{\mathbf{x},\boldsymbol{\partial}} \subset I : c^\infty$.

Conversely, let $G \in I : c^\infty$, say $c^d G \in I$. Then $G \in R[\mathbf{x}][\boldsymbol{\partial}]$ and $c^d G \in J$. Since $1 - cy$ belongs to J,

$$1 - (cy)^d = (1 + cy + (cy)^2 + \cdots + (cy)^{d-1})(1 - cy) \in J$$

Since y and c commute with every element of $R[\mathbf{x}, y][\boldsymbol{\partial}, \partial_y]$,

$$\left(1 - (cy)^d\right) G = G \left(1 - (cy)^d\right) \in J.$$

Again, $(cy)^d G = y^d (c^d G) \in J$ because $c^d G \in J$. It follows that

$$G = \left(1 - (cy)^d\right) G + (cy)^d G \in J.$$

Thus, $G \in J_{\mathbf{x},\boldsymbol{\partial}}$. $\square$

By the above proposition, a Gröbner basis of $I : c^\infty$ with $c \in R$ can be computed by elimination as explained in the previous section. For the case $R = \mathbb{Q}[t]$ with t being an indeterminate, [31] contains an implementation for computing saturation ideals with respect to a constant.

Chapter 3

Univariate Contraction of Ore Ideals

This chapter contains the first contribution of the thesis. We summarize the main results as below:

(i) Theorem 3.2.3 characterizes the connection between contraction ideals and desingularized operators (Section 3.2).

(ii) Theorem 3.3.6 and Algorithm 3.3.8 give a method to compute contraction ideals (Section 3.3).

(iii) Theorem 3.4.4 and Algorithm 3.4.5 give a method to determine a completely desingularized operator (Section 3.4).

This work is published in ISSAC'16 [50].

3.1 Preliminaries

3.1.1 Notations

Throughout the chapter, we let R be a principal ideal domain. For instance, R can be the ring of integers or that of univariate polynomials over a field. Note that $R[x]$ is a unique factorization domain. So every nonzero polynomial f in $R[x]$ can be written as cg, where $c \in R$ and $g \in R[x]$ whose coefficients have a trivial greatest common divisor. We call c the content and g the primitive part of f. They are unique up to multiplication by units of R.

Let $R[x][\partial]$ be the univariate Ore algebra, which is defined in Section 2.1. Given an operator $L \in R[x][\partial]$, we can uniquely write it as

$$L = \ell_r\partial^r + \ell_{r-1}\partial^{r-1} + \cdots + \ell_0$$

with $\ell_0, \ldots, \ell_r \in R[x]$ and $\ell_r \neq 0$. We call r the *order* and ℓ_r the *leading coefficient* of L. They are denoted by $\deg_\partial(L)$ and $\mathrm{lc}_\partial(L)$, respectively. Assume that $P \in R[x][\partial]$ is of order k. A repeated use of the commutation rule yields

$$\mathrm{lc}_\partial(PL) = \mathrm{lc}_\partial(P)\sigma^k(\mathrm{lc}_\partial(L)). \tag{3.1}$$

For a subset S of $R[x][\partial]$, the left ideal generated by S is denoted by $R[x][\partial] \cdot S$.

Let Q_R be the quotient field of R. Then $Q_R(x)[\partial]$ is an Ore algebra containing $R[x][\partial]$. For each operator $L \in R[x][\partial]$, we define the *contraction ideal* of L to be $Q_R(x)[\partial]L \cap R[x][\partial]$ and denote it by $\mathrm{Cont}(L)$.

3.1.2 Removability

We generalize some terminology given in [10, 11] by replacing the coefficient ring $\mathbb{K}[x]$ with $R[x]$, where $\mathbb{K}$ is a field.

Definition 3.1.1. *Let $L \in R[x][\partial]$ with positive order, and p be a divisor of $\mathrm{lc}_\partial(L)$ in $R[x]$.*

(i) We say that p is removable *from L at order k if there exist $P \in Q_R(x)[\partial]$ with order k, and $w, v \in R[x]$ with $\gcd(p, w) = 1$ in $R[x]$ such that*

$$PL \in R[x][\partial] \quad \text{and} \quad \sigma^{-k}(\mathrm{lc}_\partial(PL)) = \frac{w}{vp}\,\mathrm{lc}_\partial(L).$$

*We call P a p-*removing operator for L over $R[x]$*, and PL the corresponding p-*removed operator.

(ii) We simply say that p is removable *from L if it is removable at order k for some $k \in \mathbb{N}$. Otherwise, p is called* non-removable *from L.*

Note that every p-removed operator lies in $\mathrm{Cont}(L)$.

Example 3.1.2. *In the difference Ore algebra $\mathbb{Z}[n][\partial]$, where $\partial n = (n+1)\partial$. Let $L = n\partial + 1$. By [10, Lemma 4], n is non-removable from L.*

Example 3.1.3. *In the example of Chapter 1, $(1 + 16n)^2$ is removable from L at order 1, and T is the corresponding $(1 + 16n)^2$-removed operator for L.*

Example 3.1.4. *In the differential Ore algebra $\mathbb{Z}[x][\partial]$, where $\partial x = x\partial + 1$, let*

$$L = x(x - 1)\partial - 1.$$

Then $(1-x)\partial^2 - 2\partial = \left(\frac{1}{x}\partial\right) L$ is an x-removed operator for L (see [11, Example 3]).

In order to get an order bound for p-removing operators over $\mathbb{K}[x]$, the authors of [10] provide a convenient form of p-removing operators. We derive a similar form over $R[x]$ and use it in Section 3.4.

Lemma 3.1.5. *Let $L \in R[x][\partial]$ with positive order. Assume that $p \in R[x]$ is removable from L at order k. Then there exists a p-removing operator for L over $R[x]$ in the form*

$$\frac{p_0}{\sigma^k(p)^{d_0}} + \frac{p_1}{\sigma^k(p)^{d_1}}\partial + \cdots + \frac{p_k}{\sigma^k(p)^{d_k}}\partial^k,$$

where p_i belongs to $R[x]$, $\gcd(p_i, \sigma^k(p)) = 1$ in $R[x]$ or $p_i = 0$, $i = 0, 1, \ldots, k$, and $d_k \geq 1$.

Proof. By (3.1) and Definition 3.1.1 (i), $\mathrm{lc}_\partial(P) = \sigma^k(w/(vp))$ for some w, v in $R[x]$ with the property $\gcd(w, p) = 1$. Then we can write a p-removing operator for L over $R[x]$ in the form

$$P = \frac{p_0}{q_0\sigma^k(p)^{d_0}} + \frac{p_1}{q_1\sigma^k(p)^{d_1}}\partial + \cdots + \frac{p_k}{q_k\sigma^k(p)^{d_k}}\partial^k,$$

where $p_i, q_i \in R[x]$, $\gcd(p_iq_i, \sigma^k(p)) = 1$ in $R[x]$ or $p_iq_i = 0$, $i = 0, \ldots, k$, $d_k \geq 1$. Let

$$\tilde{P} = \left(\prod_{i=0}^{k} q_i\right) P, \quad \tilde{p}_i = p_i \left(\prod_{j=0}^{k} q_j\right)/q_i \text{ for } i = 0, \ldots, k.$$

Then

$$\tilde{P} = \frac{\tilde{p}_0}{\sigma^k(p)^{d_0}} + \frac{\tilde{p}_1}{\sigma^k(p)^{d_1}}\partial + \cdots + \frac{\tilde{p}_k}{\sigma^k(p)^{d_k}}\partial^k,$$

where $\gcd(\tilde{p}_i, \sigma^k(p)) = 1$ in $R[x]$ or $\tilde{p}_i = 0$, $i = 0, \ldots, k$. Moreover,

$$\sigma^{-k}(\mathrm{lc}_\partial(\tilde{P}L)) = \frac{\sigma^{-k}(\tilde{p}_k)}{p^{d_k}}\mathrm{lc}_\partial(L).$$

By Definition 3.1.1, $\tilde{P}$ is a p-removing operator for L over $R[x]$ with the required form. $\square$

3.2 Desingularization and contraction

In this section, we define the notion of desingularized operators, and connect it with contraction ideals. As a matter of notation, for an operator $L \in R[x][\partial]$, we set

$$M_k(L) = \{P \in \mathrm{Cont}(L) \mid \deg_\partial(P) \leq k\}.$$

Note that $M_k(L)$ is a left $R[x]-$submodule of $\mathrm{Cont}(L)$. We call it the kth submodule of $\mathrm{Cont}(L)$. When the operator L is clear from context, $M_k(L)$ is simply denoted by M_k.

Definition 3.2.1. *Let $L \in R[x][\partial]$ with order $r > 0$, and*

$$\mathrm{lc}_\partial(L) = cp_1^{e_1} \cdots p_m^{e_m}, \tag{3.2}$$

where $c \in R$ and $p_1, \ldots, p_m \in R[x] \setminus R$ are irreducible and pairwise coprime. An operator $T \in R[x][\partial]$ of order k is called a desingularized operator *for L if $T \in \mathrm{Cont}(L)$ and*

$$\sigma^{r-k}(\mathrm{lc}_\partial(T)) = \frac{a}{bp_1^{k_1} \cdots p_m^{k_m}}\mathrm{lc}_\partial(L), \tag{3.3}$$

where $a, b \in R$ with $b \neq 0$, and $p_i^{d_i}$ is non-removable from L for each $d_i > k_i$, $i = 1 \ldots m$.

According to [11, Lemma 4], desingularized operators always exist over $Q_R[x][\partial]$. By clearing denominators, they also exist over $R[x][\partial]$.

Lemma 3.2.2. *Let $L \in R[x][\partial]$ be of order $r > 0$, and $k \in \mathbb{N}$ with $k \geq r$. Assume that T is a desingularized operator for L and $\deg_\partial(T) = k$.*

(i) $\deg_x(\mathrm{lc}_\partial(T)) = \min\{\deg_x(\mathrm{lc}_\partial(Q)) \mid Q \in M_k(L) \setminus \{0\}\}$.

(ii) $\partial^i T$ is a desingularized operator for L for each $i \in \mathbb{N}$.

(iii) Set $\mathrm{lc}_\partial(T) = ag$, where $a \in R$ and $g \in R[x]$ is primitive. Then, for all $F \in \mathrm{Cont}(L)$ of order j with $j \geq k$, we have that $\sigma^{j-k}(g)$ divides $\mathrm{lc}_\partial(F)$ in $R[x]$.

Proof. (i) Let $t = \mathrm{lc}_\partial(T)$ and

$$d = \min\{\deg_x(\mathrm{lc}_\partial(Q)) \mid Q \in M_k(L) \setminus \{0\}\}.$$

Suppose that $d < \deg_x(t)$. Then there exists $Q \in \mathrm{Cont}(L)$ with $\deg_x(\mathrm{lc}_\partial(Q)) = d$. Without loss of generality, we can assume that $\deg_\partial(Q) = k$, because the leading coefficients of Q and $\partial^i Q$ are of the same degree for all $i \in \mathbb{N}$.

By pseudo-division in $R[x]$, we have that

$$st = q\,\mathrm{lc}_\partial(Q) + h$$

for some $s \in R\setminus\{0\}$, $q, h \in R[x]$, and $h = 0$ or $\deg_x(h) < d$. If h were nonzero, then $sT - qQ$ would be a nonzero operator of order k in $\mathrm{Cont}(L)$ whose leading coefficient is of degree less than d, a contradiction. Thus, $st = q\,\mathrm{lc}_\partial(Q)$. In particular, $\deg_x(q)$ is positive, as $d < \deg_x(t)$. It follows from (3.3) that

$$\sigma^{r-k}(\mathrm{lc}_\partial(Q)) = \sigma^{r-k}\left(\frac{st}{q}\right) = \frac{sa}{\sigma^{r-k}(q)bp_1^{k_1}\cdots p_m^{k_m}}\,\mathrm{lc}_\partial(L),$$

which belongs to $R[x]$. Hence, $\sigma^{r-k}(q)$ divides $\mathrm{lc}_\partial(L)$ in $R[x]$. Consequently, there exists an integer $i \in \{1\ldots m\}$ such that p_i divides $\sigma^{r-k}(q)$ in $R[x]$. This implies that p^{k_i+1} is removable from L, a contradiction.

(ii) It is immediate from Definition 3.2.1.

(iii) Let $\mathrm{lc}_\partial(F) = uf$, where $u \in R$ and f is primitive in $R[x]$. By (ii), $\partial^{j-k}T$ is a desingularized operator whose leading coefficient is $a\sigma^{j-k}(g)$. A similar argument as used in the proof of the first assertion implies that

$$vf = p\sigma^{j-k}(g) \quad \text{for some } v \in R \setminus \{0\} \text{ and } p \in R[x].$$

By Gauss's Lemma in $R[x]$, it follows that $\sigma^{j-k}(g) \mid f$. □

We describe a relation between desingularized operators and contraction ideals.

Theorem 3.2.3. *Let $L \in R[x][\partial]$ with order $r > 0$. Assume that T is a desingularized operator for L. Let $\mathrm{lc}_\partial(T) = ag$, where $a \in R$ and g is primitive in $R[x]$. If k is such that $T \in M_k$ for some $k \in \mathbb{N}$, then*

$$\mathrm{Cont}(L) = (R[x][\partial] \cdot M_k) : a^\infty.$$

Proof. By Lemma 3.2.2 (ii), we may assume that the order of T is equal to k. Set

$$J = (R[x][\partial] \cdot M_k) : a^\infty.$$

First, assume that $F \in J$. Then there exists $j \in \mathbb{N}$ such that $a^j F \in R[x][\partial] \cdot M_k$. It follows that $F \in Q_R(x)[\partial]L$. Thus, $F \in \mathrm{Cont}(L)$ by definition.

Next, note that $\mathrm{Cont}(L) = \bigcup_{i=r}^{\infty} M_i$ and that $M_i \subseteq M_{i+1}$. Therefore, it suffices to show $M_i \subseteq J$ for all $i \geq k$. We proceed by induction on i.

For $i = k$, we have $M_k \subseteq J$ by definition.

Suppose that the claim holds for i. For any $F \in M_{i+1} \backslash M_i$, we have $\deg_\partial(F) = i + 1$. By Lemma 3.2.2 (iii),

$$\mathrm{lc}_\partial(F) = p\sigma^{i+1-k}(g) \text{ for some } p \in R[x].$$

Then $\mathrm{lc}_\partial(aF) = \mathrm{lc}_\partial(p\partial^{i+1-k}T)$. It follows that $aF - p\partial^{i+1-k}T \in M_i$. Since

$$p\partial^{i+1-k}T \in R[x][\partial] \cdot M_k \subseteq R[x][\partial] \cdot M_i,$$

we have that $aF \in R[x][\partial] \cdot M_i$. On the other hand, $M_i \subset J$ by the induction hypothesis. Thus, we have $aF \in R[x][\partial] \cdot J$, which is J. Accordingly, $F \in J$ by the definition of saturation. □

When R is a field, the above theorem simplifies to the following corollary.

Corollary 3.2.4. *Let $L \in \mathbb{K}[x][\partial]$ be an operator of positive order, where $\mathbb{K}$ is a field. Assume that T is a desingularized operator of L. If k is a positive integer such that $T \in M_k$, then*

$$\mathrm{Cont}(L) = \mathbb{K}[x][\partial] \cdot M_k$$

Proof. Note that $\mathrm{lc}_\partial(T)$ is a primitive polynomial in $\mathbb{K}[x]$. By Theorem 3.2.3, we have

$$\mathrm{Cont}(L) = (\mathbb{K}[x][\partial] \cdot M_k) : 1^\infty = \mathbb{K}[x][\partial] \cdot M_k.$$

□

3.3 An algorithm for computing contraction ideals

3.3.1 Upper bounds for the orders of desingularized operators

First, we translate an upper bound for the order of a desingularized operator over $Q_R[x]$ to $R[x]$.

Lemma 3.3.1. *Let $L \in R[x][\partial]$ with order $r > 0$, and $p \in R[x]$ be a primitive polynomial and a divisor of $\mathrm{lc}_\partial(L)$. Assume that there exists a p-removing operator for L over $Q_R[x]$. Then there exists a p-removing operator for L over $R[x]$ of the same order as the one over $Q_R[x]$.*

Proof. Assume that $P \in Q_R(x)[\partial]$ is a p-removing operator for L over $Q_R[x]$. Let P be of order k. Then PL is of the form

$$PL = \frac{a_{k+r}}{b_{k+r}}\partial^{k+r} + \cdots + \frac{a_1}{b_1}\partial + \frac{a_0}{b_0}$$

for some $a_i \in R[x], b_i \in R \setminus \{0\}$, $i = 0, \ldots, k+r$. Moreover,

$$\sigma^{-k}\left(\mathrm{lc}_\partial(PL)\right) = \frac{w}{vp}\,\mathrm{lc}_\partial(L),$$

where $w, v \in R[x]$ with $\gcd(w, p) = 1$.

Let $b = \mathrm{lcm}(b_0, b_1, \ldots, b_{k+r})$ in R and $P' = bP$. Then

$$P'L \in R[x][\partial] \quad \text{and} \quad \sigma^{-k}(\mathrm{lc}_\partial(PL)) = \frac{bw}{vp}\,\mathrm{lc}_\partial(L).$$

Since p is primitive, we have that $\gcd(bw, p) = 1$ in $R[x]$. Therefore, P' is also a p-removing operator of order k. $\square$

By the above lemma, an order bound for a p-removing operator over $Q_R[x]$ is also an order bound for a p-removing operator over $R[x]$. The former has been well-studied in the literature. In the shift case, let p be a irreducible factor of $\mathrm{lc}_\partial(L)$ such that p^k is removable from L but p^{k+1} is non-removable, where $k \in \mathbb{Z}^+$. References [10, Lemma 4] and [23, Lemma 4.3.3] give an upper bound for the order of a p^k-removing operator, and we denote it as o_p. Based on the proof of [11, Lemma 4], we know that an upper bound for a desingularized operator is equal to

$$\deg_\partial(L) + \max\{o_p \;:\; p \mid \mathrm{lc}_\partial(L) \;\text{ and }\; p \text{ is irreducible}\}.$$

In the differential case, [47, Algorithm 3.4] gives an upper bound for generators of the contraction ideal over $Q_R[x][\partial]$. Therefore, we can derive an upper bound for a desingularized operator. For details, see Remark 3.3.5.

3.3.2 Determining the kth submodule of contraction ideals

By Theorem 3.2.3, determining a contraction ideal amounts to finding a desingularized operator T and a spanning set of M_k over $R[x]$, where k is an upper bound for the order of T. The definition of M_k is given in the first paragraph of Section 3.2.

Next, we present an algorithm for constructing a spanning set for $M_k(L)$ over $R[x]$, where L is a nonzero operator in $R[x][\partial]$ and k is a positive integer. To this end, we embed M_k into the free module $R[x]^{k+1}$ over $R[x]$.

Let us recall the right division in $Q_R(x)[\partial]$ (see [6, Section 3] and [42, page 483]). For each pair $F, G \in Q_R(x)[\partial]$ with $G \neq 0$, there exist unique elements $Q, R \in Q_R(x)[\partial]$ with the properties $\deg_\partial(R) < \deg_\partial(G)$ or $R = 0$ such that $F = QG + R$. We call R the *right remainder* of F by G and denote it by $\mathrm{rrem}(F, G)$.

Let $F \in R[x][\partial]$ with order k. Then $F \in M_k$ if and only if $F \in Q_R(x)[\partial]L$, which is equivalent to $\mathrm{rrem}(F, L) = 0$. Assume that $F = z_k\partial^k + \ldots + z_0$, where $z_k, \ldots, z_0 \in R[x]$ are to be determined. Then $\mathrm{rrem}(F, L) = 0$ gives rise to a linear system

$$(z_k, \ldots, z_0)A = \mathbf{0}, \tag{3.4}$$

where A is a $(k+1) \times r$ matrix over $Q_R(x)$. Clearing denominators of the elements in A, we may further assume that A is a matrix over $R[x]$. We are concerned with the solutions of (3.4) *over* $R[x]$. Set

$$N_k = \left\{ (f_k, \ldots, f_0) \in R[x]^{k+1} \mid (f_k, \ldots, f_0)A = \mathbf{0} \right\}.$$

We call N_k the module of syzygies defined by (3.4). With the notation just specified, the following theorem is evident.

Theorem 3.3.2.

$$\begin{array}{cccc} \phi: & M_k & \longrightarrow & N_k \\ & \sum_{i=0}^{k} f_i\partial^i & \mapsto & (f_k, \ldots, f_0) \end{array}$$

is a module isomorphism over $R[x]$.

By Theorem 3.3.2, M_k is a finitely generated module over $R[x]$. To find a spanning set of M_k over $R[x]$, it suffices to compute a spanning set of the module of syzygies defined by (3.4) over $R[x]$. When R is a field, we just need to solve (3.4) over a principal ideal domain [46, Chapter 5]. When R is the ring of integers or the ring of univariate polynomials over a field, we can use Gröbner bases of polynomials over a principal domain [27, 19]. The implementations of these are available in computer algebra systems such as `Macaulay2` [19] and `Singular` [17].

3.3.3 The kth coefficient ideal of contraction ideals

To prove the correctness of our algorithm for determining contraction ideals, we introduce the concept of kth coefficient ideal of contraction ideals. This notion also helps us derive an upper bound for the order of a desingularized operator in the differential case.

For $k \in \mathbb{Z}^+$, we define

$$I_k = \left\{ [\partial^k]P \mid P \in M_k \right\} \cup \{0\},$$

where $[\partial^k]P$ stands for the coefficient of ∂^k in P. It is clear that I_k is an ideal of $R[x]$. We call I_k the kth coefficient ideal of $\mathrm{Cont}(L)$. By the commutation rule, $\sigma(I_k) \subset I_{k+1}$.

Lemma 3.3.3. *Let $L \in R[x][\partial]$ be of positive order. If the kth submodule M_k of* $\mathrm{Cont}(L)$ *has a spanning set $\{B_1, \ldots, B_\ell\}$ over $R[x]$, then the kth coefficient ideal*

$$I_k = \left\langle [\partial^k]B_1, \ldots, [\partial^k]B_\ell \right\rangle.$$

Proof. Obviously, $\langle [\partial^k]B_1, \ldots, [\partial^k]B_\ell \rangle \subseteq I_k$. Let $f \in I_k$. Then $f = \mathrm{lc}_\partial(F)$ for some $F \in M_k$ with $\deg_\partial(F) = k$. Since M_k is generated by $\{B_1, \ldots, B_\ell\}$ over $R[x]$,

$$F = h_1 B_1 + \cdots + h_\ell B_\ell, \quad \text{where } h_1, \ldots, h_\ell \in R[x].$$

Thus, $f = h_1 \left([\partial^k]B_1\right) + \cdots + h_\ell \left([\partial^k]B_\ell\right)$. Consequently, $f \in \langle [\partial^k]B_1, \ldots, [\partial^k]B_\ell \rangle$. □

The next technical lemma not only helps us derive an upper bound for the order of a desingularized operator, but also serves as a step-stone to construct completely desingularized operators.

Lemma 3.3.4. *Let L be an operator in $R[x][\partial]$ with positive order r, and $k \geq r$. Then we have that $R[x][\partial] \cdot M_k = R[x][\partial] \cdot M_{k+1}$ if and only if $\sigma(I_k) = I_{k+1}$.*

Proof. Assume that $\sigma(I_k) = I_{k+1}$. Since $M_k \subset M_{k+1}$, it suffices to prove that

$$M_{k+1} \subset R[x][\partial] \cdot M_k.$$

For each $T \in M_{k+1} \setminus M_k$, we have that $\mathrm{lc}_\partial(T) \in \sigma(I_k)$. Thus, there exists $F \in M_k$ such that

$$\sigma(\mathrm{lc}_\partial(F)) = \mathrm{lc}_\partial(T).$$

In other words, $T - \partial F \in M_k$. Consequently, $T \in R[x][\partial] \cdot M_k$.

Conversely, assume that $R[x][\partial] \cdot M_{k+1} = R[x][\partial] \cdot M_k$. It suffices to prove the inclusion relation $I_{k+1} \subseteq \sigma(I_k)$ because $\sigma(I_k) \subseteq I_{k+1}$ by definition. Let $\mathcal{B}$ be a spanning set of M_k over $R[x]$. Then $\mathcal{B}$ is also a basis of the left ideal $R[x][\partial] \cdot M_k$.

Let $\prec$ be the term order such that $x^{\ell_1}\partial^{m_1} \prec x^{\ell_2}\partial^{m_2}$ if either $m_1 < m_2$ or $m_1 = m_2$ and $\ell_1 < \ell_2$. Since $\deg_\partial(P) \leq k$ for each $P \in \mathcal{B}$, S-polynomials and G-polynomials [5, Definition 10.9] formed by elements in M_k have orders no more than k. By Buchberger's algorithm, there exists a Gröbner basis $\mathcal{G}$ of $R[x][\partial] \cdot \mathcal{B}$ with respect to $\prec$ with $\deg_\partial(G) \leq k$ for each $G \in \mathcal{G}$.

For $p \in I_{k+1} \setminus \{0\}$, there exists $T \in M_{k+1} \setminus M_k$ such that $\mathrm{lc}_\partial(T) = p$. Since T is an operator in $R[x][\partial] \cdot M_{k+1}$, we have $T \in R[x][\partial] \cdot M_k$. It follows that T is reduced to zero by $\mathcal{G}$. Thus,

$$T = \sum_{G \in \mathcal{G}} V_G G \quad \text{with} \quad \mathrm{HT}(V_G G) \preceq \mathrm{HT}(T). \tag{3.5}$$

By the choice of term order, $\deg_\partial(V_G G) \leq k + 1$. If $V_G G$ is of order $k + 1$, then

$$\mathrm{lc}_\partial(V_G G) = a_G\, \sigma^{k+1-d_G}(\mathrm{lc}_\partial(G)),$$

where a_G is in $R[x]$ and d_G is the order of G. Comparing the leading coefficients of operators on both sides of (3.5) and noticing $\deg_\partial(T) = k+1$, we have

$$p = \sum_{\deg_\partial(V_G G)=k+1} a_G\, \sigma^{k+1-d_G}(\mathrm{lc}_\partial(G)).$$

It follows that

$$\sigma^{-1}(p) = \sum_{\deg_\partial(V_G G)=k+1} \sigma^{-1}(a_G)\, \sigma^{k-d_G}(\mathrm{lc}_\partial(G)). \tag{3.6}$$

On the other hand, $\sigma^{k-d_G}(\mathrm{lc}_\partial(G)) = \mathrm{lc}_\partial\left(\partial^{k-d_G}G\right)$ implies that $\sigma^{k-d_G}(\mathrm{lc}_\partial(G)) \in I_k$. We have that $\sigma^{-1}(p) \in I_k$ by (3.6). Thus, $I_{k+1} \subset \sigma(I_k)$. $\square$

Remark 3.3.5. *In the differential case, σ is the identity map. The paper [47, Algorithm 3.4] gives an upper bound for generators of the contraction ideal over $Q_R[x][\partial]$, which is denoted as k. Then* $\mathrm{Cont}(L) = Q_R[x][\partial] \cdot M_k$. *Thus, for each $\ell \geq k$,*

$$Q_R[x][\partial] \cdot M_\ell = Q_R[x][\partial] \cdot M_{\ell+1}.$$

According to the above lemma, $I_\ell = I_k$ for each $\ell \geq k$. Assume that T is a desingularized operator of L. Without loss of generality, we may further assume that $\deg_\partial(T) = m > k$. *Since $I_m = I_k$, there exists $\tilde{T} \in \mathrm{Cont}(L)$ such that $\mathrm{lc}_\partial(\tilde{T}) = \mathrm{lc}_\partial(T)$. By Definition 3.2.1, $\tilde{T}$ is also a desingularized operator of L. Therefore, k is also an upper bound for a desingularized operator of L.*

3.3.4 Determining bases of contraction ideals

Based on the connection between contraction ideals and desingularized operators (Theorem 3.2.3), we need to construct a desingularized operator. In the shift case, when R is a field, the paper [10] gives an algorithm for constructing desingularized operators. When R is a principal ideal domain, the following theorem gives an algorithm for constructing desingularized operators. It includes both the differential and the difference case.

Theorem 3.3.6. *Let $L \in R[x][\partial]$ be of positive order. Assume that the kth submodule M_k of* $\mathrm{Cont}(L)$ *contains a desingularized operator for L. Let s be a nonzero element in the kth coefficient ideal with minimal degree. Then an operator S in M_k with leading coefficient s is a desingularized operator.*

Proof. Assume that T is a desingularized operator in M_k. By Lemma 3.2.2 (ii), we may assume that the order of T is equal to k. Let $t = \mathrm{lc}_\partial(T)$. Then $\deg(t) = \deg(s)$ by Lemma 3.2.2 (i). Let u be the leading coefficient of s with respect to x and v be that of t. Then $ut - vs$ is zero. Otherwise, we have that $uT - vS$ would be an operator of order k whose leading coefficient with respect to ∂ has degree lower than $\deg_x(t)$, a contradiction to Lemma 3.2.2 (i). It follows from $ut = vs$ and Definition 3.2.1 that S is a desingularized operator. $\square$

Remark 3.3.7. *Let L be an operator in $R[x][\partial]$ of positive order. We can compute a spanning set $\{B_1, \ldots, B_\ell\}$ for the kth submodule of* $\mathrm{Cont}(L)$ *by Theorem 3.3.2, where k is an upper bound on the order of a desingularized operator for L.*

Set $b_i = [\partial^k]B_i$, $i = 1, \ldots, \ell$. By Lemma 3.3.3, the kth coefficient ideal I_k of $\mathrm{Cont}(L)$ *is generated by $\{b_1, \ldots, b_\ell\}$. Let $\bar{I}_k$ be the extension ideal [5, Section 1.10] of I_k in $Q_R[x]$. Since $Q_R[x]$ is a principal ideal domain, we have that $\bar{I}_k = \langle s' \rangle$ for some $s' \in Q_R[x]$. Then there exist $c_1', \ldots, c_\ell' \in Q_R[x]$ such that $c_1' b_1 + \ldots + c_\ell' b_\ell = s'$. By clearing denominators, we can find $c_1, \ldots, c_\ell \in R[x]$ such that*

$$c_1 b_1 + \cdots + c_\ell b_\ell = s,$$

where $s = cs'$ for some $c \in R$. Then s is an element in I_k with minimal degree. It follows from Theorem 3.3.6 that $T = c_1 B_1 + \cdots + c_\ell B_\ell$ is a desingularized operator for L with $\mathrm{lc}_\partial(T) = s$.

Let a be the content of s. Note that a is unique up to a unit because $R[x]$ is a unique factorization domain. By Theorem 3.2.3, $\mathrm{Cont}(L)$ is the saturation of $R[x][\partial] \cdot M_k$ with respect to a. Note that a is contained in the center of $R[x][\partial]$. Therefore, a basis of the saturation ideal can be computed in the same way as in the commutative case. For details, see Proposition 2.10.1.

Next, we outline our method for determining contraction ideals.

Algorithm 3.3.8. *Given $L \in R[x][\partial]$ and an order bound k for desingularized operators of L, compute a basis of* $\mathrm{Cont}(L)$.

(1) Compute a spanning set of M_k over R[x].

(2) Compute a desingularized operator T, and set a to be the content of $\mathrm{lc}_\partial(T)$.

(3) Compute a basis of $(R[x][\partial] \cdot M_k) : a^\infty$.

The termination of this algorithm is evident. Its correctness follows from Theorem 3.2.3. In literature, we only know order bounds for desingularized operators in the differential and difference cases, respectively.

In the shift case, a bound is derived from [10, Lemma 4]. More concretely, we factor $\mathrm{lc}_\partial(L)$ and compute the maximum of the dispersions [38, Definition 1] of the factors with the trailing coefficient. In the differential case, we can follow steps 1, 2 and 3 in [47, Algorithm 3.4] to rewrite the input operator as a b-function [47, Algorithm 2.2] in the algebraic extension of each factor of $\mathrm{lc}_\partial(L)$, and bound integer roots of the trailing coefficient in each b-function. By Remark 3.3.5, we can derive an upper bound for the order of a desingularized operator in this case.

In step 1, we need to solve linear systems over $R[x]$ as stated in Theorem 3.3.2. This can be done by a Gröbner basis computation. In step 2, T is computed according to Theorem 3.3.6 and the extended Euclidean algorithm in $Q_R[x]$.

The last step is carried out according to Proposition 2.10.1, the computation is similar to that of saturation ideals in the commutative case.

Remark 3.3.9. *When R is a field, the content of $\mathrm{lc}_\partial(T)$ is equal to 1. Therefore, we just need to execute step 1 and 2 of the above algorithm in this case.*

Example 3.3.10. *Let $\mathbb{Q}[t][n][\partial]$ be the shift Ore algebra, where the commutation rules are*

$$\partial n = (n+1)\partial \text{ and } \partial t = t\partial.$$

Consider

$$L = (n-1)(n+t)\partial + n + t + 1.$$

By [10, Lemma 4], we obtain an order bound 2 for a desingularized operator. Thus, M_2 contains a desingularized operator for L. In step 1 of Algorithm 3.3.8, we find that M_2 is generated by

$$\begin{aligned} T_1 &= (2+t)n\partial^2 + (4-n+t)\partial - 1, \\ T_2 &= (n-1)n\partial^2 + 2(n-1)\partial + 1, \end{aligned}$$

where T_1 is a desingularized operator, $\mathrm{lc}_\partial(T_1) = (2+t)n$. Using Gröbner bases, we find that

$$\mathrm{Cont}(L) = (\mathbb{Q}[t][n][\partial] \cdot M_2) : (2+t)^\infty$$

is generated by $\{L, T_1\}$.

Let us consider the example in Section 1.1 of Chapter 1.

Example 3.3.11. *In the shift Ore algebra $\mathbb{Z}[n][\partial]$, let*

$$L = (1+16n)^2\partial^2 - 32(7+16n)\partial - (1+n)(17+16n)^2.$$

By [10, Lemma 4], we obtain an order bound 3 for a desingularized operator. Thus, M_3 contains a desingularized operator for L. In step 1 of Algorithm 3.3.8, we find that M_3 is generated by $\{L, \tilde{T}\}$, where $\tilde{T}$ is given in (1.1). Note that $\mathrm{lc}_\partial(\tilde{T}) = 1$. Thus, $\tilde{T}$ is a desingularized operator. Consequently,

$$\mathrm{Cont}(L) = (\mathbb{Z}[n][\partial] \cdot \{L, \tilde{T}\}) : 1^\infty = \mathbb{Z}[n][\partial] \cdot \{L, \tilde{T}\}.$$

Example 3.3.12. *Let $\mathbb{Z}[x][\partial]$ be the differential Ore algebra, in which the commutation rule is $\partial x = x\partial + 1$. Consider the operator $L = x\partial^2 - (x+2)\partial + 2 \in \mathbb{Z}[x][\partial]$ from [4]. By [47, Algorithm 3.4], we obtain an order bound 4 for a desingularized operator. Thus, M_4 contains a desingularized operator for L. In step 1 of Algorithm 3.3.8, we find that M_4 is generated by $\{L, \partial L, T\}$, where $T = \partial^4 - \partial^3$. Note that $\mathrm{lc}_\partial(T) = 1$. Thus, T is a desingularized operator. Consequently,*

$$\mathrm{Cont}(L) = (\mathbb{Z}[x][\partial] \cdot \{L, \partial L, T\}) : 1^\infty = \mathbb{Z}[x][\partial] \cdot \{L, T\}.$$

3.4 Complete desingularization

As seen in Chapater 1, the recurrence operator

$$L = (1 + 16n)^2\partial^2 - (224 + 512n)\partial - (1 + n)(17 + 16n)^2$$

has a desingularized operator T with leading coefficient 64. But the content of $\mathrm{lc}_\partial(L)$ is 1. The redundant content 64 has been removed by computing another desingularized operator $\tilde{T}$ in (1.1). This enables us to see immediately that the sequence annihilated by L is an integer sequence when its initial values are integers.

Recall that a sequence $(a_n)_{n\geq 0}$ is called a P-recursive sequence over $\mathbb{Z}$ if there exists a nonzero recurrence operator $L \in \mathbb{Z}[n][\partial]$ such that $L(a_n) = 0$ for each $n \geq 0$.

Krattenthaler and Müller propose the following conjecture in [33, 41]:

Conjecture 3.4.1. *Let $(a_n)_{n\geq 0}$ and $(b_n)_{n\geq 0}$ be two P-recursive sequences over $\mathbb{Z}$. If there exist two recurrence operators L and T of $(a_n)_{n\geq 0}$ and $(b_n)_{n\geq 0}$ such that*

$$\mathrm{lc}_\partial(L) = n + \deg_\partial(L) \text{ and } \mathrm{lc}_\partial(T) = n + \deg_\partial(T),$$

respectively, then there also exists a recurrence operator P of $(n!a_nb_n)_{n\geq 0}$ such that

$$\mathrm{lc}_\partial(P) = n + \deg_\partial(P).$$

To test the conjecture for the two particular sequences, one may first compute an annihilator L of $(n!a_nb_n)_{n\geq 0}$, and then look for a nonzero operator in $\mathrm{Cont}(L)$ whose leading coefficient has both minimal degree and "minimal" content with respect to n. When the content is equal to 1, the conjecture is true for these sequences.

These two observations motivate us to define the notion of completely desingularized operators.

Definition 3.4.2. *Let $L \in R[x][\partial]$ with positive order, and Q a desingularized operator for L. Set c be the content of $\mathrm{lc}_\partial(Q)$. We call Q a* completely desingularized operator *for L if c divides the content of the leading coefficient of every desingularized operator for L.*

To see the existence of completely desingularized operators, suppose that L is of order r. For a desingularized operator T of order k, equations (3.2) and (3.3) in Definition 3.2.1 enable us to write

$$\sigma^{r-k}\left(\mathrm{lc}_\partial(T)\right) = c_T\, g, \tag{3.7}$$

where $c_T \in R$ and $g = p_1^{e_1-k_1} \cdots p_s^{e_m-k_m}$. Note that g is primitive and independent of the choice of desingularized operators.

Lemma 3.4.3. *Let $L \in R[x][\partial]$ with order $r > 0$. Set I to be the set consisting of zero and c_T given in (3.7) for all desingularized operators for L. Then I is an ideal of R.*

Proof. By Definition 3.2.1, the product of a nonzero element of R and a desingularized operator for L is also a desingularized one. So it suffices to show that I is closed under addition. Let T_1 and T_2 be two desingularized operators of orders k_1 and k_2, respectively. Assume that $k_1 \geq k_2$. By (3.7),

$$\sigma^{r-k_1}\left(\mathrm{lc}_\partial(T_1)\right) = c_1\, g \quad \text{and} \quad \sigma^{r-k_2}\left(\mathrm{lc}_\partial(T_2)\right) = c_2\, g.$$

If $c_1 + c_2 = 0$, then there is nothing to prove. Otherwise, a direct calculation implies that

$$\mathrm{lc}_\partial(T_1) = c_1 \sigma^{k_1-r}(g) \quad \text{and} \quad \mathrm{lc}_\partial\left(\partial^{k_1-k_2} T_2\right) = c_2 \sigma^{k_1-r}(g).$$

Thus, $T_1 + \partial^{k_1-k_2} T_2$ has leading coefficient $(c_1+c_2)\sigma^{k_1-r}(g)$. Accordingly, $T_1 + \partial^{k_1-k_2} T_2$ is a desingularized one, which implies that $c_1 + c_2$ belongs to I. □

Since R is a principal ideal domain, I in the above lemma is generated by an element c, which corresponds to a completely desingularized operator.

By Lemma 3.3.4, $I_j = \sigma^{j-\ell}(I_\ell)$ whenever $j \geq \ell$ and $\mathrm{Cont}(L) = R[x][\partial] \cdot M_\ell$. In this case, a basis of I_j can be obtain by shifting a basis of I_ℓ, which allows us to find a completely desingularized operator.

Theorem 3.4.4. *Let $L \in R[x][\partial]$ with order $r > 0$. Assume that the ℓth submodule M_ℓ of* $\mathrm{Cont}(L)$ *contains a basis of* $\mathrm{Cont}(L)$*. Let I_ℓ be the ℓth coefficient ideal of* $\mathrm{Cont}(L)$*, and* $\mathbf{G}$ *a reduced Gröbner basis of I_ℓ. Let $f \in \mathbf{G}$ be of the lowest degree in x and F be the operator in* $\mathrm{Cont}(L)$ *with $\mathrm{lc}_\partial(F) = f$. Then F is a completely desingularized operator for L.*

Proof. By Lemma 3.4.3, $\mathrm{Cont}(L)$ contains a completely desingularized operator S. Let $j = \deg_\partial(S)$. Then $\mathrm{lc}_\partial(S)$ is in I_j for some $j \geq \ell$. By Lemma 3.3.4, $\sigma^{j-\ell}(I_\ell) = I_j$. It follows that $\sigma^{\ell-j}(\mathrm{lc}_\partial(S))$ belongs to I_ℓ. By (3.7), we have

$$\sigma^{r-j}\left(\mathrm{lc}_\partial(S)\right) = c_S\, g,$$

where $c_S \in R$ and g is a primitive polynomial in $R[x]$. A direct calculation implies that

$$\sigma^{\ell-j}(\mathrm{lc}_\partial(S)) = c_S \sigma^{\ell-r}(g).$$

Since $\sigma^{\ell-j}(\mathrm{lc}_\partial(S)) \in I_\ell$, so does $c_S \sigma^{\ell-r}(g)$.

Note that F is a desingularized operator by Theorem 3.3.6. By equation (3.7),

$$\sigma^{r-\ell}\left(f\right) = c_F\, g,$$

where $c_F \in R$. Thus, $f = c_F \sigma^{\ell-r}(g)$.

Since $\mathbf{G}$ is a reduced Gröbner basis of I_ℓ, we know that f is the unique polynomial in $\mathbf{G}$ with minimal degree. Moreover, $c_S \sigma^{l-r}(g)$ is of minimal degree in I_ℓ. So it can be reduced to zero by f. Thus, $c_F \mid c_S$. On the other hand, $c_S \mid c_F$ by Definition 3.4.2. Thus, c_S and c_F are associated to each other. Consequently, F is a completely desingularized operator for L. □

The construction in the above theorem leads to the following algorithm.

Algorithm 3.4.5. *Given $L \in R[x][\partial]$ and an order bound k for desingularized operators of L, compute a completely desingularized operator for L.*

(1) Compute a basis $\mathcal{A}$ of $\mathrm{Cont}(L)$ by Algorithm 3.3.8.

(2) Set ℓ to be the highest order among the elements in $\mathcal{A}$. Compute a spanning set of M_ℓ over $R[x]$.

(3) Set $\mathcal{B}' = \{B \in \mathcal{B} \mid \deg_\partial(B) = \ell\}$. Compute a reduced Gröbner basis $\mathbf{G}$ of

$$\left\langle \left\{ \mathrm{lc}_\partial(B) \mid B \in \mathcal{B}' \right\} \right\rangle.$$

(4) Set f to be the polynomial in $\mathbf{G}$ whose degree is the lowest one in x. Tracing back to the computation of step 3, one can find $u_B \in R[x]$ such that $f = \sum_{B \in \mathcal{B}'} u_B \,\mathrm{lc}_\partial(B)$.

(5) Output $\sum_{B \in \mathcal{B}'} u_B B$.

The termination of this algorithm is evident. Its correctness follows from Theorem 3.4.4.

Example 3.4.6. *Consider two sequences $(a_n)_{n\geq 0}$ and $(b_n)_{n\geq 0}$ satisfying the following two recurrence equations [33]*

$$n a_n = a_{n-1} + a_{n-2} \quad \textit{and} \quad n b_n = b_{n-1} + b_{n-5},$$

respectively. The sequence $c_n = n! a_n b_n$ has an annihilator $L \in \mathbb{Z}[n][\partial]$ with

$$\deg_\partial(L) = 10 \textit{ and } \mathrm{lc}_\partial(L) = (n+10)(n^6 + 47n^5 + \cdots + 211696).$$

In step 1 of the above algorithm, $\mathrm{Cont}(L) = R[x][\partial] \cdot M_{14}$. In steps 2 and 3, we observe that I_{14} is generated by $n+14$. In other words, we obtain a completely desingularized operator T of order 14 with $\mathrm{lc}_\partial(T) = n + 14$. Translated into the recurrence equations of c_n, we have

$$n c_n = \alpha_1 c_{n-1} + \cdots + \alpha_{14} c_{n-14},$$

for certain $\alpha_i \in \mathbb{Z}[n]$, $i = 1, \ldots, 14$, which are too large to be represented here. This confirms Krattenthaler's conjecture for the sequences $(a_n)_{n\geq 0}$ and $(b_n)_{n\geq 0}$.

Note that it is impossible to have a completely desingularized operator of order less than 14. In fact, for some lower orders, one can obtain

$$\begin{aligned}
\sigma^{-11}(I_{11}) &= \langle 11104n, 4n(n-466), n(n^2 - 34n + 1336) \rangle, \\
\sigma^{-12}(I_{12}) &= \langle 4n, n(n-24) \rangle, \\
\sigma^{-13}(I_{13}) &= \langle 2n, n(n-26) \rangle.
\end{aligned}$$

They cannot produce a leading coefficient whose degree and content are both minimal.

Example 3.4.7. *Consider the following recurrence equations:*

$$\begin{aligned} na_n &= (31n-6)a_{n-1} + (49n-110)a_{n-2} + (9n-225)a_{n-3}, \\ nb_n &= (4n+13)b_{n-1} + (69n-122)b_{n-2} + (36n-67)b_{n-3}. \end{aligned}$$

Let $c_n = n!a_n b_n$, which has an annihilator $L \in \mathbb{Z}[n][\partial]$ of order 10 with $\mathrm{lc}_\partial(L) = (n+9)\alpha$, where $\alpha \in \mathbb{Z}[n]$ and $\deg_n(\alpha) = 20$.

By the known algorithms for desingularization in [2, 1, 10, 11], we find that c_n satisfies the recurrence equation

$$\beta n c_n = \beta_1 c_{n-1} + \ldots + \beta_{10} c_{n-10},$$

where β is an 853-digit integer, $\beta_i \in \mathbb{Z}[n]$, $i = 1, \ldots, 10$.

On the other hand, Algorithm 3.4.5 finds a completely desingularized operator T for L of order 14 whose leading coefficient is $n + 14$. Translation into the recurrence equation of c_n yields

$$nc_n = \gamma_1 c_{n-1} + \cdots + \gamma_{14} c_{n-14},$$

where $\gamma_i \in \mathbb{Z}[n]$ are certain polynomials.

Let $L \in R[x][\partial]$ with positive order and T a desingularized operator for L. Then the degree of $\mathrm{lc}_\partial(T)$ in x is equal to

$$d = \deg_x(\mathrm{lc}_\partial(L)) - (\deg_x(p_1)k_1 + \cdots + \deg_x(p_m)k_m),$$

where $k_1, \ldots, k_m$ are given in Definition 3.2.1. Hence, $\mathrm{Cont}(L)$ cannot contain any operator whose leading coefficient has degree lower than d.

We provide a lower bound for the content of the leading coefficients of operators in $\mathrm{Cont}(L)$ with respect to the divisibility relation on R. To this end, we write

$$L = a_k f_k(x)\partial^k + a_{k-1} f_{k-1}(x)\partial^{k-1} + \cdots + a_0 f_0(x)$$

where $a_i \in R$ and $f_i(x) \in R[x]$ is primitive, $i = 0, 1, \ldots, k$. We say that L is *R-primitive* if

$$\gcd(a_0, a_1, \ldots, a_k) = 1.$$

As an easy consequence of [12, Lemma 9.5], Gauss's lemma in the commutative case also holds for R-primitive polynomials.

Lemma 3.4.8. *Let P and Q be two operators in $R[x][\partial]$. If P and Q are R-primitive, so is PQ.*

Proof. First, we recall a result in [39, Theorem 3.7, Corollary 3.8] or [8, Corollary 3.15]. Assume that A is a ring with endomorphism $\sigma : A \to A$ and σ-derivation $\delta : A \to A$. Let $I \subseteq A$ be a σ-δ-ideal, that is, an ideal such that $\sigma(I) \subseteq I$ and $\delta(I) \subseteq I$. Then there exists a unique ring homomorphism

$$\chi : A[\partial; \sigma, \delta] \to (A/I)[\tilde{\partial}; \tilde{\sigma}, \tilde{\delta}]$$

such that $\chi|_A : A \to A/I$ is the canonical homomorphism, and $\chi(\partial) = \tilde{\partial}$, where $\tilde{\sigma}$ and $\tilde{\delta}$ are the homomorphism and $\tilde{\sigma}$-derivation induced by σ and δ, respectively.

Let p be a prime element of R and $I = \langle p \rangle$ be the corresponding ideal in $R[x]$. Then we have that I is a σ-δ-ideal. From the above paragraph, there exists a unique homomorphism

$$\chi : R[x][\partial; \sigma, \delta] \to (R[x]/I)[\tilde{\partial}; \tilde{\sigma}, \tilde{\delta}]$$

such that $\chi|_{R[x]} : R[x] \to R[x]/I$ is the canonical homomorphism, and $\chi(\partial) = \tilde{\partial}$. Note that we have $\sigma^{-1}(I) \subset I$, because, for $pf \in I$ with $f \in R[x]$, $\sigma^{-1}(pf) = p\sigma^{-1}(f) \in I$. It follows that $\tilde{\sigma}$ is an injective endomorphism of A/I. On the other hand, $R[x]/I$ is a domain because I is a prime ideal. Thus, $(R[x]/I)[\tilde{\partial}; \tilde{\sigma}, \tilde{\delta}]$ is a domain because $R[x]/I$ is a domain and $\tilde{\sigma}$ is injective. Since P and Q are R-primitive, we have that $\chi(P)\chi(Q) \neq 0$. So, we have that $\chi(PQ) \neq 0$, because χ is a homomorphism. Since p is an arbitrary prime element of R, we conclude that PQ is R-primitive. □

There are more sophisticated variants of Gauss's lemma for Ore operators in [32, Proposition 2] and [12, Lemma 9.5].

Theorem 3.4.9. *Let $L \in R[x][\partial]$ with positive order and c be a non-unit element of R. If the operator L is R-primitive and $c \mid \mathrm{lc}_\partial(L)$, then for each $Q \in \mathrm{Cont}(L) \setminus \{0\}$, we have $c \mid \mathrm{lc}_\partial(Q)$.*

Proof. Without loss of generality, we assume that c is removable. Suppose that $c \nmid \mathrm{lc}_\partial(Q)$. By Definition 3.1.1, there exists a c-removing operator P such that

$$PL \in R[x][\partial].$$

By Lemma 3.1.5, we can write

$$P = \frac{p_0}{c^{d_0}} + \frac{p_1}{c^{d_1}}\partial + \cdots + \frac{p_k}{c^{d_k}}\partial^k$$

where $p_i \in R[x]$, $\gcd(p_i, c) = 1$ in $R[x]$, $i = 0, \ldots, k$ and $d_k \geq 1$. Let

$$d = \max_{0 \leq i \leq k} d_i \quad \text{and} \quad P_1 = c^d P.$$

Then the content w of P_1 with respect to ∂ is $\gcd(p_0, \ldots, p_k)$ because $\gcd(p_i, c) = 1$ for each $i = 0, \ldots, k$. Let $P_1 = wP_2$. Then P_2 is the primitive part of P_1. In particular, P_2 is R-primitive. Then

$$wP_2L = c^d PL.$$

Since $\gcd(w, c) = 1$ and $PL \in R[x][\partial]$, we have that c divides the content of P_2L with respect to ∂. Since c is a non-unit element of R, it follows that P_2L is not R-primitive, a contradiction to Lemma 3.4.8. □

Example 3.4.10. *In the shift Ore algebra* $\mathbb{Z}[n][\partial]$*, we consider the following* $\mathbb{Z}$*-primitive operator*

$$\begin{aligned} L &= 3(n+2)(3n+4)(3n+5)(7n+3)\left(25n^2+21n+2\right) \\ &\quad \partial^2 + (-58975n^6 - 347289n^5 - 798121n^4 - 902739n^3 \\ &\quad -519976n^2 - 141300n - 13680)\partial + 24(2n+1) \\ &\quad (4n+1)(4n+3)(7n+10)\left(25n^2+71n+48\right). \end{aligned}$$

It annihilates $\binom{4n}{n}+3^n$*. We observe that* 3 *is a constant factor of* $\mathrm{lc}_\partial(L)$*. By Theorem 3.4.9, for each* $Q \in \mathrm{Cont}(L)\setminus\{0\}$*, we have* 3 *is non-removable.*

3.5 Proof of Krattenthaler's conjecture in two special cases

In this section, we give proofs for two special cases of Conjecture 3.4.1. In the first case, $(a_n)_{n\geq 0}$ satisfies a first order linear recurrence equation, and $(b_n)_{n\geq 0}$ satisfies an arbitrary order linear recurrence equation. In the second case, $(a_n)_{n\geq 0}$ satisfies a second order linear recurrence equation, and $(b_n)_{n\geq 0}$ satisfies a third order linear recurrence equation. We prove Krattenthaler's conjecture by Theorem 3.3.2 and symbolic computation in this case.

Proposition 3.5.1. *Consider the following linear recurrence equations:*

$$\begin{aligned} na_n &= \alpha a_{n-1}, \\ nb_n &= \beta_1 b_{n-1} + \cdots + \beta_t b_{n-t}, \end{aligned}$$

where $t \in \mathbb{N}$*,* $\alpha, \beta_i \in \mathbb{Z}[n]$*,* $1 \leq i \leq t$*. Then* $c_n = n!a_nb_n$ *satisfies the following linear recurrence equation:*

$$nc_n = \gamma_1 c_{n-1} + \cdots + \gamma_t c_{n-t},$$

where $\gamma_i = \beta_i \prod_{j=0}^{i-1} \alpha(n-j)$*,* $1 \leq i \leq t$*.*

Proof. Let $i \in \{1,\ldots,t\}$. Since $na_n = \alpha(n)a_{n-1}$, we have

$$\frac{1}{a_{n-i}} = \prod_{j=0}^{i-1}\left(\frac{\alpha(n-j)}{n-j}\right)\cdot\frac{1}{a_n}.$$

Therefore,

$$b_{n-i} = \frac{c_{n-i}}{(n-i)!a_{n-i}} = \left(\prod_{j=0}^{i-1}\alpha(n-j)\right)\cdot\frac{c_{n-i}}{n!a_n}$$

Substitute the above formula into the linear recurrence equation satisfied by b_n and multiply $n!a_n$ from both sides, we get

$$nc_n = \gamma_1 c_{n-1} + \cdots + \gamma_t c_{n-t},$$

where $\gamma_i = \beta_i \prod_{j=0}^{i-1} \alpha(n-j)$, $1 \leq i \leq t$. □

Assume that R is a ring of multivariate commutative polynomials with integer coefficients. Then, it is straightforward to prove that Theorem 3.3.2 still holds for the Ore algebra $R[x][\partial]$ because the proof does not use the fact that R is a principal ideal domain. This observation leads to the following result.

Proposition 3.5.2. *Consider the following linear recurrence equations:*

$$\begin{aligned} na_n &= \alpha_1 a_{n-1} + \alpha_2 a_{n-2}, \\ nb_n &= \beta_1 b_{n-1} + \beta_2 b_{n-2} + \beta_3 b_{n-3}, \end{aligned}$$

where α_i, β_j are indeterminates. $1 \leq i \leq 2, 1 \leq j \leq 3$. Then $c_n = n! a_n b_n$ satisfies the following linear recurrence equation:

$$nc_n = \gamma_1 c_{n-1} + \cdots + \gamma_9 c_{n-9},$$

where $\gamma_i \in \mathbb{Z}[\alpha_1, \alpha_2, \alpha_3, \beta_1, \beta_2][n]$, $1 \leq i \leq 9$.

Proof. Let $R = \mathbb{Z}[\alpha_1, \alpha_2, \alpha_3, \beta_1, \beta_2]$. Using the package `HolonomicFunctions` [31], we find that c_n has an annihilator $L \in R[x][\partial]$ of order 6, where $\mathrm{lc}_\partial(L) = (n+6)\alpha$ for some $\alpha \in R[n]$. Using `Macaulay2` [19], we find that there is an operator T in M_9 with $\mathrm{lc}_\partial(T) = n + 9$. Translation into the linear recurrence equation of c_n yields

$$nc_n = \gamma_1 c_{n-1} + \cdots + \gamma_9 c_{n-9},$$

where $\gamma_i \in R[n]$, $1 \leq i \leq 9$. □

Chapter 4

Apparent Singularities of D-finite Systems

The material in this chapter is joint work with Ziming Li and Manuel Kauers. For details, see [26]. The main purpose is to generalize the two facts about apparent singularities sketched in Chapter 1 to the multivariate case.

4.1 Basic concepts

4.1.1 Rings of differential operators

Throughout the thesis, we assume that $\mathbb{K}$ is a field of characteristic zero and n is a nonnegative integer. For instance, $\mathbb{K}$ can be the field of complex numbers. Let $\mathbb{K}[\mathbf{x}] = \mathbb{K}[x_1, \ldots, x_n]$ be the ring of usual commutative polynomials over $\mathbb{K}$, where $x_1, \ldots, x_n$ are indeterminates. The quotient field of $\mathbb{K}[\mathbf{x}]$ is denoted as $\mathbb{K}(\mathbf{x}) = \mathbb{K}(x_1, \ldots, x_n)$. Then we have the *ring of differential operators with rational function coefficients* $\mathbb{K}(x_1, \ldots, x_n)[\partial_1, \ldots, \partial_n]$, in which the addition is coefficientwise and the multiplication is defined by associativity via the commutation rules

(i) $\partial_i \partial_j = \partial_j \partial_i$;

(ii) $\partial_i f = f \partial_i + \frac{\partial f}{\partial x_i}$ for each $f \in \mathbb{K}(\mathbf{x})$,

where $\frac{\partial f}{\partial x_i}$ is the usual derivative of f with respect to x_i, $i = 1, \ldots, n$. This ring is an Ore algebra [43, 14] and we write it as $\mathbb{K}(\mathbf{x})[\boldsymbol{\partial}]$.

Another ring is $\mathbb{K}[\mathbf{x}][\boldsymbol{\partial}] := \mathbb{K}[x_1, \ldots, x_n][\partial_1, \ldots, \partial_n]$, which is a subring of $\mathbb{K}(\mathbf{x})[\boldsymbol{\partial}]$. We call it the *ring of differential operators with polynomial coefficients* or the *Weyl algebra* [44, Section 1.1].

A left ideal I in $\mathbb{K}(\mathbf{x})[\boldsymbol{\partial}]$ is called *D-finite* if the quotient $\mathbb{K}(\mathbf{x})[\boldsymbol{\partial}]/I$ is a $\mathbb{K}(\mathbf{x})$-vector space of finite dimension. We call the dimension of $\mathbb{K}(\mathbf{x})[\boldsymbol{\partial}]/I$ as a $\mathbb{K}(\mathbf{x})$-vector space the *rank* of I and denote it by $\operatorname{rank}(I)$.

For a subset S of $\mathbb{K}(\mathbf{x})[\boldsymbol{\partial}]$, the left ideal generated by S is denoted by $\mathbb{K}(\mathbf{x})[\boldsymbol{\partial}]S$.

For instance, let $I = \mathbb{Q}(x_1, x_2)[\partial_1, \partial_2]\ \{\partial_1 - 1, \partial_2 - 1\}$. Then I is D-finite because the quotient $\mathbb{Q}(x_1, x_2)[\partial_1, \partial_2]/I$ is a $\mathbb{Q}(x_1, x_2)$-vector space of dimension 1. Thus, $\operatorname{rank}(I) = 1$.

4.1.2 Gröbner bases

Since $\mathbb{K}(\mathbf{x})[\boldsymbol{\partial}]$ is not included in the Ore algebras as described in Section 2.1, we briefly recall some notations about Gröbner bases in this ring. Gröbner bases in $\mathbb{K}[\mathbf{x}][\boldsymbol{\partial}]$ and $\mathbb{K}(\mathbf{x})[\boldsymbol{\partial}]$ are well known [28, 44] and implementations for them are available for example in the Maple package `Mgfun` [13] and in the Mathematica package `HolonomicFunctions.m` [31]. Throughout the chapter, we assume that Gröbner bases are reduced.

Let $\prec$ [1] be a graded order [16, Definition 1, page 55] on $\mathbb{N}^n$. Since there is a one-to-one correspondence between terms in $\mathrm{T}(\boldsymbol{\partial})$ and elements in $\mathbb{N}^n$, the ordering $\prec$ will give us an ordering on $\mathrm{T}(\boldsymbol{\partial})$: if $\mathbf{u} \prec \mathbf{v}$ according to this ordering, we will also say that $\boldsymbol{\partial}^{\mathbf{u}} \prec \boldsymbol{\partial}^{\mathbf{v}}$.

For a Gröbner basis G in $\mathbb{K}(\mathbf{x})[\boldsymbol{\partial}]$, we denote by $\mathrm{HT}(G)$ the set of head terms of G, by $\mathrm{HC}(G)$ the set of head coefficients of G, and by $\mathrm{PT}(G)$ the set of parametric terms of G. Recall that a head term of G is the highest term in an element of G, a head coefficient of G is the coefficient with respect to a head term of G, and a parametric term of G is a term not divisible by any element of $\mathrm{HT}(G)$. Note that parametric terms of G form a basis of the quotient $\mathbb{K}(\mathbf{x})[\boldsymbol{\partial}]/(\mathbb{K}(\mathbf{x})[\boldsymbol{\partial}]G)$ as a $\mathbb{K}(\mathbf{x})$-vector space.

If $\mathbb{K}(\mathbf{x})[\boldsymbol{\partial}]G$ is D-finite, then $|\mathrm{PT}(G)|$ is also called the rank of G, and we denote it by $\operatorname{rank}(G)$. Note that the rank of G is equal to that of $\mathbb{K}(\mathbf{x})[\boldsymbol{\partial}]G$.

4.2 Singularities and ordinary points

4.2.1 Ordinary points

Assume that $G = \{G_1, \ldots, G_k\}$ is a finite set in $\mathbb{K}[\mathbf{x}][\boldsymbol{\partial}]$ such that G is a Gröbner basis with respect to $\prec$. Motivated by the material after [44, Lemma 1.4.21], we give definitions of singularities and ordinary points of G.

Definition 4.2.1. *Set $f \in \mathbb{K}[\mathbf{x}]$ to be $\operatorname{lcm}(\mathrm{HC}(G_1), \ldots, \mathrm{HC}(G_k))$.*

(i) A zero of f in $\overline{\mathbb{K}}^n$ is called a singularity *of G.*

(ii) A point in $\overline{\mathbb{K}}^n$ that is not a singularity of G is called an ordinary point *of G.*

The above definitions are compatible with those in the univariate case [1, 11]. Note that the origin is an ordinary point of G if and only if each constant term of $\mathrm{HC}(G)$ is nonzero.

Example 4.2.2. *Consider the Gröbner basis [35, Example 3] in $\mathbb{Q}(x_1, x_2)[\partial_1, \partial_2]$*

$$G = \{x_1\partial_1^2 - (x_1x_2 - 1)\partial_1 - x_2, x_2\partial_2 - x_1\partial_1\}.$$

[1] In examples, we use the graded inversed [16, page 60] lexicographic order.

In this case, $\mathrm{HT}(G) = \{\partial_1^2, \partial_2\}$, $\mathrm{HC}(G) = \{x_1, x_2\}$ *and* $\mathrm{PT}(G) = \{1, \partial_1\}$. *Moreover,*

$$\mathrm{lcm}(x_1, x_2) = x_1 x_2.$$

Thus, the singularities of G *are*

$$\{(a, b) \in \overline{\mathbb{Q}}^2 \mid a = 0 \text{ or } b = 0\},$$

which are two lines in $\overline{\mathbb{Q}}^2$. *Note that the origin is not an ordinary point of* G.

Example 4.2.3. *Consider the Gröbner basis in* $\mathbb{Q}(x_1, x_2)[\partial_1, \partial_2]$

$$G = \{\partial_2 - \partial_1, \partial_1^2 + 1\}.$$

We find that $\mathrm{HT}(G) = \{\partial_1^2, \partial_2\}$, $\mathrm{HC}(G) = \{1\}$ *and* $\mathrm{PT}(G) = \{1, \partial_1\}$. *Furthermore,*

$$\mathrm{lcm}(1, 1) = 1.$$

So, G *has no singularity. Note that the origin is an ordinary point of* G.

4.2.2 Indicial polynomials

We will characterize ordinary and apparent singularities in terms of formal power series solutions of G. Indicial polynomials are useful to describe solutions of this type.

Let $\delta_i = x_i \partial_i$ be the Euler operator with respect to x_i, $i = 1, \ldots, n$. By a *term,* we now mean a product

$$x_1^{u_1} \cdots x_n^{u_n}, \quad \partial_1^{v_1} \cdots \partial_n^{v_n} \text{ or } \delta_1^{w_1} \cdots \delta_n^{w_n},$$

where $u_i, v_i, w_i \in \mathbb{N}$, $i = 1, \ldots, n$. For brevity, we set $\mathbf{u} = (u_1, \ldots, u_n)$. Then we may denote terms as $\mathbf{x}^{\mathbf{u}}$, $\boldsymbol{\partial}^{\mathbf{v}}$ and $\boldsymbol{\delta}^{\mathbf{w}}$.

Recall the following properties concerning Euler operators. Let $\mathrm{T}(\mathbf{x})$ be the commutative monoid generated by $x_1, \ldots, x_n$. We denote the m-th falling factorial [24, Section 3.1] of x_i by

$$(x_i)^{\underline{m}} = x_i(x_i - 1) \cdots (x_i - m + 1),$$

where $m \in \mathbb{N}$, $i = 1, \ldots, n$. As a matter of convention, we set $(x_i)^{\underline{0}} = 1$. Let $\mathbb{K}[[\mathbf{x}]]$ be the ring of formal power series with respect to variables $x_1, \ldots, x_n$. For $P \in \mathbb{K}[\mathbf{x}][\boldsymbol{\partial}]$ and $f \in \mathbb{K}[[\mathbf{x}]]$, there is a natural action of P on f, which is denoted by $P(f)$. For $P, Q \in \mathbb{K}[\mathbf{x}][\boldsymbol{\partial}]$, it is straightforward to verify that

$$PQ(f) = P(Q(f)). \tag{4.1}$$

Proposition 4.2.4. *The following assertions hold for Euler operators:*

(i) For each $m \in \mathbb{N}$ *and* $i \in \{1, \ldots, n\}$, $x_i^m \partial_i^m = (\delta_i)^{\underline{m}}$.

(ii) For each $p \in \mathbb{K}[\mathbf{x}]$ *and* $\mathbf{x}^{\mathbf{u}} \in \mathrm{T}(\mathbf{x})$, *we have* $p(\boldsymbol{\delta})(\mathbf{x}^{\mathbf{u}}) = p(\mathbf{u})\mathbf{x}^{\mathbf{u}}$.

Proof. (i) We do induction on m. For $m = 1$, it follows from the definition of Euler operators. Assume that the statement hold for m. Then

$$\begin{array}{rcl} x_i^{m+1}\partial_i^{m+1} & = & x_i^m(x_i\partial_i^m)\partial_i \\ & = & x_i^m(\partial_i^m x_i - m\partial_i^{m-1})\partial_i \\ & = & (x_i^m\partial_i^m)(x_i\partial_i) - m(x_i^m\partial_i^m) \\ & = & (\delta_i)\underline{m}(\delta_i - m) \\ & = & (\delta_i)\underline{m+1} \end{array}$$

(ii) Since a polynomial in $\mathbb{K}[\mathbf{x}]$ is a $\mathbb{K}$-linear combination of terms, it suffices to prove this statement for terms. Furthermore, we know that δ_i is commutative with x_j if $i \neq j$. Therefore, we just need to prove this statement for terms of δ_i and x_i, where $i \in \{1, \dots, n\}$. Let δ_i^s and x_i^t be two arbitrary terms of δ_i and x_i, where s and t are nonnegative integers. We do induction on s. For the case $s = 1$, $\delta_i(x_i^t) = tx_i^t$. Assume that the statement holds for $s - 1$. Then

$$\begin{array}{rcl} \delta_i^s(x_i^t) & = & \delta_i^{s-1}(\delta_i(x_i^t)) \\ & = & \delta_i^{s-1}(tx_i^t) \\ & = & t\delta_i^{s-1}(x_i^t) \\ & = & t\, t^{s-1}x_i^t \\ & = & t^s x_i^t \end{array}$$

□

Let $P \in \mathbb{K}[\mathbf{x}][\boldsymbol{\partial}]$ with $P = \sum_{|\mathbf{u}|\leq m} c_{\mathbf{u}}\boldsymbol{\partial}^{\mathbf{u}}$, where $c_{\mathbf{u}}$ belongs to $\mathbb{K}[\mathbf{x}]$, $m \in \mathbb{N}$ is minimal, that is, there exists a $\mathbf{v} \in \mathbb{N}^n$ such that $|\mathbf{v}| = m$ and $c_{\mathbf{v}}$ is nonzero. We call m the *order* [3, Section 2] of P.

Set $\mathbf{m} = (m, \dots, m) \in \mathbb{N}^n$. By item (i) of the above proposition, we have

$$\begin{array}{rcl} \mathbf{x}^{\mathbf{m}}P & = & \sum_{|\mathbf{u}|\leq m} c_{\mathbf{u}}\mathbf{x}^{\mathbf{m}}\boldsymbol{\partial}^{\mathbf{u}} \\ & = & \sum_{|\mathbf{u}|\leq m} c_{\mathbf{u}}\,(x_1^m\partial_1^{u_1}\cdots x_n^m\partial_n^{u_n}) \\ & = & \sum_{|\mathbf{u}|\leq m} c_{\mathbf{u}}\left(x_1^{m-u_1}(\delta_1)\underline{u_1}\cdots x_n^{m-u_n}(\delta_n)\underline{u_n}\right) \\ & = & \sum_{\mathbf{v}\in T}\mathbf{x}^{\mathbf{v}}\left(\sum_{|\mathbf{u}|\leq m} c_{\mathbf{u},\mathbf{v}}\boldsymbol{\delta}^{\mathbf{u}}\right) \end{array}$$

where T is a finite set in $\mathbb{N}^n$, and $c_{\mathbf{u},\mathbf{v}} \in \mathbb{K}$.

Let $\prec$ be the order on $\mathbb{N}^n$ as specified in Section 4.1.2. Since there is a one-to-one correspondence between terms in $\mathrm{T}(\mathbf{x})$ and elements in $\mathbb{N}^n$, the ordering $\prec$ will give us an ordering on $\mathrm{T}(\mathbf{x})$: if $\mathbf{u} \prec \mathbf{v}$ according to this ordering, we will also say that $\mathbf{x}^{\mathbf{u}} \prec \mathbf{x}^{\mathbf{v}}$.

Set $\mathbb{K}[\mathbf{y}] = \mathbb{K}[y_1, \dots, y_n]$ to be the ring of usual commutative polynomials with indeterminates $y_1, \dots, y_n$.

Definition 4.2.5. *Assume that P is an operator in $\mathbb{K}[\mathbf{x}][\boldsymbol{\partial}]$ of order m with*

$$\mathbf{x}^{\mathbf{m}}P = \sum_{\mathbf{v}\in T}\mathbf{x}^{\mathbf{v}}\left(\sum_{|\mathbf{u}|\leq m} c_{\mathbf{u},\mathbf{v}}\boldsymbol{\delta}^{\mathbf{u}}\right),$$

where $\mathbf{m} = (m, \ldots, m) \in \mathbb{N}^n$*. Let* $\mathbf{x}^{\mathbf{v}_0}$ *be the minimal term among* $\{x^{\mathbf{v}} \mid \mathbf{v} \in T\}$ *with respect to* $\prec_2$*. We call*

$$\sum_{|\mathbf{u}| \leq m} c_{\mathbf{u},\mathbf{v}_0} \mathbf{y}^{\mathbf{u}} \in \mathbb{K}[\mathbf{y}]$$

the indicial polynomial *of* P*, and denote it as* $\operatorname{ind}(P)$*. We further define* $\operatorname{ind}(0) := 0$*.*

The above definition is compatible with the univariate case [23, 44], and was already used in the multivariate setting by [3, Definition 11].

Assume that $f \in \mathbb{K}[[\mathbf{x}]]$ with

$$f = c_{\mathbf{w}} \mathbf{x}^{\mathbf{w}} + \text{ higher monomials with respect to } \prec .$$

We call $\mathbf{w}$ and $\mathbf{x}^{\mathbf{w}}$ the *initial exponent* and the *initial term* of f, respectively. The initial term of f is denoted as $\operatorname{in}(f)$.

Proposition 4.2.6. *Assume that* $G \subset \mathbb{K}[\mathbf{x}][\boldsymbol{\partial}]$ *is a finite set and* f *is a formal power series solution of* G *with initial exponent* $\mathbf{w}$*. Then* $\mathbf{w}$ *is a root of* $\operatorname{ind}(P)$ *for each* $P \in G$*.*

Proof. Assume that $P \in G$ is an operator of order m with

$$\mathbf{x}^{\mathbf{m}} P = \sum_{\mathbf{v} \in T} \mathbf{x}^{\mathbf{v}} \left(\sum_{|\mathbf{u}| \leq m} c_{\mathbf{u},\mathbf{v}} \boldsymbol{\delta}^{\mathbf{u}} \right),$$

where $\mathbf{m} = (m, \ldots, m) \in \mathbb{N}^n$, $\mathbf{x}^{\mathbf{v}_0}$ is the minimal term among $\{\mathbf{x}^{\mathbf{v}} \mid \mathbf{v} \in T\}$. By item (ii) of Proposition 4.2.4, we have

$$\begin{aligned}
(\mathbf{x}^{\mathbf{m}} P)(f) &= \left[\textstyle\sum_{\mathbf{v} \in T} \mathbf{x}^{\mathbf{v}} \left(\sum_{|\mathbf{u}| \leq m} c_{\mathbf{u},\mathbf{v}} \boldsymbol{\delta}^{\mathbf{u}} \right) \right] (\mathbf{x}^{\mathbf{w}} + \text{ higher monomials}) \\
&= \mathbf{x}^{\mathbf{v}_0} \left(\textstyle\sum_{|\mathbf{u}| \leq m} c_{\mathbf{u},\mathbf{v}_0} \boldsymbol{\delta}^{\mathbf{u}} \right) (\mathbf{x}^{\mathbf{w}}) + \text{ higher monomials} \\
&= \left(\textstyle\sum_{|\mathbf{u}| \leq m} c_{\mathbf{u},\mathbf{v}_0} \mathbf{w}^{\mathbf{u}} \right) \mathbf{x}^{\mathbf{v}_0 + \mathbf{w}} + \text{ higher monomials} \\
&= 0
\end{aligned}$$

Thus,

$$\sum_{|\mathbf{u}| \leq m} c_{\mathbf{u},\mathbf{v}_0} \mathbf{w}^{\mathbf{u}} = 0.$$

i.e., $\operatorname{ind}(P)(\mathbf{w}) = 0$. □

Example 4.2.7. *Consider the Gröbner basis* $G = \{G_1, G_2\}$ *in* $\mathbb{Q}(x_1, x_2)[\partial_1, \partial_2]$*, where*

$$G_1 = x_1 x_2 \partial_2 - x_1 x_2 \partial_1 + (-x_1 + x_2), G_2 = x_1^2 \partial_1^2 - 2x_1 \partial_1 + (2 + x_1^2).$$

By computation, we find that $\operatorname{ind}(G_1) = y_2 - 1$*,* $\operatorname{ind}(G_2) = (y_1 - 1)(y_1 - 2)$*. It is straightforward to verify that* G *has two formal power series solutions*

$$\{f_1 = x_1 x_2 \sin(x_1 + x_2), f_2 = x_1 x_2 \cos(x_1 + x_2)\},$$

with $\operatorname{in}(f_1) = x_1^2 x_2$ *and* $\operatorname{in}(f_2) = x_1 x_2$*. The corresponding initial exponents*

$$\{(2, 1), (1, 1)\}$$

are the roots of $\operatorname{ind}(G_1)$ *and* $\operatorname{ind}(G_2)$*.*

4.2.3 Indicial ideals

Definition 4.2.8. *Let $G \subset \mathbb{K}[\mathbf{x}][\boldsymbol{\partial}]$ be a finite set. We call*

$$\{\mathrm{ind}(P) \mid P \in \mathbb{K}(\mathbf{x})[\boldsymbol{\partial}]G \cap \mathbb{K}[\mathbf{x}][\boldsymbol{\partial}]\}$$

the indicial ideal *of G, and denote it as* $\mathrm{ind}(G)$*.*

Proposition 4.2.9. *The indicial ideal of G is an ideal in $\mathbb{K}[\mathbf{y}]$.*

Proof. Assume that $a, b \in \mathrm{ind}(G) \setminus \{0\}$ with $a = \mathrm{ind}(P)$ and $b = \mathrm{ind}(Q)$, where P and Q belong to $\mathbb{K}(\mathbf{x})[\boldsymbol{\partial}]G \cap \mathbb{K}[\mathbf{x}][\boldsymbol{\partial}]$. If $a + b = 0$, then we are done. Otherwise, let u and v be the order of P and Q, respectively. Set $\mathbf{u} = (u, \ldots, u), \mathbf{v} = (v, \ldots, v)$ to be two vectors in $\mathbb{N}^n$. Then

$$\begin{aligned} \mathbf{x}^{\mathbf{u}} P &= \mathbf{x}^{\mathbf{s}} \left(\textstyle\sum_{|\mathbf{u}| \le u} c_{\mathbf{u},\mathbf{s}} \boldsymbol{\delta}^{\mathbf{u}} \right) + \text{ higher terms,} \\ \mathbf{x}^{\mathbf{v}} Q &= \mathbf{x}^{\mathbf{t}} \left(\textstyle\sum_{|\mathbf{u}| \le v} c_{\mathbf{u},\mathbf{t}} \boldsymbol{\delta}^{\mathbf{u}} \right) + \text{ higher terms.} \end{aligned}$$

Let $L = \mathbf{x}^{\mathbf{t}}(\mathbf{x}^{\mathbf{u}} P) + \mathbf{x}^{\mathbf{s}}(\mathbf{x}^{\mathbf{v}} Q) \in \mathbb{K}(\mathbf{x})[\boldsymbol{\partial}]G \cap \mathbb{K}[\mathbf{x}][\boldsymbol{\partial}]$. Then

$$L = \mathbf{x}^{\mathbf{s}+\mathbf{t}} \left(\sum_{|\mathbf{u}| \le u} c_{\mathbf{u},\mathbf{s}} \boldsymbol{\delta}^{\mathbf{u}} + \sum_{|\mathbf{u}| \le v} c_{\mathbf{u},\mathbf{t}} \boldsymbol{\delta}^{\mathbf{u}} \right) + \text{ higher terms.}$$

Let m be the order of L and $\mathbf{m} = (m, \ldots, m)$. Then

$$\mathbf{x}^{\mathbf{m}} L = \mathbf{x}^{\mathbf{s}+\mathbf{t}+\mathbf{m}} \left(\sum_{|\mathbf{u}| \le u} c_{\mathbf{u},\mathbf{s}} \boldsymbol{\delta}^{\mathbf{u}} + \sum_{|\mathbf{u}| \le v} c_{\mathbf{u},\mathbf{t}} \boldsymbol{\delta}^{\mathbf{u}} \right) + \text{ higher terms.}$$

Thus, $a + b = \mathrm{ind}(L)$.

Assume that $r \in \mathbb{K}[\mathbf{y}] \setminus \{0\}$ and $a \in \mathrm{ind}(G) \setminus \{0\}$ with $a = \mathrm{ind}(P)$. We prove that

$$ra \in \mathrm{ind}(G).$$

Since r is a sum of monomials on $y_1, \ldots, y_n$, it suffices to prove that $ra \in \mathrm{ind}(G)$ for each monomial r by the above argument. Assume that $r = c\mathbf{y}^{\mathbf{w}}$, where $c \in \mathbb{K}$ and $\mathbf{w}$ is equal to $(w_1, \ldots, w_n) \in \mathbb{N}^n$. Let u be the order of P and $\mathbf{u} = (u, \ldots, u) \in \mathbb{N}^n$. Then

$$\mathbf{x}^{\mathbf{u}} P = \mathbf{x}^{\mathbf{s}} \left(\sum_{|\mathbf{u}| \le u} c_{\mathbf{u},\mathbf{s}} \boldsymbol{\delta}^{\mathbf{u}} \right) + \text{ higher terms,}$$

where $\mathbf{s} = (s_1, \ldots, s_n) \in \mathbb{N}^n$. Let $H = c\left(\prod_{i=1}^n (\delta_i - s_i)^{w_i}\right) \mathbf{x}^{\mathbf{u}} P$. Then

$$\begin{aligned} H &= c\left(\textstyle\prod_{i=1}^n (\delta_i - s_i)^{w_i}\right) \mathbf{x}^{\mathbf{s}} \left(\textstyle\sum_{|\mathbf{u}| \le u} c_{\mathbf{u},\mathbf{s}} \boldsymbol{\delta}^{\mathbf{u}} \right) + \text{ higher terms} \\ &= c\left(\textstyle\prod_{i=1}^n (\delta_i - s_i)^{w_i} x_i^{s_i}\right) \left(\textstyle\sum_{|\mathbf{u}| \le u} c_{\mathbf{u},\mathbf{s}} \boldsymbol{\delta}^{\mathbf{u}} \right) + \text{ higher terms} \\ &= c\left(\textstyle\prod_{i=1}^n x_i^{s_i} \delta_i^{w_i}\right) \left(\textstyle\sum_{|\mathbf{u}| \le u} c_{\mathbf{u},\mathbf{s}} \boldsymbol{\delta}^{\mathbf{u}} \right) + \text{ higher terms} \\ &= \mathbf{x}^{\mathbf{s}} \left(c\boldsymbol{\delta}^{\mathbf{w}} \textstyle\sum_{|\mathbf{u}| \le u} c_{\mathbf{u},\mathbf{s}} \boldsymbol{\delta}^{\mathbf{u}} \right) + \text{ higher terms.} \end{aligned}$$

Let $\tilde{m}$ be the order of H and $\tilde{\mathbf{m}} = (\tilde{m}, \ldots, \tilde{m})$. Then

$$\mathbf{x}^{\tilde{\mathbf{m}}} H = \mathbf{x}^{\mathbf{s}+\tilde{\mathbf{m}}} \left(c\boldsymbol{\delta}^{\mathbf{w}} \sum_{|\mathbf{u}| \leq u} c_{\mathbf{u},\mathbf{s}} \boldsymbol{\delta}^{\mathbf{u}} \right) + \text{ higher terms.}$$

Thus, $ra = \operatorname{ind}(H)$. $\square$

Proposition 4.2.10. *Let $G \in \mathbb{K}[\mathbf{x}][\boldsymbol{\partial}]$ be a finite set such that $\mathbb{K}(\mathbf{x})[\boldsymbol{\partial}]G$ is D-finite. Then $\operatorname{ind}(G)$ is zero-dimensional ideal in $\mathbb{K}[\mathbf{y}]$.*

Proof. Since $\mathbb{K}(\mathbf{x})[\boldsymbol{\partial}]G$ is D-finite, there exists an operator $P \in \mathbb{K}[\mathbf{x}][\boldsymbol{\partial}]$ of order m such that $P \in \mathbb{K}(\mathbf{x})[\boldsymbol{\partial}]G \cap \mathbb{K}[\mathbf{x}][\partial_1]$ (see, e.g., [30, Proposition 2.10] for a proof). By item (i) of Proposition 4.2.4, we have

$$\begin{aligned} x_1^m P &= x_1^m \left(c_0 + c_1\partial_1 + \cdots + c_m \partial_1^m\right) \\ &= c_0 x_1^m + c_1 x_1^{m-1}\delta_1 + \cdots + c_m (\delta_1)^{\underline{m}} \\ &= \textstyle\sum_{\mathbf{v}\in T} \mathbf{x}^{\mathbf{v}} \left(\sum_{a \leq m} c_{\mathbf{u},\mathbf{v}} \delta_1^a \right) \end{aligned}$$

Thus, $\operatorname{ind}(P) \in \mathbb{K}[y_1] \setminus \{0\}$. Similarly, for each $i = 2, \ldots, n$, there exists a univariate polynomial $a_i \in \mathbb{K}[y_i] \setminus \{0\}$, which belong to $\operatorname{ind}(G)$. By [16, Theorem 6, page 251], $\operatorname{ind}(G)$ is zero-dimensional. $\square$

By the above proof, we can construct a sub-ideal J of $\operatorname{ind}(G)$ such that J is zero-dimensional. However, the proposition does not necessarily give access to a basis of $\operatorname{ind}(G)$.

Definition 4.2.11. *Let $G \in \mathbb{K}[\mathbf{x}][\boldsymbol{\partial}]$ be a finite set such that $\mathbb{K}(\mathbf{x})[\boldsymbol{\partial}]G$ is D-finite. Assume that $\langle f_1, \ldots, f_\ell \rangle \subset \operatorname{ind}(G)$ is a zero-dimensional ideal in $\mathbb{K}[\mathbf{y}]$. We call the set*

$$\{\mathbf{w} \in \mathbb{N}^n \mid f_i(\mathbf{w}) = 0, 1 \leq i \leq \ell\}$$

a set of initial exponent candidates *of G.*

By Proposition 4.2.6, the set of initial exponents of formal power series solutions of G must be contained in a set of initial exponent candidates of G. Sometimes, the converse is also true.

Example 4.2.12. *Consider the Gröbner basis $G = \{G_1, G_2\}$ from Example 4.2.7, where*

$$G_1 = x_1x_2\partial_2 - x_1x_2\partial_1 + (-x_1 + x_2), G_2 = x_1^2\partial_1^2 - 2x_1\partial_1 + (2 + x_1^2).$$

By computation, we find that $\operatorname{ind}(G_1) = y_2 - 1$, $\operatorname{ind}(G_2) = (y_1 - 1)(y_1 - 2)$. By the above definition, the set

$$\{(2,1), (1,1)\}$$

is a set of initial exponent candidates of G. Actually, $(2,1)$ and $(1,1)$ are initial exponents of the following formal power series solutions

$$x_1x_2 \sin(x_1 + x_2) \text{ and } x_1x_2 \cos(x_1 + x_2),$$

respectively.

The following example shows that initial candidates of G do not necessarily give rise to formal power series solutions of G.

Example 4.2.13. *Consider the Gröbner basis in* $\mathbb{Q}(x_1, x_2)[\partial_1, \partial_2]$*:*

$$\begin{aligned} G &= \{G_1, G_2\} \\ &= \{x_1x_2\partial_2 + (-x_1^2 + 2x_1x_2)\partial_1 - 2x_2, (x_1^3 - x_1^2x_2)\partial_1^2 + 2x_1x_2\partial_1 - 2x_2\} \end{aligned}$$

By computation, we find that $\mathrm{ind}(G_1) = y_2 - y_1$ *and* $\mathrm{ind}(G_2) = (y_1 - 1)y_1$*. Thus, a set of initial exponent candidates of* G *is*

$$S = \{(0, 0), (1, 1)\}$$

Actually, $\mathrm{sol}(G)$ *is spanned by* $\{\frac{x_1}{x_1 - x_2}, x_1x_2\}$*. In this case,* $(1, 1)$ *is the initial exponent of* x_1x_2*. However,* $(0, 0)$ *does not give rise to a formal power series solution of* G*.*

4.3 Characterization of ordinary points

Let $G \subset \mathbb{K}[\mathbf{x}][\boldsymbol{\partial}]$ be a finite set such that G is a Gröbner basis with respect to $\prec$. Let $\mathrm{PE}(G)$ be the set of exponents of elements of $\mathrm{PT}(G)$. In this section, we characterize an ordinary point of G in terms of formal power series solutions at this point. Assume that $P \in \mathbb{K}[\mathbf{x}][\boldsymbol{\partial}]$ with

$$P = c_{\mathbf{u}_m}\boldsymbol{\partial}^{\mathbf{u}_m} + c_{\mathbf{u}_{m-1}}\boldsymbol{\partial}^{\mathbf{u}_{m-1}} + \cdots + c_{\mathbf{u}_0}\boldsymbol{\partial}^{\mathbf{u}_0},$$

where $c_{\mathbf{u}_i} \in \mathbb{K}[\mathbf{x}]$, $i = 0, \ldots, m$. We say that P is *primitive* if

$$\gcd(c_{\mathbf{u}_0}, c_{\mathbf{u}_1}, \ldots, c_{\mathbf{u}_m}) = 1.$$

The main result of this section is as follows:

Theorem 4.3.1. *Assume that every element in* G *is primitive and the left ideal* $\mathbb{K}(\mathbf{x})[\boldsymbol{\partial}]G$ *is D-finite. Then the origin is an ordinary point of* G *if and only if* G *has* $\mathrm{rank}(G)$ *many* $\mathbb{K}$*-linearly independent formal power series solutions whose initial exponents are exactly those in* $\mathrm{PE}(G)$*.*

The above theorem is compatible with the univariate case [1, Proposition 6].

In order to prove it, we need to recall some basic facts concerning multivariate formal power series and Wronskians in the partial differential case.

Set

$$f = \sum_{\mathbf{u} \in \mathbb{N}^n} \frac{c_{\mathbf{u}}}{\mathbf{u}!}\mathbf{x}^{\mathbf{u}},$$

where $c_{\mathbf{u}} \in \mathbb{K}$ and $\mathbf{u}! = (u_1!) \cdots (u_n!)$. There is a ring homomorphism ϕ from $\mathbb{K}[[\mathbf{x}]]$ to $\mathbb{K}$ that maps f to $c_{\mathbf{0}}$. In other words, taking the constant term of a formal power series gives rise to a ring homomorphism. An easy calculation shows that

$$\boldsymbol{\partial}^{\mathbf{u}}(f) = c_{\mathbf{u}} + g,$$

where $g \in \mathbb{K}[[\mathbf{x}]]$ with $\phi(g) = 0$. It follows that

$$\phi\left(\boldsymbol{\partial}^{\mathbf{u}}(f)\right) = c_{\mathbf{u}}. \tag{4.2}$$

Thus, we can determine whether a formal power series is zero by differentiating and taking constant terms, as stated in the next lemma.

Lemma 4.3.2. *Let $f \in \mathbb{K}[[\mathbf{x}]]$. Then $f = 0$ if and only if, for all $\mathbf{u} \in \mathbb{N}^n$,*

$$\phi\left(\boldsymbol{\partial}^{\mathbf{u}}(f)\right) = 0.$$

Proof. It is straightforward. □

The following fact appears in [18] for $s = 1$, but the proof applies literally also for arbitrary values of s.

Lemma 4.3.3. *Let $p_1, p_2, \ldots, p_s$ and q be polynomials in $\mathbb{K}[\mathbf{x}]$ with*

$$\gcd(p_1, p_2, \ldots, p_s, q) = 1 \text{ in } \mathbb{K}[\mathbf{x}].$$

If p_i/q has a power series expansion for each $i \in \{1, 2, \ldots, s\}$, then the constant term of q is nonzero.

Proof. We proceed by induction on n. For $n = 1$, the lemma follows from the fact that any polynomial in x_1 can be expressed as $x_1^m h(x_1)$, where $m \in \mathbb{N}$ and $h(x_1)$ is a polynomial with $h(0) \neq 0$.

Now let us assume that the theorem is true for rational power series in fewer than n variables. For the moment, let us regard $p_1, \ldots, p_s$ and q as polynomials in $x_2, \ldots, x_n$ with coefficients in the field $\mathbb{K}(x_1)$. Since $p_1, \ldots, p_s$ and q still have no common factor, the induction hypothesis shows that the constant term of q is nonzero. Returning to $\mathbb{K}[x_1, x_2, \ldots, x_n]$, we find that q contains a power of x_1 with nonzero coefficient.

Since $p_1, \ldots, p_s$ and q have no common factor in $\mathbb{K}[\mathbf{x}]$, they still have no common factor in $\mathbb{K}(x_2, \ldots, x_n)[x_1]$. Therefore, there exists $a_1, \ldots, a_s$ and b in $\mathbb{K}(x_2, \ldots, x_n)[x_1]$ such that

$$a_1 p_1 + \ldots + a_s p_s + bq = 1 \tag{4.3}$$

Let d be the least common multiple of denominators of $a_1, \ldots, a_s$ and b. Then d is a nonzero polynomial in $\mathbb{K}[x_2, \ldots, x_n]$. Set $\tilde{a_i} = d a_i$ and $\tilde{b} = db$, $i = 1, \ldots, s$. By (4.3), we have

$$\tilde{a_1} p_1 + \cdots + \tilde{a_s} p_s + \tilde{b} q = d.$$

In other words, there exist polynomials $\tilde{a_1}, \ldots, \tilde{a_s}$ and $\tilde{b}$ in $\mathbb{K}[x_1, \ldots, x_n]$ such that the polynomial $\tilde{a_1} p_1 + \cdots + \tilde{a_s} p_s + \tilde{b} q$ is nonzero and free of x_1. Let

$$r = \tilde{a_1}(p_1/q) + \cdots + \tilde{a_s}(p_s/q) + \tilde{b}.$$

Then r is in $\mathbb{K}[[x_1, \ldots, x_n]]$ and qr is in $\mathbb{K}[x_2, \ldots, x_n]$.

If c is in $\mathbb{K}[[x_1, \ldots, x_n]]$, we write $[x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}]c$ for the coefficient of $x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$ in c. Now let i be the least integer for which $[x_1^i]q \neq 0$. (We have seen that such an i exists.) Pick $j_1, j_2, \ldots, j_n$ satisfying

(i) $[x_1^{j_1}x_2^{j_2}\cdots x_n^{j_n}]r \neq 0$;

(ii) subject to (i), $j_2+\cdots+j_n$ is as small as possible;

(iii) subject to (i) and (ii), j_1 is as small as possible.

We claim that
$$[x_1^{i+j_1}x_2^{j_2}\cdots x_n^{j_n}](qr) = ([x_1^i]q)([x_1^{j_1}x_2^{j_2}\cdots x_n^{j_n}]r) \tag{4.4}$$

To show this, it suffices to show that if $k_1,\dots,k_n,\ell_1,\dots,\ell_n$ are such that
$$x_1^{k_1}\cdots x_n^{k_n}x_1^{\ell_1}\cdots x_n^{\ell_n} = x_1^{i+j_1}x_2^{j_2}\cdots x_n^{j_n}$$
with $[x_1^{k_1}\cdots x_n^{k_n}]q \neq 0$ and $[x_1^{\ell_1}\cdots x_n^{\ell_n}]r \neq 0$, then $k_1 = i$, $k_u = 0$ for $u > 1$, and $\ell_v = j_v$ for all v.

Since $k_u + \ell_u = j_u$ for $u > 1$, we have
$$\ell_2+\cdots+\ell_n = (j_2+\cdots+j_n)-(k_2+\cdots+k_n).$$

By (ii), we have $k_u = 0$ for $u > 1$, and hence $\ell_v = j_v$ for $v > 1$. Since $[x_1^{k_1}]q \neq 0$, the definition of i implies $k_1 \geq i$. Then
$$i + j_1 = k_1 + \ell_1 \geq i + \ell_1.$$

So, $j_1 \geq \ell_1$. By (iii), $j_1 = \ell_1$ and (4.4) is proved.

It follows that $[x_1^{i+j_1}x_2^{j_2}\cdots x_n^{j_n}](qr) \neq 0$. Since qr is free of x_1, we have that $i + j_1 = 0$. So, $i = 0$. Thus, $[1]q \neq 0$.

□

Assume that $\mathbb{E}$ is a universal differential field extension [29, Section 7, page 133] of $\mathbb{K}(\mathbf{x})$ which contains $\mathbb{K}[[\mathbf{x}]]$. Let $\mathbb{C}_{\mathbb{E}}$ be the field of constant in $\mathbb{E}$. Then the field $\mathbb{C}_{\mathbb{E}}$ contains $\mathbb{K}$. Set $\mathrm{sol}(G)$ to be the solution space of G, which is contained in $\mathbb{E}$ and is a vector space over $\mathbb{C}_{\mathbb{E}}$. Assume that $\mathbb{K}(\mathbf{x})[\boldsymbol{\partial}]G$ is D-finite. It follows from [29, Proposition 2, Corollary 1, page 151–152] that
$$\mathrm{rank}(G) = \dim_{\mathbb{C}_{\mathbb{E}}} \mathrm{sol}(G). \tag{4.5}$$

For $\theta_1,\theta_2,\dots,\theta_\ell \in \mathrm{T}(\boldsymbol{\partial})$ and $\ell \in \mathbb{Z}^+$, the exterior product
$$\lambda = \theta_1 \wedge \theta_2 \wedge \cdots \wedge \theta_\ell$$
is defined as a multi-linear mapping from $\mathbb{E}^\ell$ to $\mathbb{E}$:
$$\lambda(\mathbf{z}) = \begin{vmatrix} \theta_1(z_1) & \theta_1(z_2) & \cdots & \theta_1(z_\ell) \\ \theta_2(z_1) & \theta_2(z_2) & \cdots & \theta_2(z_\ell) \\ \vdots & \vdots & \ddots & \vdots \\ \theta_\ell(z_1) & \theta_\ell(z_2) & \cdots & \theta_\ell(z_\ell) \end{vmatrix}$$
for $\mathbf{z} = (z_1,z_2,\dots,z_\ell) \in \mathbb{E}^\ell$.

Let $\{\xi_1, \ldots, \xi_d\}$ be the parametric terms of G with

$$1 = \xi_1 \prec \xi_2 \prec \cdots \prec \xi_d.$$

We call the element $w_G = (\xi_1 \wedge \cdots \wedge \xi_d)$ the *Wronskian operator* of G.

Proof of Theorem 4.3.1: *Necessity*: Assume that the origin is an ordinary point of G. First, we show how to construct formal power series solutions of G. This approach originates from a technical report [49].

Let $\theta_1, \ldots, \theta_k$ be the head terms of elements in G. Then the elements of G can be written as

$$G_i = \ell_i \theta_i + \text{a } \mathbb{K}[\mathbf{x}]\text{-linear combination of parametric terms,}$$

where $\ell_i \in \mathbb{K}[\mathbf{x}]$ and $i = 1, \ldots, k$.

By the remark after Definition 4.2.1, we know that none of the ℓ_i's vanish at the origin. We associate to each term $\lambda = \boldsymbol{\partial}^{\mathbf{u}} \in \mathrm{PT}(G)$ an arbitrary constant $c_{\mathbf{u}} \in \mathbb{K}$. We will also write c_λ for this constant. For a non-parametric term $\theta = \boldsymbol{\partial}^{\mathbf{v}}$, let N_θ be the reduced form of θ with respect to G. Although N_θ belongs to $\mathbb{K}(\mathbf{x})[\boldsymbol{\partial}]$, there exists a power product ℓ_θ of $\ell_1, \ldots, \ell_k$ such that $\ell_\theta N_\theta \in \mathbb{K}[\mathbf{x}][\boldsymbol{\partial}]$. Write

$$\ell_\theta(\mathbf{x}) N_\theta = \sum_{\lambda \in \mathrm{PT}(G)} a_{\theta,\lambda}(\mathbf{x}) \lambda$$

with $a_{\theta,\lambda} \in \mathbb{K}[\mathbf{x}]$. Set

$$c_\theta = \ell_\theta(\mathbf{0})^{-1} \sum_{\lambda \in \mathrm{PT}(G)} a_{\theta,\lambda}(\mathbf{0}) c_\lambda.$$

This constant is also denoted by $c_{\mathbf{v}}$.

Let

$$f = \sum_{\mathbf{u} \in \mathbb{N}^n} \frac{c_{\mathbf{u}}}{\mathbf{u}!} \mathbf{x}^{\mathbf{u}}.$$

Using (4.2) and the ring homomorphism ϕ, we can rewrite the definition of c_θ as

$$\phi\left(\ell_\theta(\mathbf{x})\theta(f)\right) = \phi((\ell_\theta(\mathbf{x}) N_\theta)(f)). \tag{4.6}$$

Note that ℓ_θ can be chosen to be any power product of $\ell_1, \ldots, \ell_k$ such that $\ell_\theta N_\theta$ belongs to $\mathbb{K}[\mathbf{x}][\boldsymbol{\partial}]$.

We claim that f is a formal power series solution of G, that is,

$$G_i(f) = 0, \quad i = 1, \ldots, k. \tag{4.7}$$

By (4.1) and Lemma 4.3.2, it suffices to show that, for all $\mathbf{u} \in \mathbb{N}^n$ and $i \in \{1, \ldots, k\}$,

$$\phi\left(\boldsymbol{\partial}^{\mathbf{u}} G_i(f)\right) = 0. \tag{4.8}$$

We prove (4.8) by Noetherian induction on the term order $\prec$.

Starting with $\xi = \boldsymbol{\partial}^{\mathbf{0}}$, we can write

$$\xi G_i = G_i = \ell_i(\mathbf{x})\theta_i - \sum_{\lambda \in \mathrm{PT}(G)} a_{\theta_i,\lambda}(\mathbf{x})\lambda, \tag{4.9}$$

where $a_{\theta_i,\lambda} \in \mathbb{K}[\mathbf{x}]$. It follows that

$$\ell_i(\mathbf{x})N_{\theta_i} = \sum_{\lambda \in \mathrm{PT}(G)} a_{\theta_i,\lambda}(\mathbf{x})\lambda.$$

Since

$$c_{\theta_i} = \ell_i(\mathbf{0})^{-1} \sum_{\lambda \in \mathrm{PT}(G)} a_{\theta_i,\lambda}(\mathbf{0})c_\lambda,$$

we have

$$\ell_i(\mathbf{0})c_{\theta_i} - \sum_{\lambda \in \mathrm{PT}(G)} a_{\theta_i,\lambda}(\mathbf{0})c_\lambda = 0.$$

By (4.2),

$$\phi(\ell_i(\mathbf{x}))\phi(\theta_i(f)) - \sum_{\lambda \in \mathrm{PT}(G)} \phi(a_{\theta_i,\lambda}(\mathbf{x}))\phi(\lambda(f)) = 0.$$

Since ϕ is a ring homomorphism, we have

$$\phi\left(\ell_i(\mathbf{x})\theta_i(f) - \sum_{\lambda \in \mathrm{PT}(G)} a_{\theta_i,\lambda}(\mathbf{x})\lambda(f)\right) = 0.$$

By (4.9), $\phi(G_i(f)) = 0$.

Assume that ξ is a term higher than $\boldsymbol{\partial}^{\mathbf{0}}$ and, for all $\tilde{\xi}$ below ξ and all $i \in \{1, \ldots, k\}$,

$$\phi(\tilde{\xi}G_i(f)) = 0.$$

Reducing $\xi\theta_i$ modulo G, we have

$$\ell(\mathbf{x})\xi\theta_i = p_\xi(\mathbf{x})(\xi G_i) + \left(\sum_{\tilde{\xi} \prec \xi} \sum_{s=1}^{k} p_{\tilde{\xi},s}(\mathbf{x})(\tilde{\xi}G_s)\right) + \ell(\mathbf{x})N_{\xi\theta_i},$$

where $\ell(\mathbf{x})$ and $p_\xi(\mathbf{x})$ are two power products of $\ell_1(\mathbf{x}), \ldots, \ell_k(\mathbf{x})$ and $p_{\tilde{\xi},s}(\mathbf{x})$ belongs to $\mathbb{K}[\mathbf{x}]$ for all $\tilde{\xi} \prec \xi$. Moreover, $\ell(\mathbf{x})N_{\xi\theta_i}$ belongs to $\mathbb{K}[\mathbf{x}][\boldsymbol{\partial}]$. Applying the above equality to f, we get

$$\ell(\mathbf{x})\xi\theta_i(f) = p_\xi(\mathbf{x})(\xi G_i)(f) + \left(\sum_{\tilde{\xi} \prec \xi} \sum_{s=1}^{k} p_{\tilde{\xi},s}(\mathbf{x})(\tilde{\xi}G_s)(f)\right) + \ell(\mathbf{x})N_{\xi\theta_i}(f).$$

Applying ϕ to the above equality yields

$$\phi\left(\ell(\mathbf{x})\xi\theta_i(f)\right) = p_\xi(\mathbf{0})\phi(\xi G_i(f)) + \sum_{\tilde{\xi}\prec\xi}\sum_{s=1}^{k} p_{\tilde{\xi},s}(\mathbf{0})\phi(\tilde{\xi}G_s(f))$$
$$+\, \phi\left(\left(\ell(x,y)N_{\xi\theta_k}\right)(f)\right).$$

By the induction hypothesis, $\phi(\tilde{\xi}G_s(f)) = 0$ for all $\tilde{\xi} \prec \xi$ and $s \in \{1,\ldots,k\}$. Thus,

$$\phi\left(\ell(\mathbf{x})\xi\theta_i(f)\right) = p_\xi(\mathbf{0})\phi(\xi G_i(f)) + \phi\left(\left(\ell(\mathbf{x})N_{\xi\theta_i}\right)(f)\right).$$

By (4.6), we have

$$p_\xi(\mathbf{0})\phi(\xi G_i(f)) = 0.$$

Since $p_\xi(\mathbf{0})$ is nonzero, $\phi(\xi G_i(f))$ is equal to zero. This proves (4.8). Therefore, our claim (4.7) holds. Since there are $\mathrm{rank}(G)$ parametric terms, the D-finite system G has $\mathrm{rank}(G)$ many $\mathbb{K}$-linearly independent formal power series solutions with initial exponents in $\mathrm{PE}(G)$.

Sufficiency: Without loss of generality, for each $P \in G$, we may assume that P is not a monomial with respect to $\boldsymbol{\partial}$ (Otherwise, P is just a term in $\mathbb{K}(\mathbf{x})[\boldsymbol{\partial}]$ because P is primitive.). Let $\{\theta_1,\ldots,\theta_k\}$ and $\{\ell_1,\ldots,\ell_k\}$ be the head terms and head coefficients of G, respectively. By the remark after Definition 4.2.1, we just need to prove that the constant term of ℓ_i is non-zero for each $i = 1,\ldots,k$.

Let $d = \mathrm{rank}(G)$. Assume that $f_1,\ldots,f_d$ are $\mathbb{K}$-linearly independently formal power series solutions of G and the initial exponent of f_j is equal to the exponent of ξ_j for each index $j \in \{1,\ldots,d\}$. By equation (4.2),

$$\begin{array}{rcll} \phi(\xi_i(f_j)) & = & 0 & \text{for } 1 \le i < j \le d, \\ \phi(\xi_j(f_j)) & \ne & 0 & \text{for } 1 \le j \le d. \end{array}$$

Let $\mathbf{f} = (f_1,\ldots,f_d)$. By the above equations, the constant term of $w_G(\mathbf{f})$ is nonzero. Thus, the formal power series $w_G(\mathbf{f})$ is invertible in $\mathbb{K}[[\mathbf{x}]]$. By [36, Lemma 8], $f_1,\ldots,f_d$ form a fundamental system of $\mathrm{sol}(G)$.

Let $F_i = (w_L \wedge \theta_i)(\mathbf{f},\cdot)$, which is the following $(d+1)\times(d+1)$ determinant

$$\begin{vmatrix} \xi_1(f_1) & \xi_1(f_2) & \cdots & \xi_1(f_d) & \xi_1 \\ \xi_2(f_1) & \xi_2(f_2) & \cdots & \xi_2(f_d) & \xi_2 \\ \vdots & \vdots & & \vdots & \vdots \\ \xi_d(f_1) & \xi_d(f_2) & \cdots & \xi_d(f_d) & \xi_d \\ \theta_i(f_1) & \theta_i(f_2) & \cdots & \theta_i(f_d) & \theta_i \end{vmatrix}.$$

By [35, Lemma 4], we have

$$F_i = \frac{w_G(\mathbf{f})}{\ell_i} G_i.$$

Since $w_G(\mathbf{f})$ is invertible in $\mathbb{K}[[\mathbf{x}]]$, we have

$$\frac{1}{\ell_i} G_i = w_G(\mathbf{f})^{-1} F_i \in \mathbb{K}[[\mathbf{x}]][\boldsymbol{\partial}]. \tag{4.10}$$

Since G_i is primitive, we can write G_i as

$$\ell_i \theta_i + \sum_{j=1}^{d} \ell_{ij} \xi_j,$$

where $\ell_{ij} \in \mathbb{K}[\mathbf{x}]$ and $\gcd(\ell_i, \ell_{i1}, \ldots, \ell_{id}) = 1$. By (4.10), we have

$$\frac{\ell_{ij}}{\ell_i} \in \mathbb{K}[[\mathbf{x}]] \quad \text{for each} \quad j = 1, \ldots, d.$$

It follows from Lemma 4.3.3 that the constant term of ℓ_i is non-zero. □

Note that the proof for the necessity of the above theorem also holds for an arbitrary left (not necessarily D-finite) ideal $\mathbb{K}(\mathbf{x})[\boldsymbol{\partial}]G$, provided that the origin is an ordinary point of G.

4.4 Apparent singularities and desingularization

Let $G \subset \mathbb{K}[\mathbf{x}][\boldsymbol{\partial}]$ be the same as in the beginning of the last section and suppose the left ideal $\mathbb{K}(\mathbf{x})[\boldsymbol{\partial}]G$ is D-finite.

4.4.1 Definitions

Definition 4.4.1. *Let d be the rank of G.*

(i) Assume that the origin is a singularity of G. We call the origin an apparent singularity *of G if G has d many $\mathbb{K}$-linearly independent formal power series solutions.*

(ii) Assume that $M \subset \mathbb{K}[\mathbf{x}][\boldsymbol{\partial}]$ is a finite set such that M is a Gröbner basis with respect to $\prec$ and $\mathbb{K}(\mathbf{x})[\boldsymbol{\partial}] \cdot M$ is D-finite. Let ℓ be the rank of M with $\ell > d$. We call M an ℓth-order left multiple *of G if*

$$\mathbb{K}(\mathbf{x})[\boldsymbol{\partial}]M \subset \mathbb{K}(\mathbf{x})[\boldsymbol{\partial}]G.$$

The above definition is compatible with the univariate case [1, Definition 5].

Example 4.4.2. *The solution space* $\mathrm{sol}(G)$ *of the Gröbner basis*

$$G = \{x_2\partial_2 + \partial_1 - x_2 - 1, \partial_1^2 - \partial_1\}$$

in $\mathbb{K}(x_1, x_2)[\partial_1, \partial_2]$ is generated by $\{\exp(x_1 + x_2), x_2 \exp(x_2)\}$. In this case,

$$\mathrm{HT}(G) = \{\partial_2, \partial_1^2\}, \mathrm{HC}(G) = \{x_2, 1\} \text{ and } \mathrm{PT}(G) = \{1, \partial_1\}.$$

Moreover, $\operatorname{lcm}(x_2, 1) = x_2$. *Therefore, the origin is a singularity of* G *and* G *has two* $\mathbb{Q}$-*linearly independent formal power series solutions. So, it follows from item (i) of the above definition that the origin is an apparent singularity of* G.

Let M *be another Gröbner basis with*

$$\mathbb{K}(\mathbf{x})[\boldsymbol{\partial}] \cdot M = \mathbb{K}(\mathbf{x})[\boldsymbol{\partial}]G \cap \mathbb{K}(\mathbf{x})[\boldsymbol{\partial}] \cdot \{x_1\partial_1 - 1, \partial_2\}.$$

We find that rank$(M) = 3$. *By item (ii) of the above definition,* M *is a* 3*rd-order left multiple of* G.

Example 4.4.3. *The solution space* $\operatorname{sol}(G)$ *of the Gröbner basis*

$$G = \{x_2^2\partial_2 - x_1^2\partial_1 + x_1 - x_2, \partial_1^2\}$$

in $\mathbb{K}(x_1, x_2)[\partial_1, \partial_2]$ *is generated by* $\{x_1 + x_2, x_1x_2\}$. *In this case,*

$$\mathrm{HT}(G) = \{\partial_2, \partial_1^2\}, \mathrm{HC}(G) = \{x_2^2, 1\} \text{ and } \mathrm{PT}(G) = \{1, \partial_1\}.$$

Moreover, $\operatorname{lcm}(x_2^2, 1) = x_2^2$. *Therefore, the origin is a singularity of* G *and* G *has two* $\mathbb{K}$-*linearly independent formal power series solutions. So, it follows from item (i) of Definition 4.4.1 that the origin is an apparent singularity of* G.

Set

$$S = \{(0,0), (0,1), (2,0), (0,2)\}.$$

Let M *be another Gröbner basis with*

$$\mathbb{K}(\mathbf{x})[\boldsymbol{\partial}] \cdot M = \mathbb{K}(\mathbf{x})[\boldsymbol{\partial}]G \cap \left(\bigcap_{(s,t)\in S} \mathbb{K}(\mathbf{x})[\boldsymbol{\partial}] \cdot \{x_1\partial_1 - s, x_2\partial_2 - t\} \right)$$

We find that rank$(M) = 6$. *By item (ii) of Definition 4.4.1,* M *is a* 6*th-order left multiple of* G.

4.4.2 Rank formula of D-finite ideals

In order to prove Theorem 4.4.6, we need a rank formula of D-finite ideals.

Lemma 4.4.4. [2] *Let* V *be a vector space and* U, W *be two subspaces of* V. *Set*

$$\begin{array}{rccl} \psi: & V/(U\cap W) & \to & V/U \times V/W \\ & v + U\cap W & \mapsto & (v+U, -v+W), \end{array}$$

and

$$\begin{array}{rccl} \phi: & V/U \times V/W & \to & V/(U+W) \\ & (a+U, b+W) & \mapsto & a+b+U+W. \end{array}$$

Then

$$0 \to V/(U\cap W) \xrightarrow{\psi} V/U \times V/W \xrightarrow{\phi} V/(U+W) \to 0$$

is an exact sequence.

[2] We thank Professor Yang Han for showing us this lemma, which shortens our proof of the rank formula.

Proof. It is straightforward to see that ψ and ϕ are well-defined injective and surjective homomorphisms, respectively. Note that $(a+U, b+W) \in \ker(\phi)$ if and only if there exist elements $u \in U, w \in W$ such that $a+b = u+w$, *i.e.*, $a = u+w-b$. In other words,

$$\begin{aligned} \ker(\phi) &= \{(u+w-b+U, b+W) \mid u \in U, w \in W \text{ and } b \in V\} \\ &= \{((w-b)+U, b+W) \mid w \in W, b \in V\} \end{aligned}$$

Let $v = w-b$, we get

$$\begin{aligned} \ker(\phi) &= \{(v+U, w-v+W) \mid v \in V, w \in W\} \\ &= \{(v+U, -v+W) \mid v \in V\} \end{aligned}$$

Thus, $\ker(\phi) = \psi\left(V/(U+W)\right)$. ☐

Corollary 4.4.5. *Let $I, J \subset \mathbb{K}(\mathbf{x})[\boldsymbol{\partial}]$ be left ideals of finite rank. Then*

(i) $\operatorname{rank}(I \cap J) + \operatorname{rank}(I+J) = \operatorname{rank}(I) + \operatorname{rank}(J)$

(ii) $\operatorname{rank}(I \cap J) = \operatorname{rank}(I) + \operatorname{rank}(J)$ *if* $\operatorname{sol}(I) \cap \operatorname{sol}(J) = \{0\}$.

Proof. (i) It follows from the definition of rank and the above lemma.

(ii) It is straightforward to see that $\operatorname{sol}(I+J) = \operatorname{sol}(I) \cap \operatorname{sol}(J) = \{0\}$. Therefore, the claim follows from equation (4.5) and item 1. ☐

4.4.3 Removing and detecting apparent singularities

The following theorem is a generalization of [1, Proposition 7], which gives the connection between apparent singularities and ordinary points. As a matter of notation, we set

$$U_m = \{\mathbf{u} \in \mathbb{N}^n \mid |\mathbf{u}| \leq m\},$$

where $m \in \mathbb{N}$.

Theorem 4.4.6. *Let $d = \operatorname{rank}(G)$. Assume that the origin is a singularity of G and S is a set of initial exponent candidates of G with the property $|S| \geq d$. Let $m = \max\{|\mathbf{u}| \mid \mathbf{u} \in S\}$. Then the following two claims are equivalent:*

(i) The origin is an apparent singularity of G;

(ii) There exists a subset B of S with $|B| = d$, such that the origin is an ordinary point of the left multiple M of G, where M is a Gröbner basis of

$$\mathbb{K}(\mathbf{x})[\boldsymbol{\partial}]G \cap \left(\bigcap_{\mathbf{u} \in U_m \setminus B} \mathbb{K}(\mathbf{x})[\boldsymbol{\partial}] \cdot \{x_i\partial_i - u_i | 1 \leq i \leq n\} \right) \tag{4.11}$$

Lemma 4.4.7. *Let I be a left ideal in $\mathbb{E}[\boldsymbol{\partial}]$ with finite rank. Then*

$$\operatorname{ann}(\operatorname{sol}(I)) = I.$$

Proof. It follows from [29, Proposition 2, Corollary 1, page 151–152]. □

For $m \in \mathbb{N}$, we set $\Theta_m = \{\boldsymbol{\partial}^{\mathbf{u}} \mid |\mathbf{u}| = m+1\}$.

Lemma 4.4.8. *Let M be a Gröbner basis with respect to $\prec$ and $\ell = \mathrm{rank}(M)$. Assume that $\mathrm{sol}(M)$ is spanned by ℓ many $\mathbb{K}$-linearly independent formal power series $f_1, \ldots, f_\ell$ with initial exponents U_m for some $m \in \mathbb{N}$. Then*

$$\mathrm{HT}(M) = \Theta_m.$$

Proof. Without loss of generality, we may assume that

$$1 = \mathrm{in}(f_1) \prec \mathrm{in}(f_2) \prec \cdots \prec \mathrm{in}(f_\ell).$$

Let $\Theta_m = \{\theta_1, \ldots, \theta_t\}$. Set $\xi_1, \ldots, \xi_\ell$ to be terms of $\mathrm{T}(\boldsymbol{\partial})$ such that the exponent of ξ_j is the same as that of $\mathrm{in}(f_j)$, $j = 1, \ldots, \ell$.

Let $\mathbf{f} = (f_1, \ldots, f_\ell)$ and $w_M = (\xi_1 \wedge \ldots \wedge \xi_\ell)$. Similar to the argument in the proof of Theorem 4.4.6, we know that $w_M(\mathbf{f})$ in invertible in $\mathbb{K}[[\mathbf{x}]]$. By equation (4.5) and [36, Lemma 8], $f_1, \ldots, f_\ell$ form a fundamental system of $\mathrm{sol}(M)$.

Let $F_i = (w_M \wedge \theta_i)(\mathbf{f}, \cdot)$ for $i = 1, \ldots, t$. Since $\prec$ is a total degree term order on $\mathrm{T}(\boldsymbol{\partial})$, we know that $\xi_j \prec \theta_i$ for $j = 1, \ldots, \ell$. Moreover, the coefficient of θ_i in F_i is $w_M(\mathbf{f}) \neq 0$. Thus, the head term of F_i is θ_i. Since $F_i(f_j) = 0$ for $j = 1, \ldots, \ell$, it follows that $\mathrm{sol}(M) \subset \mathrm{sol}(F_i)$.

Note that M is also a Gröbner basis in $\mathbb{E}[\boldsymbol{\partial}]$ with respect to $\prec$. Since $\mathrm{sol}(M) \subset \mathrm{sol}(F_i)$, it follows that $\mathrm{ann}(\mathrm{sol}(F_i)) \subset \mathrm{ann}(\mathrm{sol}(M))$. By Lemma 4.4.7, we have that $F_i \in \mathbb{E}[\boldsymbol{\partial}] \cdot M$. Since $\mathrm{HT}(F_i) = \theta_i$, we have that there exists F in M such that $\mathrm{HT}(F)$ divides θ_i. On account of M being a reduced Gröbner basis, it implies that $\mathrm{PT}(M)$ is contained in $\{\xi_1, \ldots, \xi_\ell\}$. Since $\mathrm{rank}(M) = \ell$, we conclude that

$$\mathrm{PT}(M) = \{\xi_1, \ldots, \xi_\ell\}.$$

In other words, $\mathrm{HT}(M) = \Theta_m$. □

Proof of Theorem 4.4.6: $(i) \Rightarrow (ii)$: Let $f_1, \ldots, f_d$ be $\mathbb{K}$-linearly independent formal power series solutions of G with $\mathrm{in}(f_i) = \mathbf{x}^{\mathbf{u}_i}$, $1 \leq i \leq d$. By equation (4.5) and [36, Lemma 8], $f_1, \ldots, f_d$ form a fundamental system of $\mathrm{sol}(G)$. Set $B = \{\mathbf{u}_i \mid i = 1, \ldots, d\}$. Then B is a subset of S. Let M be the Gröbner basis as in (4.11). For each $\mathbf{v} \in U_m \setminus B$, the single term $\mathbf{x}^{\mathbf{v}}$ forms a fundamental system of solutions of $\mathbb{K}(\mathbf{x})[\boldsymbol{\partial}] \cdot \{x_i \partial_i + v_i \mid 1 \leq i \leq n\}$. Set

$$\ell = |U_m| \text{ and } \{f_{d+1}, \ldots, f_\ell\} = \{\mathbf{x}^{\mathbf{v}} \mid \mathbf{v} \in U_m \setminus B\}.$$

By Corollary 4.4.5, $\mathrm{rank}(M) = \ell$ and $\mathrm{sol}(M)$ is spanned by ℓ many $\mathbb{K}$-linearly independent formal power series $f_1, \ldots, f_\ell$ with initial exponents U_m. By Lemma 4.4.8, we have that

$$\mathrm{HT}(M) = \Theta_m.$$

It follows from Theorem 4.3.1 that the origin is an ordinary point of M.

$(ii) \Rightarrow (i)$: Since M is a left multiple of G, it follows that $\mathrm{sol}(G) \subset \mathrm{sol}(M)$. On the other hand, it follows from Theorem 4.3.1, equation (4.5) and [36, Lemma 8] that $\mathrm{sol}(M)$ has a basis in $\mathbb{K}[[\mathbf{x}]]$. Assume that $\{f_1, \ldots, f_\ell\} \subset \mathbb{K}[[\mathbf{x}]]$ is a basis of $\mathrm{sol}(M)$. Next, we prove that $\mathrm{sol}(G)$ also has a basis in $\mathbb{K}[[\mathbf{x}]]$. Since $\mathrm{sol}(G) \subset \mathrm{sol}(M)$, $\{f_1, \ldots, f_\ell\}$ is also a spanning set of $\mathrm{sol}(G)$ over $\mathbb{C}_\mathbb{E}$. Assume that $f = z_1 f_1 + \ldots + z_\ell f_\ell$, where $z_1, \ldots, z_\ell \in \mathbb{C}_\mathbb{E}$ are to be determined. Let $G = \{G_1, \ldots, G_k\}$. Consider

$$G_j(f) = 0, \quad j = 1, \ldots, k.$$

It is equivalent to

$$z_1 G_j(f_1) + \cdots + z_\ell G_j(f_\ell) = 0, \quad j = 1, \ldots, k.$$

By comparing the coefficients of $\mathbf{x}^\mathbf{w} (\mathbf{w} \in \mathbb{N}^n)$ in both sides of the above equations, we derive a system of linear equations, whose coefficient vectors belong to $\mathbb{K}^\ell$. Let V be the vector space spanned by those coefficient vectors over $\mathbb{K}$. Assume that $\{\mathbf{v}_1, \ldots, \mathbf{v}_r\}$ is a basis of V. Set $\mathbf{z} = (z_1, \ldots, z_\ell)$ and A to be the matrix in $\mathbb{K}^{r \times \ell}$ with row vectors $\mathbf{v}_1, \ldots, \mathbf{v}_r$. Then we have

$$f \in \mathrm{sol}(G) \quad \text{if and only if} \quad A\mathbf{z} = \mathbf{0}. \tag{4.12}$$

Set $\ker(A) = \{\mathbf{z} \in \mathbb{C}_\mathbb{E}^\ell \mid A\mathbf{z} = \mathbf{0}\}$. Then $\ker(A)$ has a basis $\{\mathbf{s}_1, \ldots, \mathbf{s}_t\}$ in $\mathbb{K}^\ell$. Assume that $\mathbf{s}_i = (s_{i1}, \ldots, s_{i\ell})$, where $i = 1, \ldots, t$. Set $g_i = s_{i1} f_1 + \cdots + s_{i\ell} f_\ell$, $i = 1, \ldots, t$. By (4.12), we have that $\{g_1, \ldots, g_t\}$ is a spanning set of $\mathrm{sol}(G)$ over $\mathbb{C}_\mathbb{E}$. Since $\{\mathbf{s}_1, \ldots, \mathbf{s}_t\}$ is a basis of $\ker(A)$ and $f_1, \ldots, f_\ell$ are $\mathbb{K}$-linearly independent, a direct verification implies that $g_1, \ldots, g_t$ are $\mathbb{K}$-linearly independent. By [36, Lemma 8], $g_1, \ldots, g_t$ are $\mathbb{C}_\mathbb{E}$-linearly independent. Thus, $\{g_1, \ldots, g_t\}$ is a basis of $\mathrm{sol}(G)$ in $\mathbb{K}[[\mathbf{x}]]$. Consequently, it follows from item (ii) of Definition 4.4.1 that the origin is an apparent singularity of G. $\square$

Note that if the origin is an apparent singularity of G and B is the set of initial exponents of $\mathrm{sol}(G)$, then the proof of "$(i) \Rightarrow (ii)$" in Theorem 4.4.6 also works for the choice $S = B$. Besides, the proof of "$(ii) \Rightarrow (i)$" in Theorem 4.4.6 is not constructive. It would be nice to design an algorithm to compute a basis of formal power series solutions at (not necessarily apparent) singularities for a D-finite system. More precisely, set

$$V = \{f \in \mathbb{K}[[\mathbf{x}]] \mid P(f) = 0 \text{ for each } P \in G\}.$$

Then V is a $\mathbb{K}$-vector space of finite dimension. The problem is to design an algorithm to compute a basis of V. Currently, we are working on this problem.

One application of Theorem 4.4.6 is desingularization. We outline the algorithm as follows:

Algorithm 4.4.9. *Given $G \subset \mathbb{K}[\mathbf{x}][\boldsymbol{\partial}]$ as in the beginning of this section, the origin being an apparent singularity of G with initial exponents B of* $\mathrm{sol}(G)$. *Compute a left multiple M of G such that the origin is an ordinary point of M.*

(1) Let $m = \max\{|\mathbf{u}| \mid \mathbf{u} \in B\}$ and $S = B$.

(2) Compute a Gröbner basis M of the ideal described in (4.11), and output M.

The termination of the above algorithm is obvious. The correctness follows from Theorem 4.4.6 and the above remark.

Example 4.4.10. *Consider the Gröbner basis from Example 4.4.2:*

$$G = \{x_2\partial_2 + \partial_1 - x_2 - 1, \partial_1^2 - \partial_1\},$$

where $\mathrm{sol}(G)$ *is spanned by* $\{\exp(x_1 + x_2), x_2 \exp(x_2)\}$ *with initial exponents*

$$B = \{(0,0), (0,1)\}.$$

In this case, the origin is an apparent singularity of G.

Let $U_1 = \{(i,j) \in \mathbb{N}^2 \mid i + j \leq 1\} = \{(0,0), (1,0), (0,1)\}$. *Then*

$$U_1 \setminus B = \{(1,0)\}.$$

Let M *be another Gröbner basis with*

$$\mathbb{K}(\mathbf{x})[\boldsymbol{\partial}] \cdot M = \mathbb{K}(\mathbf{x})[\boldsymbol{\partial}]G \cap \mathbb{K}(\mathbf{x})[\boldsymbol{\partial}] \cdot \{x_1\partial_1 - 1, \partial_2\}.$$

Since the size of M *is big, we do not display it here. We only mention that*

$$\mathrm{HC}(M) = \{1 - x_1 - x_1x_2\}.$$

So, it follows from Definition 4.2.1 that M *is a left multiple of* G *for which the origin is an ordinary point.*

Example 4.4.11. *Consider the Gröbner basis in Example 4.4.3:*

$$G = \{x_2^2\partial_2 - x_1^2\partial_1 + x_1 - x_2, \partial_1^2\},$$

where $\mathrm{sol}(G)$ *is spanned by* $\{x_1 + x_2, x_1x_2\}$ *with initial exponents*

$$B = \{(1,0), (1,1)\}.$$

In this case, the origin is an apparent singularity of G. *Then*

$$U_2 \setminus B = \{(0,0), (0,1), (2,0), (0,2)\}.$$

Let M *be another Gröbner basis with*

$$\mathbb{K}(\mathbf{x})[\boldsymbol{\partial}] \cdot M = \mathbb{K}(\mathbf{x})[\boldsymbol{\partial}]G \cap \left(\bigcap_{(s,t) \in U_2 \setminus B} \mathbb{K}(\mathbf{x})[\boldsymbol{\partial}] \cdot \{x_1\partial_1 - s, x_2\partial_2 - t\} \right)$$

We find that

$$M = \{\partial_1^3, \partial_1^2\partial_2, \partial_1\partial_2^2, \partial_2^3\}.$$

So, it follows from Definition 4.2.1 that M *is a left multiple of* G *for which the origin is an ordinary point.*

We can also use Theorem 4.4.6 to decide whether the origin is apparent or not. We outline the algorithm as follows:

Algorithm 4.4.12. *Given $G \subset \mathbb{K}[\mathbf{x}][\boldsymbol{\partial}]$ as in the beginning of this section, the origin being a singularity of G. Decide whether the origin is apparent or not.*

(1) Let $d = \operatorname{rank}(G)$. Compute a set of initial exponent candidates S of G. If $|S| < d$, then the origin is not apparent. Otherwise, go to step 2.

(2) Compute $\mathbf{B} = \{B \subset S \mid |B| = d\}$. For each $B \in \mathbf{B}$, compute a Gröbner basis M_B of the ideal described by (4.11). If there exists $B \in \mathbf{B}$ such that the origin is an ordinary point of M_B, then the origin is an apparent singularity of G. Otherwise, the origin is not apparent.

The termination of the above algorithm is obvious. The correctness follows from Theorem 4.4.6.

Example 4.4.13. *Consider the Gröbner basis in Example 4.2.13:*

$$\begin{aligned} G &= \{G_1, G_2\} \\ &= \{x_1x_2\partial_2 + (-x_1^2 + 2x_1x_2)\partial_1 - 2x_2, (x_1^3 - x_1^2x_2)\partial_1^2 + 2x_1x_2\partial_1 - 2x_2\} \end{aligned}$$

Here, $\operatorname{rank}(G) = 2$ and the origin is a singularity of G. By computation, we find that $\operatorname{ind}(G_1) = y_2 - y_1$ and $\operatorname{ind}(G_2) = (y_1 - 1)y_1$. Thus, a set of initial exponent candidates of G is

$$S = \{(0, 0), (1, 1)\}$$

Let $B = S$. Then $U_2 \setminus B = \{(1, 0), (0, 1), (2, 0), (0, 2)\}$. Let M be another Gröbner basis with

$$\mathbb{K}(\mathbf{x})[\boldsymbol{\partial}] \cdot M = \mathbb{K}(\mathbf{x})[\boldsymbol{\partial}]G \cap \left(\bigcap_{(s,t) \in U_2 \setminus B} \mathbb{K}(\mathbf{x})[\boldsymbol{\partial}] \cdot \{x_1\partial_1 - s, x_2\partial_2 - t\} \right)$$

We find that

$$\operatorname{HC}(M) = \{x_1^4 - 3x_1^3x_2 + 3x_1^2x_2^2 - x_1x_2^3, -x_1^3 + 3x_1^2x_2 - 3x_1x_2^2 + x_2^3\}$$

Thus, the origin is a singularity of M. By Theorem 4.4.6, we conclude that the origin is not an apparent singularity of G. Actually, $\operatorname{sol}(G)$ is spanned by $\{\frac{x_1}{x_1 - x_2}, x_1x_2\}$.

Example 4.4.14. *Consider the Gröbner basis in $\mathbb{Q}(x_1, x_2)[\partial_1, \partial_2]$:*

$$\begin{aligned} G &= \{G_1, G_2, G_3\} \\ &= \{(x_1 - x_2)\partial_1^2 - x_1x_2\partial_2 + x_1x_2\partial_1 + (x_1 - x_2), \\ &\quad (x_1 - x_2)\partial_1\partial_2 + (-1 - x_1x_2)\partial_2 + (1 + x_1x_2)\partial_1 + (x_1 - x_2), \\ &\quad (x_1 - x_2)\partial_2^2 - x_1x_2\partial_2 + x_1x_2\partial_1 + (x_1 - x_2)\} \end{aligned}$$

Here, $\operatorname{rank}(G) = 3$ and the origin is a singularity of G. By computation, we find that

$$\operatorname{ind}(G_1) = (y_1 - 1)y_1, \operatorname{ind}(G_2) = y_2(y_1 - 1) \text{ and } \operatorname{ind}(G_3) = (y_2 - 1)y_2.$$

Thus, a set of initial exponent candidates of G is

$$S = \{(0,0), (1,0), (1,1)\}.$$

Let $B = S$. Then $U_2 \setminus B = \{(0,1), (2,0), (0,2)\}$. Let M be another Gröbner basis with

$$\mathbb{K}(\mathbf{x})[\boldsymbol{\partial}] \cdot M = \mathbb{K}(\mathbf{x})[\boldsymbol{\partial}]G \cap \left(\bigcap_{(s,t) \in U_2 \setminus B} \mathbb{K}(\mathbf{x})[\boldsymbol{\partial}] \cdot \{x_1\partial_1 - s, x_2\partial_2 - t\} \right)$$

We find that

$$\mathrm{HC}(M) = \{-2 - x_1^2 - 2x_1x_2 - x_2^2\}.$$

Thus, the origin is an ordinary point of M. By Theorem 4.4.6, we conclude that the origin is an apparent singularity of G. Actually, $\mathrm{sol}(G)$ *is spanned by*

$$\{\sin(x_1 + x_2), \cos(x_1 + x_2), x_1x_2\}.$$

Chapter 5

Conclusion and Future Work

In this thesis, we have shown how to determine a basis of the contraction ideal generated by an Ore operator in $R[x][\partial]$, where R is a principal ideal domain. Furthermore, we have given an algorithm for computing a completely desingularized operator with minimal degree and content for its leading coefficient.

We have defined singularities and ordinary points of a D-finite system. We have characterized ordinary points of a D-finite systems by using its formal power series solutions. Last but not least, we have given the connection between apparent singularities and ordinary points, and used it to remove and detect apparent singularities in an algorithmic way.

In this thesis, we have considered contraction of Ore ideals in the univariate Ore algebra $R[x][\partial]$. A more challenging topic is to consider the corresponding problems in the multivariate Ore algebra $R[\mathbf{x}][\boldsymbol{\partial}]$.

Note that Theorem 3.3.2 can be generalized to the multivariate case in a straightforward way. Then the problem is reduced to the problem of finding upper bounds of orders of generators of contraction ideals. At the moment, we can only give upper bounds for some special cases. For the general case, it is still under investigation.

Our algorithms for univariate contraction of Ore ideals rely heavily on the computation of Gröbner bases over a principal ideal domain R. At present, the computation of Gröbner bases over R is not fully available in a computer algebra system. So the algorithms in this thesis are not yet implemented. To improve their efficiency, we need to use linear algebra over R as much as possible. One of our future goals is to implement our algorithms efficiently in some computer algebra system such as `Mathematica`.

In [11], the authors give an algorithm for desingularization of Ore operators by computing least common left multiples randomly. According to experiments, we observe that the same technique also works for the multivariate case in the differential setting. We will also try to design an analogous algorithm for that case and prove its correctness.

Bibliography

[1] S. A. Abramov, M. Barkatou, and M. van Hoeij. Apparent singularities of linear difference equations with polynomial coefficients. *AAECC*, 117–133, 2006.

[2] S. A. Abramov and M. van Hoeij. Desingularization of linear difference operators with polynomial coefficients. In *Proc. of ISSAC'99*, 269–275, New York, NY, USA, 1999. ACM.

[3] F. Aroca and J. Cano. Formal solutions of linear PDEs and convex polyhedra. *J. Symb. Comput.*, 32:717–737, 2001.

[4] M. A. Barkatou and S. S. Maddah. Removing apparent singularities of systems of linear differential equations with rational function coefficients. In *Proc. of ISSAC'15*, 53–60, New York, NY, USA, 2015. ACM.

[5] T. Becker and V. Weispfenning. *Gröbner bases, a computational approach to commutative algebra.* Springer-Verlag, New York, USA, 1993.

[6] M. Bronstein and M. Petkovšek. An introduction to pseudo-linear algebra. *Theoretical Computer Science*, pages 3 –33, 1996.

[7] M. Bronstein. *Symbolic integration I.* Springer Berlin Heidelberg New York, Germany, 2005.

[8] J. Bueso et al. *Algorithmic methods in non-commutative algebra.* Kluwer, 2003.

[9] M. Ceria and T. Mora. Buchberger-Zacharias theory of multivariate Ore extensions. Submitted to J. of Pure and Applied Algebra., 2015.

[10] S. Chen, M. Jaroschek, M. Kauers, and M. F. Singer. Desingularization explains order-degree curves for Ore operators. In *Proc. of ISSAC'13*, 157–164, New York, NY, USA, 2013. ACM.

[11] S. Chen, M. Kauers, and M. F. Singer. Desingularization of Ore operators. *J. Symb. Comput.*, 74:617–626, 2016.

[12] R. C. Churchill and Y. Zhang. Irreducibility criteria for skew polynomials. *Journal of Algebra*, 322:3797–3822, 2009.

[13] F. Chyzak. Mgfun Project. http://algo.inria.fr/chyzak/mgfun.html.

[14] F. Chyzak and B. Salvy. Non-commutative elimination in Ore algebras proves multivariate identities. *J. Symb. Comput.* , 26:187–227, 1998.

[15] S. C. Coutinho. *A primer of algebraic D-modules.* Cambridge University Press, 1995.

[16] D. Cox, J. Little and D. O'Shea. *Ideals, varieties, and algorithms.* Springer, New York, USA, 2006.

[17] W. Decker et al. *Singular, a computer algebra system for polynomial computations.* `https://www.singular.uni-kl.de/`.

[18] I. Gessel. Two theorems on rational power series. Utilitas Mathematica, 19:247–254, 1981.

[19] D. Grayson, M. Stillman, and D. Eisenbud. Macaulay2, a software system for research in algebraic geometry. `http://www.math.uiuc.edu/Macaulay2/`.

[20] A. Hillebrand and W. Schmale. Towards a effective version of a theorem of Stafford. *J. Symb. Comput.*, 32:699–716, 2001.

[21] P. J. Hilton and U. Stammbach. *A course in homological algebra.* Springer-Verlag, New York, USA, 1997.

[22] E. L. Ince. *Ordinary differential equations.* Dover, 1926.

[23] M. Jaroschek. *Removable singularities of Ore operators.* PhD thesis, RISC-Linz, Johannes Kepler Univ., 2013.

[24] M. Kauers and P. Paule. The concrete tetrahedron. Springer, 2011.

[25] M. Kauers. Algorithms for D-finite functions. `http://www.algebra.uni-linz.ac.at/people/mkauers/publications/kauers15n.pdf`.

[26] M. Kauers, Z. Li and Y. Zhang. Apparent singularities of D-finite ideals. In preparation.

[27] A. Kandri-Rody and D. Kapur. Computing a Gröbner basis of a polynomial ideal over a Euclidean domain. *J. Symb. Comput.* , 6:37–57, 1988.

[28] A. Kandri-Rody and V. Weispfenning. Non-commutative Gröbner bases in algebras of solvable type. *J. Symb. Comput.* , 9:1–26, 1990.

[29] E. Kolchin. Differential algebra and algebraic groups. Academic Press., New York, 1973.

[30] C. Koutschan. *Advanced applications of the holonomic systems approach.* PhD thesis, Johannes Kepler University Linz, 2009.

[31] C. Koutschan. *HolonomicFunctions user's guide.* RISC Report Series, Johannes Kepler Univ., 2010.

[32] J. Kovacic. An Eisenstein criterion for noncommutative polynomials. *Proceedings of the American Mathematical Society*, 34, 1972.

[33] G. Labahn et al. Workshop on symbolic combinatorics and computational differential algebra. http://www.fields.utoronto.ca/video-archive/event/411/2015.

[34] A. Leykin. Algorithmic proofs of two theorems of Stafford. *J. Symb. Comput.*, 38:1535–1550, 2004.

[35] Z. Li, F. Schwarz and S. Tsarev. *Factoring zero-dimensional ideals of linear partial differential operators.* In *Proc. of ISSAC'02*, 168–175, New York, NY, USA, 2002, ACM.

[36] Z. Li, M. Singer, M. Wu and D. Zheng. *A recursive method for determining the one-dimensional submodules of Laurent-Ore modules.* In *Proc. of ISSAC'06*, 220–227, New York, NY, USA, 2002, ACM.

[37] Z. Li and Y. Zhang. A note on Groebner bases of Ore polynomials over a PID. `http://www.algebra.uni-linz.ac.at/people/yzhang/GB.pdf`.

[38] Y. Man and F. Wright. Fast polynomial dispersion computation and its application to indefinite summation. In *Proc. of ISSAC'94*, 175–180 , New York, NY, USA, 1994, ACM.

[39] J. Middeke. *A computational view on normal forms of matrices of Ore polynomials.* PhD thesis, Johannes Kepler University Linz, 2011.

[40] T. Mora. *Solving polynomial equation systems* Vol. IV. Cambridge University Press, 2016.

[41] T. W. Müller. *Polynomial recurrences and modular subgroup arithmetic.* Preprint, 2004.

[42] Ø. Ore. Theory of non-commutative polynomials. *Annals of Mathematics*, 34(3):480-508, 1933.

[43] D. Robertz. *Formal algorithmic elimination for PDEs.* Springer, 2014.

[44] M. Saito, B. Sturmfels, and N. Takayama. *Gröbner deformations of hypergeometric differential equations.* Springer-Verlag, New York, USA, 1999.

[45] R. P. Stanley. *Differentiably finite power series. European Journal of Combinatorics*, 1:175–188, 1980.

[46] A. Storjohann. *Algorithms for matrix canonical forms.* PhD thesis, Swiss Federal Institute of Technology Zurich, 2000.

[47] H. Tsai. Weyl closure of a linear differential operator. *J. Symb. Comput.* , 29:747–775, 2000.

[48] H. Tsai. Algorithms for algebraic analysis. PhD thsis, University of California at Berkeley, 2000.

[49] W. Wu. *On the foundation of differential algebraic geometry.* MM Research Preprint 3:1–29, 1989.

[50] Y. Zhang. *Contraction of Ore ideals with applications.* In *Proc. of ISSAC'16*, 413–420, New York, NY, USA, 2016, ACM.

Curriculum Vitae

Personal Data

Full name	Yi Zhang
Date of birth	December 12, 1988
Place of birth	Changzhou, Jiangsu Province, China
Nationality	Chinese

Contact

E-mail	zhangy@amss.ac.cn
Address	Institute for Algebra Johannes Kepler Universität Altenbergerstraße 69, A-4040 Linz, Austria
Office	S2 0373-2 (Science Park II)
Phone	+43 732 2468 6857
Fax	+43 732 2468 6852
Homepage	http://www.algebra.uni-linz.ac.at/people/yzhang/

Education

07/2015 – present	Ph.D. studies in symbolic computation, Institute for Algebra, Johannes Kepler University Linz, Austria.
09/2013 – 06/2015	Ph.D. studies in symbolic computation, Research Institute for Symbolic Computation, Johannes Kepler University Linz, Austria.
09/2011 – 07/2013	Master studies in applied mathematics, Key Laboratory of Mathematics Mechanization, Academy of Mathematics and Systems Science, University of Chinese Academy of Sciences, Beijing, China.
09/2007 – 07/2011	Bachelor of science in mathematics, School of Mathematical Sciences, Soochow University, Suzhou, China.

Awards

ACM Distinguished Student Author Award at ISSAC'16, SIGSAM.

Publications

- Manuel Kauers, Ziming Li and Yi Zhang. *Apparent Singularities of D-finite Systems*, in preparation, 2016.
- Yi Zhang. *Contraction of Ore Ideals with Applications.* In *Proceedings of the 2016 International Symposium on Symbolic and Algebraic Computation*, pp. 413-420, ACM Press, 2016. DOI:10.1145/2930889.2930890.

Talks

5. *Contraction of Linear Difference and Differential Operators.* Contributed talk at ISSAC'16 (the 41st International Symposium on Symbolic and Algebraic Computation), Wilfrid Laurier University, Waterloo, Canada, July, 2016.

4. *Contraction of Linear Difference and Differential Operators.* Invited talk at the seminar of Center for Combinatorics, Nankai University, Tianjin, China, June, 2016.

3. *An Algorithm for Contraction of an Ore Ideal.* Invited talk at the seminar of Institute of Discrete Mathematics and Geometry, Vienna University of Technology, Vienna, Austria, October, 2015.

2. *The Restriction Problem for D-finite Functions.* Contributed talk at the Workshop on Computational and Algebraic Methods in Statistics, The University of Tokyo, Tokyo, Japan, March, 2015.

1. *An Algorithm for Decomposing Multivariate Hypergeometric Terms.* Contributed talk at CM'13 (the 5th National Conference of Computer Mathematics), Jilin University, Changchun, China, August, 2013.

Peer-Reviewing Activities

- Journal of Symbolic Computation