JOHANNES KEPLER
UNIVERSITÄT LINZ | JKU

TNF

Technisch-Naturwissenschaftliche
Fakultät

Removable Singularities of Ore Operators

DISSERTATION

zur Erlangung des akademischen Grades

Doktor

im Doktoratsstudium der

Technischen Wissenschaften

Eingereicht von:
Maximilian Jaroschek

Angefertigt am:
Research Institute for Symbolic Computation

Beurteilung:
Priv.-Doz. Dr. Manuel Kauers (Betreuung)
Prof. Michael F. Singer, PhD

Linz, November 2013

Abstract

Ore algebras are an algebraic structure used to model many different kinds of functional equations like differential and recurrence equations. The elements of an Ore algebra are polynomials for which the multiplication is defined to be usually non-commutative. As a consequence, Gauß' lemma does not hold in many Ore polynomial rings and hence the product of two primitive Ore polynomials is not necessarily primitive. This observation leads to the distinction of non-removable and removable factors and to the study of desingularizing operators.

Desingularization is the problem of finding a left multiple of a given Ore operator in which some factor of the leading coefficient of the original operator is removed. We derive a normal form for such left factors and unify known results for differential and shift operators into one desingularization algorithm. Furthermore, we analyze the effect of removable and non-removable factors on computations with Ore operators.

The set of operators of an Ore algebra that give zero when applied to a given function forms a left ideal. The cost of computing an element of this ideal depends on the size of the coefficients (the degree) and the order of the operator. In order to be able to predict or reduce these costs, we derive an order-degree curve. For a given Ore operator, this is a curve in the (r, d)-plane such that for all points (r, d) above this curve, there exists a left multiple of order r and degree d of the given operator. We show how desingularization yields order-degree curves which are extremely accurate in examples. When computed for the generator of an operator ideal from applications like physics or combinatorics, the resulting bound is usually sharp.

The generator of a left ideal in an Ore polynomial ring is the greatest common right divisor of the ideal elements, which can be computed by the Euclidean algorithm. Polynomial remainder sequences contain the intermediate results of the Euclidean algorithm when applied to (non-)commutative polynomials. The running time of the algorithm is dependent on the size of the coefficients of the remainders. Different methods have been studied to make these as small as possible. The subresultant sequence of two polynomials is a polynomial remainder sequence in which the size of the coefficients is optimal in the generic case, but when taking the input from applications,

the coefficients are often larger than necessary. We generalize two improvements of the subresultant sequence to Ore polynomials, in which we show that the non-removable factors of the greatest common right divisor appear as content. Based on this result we show how to divide out this content during the Euclidean algorithm and derive a new bound for the minimal coefficient size of the remainders. Our approach also yields a new proof for the results in the commutative case, providing a new point of view on the origin of the extraneous factors of the coefficients.

Zusammenfassung

Bei Ore-Algebren handelt es sich um eine algebraische Struktur zur Modellierung von vielen verschiedenen Arten von Funktionalgleichungen wie etwa Differential- und Rekurrenzgleichungen. Die Elemente einer Ore-Algebra sind Polynome für welche die Multiplikation derart definiert ist, dass das Kommutativgesetz üblicherweise nicht gilt. Als Folge dessen besitzt auch Gauß' Lemma in vielen Ore-Polynomringen keine Gültigkeit, so dass das Produkt zweier primitiver Ore-Polynome nicht notwendigerweise primitiv ist. Diese Beobachtung führt zu der Unterscheidung von entfernbaren und nicht-entfernbaren Faktoren und dem Studium desingularisierender Operatoren.

Als Desingularisierung bezeichnet man das Problem, ein Linksvielfaches eines gegebenen Ore-Operators zu finden, bei dem ein Faktor des führenden Koeffizienten des Ausgangsoperators entfernt wurde. Neben der Herleitung einer Normalform für solche Linksfaktoren vereinen wir auch bekannte Ergebnisse für Differential- und Shiftoperatoren in einem Desingularisierungsalgorithmus. Danach wenden wir uns den Auswirkungen zu, die entfernbare und nicht-entfernbare Faktoren bei Rechnungen mit Ore-Operatoren haben können.

Die Menge von Operatoren einer Ore-Algebra, die, angewandt auf eine gegebene Funktion, Null ergeben, bilden ein Linksideal. Die Kosten zur Berechnung eines Elements in diesem Ideal hängen von der Größe der Koeffizienten (dem Grad) sowie der Ordnung des Operators ab. Um diese Kosten vorhersagen oder reduzieren zu können, bestimmen wir eine Ordnungs-Grad-Kurve. Für einen gegebenen Operator ist dies eine Kurve in der (r, d)-Ebene, so dass die Existenz eines Linksvielfachen von Ordnung r und Grad d für alle Paare (r, d) oberhalb der Kurve garantiert ist. Wir zeigen, wie das Problem der Desingularisierung zur Bestimmung von Ordnungs-Grad-Kurven herangezogen werden kann, welche in vielen Beispielen von herausragender Genauigkeit sind. Für erzeugende Elemente von Idealen aus Anwendungsfällen, wie etwa der Physik oder der Kombinatorik, ist die Schranke in aller Regel scharf.

Das erzeugende Element eines Linksideals in einem Ore-Polynomring ist der größte gemeinsame Rechtsteiler der Idealelemente und kann mithilfe des Euklidischen Algorithmus berechnet werden. Polynomielle Restefolgen

enthalten die Zwischenergebnisse, die bei der Anwendung des Euklidischen Algorithmus auf (nicht-)kommutative Polynome auftreten. Die Laufzeit des Algorithmus ist von der Größe der Koeffizienten der Reste abhängig. Es wurden verschiedene Wege untersucht, um diese so klein wie möglich zu halten. Die Subresultantenfolge zweier Polynome ist eine polynomielle Restefolge, in der die Größe der Koeffizienten im generischen Fall optimal, bei Berechnungen in Anwendungen jedoch oft größer als notwendig ist. Wir verallgemeinern zwei Optimierungen der Subresultantenfolge auf Ore-Polynome und zeigen, in welcher Weise die nicht-entfernbaren Faktoren des größten gemeinsamen Rechtsteilers als Inhalt der Reste auftreten. Basierend auf diesem Resultat beschreiben wir, wie dieser Inhalt während der Ausführung des Euklidischen Algorithmus entfernt werden kann und wir geben außerdem eine neue Schranke für die minimale Koeffizientengröße der Reste an. Unser Ansatz führt uns auch zu einem neuen Beweis im kommutativen Fall und erlaubt uns so neue Einsichten bezüglich des Ursprungs der irrelevanten Faktoren der Restekoeffizienten.

Acknowledgements

This thesis reflects the work of three years together with Manuel Kauers and it is hard to imagine I could have found a better adviser. I greatly benefited from his immense knowledge in mathematics, scientific research, programming and LaTeX. He gave me the feeling of being his colleague rather than his student while still teaching me countless valuable skills and I hope we will find the opportunity to work together in the future.

By Manuel I was introduced to many great mathematicians in the symbolic computation community whose helpful input is present in large parts of my work. Discussions with Christoph Koutschan, Ziming Li, Michael Singer and Shaoshi Chen often gave me new insight to problems and pointed me towards their solutions.

This work was supported by the Austrian Science Fund (FWF) grant Y464-N18 and the strategic program 'Innovatives OÖ 2010' by the Upper Austrian Government.

During my time in Linz I made many new friends I really wouldn't want to miss. For all the great times and all the encouragement and help, thank you Jakob, Hamid, Zaf, Nebiye, Yongjae, Matteo, Cevo, Madalina, Manuela, Rika and many more who will never read this anyway.

Most importantly I want to thank my family for always supporting me and making my life awesome. I want to dedicate this work to my parents: My father, who I wish could have read this, is my role model and it makes me happy to think that he would have been the proudest father in the world, had he ever known. With her neverending care and love, my mother is the main reason why I was able to achieve all this. Thank you.

All sentimentality aside, I want to add: Oh yeah!

Contents

Chapter 1

Introduction

In combinatorics, a problem which one might face frequently is the following: assume we are given a combinatorial description of a number sequence. This description might be something in the vein of

- Given a stepset in $\mathbb{N}^3$ and an $n \in \mathbb{N}$, how many paths of length n are there that do not leave the octant $\mathbb{N}^3$?
- Given an algorithm and an input of size n, how many elementary operations are performed during the execution of the algorithm?

Most often, the answer to such questions can be given in form of a holonomic function. In the univariate case, with which we are concerned in this thesis, an object is called holonomic if it satisfies a linear functional equation with polynomial coefficients, for instance a recurrence relation or a differential equation. This class of objects contains many functions and sequences that arise from a diverse range of applications. The Gaussian hypergeometric function, the error function, the gamma function, trigonometric functions, exp and log are only some of the prime examples. Salvy [45] estimated that around 65% of the entries in Abramowitz/Stegun [4] as well as some 25% of the entries in Sloane's Online Encyclopedia of Integer Sequences [49] are holonomic.

Holonomic functions proved themselves particularly useful in the area of computer algebra which deals with special functions and combinatorial sequences. The algebraic properties satisfied by the class of holonomic functions allow the design of a number of algorithms that solve many problems related to this class. In [50], Stanley shows that the class of holonomic objects is closed under several operations, including addition and multiplication, by giving constructive proofs. In the multivariate setting, holonomy is also preserved under definite summation and integration, which was proven by Zeilberger in [57], where he also gives algorithms to execute those operations. These and other algorithms for holonomic functions lead to solutions of difficult problems in many scientific contexts, e.g. [36, 11, 7]. Among

others, such problems include the analysis of the asymptotic behavior of holonomic sequences [55], proving holonomic function identities [46, 19, 20], solving definite summation and integration problems [54, 56, 18, 34] and finding solutions to linear functional equations [44, 48].

To handle holonomic objects algorithmically, one needs to be able to represent them with a finite amount of data. Such a representation is given by Ore operators, elements of non-commutative polynomial rings called Ore algebras (formal definitions will be given later in Chapter 3). Under suitable circumstances, a holonomic object is uniquely determined by a single (non-zero) operator that maps it to zero, plus a certain finite number of initial values. The converse, however, does not hold. For a given holonomic object, there are infinitely many Ore operators in a fixed Ore algebra, called annihilating operators, that map the object to zero.

Depending on the particular computational problem at hand, certain operators may be better than others. Often, the best choice is an operator of minimal possible order, because any higher order operator would only slow down the calculation.

Sequences that are represented by a linear recurrence with polynomial coefficients are asymptotically equivalent to linear combinations of a certain generalized series which can be obtained from the recurrence. This means that in order to get useful information about the asymptotic behavior of a sequence, a promising approach is to look at these generalized series obtained from a least order operator. Operators of higher orders usually contain additional useless series that make this task much more difficult. [23]

Differential operators can be used to prove that two functions are equal. Equality holds if both functions satisfy the same differential equation and share the same initial values. The number of initial values that have to be checked depends on the order of the differential equation, so for lower order differential equations, fewer initial values have to be computed. As an example, one might try to prove

$$\int_{-\infty}^{\infty} f(x,t)dt = F(x),$$

for given complex functions $f(x,t)$ and $F(x)$. If these functions are of a particular kind, one can compute a differential equation for the left hand side by using the method of creative telescoping introduced by Zeilberger in [5]. Such a differential equation might be of order 3 and if $F(x)$ is also a solution of this differential equation, it has to be shown that the first three initial values agree to prove the identity. If there exists a second order differential equation for both sides of the equation, only two initial values have to be computed, which might be considerably easier.

On the other hand, if the output of some algorithm is an Ore operator, it is sometimes possible to gain speed by computing not the minimal order operator but one with slightly higher order and polynomial coefficients of

much smaller degree. Such improvements recently been reported for several different contexts [9, 10, 16, 17].

Deriving and proving a recurrence for a given sequence from its combinatorial description can be a difficult task. Instead, one can try to guess a recurrence operator for the sequence [29]. Given finitely many terms of a holonomic sequence, one can set up a linear system for the undetermined coefficients of a recurrence operator that should give zero when applied to the terms and try to find a non-zero solution to it. The degrees of freedom one has in this process are choosing the order of the recurrence and the degree of its polynomial coefficients. These cannot be chosen to be arbitrarily high, but the number of known terms of the sequence limits the size of the product $\mathit{order} \times \mathit{degree}$. If one wants to find a least order operator by this method, the number of equations in the linear system can be considerably high and providing the necessary amount of data might not be possible, or at least not feasible. Consider for example data from a combinatorial problem where the only known method to compute new data is of exponential complexity. Or an integer sequence from a computation in physics where there is enough data available, but the resulting linear system is too big to be solvable in a justifiable amount of time.

The need for lowest order as well as higher order operators shows the importance of the ability to convert a minimal order description into a non-minimal order description of lower degree, and vice versa. These shall be the two main problems we address in this thesis.

We start in Chapter 2 by recalling basic facts and definitions from (non-) commutative algebra. After that, we give the definition of Ore Algebras in Chapter 3. These non-commutative polynomial rings can not only be used to model recurrences and differential equations, but also many other functional equations. We will see how Ore operators act on a given set of functions and how to compute intersections and sums of solutions spaces of different operators. Two particular Ore algebras will be discussed in more detail – the ring of linear recurrence equations and the ring of linear differential equations with polynomial coefficients. [42, 12, 27, 32]

As an effect of the non-commutative multiplication, some statements that hold for commutative polynomials do not carry over to Ore polynomials. The fact that Gauß' lemma does not hold for Ore polynomials, i.e. that the product of two primitive Ore polynomials can be non-primitive, leads us to the problem of desingularization, which we treat in Chapter 4. Desingularization is the process of removing some factors of the leading coefficient of a given operator, called removable singularities, by multiplying it with another operator from the left. We study which factors qualify as removable, what a left factor needed to remove a singularity looks like, and how to construct it algorithmically. The basic algorithm will be stated for general Ore algebras, but two bounds that are required as input will be derived specifically for shift operators and differential operators. [3, 1, 52, 15]

We will use this knowledge to deal with the two problems mentioned above. In Chapter 5, we show how we can use desingularization to derive order-degree bounds for left operator ideals. These bounds will allow us to identify order-degree pairs for which we can expect an annihilating operator for a given holonomic object and it will also show why increasing the order of an operator might be helpful to speed up certain computations. In several examples we will see that the bounds are extremely accurate in applications. [15]

Finally, in Chapter 6, we aim to optimize the computation of the greatest common right divisor of two Ore polynomials with the Euclidean algorithm. The running time of the algorithm depends on the size of the coefficients of the intermediate results. If these are not primitive, the computation is slowed down by the unnecessary content. For commutative polynomials as well as for non-commutative operators, different methods have been extensively studied to find factors of the content in the sequence of remainders without computing the GCD of the coefficients of each element of the sequence [13, 14, 22, 41, 40]. Most notably in this respect are subresultant sequences, where the growth of the coefficients can be reduced from exponential to linear in the number of reduction steps in the Euclidean algorithm. When taking as input operators coming from applications like combinatorics or physics, the remainders in the subresultant sequence still have non-trivial content in many cases. We generalize two known improvements to Ore polynomials and we show that the non-removable singularities of the greatest common right divisor of the input is responsible for the extra content. [28]

Chapter 2

Preliminaries

This chapter is a recapitulation of basic concepts that will be used throughout the thesis. These topics are well known and, concerning commutative domains, covered in almost any (computer-)algebra textbook like [24] or [53]. For this reason we mostly refrain from giving proofs of the statements presented here. An introduction to non-commutative rings can be found in [37, 21].

2.1 Domains

Let $\mathbb{D}$ be a computable domain, i.e. a not necessarily commutative computable ring with an identity element and without zero divisors. A domain is called *principal left (right) ideal domain*, if every left (right) ideal is generated by a single element. Such a domain is called *principal ideal domain* if it is commutative. For $a, b \in \mathbb{D}$, we say *a divides b on the right* and write $a \mid_r b$ if there is a $c \in \mathbb{D}$ such that $b = ca$. Analogously, *a divides b on the left* ($a \mid_l b$) if $b = ac$ and *a divides b* ($a \mid b$) if $a \mid_r b$ and $\mathbb{D}$ is commutative. In this section, we allow ourselves to drop the adjectives 'left' and 'right' outside of formal definitions and theorems, only assuming commutativity if explicitly stated. A generator of an ideal in a principal ideal domain is given by the greatest common divisor of the ideal elements:

Definition 2.1.1. Let $\mathbb{D}$ be a domain and $a, b \in \mathbb{D}$. A *greatest common right divisor* (GCRD) for a and b is an element $g \in \mathbb{D}$ such that

1. $g \mid_r a$ and $g \mid_r b$.
2. If condition 1. holds for some other $g' \in \mathbb{D}$, then $g' \mid_r g$.

Greatest common left divisors (GCLDs) and – if $\mathbb{D}$ is commutative – *greatest common divisors* (GCDs) are defined analogously.

Two elements $a, b \in \mathbb{D}$ are called *left associates* if there exists a unit $u \in \mathbb{D}$ such that $a = ub$. This is an equivalence relation and if we fix

a set of representatives of the equivalence classes, then an element of $\mathbb{D}$ is called *unit normal* (with respect to left associates) if it is equal to the representative of its equivalence class. The unique unit normal (w.r.t. left associates) greatest common right divisor $\operatorname{gcrd}(a, b)$ of $a, b \in \mathbb{D}$ is called *the* greatest common right divisor of a and b and we define the greatest common left divisor $\operatorname{gcld}(a, b)$ (unit normal w.r.t. right associates) as well as the greatest common divisor $\gcd(a, b)$ (unit normal w.r.t. associates) in commutative domains accordingly. Two elements of a commutative domain are called *coprime* if their GCD is a unit.

Example 2.1.2. In $\mathbb{Z}$, one usually defines the unit normal elements to be the non-negative integers. A greatest common divisor of -12 and 18 is -6, but the unit normal GCD is 6.

While two elements always have a greatest common (left or right) divisor in a principal (left or right) ideal domain, we might not necessarily be able to compute it. An algorithm for GCD computation is available, if the domain is such that we can perform division with remainder:

Definition 2.1.3. A domain $\mathbb{E}$ is called a *left Euclidean domain* if there exists a function $\deg : \mathbb{E} \setminus \{0\} \to \mathbb{N}$, called *degree function*, such that

1. For all $a, b \in \mathbb{E} \setminus \{0\}$: $\deg(ab) \geq \deg(a)$.
2. For all $a, b \in \mathbb{E}$ with $b \neq 0$ there exist $q, r \in \mathbb{E}$ such that

$$a = qb + r, \quad \text{with } \deg(r) < \deg(b) \text{ or } r = 0. \tag{2.1.1}$$

We call q the *left quotient* $\operatorname{lquo}(a, b)$ of a and b and r their *left remainder* $\operatorname{lrem}(a, b)$. In the commutative case we say *quotient* $\operatorname{quo}(a, b)$ and *remainder* $\operatorname{rem}(a, b)$ respectively and for right Euclidean domains, (2.1.1) is changed to $a = bq + r$ and q is the *right quotient* $\operatorname{rquo}(a, b)$ and r the *right remainder* $\operatorname{rrem}(a, b)$.

As indicated by the use of the definite article in Definition 2.1.3, quotients and remainders are uniquely determined by a and b. We always assume that $\operatorname{lquo}(a, b)$, $\operatorname{rrem}(a, b)$ etc. are computable.

The *Euclidean algorithm* (Algorithm 2.1.1) takes two elements of a Euclidean domain as input and computes an associate of their GCD by iterated division with remainder. It relies on the fact that in a Euclidean domain any common divisor of two elements is also a divisor of their remainder.

A very useful representation of the GCD of two elements a, b of a principal ideal domain is given by a linear combination of a and b. Let $\mathbb{P}$ be a principal left ideal domain. For any $a, b \in \mathbb{P}$ there exist $s, t \in \mathbb{P}$ such that

$$sa + tb = \operatorname{gcrd}(a, b). \tag{2.1.2}$$

Algorithm 2.1.1: Euclidean algorithm (left division)

Input: a, b, elements of a left Euclidean domain.
Output: g such that $g = u \cdot \mathrm{gcrd}(a, b)$ for a unit u.

$(r_0, r_1) \leftarrow (a, b)$
$i \leftarrow 1$
WHILE $r_i \neq 0$:
    $r_{i+1} \leftarrow \mathrm{lrem}(r_{i-1}, r_i)$
    $i \leftarrow i + 1$
RETURN r_{i-1}

The elements s and t are called *Bézout coefficients* of a and b and are not necessarily unique (see Sections 6.1 and 6.2). For principal right ideal domains, (2.1.2) changes to:

$$as + bt = \mathrm{gcld}(a, b).$$

In Euclidean domains, a pair of Bézout coefficients can be computed by the *extended Euclidean algorithm* (EEA, Algorithm 2.1.2).

Algorithm 2.1.2: Extended Euclidean algorithm (left div.)

Input: a, b, elements of a left Euclidean domain.
Output: g, s, t such that $g = u \cdot \mathrm{gcrd}(a, b)$ for a unit u and $g = sa + tb$.

$(r_0, r_1) \leftarrow (a, b)$
$(s_0, t_0, s_1, t_1) \leftarrow (1, 0, 0, 1)$
$i \leftarrow 1$
WHILE $r_i \neq 0$:
    $(r_{i+1}, q_i) \leftarrow (\mathrm{lrem}(r_{i-1}, r_i), \mathrm{lquo}(r_{i-1}, r_i))$
    $(s_{i+1}, t_{i+1}) \leftarrow (s_{i-1} - q_i s_i, t_{i-1} - q_i t_i)$
    $i \leftarrow i + 1$
RETURN $(r_{i-1}, s_{i-1}, t_{i-1})$

Every (left or right) Euclidean domain is a principal (left or right) ideal domain. In the commutative case, elements of a Euclidean domain have a *unique prime decomposition*: An element p of a commutative domain $\mathbb{U}$ is called *prime* if it is a non-zero non-unit and whenever p divides ab for some $a, b \in \mathbb{U}$, then either a or b is divisible by p. An element p of a (commutative) domain that can be written as $p = ab$ if only if a or b is a unit is called *irreducible*. Every prime element is also irreducible but not necessarily vice versa. $\mathbb{U}$ is a *unique factorization domain* if all non-zero non-units can be expressed as a finite product of prime elements uniquely up to order and associates. Every commutative Euclidean domain is a unique factorization domain. We will see in Chapter 3 that this is not true in the non-commutative setting.

In principal (left or right) ideal domains, also the existence of least common (left or right) multiples is guaranteed:

Definition 2.1.4. Let $\mathbb{D}$ be a domain and $a, b \in \mathbb{D}$. A *least common left multiple* (LCLM) for a and b is an element $m \in \mathbb{D}$ such that

1. $a \mid_r m$ and $b \mid_r m$.

2. If condition 1. holds for some other $m' \in \mathbb{D}$, then $m \mid_r m'$.

The unique unit normal (w.r.t. left associates) least common left multiple $\operatorname{lclm}(a, b)$ of a, b is called *the* least common left multiple of a and b. *Least common right multiples* (LCRMs) and *least common multiples* (LCMs) for commutative domains as well as their unique unit normal associates $\operatorname{lcrm}(a, b)$ and $\operatorname{lcm}(a, b)$ are defined analogously.

The LCLM of two elements of a left Euclidean domain $\mathbb{E}$ can be computed by the extended Euclidean algorithm. When applied to $a, b \in \mathbb{E}$, the last iteration of the while loop in Algorithm 2.1.2 will give nonzero $s, t \in \mathbb{E}$ such that

$$sa + tb = 0,$$

and thus $m := sa$ is a common left multiple of a and b. It can be shown that m is a least common left multiple of a and b (see [12]).

For $n \in \mathbb{N}$ and a domain $\mathbb{D}$ with $\mathbb{Z} \subset \mathbb{D}$, the nth *falling factorial* of $a \in \mathbb{D}$ is $a^{\underline{n}} := \prod_{i=0}^{n-1}(a - i)$ and analogously, the *rising factorial* is $a^{\overline{n}} := \prod_{i=0}^{n-1}(a + i)$.

2.2 Commutative Polynomials

The ring of polynomials in y over a commutative domain $\mathbb{D}$ is denoted by $\mathbb{D}[y]$ and we refer to the leading coefficient of a polynomial $p \in \mathbb{D}[y]$ as $\operatorname{lc}(p)$, to the trailing coefficient of p as $\operatorname{tc}(p)$, to the ith coefficient of p as $[y^i]p$ and to $i \in \mathbb{N}$ with $[y^i]p = \operatorname{lc}(p)$ as the degree $\deg(p)$ of p (with $\deg(0) := -\infty$). Note that $\operatorname{lc}(p) \neq 0$ and $\operatorname{tc}(p) \neq 0$ for all $p \neq 0$. If $\mathbb{D}$ is a unique factorization domain, then so is $\mathbb{D}[y]$ and if $\mathbb{D}$ is a field, then $\mathbb{D}[y]$ is a Euclidean domain. In the latter case, division with remainder can be done algorithmically: Let $a, b \in \mathbb{D}[y]$ with $\deg(a) \geq \deg(b) \geq 0$ and let $d := \deg(a) - \deg(b)$. We set

$$\left.\begin{aligned} a_0 &= a, \\ q_{d-i} &= \frac{\operatorname{lc}(a_i)}{\operatorname{lc}(y^{d-i}b)}, \\ a_{i+1} &= a_i - q_{d-i}b, \end{aligned}\right\} \text{ for } 0 \leq i \leq d. \tag{2.2.1}$$

Then with $q := q_d y^d + q_{d-1} y^{d-1} + \cdots + q_0$ and $r := a - qb$ we have $\deg(r) < \deg(b)$ or $r = 0$ by construction.

When given the notion of unit normal elements in the ground domain, we can define unit normal elements in polynomial rings in a straightforward fashion. If $\mathbb{D}$ is not a fraction field, a polynomial in $\mathbb{D}[y]$ is called unit normal if its leading coefficient is unit normal. In the case that $\mathbb{K}$ is a fraction field of some fixed domain $\mathbb{D}$, a polynomial in $\mathbb{K}[y]$ is unit normal if its coefficients are fraction free and coprime in $\mathbb{D}$ and its leading coefficient is unit normal in $\mathbb{D}$.

Example 2.2.1. (Example 2.1.2 cont.) If we define unit normal integers like in Example 2.1.2, then $3y^2 - 8y + 1 \in \mathbb{Z}[y]$ is unit normal, but $-2y + 1$ is not. The unit normal equivalent of $4y^2 + \frac{8}{3} \in \mathbb{Q}[y]$ is $3y^2 + 2$.

For polynomial rings $\mathbb{P}[y]$ over a principal ideal domain $\mathbb{P}$, the greatest common divisor of the coefficients of a polynomial $p \in \mathbb{P}[y]$ is called the *content* $\operatorname{cont}(p)$ of p and p is called *primitive* if $\operatorname{cont}(p)$ is a unit. There exists a unique representation of p of the form

$$p = \operatorname{cont}(p)\tilde{p},$$

where the primitive polynomial $\tilde{p}$ is the *primitive part* $\operatorname{pp}(p)$ of p. The set of primitive polynomials over $\mathbb{D}$ is closed under multiplication:

Theorem 2.2.2 (Gauß' Lemma)**.** *The product of two primitive polynomials is again primitive.* □

The following corollary, which is an immediate consequence of Theorem 2.2.2, will play a crucial role in our subsequent considerations.

Corollary 2.2.3. *Let $\mathbb{K}$ be the fraction field of a principal ideal domain $\mathbb{P}$ and $a, b, q \in \mathbb{K}[y]$ such that*

$$a = qb.$$

If a and b are elements of $\mathbb{P}[y]$ with b being primitive in $\mathbb{P}[y]$, then also $q \in \mathbb{P}[y]$.

Proof. Assume $q \in \mathbb{K}[y] \setminus \mathbb{P}[y]$. Let d be the common denominator of the coefficients of q and c the content of dq in $\mathbb{P}[y]$. Then a/c is an element of $\mathbb{P}[y]$ because dqb is divisible by cd. We get

$$\underbrace{d\left(\frac{a}{c}\right)}_{\in\mathbb{P}[y]} = \underbrace{\left(\frac{dq}{c}\right)}_{\in\mathbb{P}[y]} b.$$

Both b and dq/c are primitive, so by Theorem 2.2.2, also da/c has to be primitive, but $\operatorname{cont}(da/c) = d$. □

It is the fact that Theorem 2.2.2 and Corollary 2.2.3 do in general not carry over to Ore polynomials that leads to the distinction of removable and non-removable singularities, as we will see in the next chapters.

Chapter 3

Ore Polynomial Rings

3.1 Basic Definitions and Properties

3.1.1 Ore Polynomial Rings

Ore polynomial rings were introduced by Øystein Ore in the 1930s. They provide a general framework for working with several different kinds of functional equations in an algebraic context and most often are the method of choice when dealing with objects like differential or recurrence equations in symbolic computation. In this section, we motivate and state some of their basic properties. For more details on the theory presented here, the interested reader is referred to [42] and [12], where most of the definitions and theorems of this section can be found unless stated otherwise. All the results in this chapter are classical and well known except for the observation that leads to Example 3.1.13.

Before we give a formal definition, let's look at a differential equation of the form:

$$a_r(y)f^{(r)}(y) + a_{r-1}(y)f^{(r-1)}(y) + \cdots + a_1(y)f'(y) + a_0(y)f(y) = 0, \quad (3.1.1)$$

where $r \in \mathbb{N}$ and the a_i are elements of $\mathbb{K}(y)$ for some field $\mathbb{K}$. The corresponding *Ore polynomial* (or *Ore operator*) is obtained by taking the left hand side of the equation and replace the ith derivative by ∂^i, where ∂ is a new indeterminate. This gives a polynomial A in ∂ with coefficients in $\mathbb{K}(y)$:

$$A = a_r\partial^r + a_{r-1}\partial^{r-1} + \cdots + a_1\partial + a_0. \quad (3.1.2)$$

We let such polynomials act on suitable functions in a natural way by defining $A(f)$ to be equal to the left hand side of equation (3.1.1). In the case of $A(f)$ being zero, we say that A *annihilates* f, that A is an *annihilator* of f and that f is a *solution* of A.

We will turn the set of all polynomials of the form (3.1.2) into a ring by equipping it with two operations, $+$ and $\cdot$. The addition will be defined

coefficientwise, so that it corresponds to the addition of equations: Let A and B be two operators and let f, g_A, g_B be functions such that $A(f) = g_A$ and $B(f) = g_B$. Then

$$(A + B)(f) = A(f) + B(f) = g_A + g_B.$$

The multiplication will be defined in such a way that it corresponds to the composition of operators: Let A and B be two operators and let f, g_A, g_B be functions such that $B(f) = g_B$ and $A(g_B) = g_A$. Then we want to have

$$(A \cdot B)(f) = A(B(f)) = A(g_B) = g_A.$$

The following definition formalizes this approach and generalizes it to other kinds of functional equations.

Definition 3.1.1. Let $\mathbb{D}$ be a commutative domain, $\mathbb{D}[X]$ the set of univariate polynomials over $\mathbb{D}$ and let $\sigma\colon \mathbb{D} \to \mathbb{D}$ be an injective endomorphism.

1. A map $\delta\colon \mathbb{D} \to \mathbb{D}$ is called *pseudo-derivation* (with respect to σ), if for all $a, b \in \mathbb{D}$

$$\delta(a + b) = \delta(a) + \delta(b) \quad \text{and} \quad \delta(ab) = \sigma(a)\delta(b) + \delta(a)b.$$

2. Let δ be a pseudo-derivation. We define the *Ore polynomial ring* $(\mathbb{D}[X], +, \cdot)$ with componentwise addition and the unique distributive and associative extension of the multiplication rule

$$Xa = \sigma(a)X + \delta(a) \qquad \text{for all } a \in \mathbb{D},$$

to arbitrary polynomials in $\mathbb{D}[X]$. To clearly distinguish this ring from the commutative polynomial ring over $\mathbb{D}$, we denote it by $\mathbb{D}[X; \sigma, \delta]$.

3. The set $\operatorname{const}(\mathbb{D}[X; \sigma, \delta]) := \{c \in \mathbb{D} \mid \sigma(c) = c \text{ and } \delta(c) = 0\}$ is the *set of constants* of $\mathbb{D}[X; \sigma, \delta]$.

An Ore polynomial ring is an algebra over its base ring, so we use the terms Ore algebra and Ore (polynomial) ring synonymously. Operators are denoted by capital letters and the ith coefficient of an operator by the corresponding lower case letter together with the index i. In general we adapt the basic notation used for polynomials – e.g. we refer to the leading coefficient of an operator A as $\operatorname{lc}(A)$ – the only exception being the polynomial degree of A in X to which we will refer as the order $\operatorname{ord}(A)$ of A. (also written as d_A.) For $a \in \mathbb{D}$ and $n \in \mathbb{N}$, we call $\sigma^n(a)$ the nth *shift* of a. For negative integers n, the nth shift is defined as the element $b \in \mathbb{D}$ for which $\sigma^{-n}(b) = a$, provided that such an element exists. From now on, $\mathbb{D}$ will be a commutative domain and $\mathbb{K}$ a field, unless otherwise stated.

Since we will often encounter products of consecutive shifts of base ring elements, we introduce the following shorthand notation to improve readability and tangibility.

Definition 3.1.2. Let $\mathbb{D}[X;\sigma,\delta]$ be an Ore polynomial ring and $n \in \mathbb{N}$. The nth *σ-factorial* of $a \in \mathbb{D}$ is defined as the product

$$a^{[n]} := \prod_{i=0}^{n-1} \sigma^i(a).$$

It is possible to extend $\mathbb{D}[X;\sigma,\delta]$ to an Ore polynomial ring over the quotient field $\mathbb{K}$ of $\mathbb{D}$ by setting $\sigma(a^{-1}) = \sigma(a)^{-1}$ and $\delta(a/b) = (b\delta(a) - a\delta(b))/(b\sigma(b))$ for $a, b \in \mathbb{D}$, $b \neq 0$ (see [39]). We will denote this ring by $\mathbb{K}[X;\sigma,\delta]$ without making it explicit that the automorphism and the pseudo-derivation are extensions of the functions used in $\mathbb{D}[X;\sigma,\delta]$. Later on, the distinction of operators in $\mathbb{D}[X;\sigma,\delta]$ and operators in $\mathbb{K}[X;\sigma,\delta] \setminus \mathbb{D}[X;\sigma,\delta]$ will be an important aspect of this work. Our study will mostly be concerned with the *contraction* of the *extension* of a left ideal $\mathcal{I}$ in $\mathbb{D}[X;\sigma,\delta]$. The extension is the smallest left ideal $\mathcal{I}'$ in $\mathbb{K}[X;\sigma,\delta]$ that contains $\mathcal{I}$ and the contraction then is the intersection of $\mathcal{I}'$ and $\mathbb{D}[X;\sigma,\delta]$. We will see in Chapter 4 that the contraction of $\mathcal{I}'$ is usually not equal to $\mathcal{I}$.

Example 3.1.3. Commonly used Ore polynomial rings are:

1. $\mathbb{D}[X] = \mathbb{D}[X;1,0]$, the ring of commutative polynomials over $\mathbb{D}$.
2. If $s_n\colon \mathbb{K}[n] \to \mathbb{K}[n]$ is the forward shift in n, i.e. $s_n(a(n)) = a(n+1)$, then $\mathbb{K}[n][S;s_n,0]$ is the ring of linear ordinary recurrence operators. (see Section 3.2.1.)
3. $\mathbb{K}[y][\partial;1,\frac{d}{dy}]$, the ring of linear ordinary differential operators. (see Section 3.2.2.)
4. If $s_{q,y}\colon \mathbb{K}(q)(y) \to \mathbb{K}(q)(y)$ is the q-shift in y, i.e. $s_{q,y}(a(y)) = a(qy)$, then $\mathbb{K}(q)(y)[S_q;s_{q,y},0]$ is the ring of linear ordinary q-shift operators.
5. If $s_{q,y}$ is as in 4. then $\mathbb{K}(q)(y)[J;s_{q,y},\frac{d}{dy}]$ is the ring of q-differential operators.

We only consider univariate operators, meaning that we have Ore rings $\mathbb{D}[X;\sigma,\delta]$ where the ring extension $\mathbb{D}[X;\sigma,\delta]/\mathbb{D}$ is generated by only one element X. A comprehensive introduction to the multivariate case can be found in [34].

3.1.2 Actions and Solutions

As already mentioned above, we assume that Ore algebras come equipped with an action on a suitable class of functions such that the multiplication of operators corresponds to their composition and that the action is linear with respect to addition. We let the set of objects $\mathcal{F}$ on which an operator can act be a $\mathbb{D}$-module. While formally module elements are not necessarily

functions, we will still refer to them as such in order to simplify terminology. Taking $\mathcal{F}$ as a $\mathbb{D}$-module allows us to form linear combinations of elements of $\mathcal{F}$ over $\mathbb{D}$ and applying an operator A on a function f yields such a linear combination of the images $X^i(f) \in \mathcal{F}$. The action of A on f therefore is completely specified by the action of the monomial X on the elements of $\mathcal{F}$.

Definition 3.1.4. Let $\mathbb{D}[X;\sigma,\delta]$ be an Ore polynomial ring and let $\mathcal{F}$ be a $\mathbb{D}$-module. A map $\tau : \mathcal{F} \to \mathcal{F}$ is called $\mathbb{D}$-*pseudo linear* (with respect to σ and δ) if for all $a \in \mathbb{D}$ and $f, g, \in \mathcal{F}$:

$$\tau(f+g) = \tau(f) + \tau(g) \qquad \text{and} \qquad \tau(af) = \sigma(a)\tau(f) + \delta(a)f.$$

Given an operator $A = \sum_{i=0}^{d_A} a_i X^i$ from an Ore ring $\mathbb{D}[X;\sigma,\delta]$ that comes with a $\mathbb{D}$-pseudo linear map τ, the action on $f \in \mathcal{F}$ then is defined as

$$A(f) := \sum_{i=0}^{d_A} a_i \tau^i(f).$$

Example 3.1.5. Let $\mathcal{F}$ be the set of all analytic functions $\mathbb{C} \to \mathbb{C}$. It can be easily checked that $\tau : \mathcal{F} \to \mathcal{F}$, $\tau(f(y)) \mapsto \frac{d}{dy} f(y)$, is a $\mathbb{C}[y]$-pseudo linear map with respect to $\sigma = 1$ and $\delta = \frac{d}{dy}$. Elements of $\mathbb{C}[y][\partial; 1, \frac{d}{dy}]$ then act on analytic functions as outlined in the beginning of this chapter.

Further Examples and more details on $\mathbb{D}$-pseudo linear maps will be presented in Section 3.2, where we will also see that it may be necessary to restrict $\mathcal{F}$ to a subclass when moving from $\mathbb{D}[X;\sigma,\delta]$ to $\mathbb{K}[X;\sigma,\delta]$, where $\mathbb{K}$ is the fraction field of $\mathbb{D}$.

It is easy to see that the set of constants of an Ore algebra $\mathbb{D}[X;\sigma,\delta]$ is a subring of $\mathbb{D}$ (or a subfield if $\mathbb{D}$ is a field) and that the set of solutions $V(A)$ of a given operator A is a module (vector space) over the constant ring (field) of $\mathbb{D}[X;\sigma,\delta]$. In case of the base ring being a field, the dimension of the solution space depends on how $\mathcal{F}$, the set of functions on which an operator can act, is chosen, but a classical argument shows that it is bounded by the order of the operator:

Theorem 3.1.6. *Let $\mathbb{K}[X;\sigma,\delta]$ be such that either $\sigma = 1$ or $\delta = 0$ and let $A \in \mathbb{K}[X;\sigma,\delta]$ be of order r. Then* $\dim(V(A)) \leq r$.

Proof. Let $A = \sum_{i=0}^{r} a_i X^i$ and $f_0, \ldots, f_r \in V(a)$. Then $(a_0, a_1, \ldots, a_r)$ is a non-zero solution of

$$\begin{pmatrix} f_0 & X(f_0) & \ldots & X^r(f_0) \\ f_1 & X(f_1) & \ldots & X^r(f_1) \\ \vdots & & & \vdots \\ f_r & X(f_r) & \ldots & X^r(f_r) \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_r \end{pmatrix} = 0,$$

so the rank of the matrix is less than $r+1$, which means that its rows are linearly dependent over $\mathbb{K}$. We have to show that they are linearly dependent over $\operatorname{const}(\mathbb{K}[X;\sigma,\delta]) \subset \mathbb{K}$. Because of their linear dependence over $\mathbb{K}$, there exists a subset $\{f'_0,\dots,f'_m\} \subset \{f_0,\dots,f_r\}$ for which the vectors $(f'_i, X(f'_i))$ with $0 \le i \le m$ are linearly dependent, but any proper non-empty subset is not. Let $c_i \in \mathbb{K}$ be such that

$$\begin{pmatrix} f'_0 \\ X(f'_0) \end{pmatrix} = \sum_{i=1}^{m} c_i \begin{pmatrix} f'_i \\ X(f'_i) \end{pmatrix}. \tag{3.1.3}$$

Comparing the image of the action on the first component on both sides of equation (3.1.3) gives

$$X(f'_0) = \sum_{i=1}^{m} X(c_i f'_i) = \sum_{i=1}^{m} \sigma(c_i)\tau(f'_i) + \sum_{i=1}^{m} \delta(c_i) f'_i,$$

and comparing the second component on both sides of the equation gives:

$$X(f'_0) = \sum_{i=1}^{m} c_i X(f'_i) = \sum_{i=1}^{m} c_i \tau(f'_i).$$

It follows that

$$\sum_{i=1}^{m} \sigma(c_i)\tau(f'_i) + \sum_{i=1}^{m} \delta(c_i) f'_i = \sum_{i=1}^{m} c_i \tau(f'_i). \tag{3.1.4}$$

If $\sigma = 1$, then this simplifies to

$$\sum_{i=1}^{m} \delta(c_i) f'_i = 0.$$

Since the f'_i with $i \neq 0$ are linearly independent, all the $\delta(c_i)$ have to be equal to 0. In the case of $\delta = 0$, (3.1.4) reduces to

$$\sum_{i=1}^{m} (\sigma(c_i) - c_i)\tau(f'_i) = 0,$$

and again by the linear independence of the f'_i $(i \neq 0)$ we get that $\sigma(c_i)$ is equal to c_i for all i. In both cases it follows that the c_i are elements of the constant field, and so the f'_i, including f'_0, are linearly dependent over $\operatorname{const}(\mathbb{K}[X;\sigma,\delta])$. □

While at first glance the conditions in Theorem 3.1.6 on σ and δ seem rather restrictive, we can always assume without loss of generality that they are satisfied. The next theorem describes how to map operators into a new Ore algebra where only σ is non-trivial and how to define an action for the new algebra such that the solution space of an operator does not change.

Theorem 3.1.7 ([2]). *Let $\mathbb{K}[X;\sigma,\delta]$ be an Ore algebra and let $b \in \mathbb{K}$ be such that $\sigma(b) \neq b$. Then the map*

$$H_b : \mathbb{K}[X;\sigma,\delta] \to \mathbb{K}[Y;\sigma,0], \quad H_b\left(\sum_{i=0}^{r} a_i X^i\right) = \sum_{i=0}^{r} a_i \left(\frac{Y+\delta(b)}{b-\sigma(b)}\right)^i,$$

is a ring isomorphism. If the set of functions on which operators from $\mathbb{K}[X;\sigma,\delta]$ can act is given by $\mathcal{F}$, we set

$$\mu : \mathcal{F} \to \mathcal{F}, \quad \mu(f) = H_b^{-1}(Y)(f),$$

and let operators from $\mathbb{K}[Y;\sigma,0]$ act on $\mathcal{F}$ via μ. Then every solution of an operator $A \in \mathbb{K}[X;\sigma,\delta]$ is a solution of $H_b(A)$ and vice versa. □

3.1.3 GCRD and LCLM

The quotient and the remainder of two commutative polynomials over a field can be computed by the reduction algorithm presented in Chapter 2. The same algorithm can also be applied to Ore polynomials, again provided that the base ring is a field.

Theorem 3.1.8. *Every Ore polynomial ring $\mathbb{K}[X;\sigma,\delta]$ is a left Euclidean domain.* □

For computing the left remainder, note that in (2.2.1), the term $\mathrm{lc}(X^{d-i}b)$ is not equal to $\mathrm{lc}(b)$ but becomes $\sigma^{d-i}(\mathrm{lc}(b))$. From Theorem 3.1.8, the existence of the (extended) Euclidean algorithm for Ore polynomials and hence the existence of greatest common right divisors follows immediately. The greatest common right divisor of two operators A and B is an operator of maximal order that divides both A and B on the right. As mentioned in the preliminaries, it is unique up to left associates, i.e. up to left multiplication by non-zero elements of $\mathbb{K}$ and also right multiplication by non-zero elements of the constant field (which commute with the operators of the algebra).

Since the multiplication of Ore polynomials corresponds to operator composition, the solution space of any right hand factor of an operator A is a subspace of $V(A)$. This fact can be used to find common solutions of several Ore polynomials.

Theorem 3.1.9. *The solution space of the GCRD of two operators $A, B \in \mathbb{K}[X;\sigma,\delta]$ is the intersection of the solution spaces of A and B.*

Proof. Let G be the GCRD of A and B. Since there are $Q_A, Q_B \in \mathbb{K}[X;\sigma,\delta]$ with $A = Q_A G$ and $B = Q_B G$, the solution space of G is a subspace of $V(A)$ and $V(B)$. Therefore $V(G) \subset V(A) \cap V(B)$.
Now let f be a common solution of A and B. By the extended Euclidean algorithm we can find $S, T \in \mathbb{K}[X;\sigma,\delta]$ with $G = SA + TB$ and get:

$$G(f) = (SA)(f) + (TB)(f) = S(A(f)) + T(B(f)) = 0.$$

This shows $V(A) \cap V(B) \subset V(G)$. □

Definition 3.1.10. The smallest left ideal $I \lhd \mathbb{D}[X;\sigma,\delta]$ that contains all the annihilating operators of $f \in \mathcal{F}$ is called the *annihilating ideal* of f in $\mathbb{D}[X;\sigma,\delta]$.

Example 3.1.11. Two annihilating operators for $p(y) = 6y^2 + y + 4 \in \mathbb{Q}[y]$ are $L_1, L_2 \in \mathbb{Q}[y][\partial; 1, \frac{d}{dy}]$ with

$$L_1 = 95\partial^2 + (144y + 12)\partial - 288, \quad L_2 = \partial^3.$$

Since $p(y)$ is an element of the solution space of L_1 and the solution space of L_2, it is also contained in the solution space of $G := \operatorname{gcrd}(L_1, L_2)$. We have that

$$G = (6y^2 + y + 4)\partial - (12y + 1).$$

G is of order 1 and since $\mathbb{Q}[y]$ does not contain zero-divisors, there is no order 0 operator that annihilates $p(y)$. By computing the GCRD of L_1 and L_2, we obtained the least order annihilating operator for $p(y)$. It is the generator of the annihilating ideal of $p(y)$ in $\mathbb{Q}(y)[\partial; 1, \frac{d}{dy}]$.
Note that while this often works in practice, it need not be the case that the GCRD is the minimal order operator of a common solution of two or more operators. Consider

$$\begin{aligned}
L_3 = {} & (570y^2 + 95y + 380)\partial^3 + (864y^3 + 786y^2 + 1823y + 523)\partial^2 \\
& + (864y^3 + 216y^2 + 588y - 1092)\partial - (1728y^2 + 2016y + 1296), \\
L_4 = {} & (36y^4 + 12y^3 + 49y^2 + 8y + 16)\partial^4 \\
& + (36y^4 + 84y^3 + 67y^2 + 57y + 20)\partial^3 \\
& + (-72y^2 - 12y + 47)\partial^2 + (144y + 12)\partial - 144.
\end{aligned}$$

These two operators are also annihilators of $p(y)$, but their GCRD is of order 2:

$$\operatorname{gcrd}(L_3, L_4) = (6y^2 + y + 4)\partial^2 + (6y^2 + y + 4)\partial - (12y + 13).$$

In order to obtain an operator whose solution space is the span of $V(A)$ and $V(B)$, one can compute a least common left multiple of A and B, an operator of minimal order that is divisible by A and B from the right. As we have seen, this can be done by the extended Euclidean algorithm, which also yields that the order of $\operatorname{lclm}(A, B)$ is bounded by $\operatorname{ord}(A) + \operatorname{ord}(B)$.

Theorem 3.1.12. *Let $\mathbb{K}[X;\sigma,\delta]$ be an Ore algebra with an action defined on $\mathcal{F}$ and let $A, B \in \mathbb{K}[X;\sigma,\delta]$ be such that the dimension of $V(A)$ is equal to the order of A and the dimension of $V(B)$ is equal to the order of B. Then the solution space of* $\operatorname{lclm}(A, B)$ *is the span of the solution spaces of A and B.*

Proof. Let L be the LCLM of A and B and let $P_A, P_B \in \mathbb{K}[X;\sigma,\delta]$ be such that $L = P_A A = P_B B$. Consider a basis $\mathcal{B}_A = (u_0, \ldots, u_m)$ of $V(A)$ and a basis $\mathcal{B}_B = (v_0, \ldots, v_n)$ of $V(B)$. For any $c_0, \ldots, c_{n+m+1} \in \operatorname{const}(\mathbb{K}[X;\sigma,\delta])$ we have

$$\begin{aligned} &L(c_0u_0 + \cdots + c_mu_m + c_{m+1}v_0 + \cdots + c_{m+n+1}v_n) \\ &\quad = L(c_0u_0 + \cdots + c_mu_m) + L(c_{m+1}v_0 + \cdots + c_{m+n+1}v_n) \\ &\quad = P_AA(c_0u_0 + \cdots + c_mu_m) + P_BB(c_{m+1}v_0 + \cdots + c_{m+n+1}v_n) \\ &\quad = 0. \end{aligned}$$

This shows $V(A) + V(B) \subset V(L)$.
For $V(L) \subset V(A) + V(B)$, first assume that A and B have no common non-zero solutions. Then the bases $\mathcal{B}_A$ and $\mathcal{B}_B$ are disjoint and $\mathcal{B}_A \cup \mathcal{B}_B$ is a basis of $V(A) + V(B)$ with $\operatorname{ord}(A) + \operatorname{ord}(B)$ elements which are annihilated by L. The quotient P_A is computed by the extended Euclidean algorithm and thus its order is bounded by $\operatorname{ord}(B)$. For the order of L we have

$$\operatorname{ord}(L) = \operatorname{ord}(P_A) + \operatorname{ord}(A) \leq \operatorname{ord}(B) + \operatorname{ord}(A).$$

By Theorem 3.1.6, $\mathcal{B}_A \cup \mathcal{B}_B$ is a basis of $V(L)$.
If A and B have common non-zero solutions, they have a non-trivial GCRD $G \in \mathbb{K}[X;\sigma,\delta]$ and $\mathcal{B}_A$ and $\mathcal{B}_B$ can be chosen such that $\mathcal{B}_A \cap \mathcal{B}_B$ has cardinality $\operatorname{ord}(G)$. We show that the order of L is bounded by $\operatorname{ord}(A) + \operatorname{ord}(B) - \operatorname{ord}(G)$, which is the number of elements in $\mathcal{B}_A \cup \mathcal{B}_B$. Let $Q_A, Q_B \in \mathbb{K}[X;\sigma,\delta]$ be such that

$$A = Q_AG, \quad B = Q_BG.$$

From

$$L = P_AA = P_AQ_AG = P_BQ_BG = P_BB,$$

we deduce that the least common left multiple of Q_A and Q_B is given by $\operatorname{lclm}(Q_A, Q_B) = P_AQ_A = P_BQ_B$, which means that the order of P_A is bounded by $\operatorname{ord}(Q_B) = \operatorname{ord}(B) - \operatorname{ord}(G)$. So

$$\operatorname{ord}(L) = \operatorname{ord}(P_AA) \leq \operatorname{ord}(Q_B) + \operatorname{ord}(A) = \operatorname{ord}(B) - \operatorname{ord}(G) + \operatorname{ord}(A).$$

Again by Theorem 3.1.6, $\mathcal{B}_A \cup \mathcal{B}_B$ is a basis of $V(L)$. □

If the condition on the dimensions of the two solution spaces in Theorem 3.1.12 is not met, the inclusion $V(L) \subset V(A) + V(B)$ does not necessarily hold. Given a vector space $\mathcal{G}$ and a subspace $\mathcal{F} \subset \mathcal{G}$, two operators in $\mathbb{K}[X;\sigma,\delta]$ may have solutions in $\mathcal{G} \setminus \mathcal{F}$ for which there exists a $\operatorname{const}(\mathbb{K}[X;\sigma,\delta])$-linear combination which lives in $\mathcal{F}$.

Example 3.1.13. (S. Chen, personal communication) Consider the ring of differential operators $\mathbb{Q}(y)[\partial; 1, \frac{d}{dy}]$ acting on $\mathcal{F} = \mathbb{Q}(y)$ via the $\mathbb{Q}(y)$-pseudo linear map $\partial(f) = \frac{d}{dy}f$. Let

$$A = \partial^2 + \frac{1}{y}\partial, \quad B = \partial^2 + \frac{1}{y(y+1)}\partial.$$

If we extend the action to the bigger space $\mathcal{G} = \mathbb{Q}(y)(\log(y))$, we get the solution spaces

$$V_{\mathcal{G}}(A) = \operatorname{span}_{\mathbb{Q}}(1, \log(y)),$$
$$V_{\mathcal{G}}(B) = \operatorname{span}_{\mathbb{Q}}(1, y + \log(y)),$$

but over $\mathcal{F}$, the solution spaces are

$$V_{\mathcal{F}}(A) = V_{\mathcal{G}}(A) \cap \mathcal{F} = \operatorname{span}_{\mathbb{Q}}(1) = V_{\mathcal{F}}(B),$$

and so also the sum $V_{\mathcal{F}}(A) + V_{\mathcal{F}}(B)$ is equal to $\operatorname{span}_{\mathbb{Q}}(1)$. On the other hand, y is contained in both $\mathcal{F}$ and the sum $V_{\mathcal{G}}(A) + V_{\mathcal{G}}(B)$ and thus it is an element of $V_{\mathcal{F}}(\operatorname{lclm}(A, B))$. This shows that over $\mathcal{F}$, the solution space of the LCLM is bigger than the sum of the solution spaces of A and B.

Contrary to the situation in unique factorization domains, it is in general not true that the LCLM of A and B can be obtained by taking the quotient $\operatorname{lquo}(AB, \operatorname{gcrd}(A, B))$, as we show in the next example:

Example 3.1.14. Let $A, B \in \mathbb{Q}(y)[\partial; 1, \frac{d}{dy}]$ with

$$A = \left(4y^2 - 1\right)\partial^2 + (-4y + 2)\,\partial + 4$$
$$B = \left(10y^2 + 11y - 8\right)\partial^2 + (-10y + 5)\,\partial + 10.$$

Then their LCLM is

$$\operatorname{lclm}(A, B) = (2y - 1)\,\partial^3 + 2\partial^2,$$

but with $G := \operatorname{gcrd}(A, B) = (2y - 1)\partial - 2$:

$$\operatorname{lquo}(AB, G) = \left(20y^3 + 32y^2 - 5y - 8\right)\partial^3 + (-22y + 11)\,\partial^2 + (20y + 32)\,\partial - 20.$$

Another major difference to the commutative case concerns factorization. Ore polynomials cannot necessarily be factored uniquely into irreducibles. Despite being a big departure from the situation for commutative polynomials, it will not play a big role in our work.

Example 3.1.15. ([38, 12]) Consider operators in $\mathbb{C}(y)[\partial; 1, \frac{d}{dy}]$. For any $a \in \mathbb{C}$ the equation

$$\partial^2 - \frac{2}{y}\partial + \frac{2}{y^2} = \left(\partial - \frac{1}{y(1+ay)}\right)\left(\partial - \frac{1+2ay}{y(1+ay)}\right),$$

holds.

3.2 Ore Algebras for Holonomic Functions

To conclude the introduction to Ore algebras, we give a more in-depth description of two types of Ore polynomials, recurrence operators and differential operators with polynomial or rational function coefficients. Both have been the topic of extensive studies and in the course of this work, most examples will be based on one of these algebras.

3.2.1 Recurrence Operators

In discrete mathematics, combinatorics, summation theory and physics, one often encounters recurrence relations of the form

$$p_r(n)t_{n+r} + p_{r-1}(n)t_{n+r-1} + \cdots + p_1(n)t_{n+1} + p_0(n)t_n = 0,$$

where the p_i are polynomials in n over some field $\mathbb{K}$. Two prime examples of such relations are the recurrence relation satisfied by the Fibonacci numbers F_n,

$$F_{n+2} - F_{n+1} - F_n = 0,$$

and the recurrence relation satisfied by the harmonic numbers $H_n = \sum_{i=1}^{n} \frac{1}{n}$,

$$(n+3)H_{n+2} + (-2n-5)H_{n+1} + (n+2)H_n = 0.$$

Recall the automorphism we defined in Example 3.1.3:

$$s_n : \mathbb{K}[n] \to \mathbb{K}[n], \quad p(n) \mapsto p(n+1).$$

These linear recurrences with polynomial coefficients are studied for example in [25, 43] and [32], where the definitions and results stated here are taken from.

In an Ore setting, linear recurrence equations are modeled via the Ore algebra $\mathbb{K}[n][S; s_n, 0]$ and its extension $\mathbb{K}(n)[S; s_n, 0]$ to allow rational function coefficients. For Ore polynomials in $\mathbb{K}[n][S; s_n, 0]$, the action of an operator is usually defined on all sequences with values in an extension field $\mathbb{F}/\mathbb{K}$ of $\mathbb{K}$, i.e. we set $\mathcal{F} = \mathbb{F}^{\mathbb{N}}$. Operators in $\mathbb{K}[n][S; s_n, 0]$ then act on sequences via the $\mathbb{K}[n]$-pseudo linear map

$$\tau : \mathcal{F} \mapsto \mathcal{F}, \quad (t_n)_{n\in\mathbb{N}} \mapsto (t_{n+1})_{n\in\mathbb{N}}.$$

There are different notions for different kinds of sequences, depending on their annihilator ideal.

Definition 3.2.1. A sequence with values in $\mathbb{F}$ is called

1. *holonomic* (or *P-finite*), if it has a non-zero annihilating ideal in $\mathbb{K}[n][S; s_n, 0]$.

2. *C-finite*, if it satisfies a linear recurrence with coefficients in $\mathbb{K}$, i.e. its annihilating ideal in $\mathbb{K}[n][S; s_n, 0]$ contains a non-zero element with maximal coefficient degree 0.

3. *hypergeometric*, if it is the solution of a linear recurrence of order 1, i.e. its annihilating ideal in $\mathbb{K}[n][S; s_n, 0]$ contains an element of order 1.

Obviously. every C-finite sequence is sequence is holonomic. Different classes are closed under different kinds of operations. In the next theorem we state some of these closure properties for hypergeometric sequences that we will encounter in some examples later on.

Theorem 3.2.2. *If $(a_n)_{n\in\mathbb{N}}$ and $(b_n)_{n\in\mathbb{N}}$ are two hypergeometric sequences, then so are*

1. $(a_n b_n)_{n\in\mathbb{N}}$,
2. $(\frac{1}{a_n})_{n\in\mathbb{N}}$,
3. (a_{un+v}) *for* $u, v \in \mathbb{N}$. □

As the next example shows, these closure properties are useful to decide whether a given sequence is hypergeometric or not.

Example 3.2.3. In later chapters, examples will often contain one of these types of the sequences:

1. Let $p(n) \in \mathbb{K}[n]$. Then the sequence $(p(n))_{n\in\mathbb{N}}$ is hypergeometric because it is annihilated by the order 1 operator

$$L = p(n)S - p(n+1).$$

It is also C-finite. Let Δ_n be the forward difference operator, i.e. $\Delta_n p(n) = p(n+1) - p(n)$. One can see easily that

$$\Delta_n^{\deg(p)+1} p(n) = 0,$$

yields a recurrence in $\mathbb{K}[n][S; s_n, 0]$ for $(p(n))_{n\in\mathbb{N}}$ with coefficients in $\mathbb{K}$.

2. The sequence $(t_n)_{n\in\mathbb{N}} = ((kn)!)_{n\in\mathbb{N}}$ with $k \in \mathbb{N} \setminus \{0\}$ fixed is hypergeometric but not C-finite. It is annihilated by the order 1 operator

$$S - \prod_{i=1}^{k} (kn + i).$$

Let L be an operator with coefficients in $\mathbb{K}$ and let $m \in \mathbb{N}$ be such that $\mathrm{tc}(L) = l_m$. Then $L(t_n)$ can be written as

$$L(t_n) = (k(n+m))!p(n),$$

where p is a polynomial in $\mathbb{K}[n]$ with $[n^0]p \neq 0$. This means that the equation $(k(n+m))!p(n) = 0$ only holds for finitely many n, so the sequence cannot be C-finite.

In general, the *shift-quotient* of a sequence $(t_n)_{n\in\mathbb{N}}$ is given by t_{n+1}/t_n. A sequence is hypergeometric if and only if the shift-quotient is a rational function $r = r_{\text{num}}/r_{\text{den}}$. It is then annihilated by the operator

$$L = r_{\text{den}}(n)S - r_{\text{num}}(n).$$

3. Combining parts 1 and 2 of this example and Theorem 3.2.2, we get that the sequence $(t_n)_{n\in\mathbb{N}}$ with

$$t_n = p(n)\frac{(k_1 n)!^{e_1}}{(k_2 n)!^{e_2}},$$

where $p \in \mathbb{K}[n]$, $k_1, k_2, e_1, e_2 \in \mathbb{N}$, is hypergeometric.

4. The sequence of harmonic numbers $(H_n)_{n\in\mathbb{N}\setminus\{0\}}$ is holonomic but not C-finite or hypergeometric.

If we extend the operator algebra $\mathbb{K}[n][S; s_n, 0]$ to operators with coefficients in $\mathbb{K}(n)$, the domain of the action has to be changed so as to preserve the correspondence between operator multiplication and operator composition.

Example 3.2.4. For $n \in \mathbb{N}$, consider the sequence

$$(t_n)_{n\in\mathbb{N}} = (\delta_{n,1})_{n\in\mathbb{N}} = (0, 1, 0, 0, 0, \dots).$$

An annihilating operator in $\mathbb{K}[n][S; s_n, 0]$ is $L = (n-1)$. If we take any $P \in \mathbb{K}[n][S; s_n, 0]$, then it is easy to see that PL is also an annihilator of $(t_n)_{n\in\mathbb{N}}$, but if we set

$$P = 1/(n-1) \in \mathbb{K}(n)[S; s_n, 0],$$

then $PL = 1$ does not annihilate $(t_n)_{n\in\mathbb{N}}$ anymore.

To avoid effects like this for operators over $\mathbb{K}(n)$, we may consider two sequences as equal if they only differ for finitely many terms. We define two sequences $(r_n)_{n\in\mathbb{N}}$ and $(t_n)_{n\in\mathbb{N}}$ to be equivalent, denoted by $(r_n)_{n\in\mathbb{N}} \sim (t_n)_{n\in\mathbb{N}}$, if there exists an $n_0 \in \mathbb{N}$ such that $r_n = t_n$ for all $n > n_0$. The elements of $\mathbb{K}^{\mathbb{N}}/\sim$ are called *germs*.

We let operators from $\mathbb{K}(n)[S; s_n, 0]$ act on elements of $\mathcal{F} = \mathbb{K}^{\mathbb{N}}/\sim$ via the map

$$\tau' : \mathcal{F} \to \mathcal{F}, \quad [(t_n)_{n\in\mathbb{N}}] \mapsto [\tau((t_n)_{n\in\mathbb{N}})],$$

where τ is as above.

As was mentioned in the previous section, the set of functions on which an operator $L \in \mathbb{D}[X;\sigma,\delta]$ can act has to be chosen big enough in order to have $\operatorname{ord}(L)$ many linearly independent solutions. It can be shown that for recurrence operators, there are $\operatorname{ord}(L)$ many linearly independent formal solutions of the form

$$(y/e)^{yu/v}\rho^y \exp\bigl(c_1 y^{1/m} + \cdots + c_{v-1}y^{1-1/m}\bigr) y^\alpha p(y^{-1/m}, \log(y)),$$

where e is Euler's constant, v is a positive integer, u is an integer, ρ is an element of an algebraic extension of the coefficient field $\mathbb{K}$, $c_1, \ldots, c_{v-1}$ are elements of $\mathbb{K}(\rho)$, m is a positive integer multiple of v, α is an element of some algebraic extension of $\mathbb{K}(\rho)$ and p is an element of $K(\rho)(\alpha)[[y]][z]$, where $\mathbb{K}[[y]]$ denotes the ring of formal power series over $\mathbb{K}$.

A frequent application of recurrence operators is in symbolic summation. The method of *creative telescoping* (see [43, 58]) finds recurrences for definite summation problems. When given a bivariate hypergeometric term $f(n,k)$ (i.e. hypergeometric in n and in k) as input that satisfies certain properties, it computes an operator $L \in \mathbb{K}[n][S; s_n, 0]$ and another hypergeometric term $g(n,k)$ such that

$$L(f(n,k)) = g(n,k+1) - g(n,k),$$

holds. Summing both sides over k then gives a (possibly inhomogeneous) recurrence for the sum $\sum_k f(n,k)$. In this context, L is called a *telescoper*. An implementation of this method in Mathematica is available from [35].

Example 3.2.5. For $f(n,k) := \binom{n}{k}$, creative telescoping gives the relation

$$f(n+1,k) - 2f(n,k) = \frac{k+1}{(k+1)-n-1}\binom{n}{k+1} - \frac{k}{k-n-1}\binom{n}{k}. \quad (3.2.1)$$

The telescoper in this case is

$$L = S - 2,$$

and

$$g(n,k) = \frac{k}{k-n-1}\binom{n}{k}.$$

Summing over all k in Equation (3.2.1) shows:

$$\sum_{k=0}^{n}\binom{n+1}{k} - 2\sum_{k=0}^{n}\binom{n}{k} = 0.$$

3.2.2 Differential Operators

Linear ordinary differential equations (ODEs) with polynomial coefficients represent a classical, yet still active field of research. Amongst others, they appear frequently in different fields of physics and engineering. An introduction to linear ODEs can be found in [27] and for more details on ODEs in symbolic computation, the reader is refered to [34], from which the theory presented in this section is taken.

Differential equations of the form

$$p_r(y)f^{(r)}(y) + p_{r-1}(y)f^{(r-1)}(y) + \cdots + p_1(y)f'(y) + p_0(y)f(y) = 0,$$

with $p_i \in \mathbb{K}[y]$ for some field $\mathbb{K}$ are modeled via the Ore algebra $\mathbb{K}[y][\partial; 1, \frac{d}{dy}]$ and its extension $\mathbb{K}(y)[\partial; 1, \frac{d}{dy}]$ to allow rational function coefficients. We usually let operators in $\mathbb{K}[y][\partial; 1, \frac{d}{dy}]$ act on elements of a differential field extension $\mathcal{F}$ of $\mathbb{K}(y)$. We define the $\mathbb{K}[y]$-pseudo linear map

$$\tau : \mathcal{F} \mapsto \mathcal{F}, \quad f \mapsto \frac{d}{dy}f.$$

Like for recurrences, we distinguish different kinds of functions depending on their annihilator ideals in $\mathbb{K}[y][\partial; 1, \frac{d}{dy}]$ and $\mathbb{K}(y)[\partial; 1, \frac{d}{dy}]$.

Definition 3.2.6. A function in a differential field extension of $\mathbb{K}(y)$ is called

1. *holonomic* (or *D-finite*), if there is a non-zero ideal in $\mathbb{K}[y][\partial; 1, \frac{d}{dy}]$ that annihilates the sequence.

2. *C-finite*, if it satisfies a linear differential equation with coefficients in $\mathbb{K}$, i.e. its annihilating ideal in $\mathbb{K}[y][\partial; 1, \frac{d}{dy}]$ contains a non-zero element with maximal coefficient degree 0.

3. *hyperexponential*, if it is the solution of a linear differential equation of order 1, i.e. its annihilating ideal in $\mathbb{K}[y][\partial; 1, \frac{d}{dy}]$ contains an element of order 1.

Similar to the closure properties given in Theorem 3.2.2, hyperexponential functions are closed under certain operations.

Theorem 3.2.7. *If f and g are two hyperexponential functions, then so are*

1. $f \cdot g$,

2. $\frac{1}{f}$.

3. $f(r)$, *where r is a rational function.* □

In later chapters, operators in examples often come from holonomic functions like the following.

Example 3.2.8. We give some examples of different holonomic functions.

1. Univariate polynomials are hyperexponential and C-finite functions. Let $p \in \mathbb{K}[y]$. Then

$$L_1 = p(y)\partial - p'(y), \quad L_2 = \partial^{\deg(p)+1}$$

   are two annihilators of p, one of order 1 and the other with coefficients in $\mathbb{K}$.

2. The function $f(y) = 1/y$ is hyperexponential but not C-finite. An order 1 annihilator is $y\partial + 1$. The set containing f and its derivatives is a basis of $\mathbb{K}[y^{-1}]$, so a differential equation with coefficients in $\mathbb{K}$ cannot exist.

3. The Gaussian hypergeometric function

$$ {}_2F_1(a, b, c, y) = \sum_{n=0}^{\infty} \frac{a^{\bar{n}} b^{\bar{n}} y^n}{c^{\bar{n}} n!}, $$

   is holonomic but not hyperexponential or C-finite. A least order differential equation for ${}_2F_1(a, b, c, y)$ is

$$y(-y+1)\partial^2 + (-(a+b+1)y + c)\partial - ab = 0.$$

4. The sequence $(t_n)_{n\in\mathbb{N}}$ is a holonomic sequence if and only if the power series given by $f(y) := \sum_{i=0}^{\infty} t_i y^i$ is a holonomic function. Algorithms to convert a recurrence for $(t_n)_{n\in\mathbb{N}}$ into a differential equation for $f(y)$ and vice versa are available and implemented, e.g. in Sage [30].

When extending the ring of linear differential operators over polynomial coefficients to operators over rational function coefficients, we face a problem similar to the situation for linear recurrence equations, where we had to move from the set of all sequences to the set of germs. Here it is necessary to move from functions to distributions, but giving details on this matter would be beyond the scope of this work.

An operator $L \in \mathbb{K}[y][\partial; 1, \frac{d}{dy}]$ has $\operatorname{ord}(L)$ many linearly independent formal solutions of the form

$$\exp\left(\int_0^y \frac{p(t^{-1/s})}{t} dt\right) q(y^{1/s}, \log(y)),$$

where s is a positive integer, p is in $\mathbb{F}[y]$, q is in $\mathbb{F}[[y]][z]$ with $y \nmid q$ unless q is zero, $\mathbb{F}$ is some algebraic extension of $\mathbb{K}$.

An application of differential operators in computer algebra is symbolic integration. In the integration analogue of creative telescoping introduced in [5], a bivariate hyperexponential term $f(y,z)$ is taken as input and an operator $L \in \mathbb{K}[y][\partial; 1, \frac{d}{dy}]$, called *telescoper*, and a hyperexponential term $g(y,z)$ are computed for which

$$L(f) = \frac{d}{dz}g,$$

holds. Integrating both sides of this equation from α to β along z then gives a (possibly inhomogeneous) differential equation for the definite integral $\int_\alpha^\beta f(y,z)dz$. An implementation of this method in Mathematica is available from [35].

Example 3.2.9. For $f(y,z) := e^{y^2z^2}\sqrt{z}$, creative telescoping yields the relation

$$-2y\frac{d}{dy}f(y,z) - 3f(y,z) = \frac{d}{dz}(2zf(y,z)). \tag{3.2.2}$$

The telescoper in this case is

$$L = (-2y)\partial - 3,$$

and

$$g(y,z) = 2zf(y,z).$$

Definite integration on both sides in Equation (3.2.2) shows that for $F(y) := \int_\alpha^\beta f(y,z)dz$ with $\alpha, \beta \in \mathbb{R}$ we get:

$$-2y\frac{d}{dy}F(y) - 3F(y) = [g(y,z)]_{z=\alpha}^{z=\beta}.$$

Chapter 4

Desingularization of Ore Operators

4.1 Removal of Singularities

In Theorem 2.2.2 it was stated that in the commutative case, the product of two primitive polynomials is again primitive. For Ore polynomials, this is not necessarily true. To illustrate this fact, we give an easy example of two primitive recurrence operators whose product is not content-free.

Example 4.1.1. Let $P, L \in \mathbb{Q}[n][S; s_n, 0]$ with $P = S+1$, $L = (n-1)S+n$. Then:

$$PL = nS^2 + 2nS + n = n(S^2 + 2S + 1).$$

This is not an exceptional case. For non-commutative polynomials arising in applications, most often it is possible to multiply the primitive generator of a left operator ideal with another primitive operator on the left such that the product has non-trivial content. In this chapter we study these left-factors, the content that can appear after the multiplication and when and how such a left-factor can be constructed. Later in Chapters 5 and 6 we will see some of the notable consequences of this idiosyncrasy of Ore operators: We will show how to balance order and coefficient degrees in operator ideals and how in the Euclidean algorithm some factors of the leading coefficients of the input operators can unecessarily slow down the computation.

Most of the work presented here was done in collaboration with Shoashi Chen, Manuel Kauers and Micheal F. Singer and – to a large extend – can be viewed as as a reformulation of results given in [3] with new proofs and slight generalizations. It was published in [15] and partly in [28].

We consider the following situation in the whole chapter. It covers many of the Ore algebras relevant in applications, in particular the Ore algebras presented in Chapter 3:

Setting. Let $\mathbb{D}$ be a Euclidean domain with degree function deg and let $\mathbb{K}$ be its fraction field. Furthermore, let $\mathbb{D}[X;\sigma,\delta]$ be an Ore polynomial ring where σ is an automorphism and suppose we are given a fixed $L \in \mathbb{D}[X;\sigma,\delta]$. Recall that there is a unique way to extend $\mathbb{D}[X;\sigma,\delta]$ to $\mathbb{K}[X;\sigma,\delta]$. (see Section 3.1) For an operator $P \in \mathbb{D}[X;\sigma,\delta]$ we denote the maximum of all the coefficient degrees by $\deg(P)$.

We start our analysis by first identifying the source of new content that can appear after multiplying L with another operator from the left. Not any arbitrary base ring element can emerge as new content. The only candidates are factors of the leading coefficient of L.

Theorem 4.1.2. *Let $L \in \mathbb{D}[X;\sigma,\delta]$ and let $p \in \mathbb{D}$ be irreducible and let $P \in \mathbb{D}[X;\sigma,\delta]$ be such that P is primitive and $p \mid \operatorname{cont}(PL)$. Set i to be the largest integer such that $p_i \neq 0$ and $p \nmid p_i$. Then*

$$\sigma^{-i}(p) \mid \operatorname{lc}(L).$$

Proof. We can write P as the sum

$$P = \underbrace{\sum_{j=0}^{i} p_j X^j}_{=:P'} + \underbrace{\sum_{j=i+1}^{d_P} p_j X^j}_{=:P''}.$$

where all the coefficients of P'' are divisible by p and the leading coefficient of P' is not. We get that

$$P'L = PL - P''L,$$

and both, the content of PL and the content of $P''L$ are divisible by p. This yields that also the content of $P'L$ and therefore $\operatorname{lc}(P'L)$ is divisible by p. The leading coefficient of $P'L$ is equal to $\operatorname{lc}(P')\sigma^i(\operatorname{lc}(L))$. Since p does not divide the leading coefficient of P', it has to divide $\sigma^i(\operatorname{lc}(L))$. □

Definition 4.1.3. Let $L \in \mathbb{D}[X;\sigma,\delta]$ and $p \in \mathbb{D}$. If there is a $P \in \mathbb{D}[X;\sigma,\delta]$ such that each irreducible factor of p together with the primitive part $\operatorname{pp}(P)$ of P meets the conditions in Theorem 4.1.2 for the same $i \in \mathbb{N}$, we call p *removable* from L and P a $\sigma^{-i}(p)$*-extracting operator* for L.

Theorem 4.1.2 justifies the nomenclature of Definition 4.1.3. If we have given a p-extracting operator P for L, the product PL can be written in the form $\sigma^i(p)\operatorname{cont}(P)L'$ with $L' \in \mathbb{D}[X;\sigma,\delta]$. Here, P was used to construct a multiple PL of L where p was *extracted*. By taking the primitive part of P in Definition 4.1.3, we avoid calling P a p-extracting operator in the case that p does not appear as a new factor in $\operatorname{cont}(PL)$ but just as part of the content of P itself.

Example 4.1.4. (Example 4.1.1 cont.) Take P and L as in Example 4.1.1.

- P is a $(n-1)$-extracting operator for L.
- Set $P_1 = (n+1)S + (n+1)$. Then:

$$P_1 L = (n+1)n(S^2 + 2S + 1).$$

  Here, P_1 is an $(n-1)$-extracting operator, but not an n-extracting operator.

- Similarly, $P_2 = nS - n$ is an $(n-1)$-extracting operator, but not an $(n-1)^2$-extracting operator.
- $P_3 = nS^2 + S + 1$ is also an $(n-1)$-extracting operator, although its order is higher than the shift with which the removable factor appears in the product PL.

We can always clear the content of a p-extracting operator and then reduce its coefficients by a shift of p without violating its p-extracting property. This will be helpful for determining necessary bounds for our desingularization algorithm later on.

Lemma 4.1.5. *Let i, p, P, L be as in Theorem 4.1.2. Set*

$$P' = \sum_{j=0}^{i} (p_j \operatorname{div} p) X^j.$$

Then also P' is a $\sigma^{-i}(p)$-extracting operator for L.

Proof. As in the proof of Theorem 4.1.2, we can split P into the sum $P = P' + P''$ where all the coefficients of P'' are divisible by p and the leading coefficient of P' is not. Then

$$PL = P'L + P''L, \text{ with } p \mid \operatorname{cont}(P''L),$$

and P' is of order i. Since we have $p \mid \operatorname{cont}(PL)$, also $\operatorname{cont}(P'L)$ has to be divisible by p. □

By extracting a factor p of the leading coefficient of L by P, we can also remove it from the product by setting $P' = \frac{1}{\sigma^{d_P}(p)} P \in \mathbb{K}[X; \sigma, \delta]$. Then $P'L$ still has coefficients in $\mathbb{D}$ and the leading coefficient of $P'L$ contains a shifted version of the leading coefficient of L where the factor p was removed.

Definition 4.1.6. Let $L \in \mathbb{D}[X; \sigma, \delta]$ and let $p \in \mathbb{D}$ be such that $p \mid \operatorname{lc}(L)$. We say that p is *removable* from L at order n and it is called a *removable singularity* of L if there exists some $P \in \mathbb{K}[X; \sigma, \delta]$ with $\operatorname{ord}(P) = n$ and

some $w, v \in \mathbb{D}$ with $\gcd(p, w) = \gcd(v, w) = 1$ such that $PL \in \mathbb{D}[X; \sigma, \delta]$ and

$$\sigma^{-n}(\mathrm{lc}(PL)) = \frac{w}{vp}\,\mathrm{lc}(L).$$

We then call P a *p-removing operator* for L, and PL the corresponding *p-removed operator*. p is simply called *removable* from L if it is removable at order n for some $n \in \mathbb{N}$. If $\gcd(p, \mathrm{lc}(L)/(vp)) = 1$, then we say *desingulariz*[*able*|*ing*|*ed*] instead of remov[able|ing|ed], respectively.

With w and v in Definition 4.1.6, we allow a p-removing operator to add new factors (in case of a non-trivial choice for w), as long as they are coprime to p, and also to remove other factors of $\mathrm{lc}(L)$ (in case of a non-trivial choice for v). It should be noted that the the terms 'removable' and 'desingularizeable' as they appear here are not standardized in the literature and are likely to differ in other publications.

It is easy to see that every p-removing operator can be turned into a p-extracting operator by clearing denominators. For getting a p-removing operator from a p-extracting operator P, first all the highest order coefficients which are divisible by $\sigma^i(p)$ (where i is as in Theorem 4.1.2) have to be set to zero and then division by an appropriate shift of p yields the desired result. By this procedure, P_3 in Example 4.1.4 gives rise to the $(n-1)$-removing operator $(1/n)S + (1/n)$.

Usually not all factors of the leading coefficient of an operator L are removable. A randomly generated operator will most likely have no removable singularities, whereas for "meaningful" operators, i.e. operators that arise in applications like combinatorics or physics, one often finds that some factors can be removed. In the context of holonomic functions and sequences, removable factors can be connected to the solutions of differential and recurrence operators. We outline this connection in an informal fashion:

Let L be an element of $\mathbb{C}[y][D; 1, \frac{d}{dy}]$ and let $\mathcal{I} = \mathcal{I}' \cap \mathbb{C}[y][D; 1, \frac{d}{dy}]$ be the contraction of the left ideal $\mathcal{I}' \lhd \mathbb{C}(y)[D; 1, \frac{d}{dy}]$ generated by L. Any singularity of a solution of L corresponds to a root of the leading coefficient of L, but not for any root of $\mathrm{lc}(L)$ there has to be a solution with a singularity at that point. Any solution of L is also a solution of every operator in $\mathcal{I}$ and so any desingularized operator for L annihilates the solutions of L as well. We will see that there is an operator in $\mathcal{I}$ with a leading coefficient that only contains all the non-removable singularities of L and it turns out that for each of those roots, there is at least one solution of L that does not admit analytic continuation to that point. Conversely, if there is a solution of L that is analytic at a root of the leading coefficient of L, this root can be removed completely. A more detailed description of desingularization and removable factors of differential equations can be found in [27].

For recurrence operators, the situation is similar. In [3] it is shown that given a numeric sequence $\{\ldots, t_{c-3}, t_{c-2}, t_{c-1}\}$ with $c \in \mathbb{C}$ and an annihilat-

ing operator $L \in \mathbb{C}[y][\partial; 1, \frac{d}{dy}]$ where c is a root of the leading coefficient, it is possible to uniquely extend the sequence to $\{\ldots, t_{c-3}, t_{c-2}, t_{c-1}, t_c\}$ if $(n-c)$ is a removable factor of L.

In the case that an operator L has two coprime factors p and q in its leading coefficient that are removable at the same order, it is not obvious that there exists a pq-removed operator of that order. The next theorem shows that this is indeed the case and that for each order $> d_L$ there is a left multiple of L with a minimal (in terms of divisibility) leading coefficient.

Theorem 4.1.7. *Let $d_T \in \mathbb{N}$ be fixed, let $\mathcal{I} \lhd \mathbb{D}[X; \sigma, \delta]$ be a left ideal and let T be any element of $\mathcal{I}$ of order d_T such that, among all the operators of order d_T in $\mathcal{I}$, its leading coefficient t is minimal with respect to the degree. Then t is independent of the choice of T (up to multiplication by units in $\mathbb{D}$) and for any $L \in \mathcal{I}$ with $d_L \leq d_T$ we have $\sigma^{d_L - d_T}(t) \mid \mathrm{lc}(L)$.*

Proof. Assume there are $T, L \in \mathcal{I}$ for which the claim $\sigma^{d_L-d_T}(t) \mid \mathrm{lc}(L)$ does not hold. We set $L' = X^{d_T-d_L}L$ and get $\mathrm{lc}(L') = \sigma^{d_T-d_L}(\mathrm{lc}(L))$, thus $t \nmid \mathrm{lc}(L')$ by assumption. Division with remainder yields nonzero $q, r \in \mathbb{D}$ such that

$$\mathrm{lc}(L') = qt + r, \quad \deg(r) < \deg(t).$$

Hence the operator $L' - qT$ is an element of $\mathcal{I}$ of order d_T whose leading coefficient has degree less than $\deg(t)$. This contradicts the choice of T.
For the uniqueness, let $T' \in \mathcal{I}$ be any other operator of order d_T with minimal leading coefficient degree. By what was just shown above, we get $\mathrm{lc}(T') \mid t$ and $t \mid \mathrm{lc}(T')$, so t and $\mathrm{lc}(T')$ are associates. □

Definition 4.1.8. Consider $\mathcal{I}$, T and t from Theorem 4.1.7. The shift $\sigma^{-d_T}(t)$ of the leading coefficient of T is called the *essential part* of $\mathcal{I}$ at order d_T. If there is no operator in $\mathcal{I}$ for some order n, the essential part of $\mathcal{I}$ at order n is defined to be 1.

Before we investigate how to construct removing operators algorithmically, we conclude our analysis of removable factors by showing that among all the essential parts of a left ideal, there exists a minimal essential part which divides all the others.

Corollary 4.1.9. *Let $\mathcal{I} \lhd \mathbb{D}[X; \sigma, \delta]$ be a left ideal and let T be any element of $\mathcal{I}$ with leading coefficient t such that $\sigma^{-d_T}(t)$ is minimal with respect to the degree. Then t is independent of the choice of T (up to multiplication by units in $\mathbb{D}$) and for any $L \in \mathcal{I}$ we have $\sigma^{d_L-d_T}(t) \mid \mathrm{lc}(L)$.*

Proof. For operators $L \in \mathcal{I}$ with order smaller than or equal to d_T, the divisibility of $\mathrm{lc}(L)$ by $\sigma^{d_L-d_T}(t)$ follows from Theorem 4.1.7, because the minimality of $\sigma^{-d_T}(t)$ implies that t is of minimal degree among all the leading coefficients of elements of $\mathcal{I}$ of order d_T. Let $d_L > d_T$ be fixed. It is sufficient to show $\sigma^{d_L-d_T}(t) \mid \mathrm{lc}(L)$ with L having minimal leading coefficient

degree among all elements of $\mathcal{I}$ of order d_L, because by Theorem 4.1.7, the leading coefficient of any operator in $\mathcal{I}$ of order d_L is divisible by the leading coefficient of L. By the choice of T, the degree of $\sigma^{-d_L}(\mathrm{lc}(L))$ is greater than or equal to the degree of $\sigma^{-d_T}(t)$. Division with remainder gives $q, r \in \mathbb{D}$ such that

$$\sigma^{-d_L}(\mathrm{lc}(L)) = q\sigma^{-d_T}(t) + r, \quad \deg(r) < \deg(\sigma^{-d_T}(t)) \text{ or } r = 0.$$

If r is zero, then $\sigma^{-d_T}(t)$ divides $\sigma^{-d_L}(\mathrm{lc}(L))$ and so also $\sigma^{d_L-d_T}(t) \mid \mathrm{lc}(L)$. Assume r is not zero. We set $L' = L - \sigma^{d_L}(q)X^{d_L-d_T}T$. Then $L' \in \mathcal{I}$ with $\mathrm{ord}(L') = \mathrm{ord}(L)$ and $\deg(\sigma^{-d_L}(\mathrm{lc}(L'))) = \deg(r) < \deg(\sigma^{-d_T}(t))$, which contradicts the choice of T. The uniqueness of t is shown as in the proof of Theorem 4.1.7. □

Definition 4.1.10. Consider $\mathcal{I}, T$ and t as in Corollary 4.1.9. We call $\sigma^{-d_T}(t)$ the *minimal essential part* of $\mathcal{I}$.

For annihilators of holonomic functions or sequences coming from applications, it can be observed that the essential parts of an annihilator ideal are usually the same for all orders greater than the order of the generator. In this case only the minimal essential part of the ideal has to be considered.

4.2 Desingularization by Linear System Solving

The question on how to compute a desingularizing operator for recurrence operators was first answered in [3] and for differential operators, it is a classical result that can be found for example in [47]. Our goal is to find a uniform approach for all Ore algebras in which the specific properties of special Ore rings like differential operators are used as little as possible. Also, unlike in [3], we want to have as much control as possible over which singularities are removed at which point and, unlike in [47], be able to reduce the multiplicity of a singularity if it cannot be removed completely.

In order to design an algorithm for desingularization, we derive a normal form for p-removing operators. While this normal form holds for Ore algebras over any Euclidean domain, the final algorithm is based on an ansatz and hence will only be formulated in the case of a commutative polynomial ring as the base ring of the Ore algebra. The next lemma provides us with the tools to normalize any p-removing operator.

Lemma 4.2.1. *Let $L \in \mathbb{D}[X;\sigma,\delta]$, let $p \in \mathbb{D}$ be removable from L, and let $P \in \mathbb{K}[X;\sigma,\delta]$ be a p-removing operator for L.*

1. *If $U \in \mathbb{D}[X;\sigma,\delta]$ with $\gcd(\mathrm{lc}(U), \sigma^{d_P+d_U}(p)) = 1$, then UP is also a p-removing operator for L.*
2. *If $P = P_1 + P_2$ for some $P_1 \in \mathbb{K}[X;\sigma,\delta]$ with $\mathrm{ord}(P_1) = \mathrm{ord}(P)$ and $P_2 \in \mathbb{D}[X;\sigma,\delta]$, then P_1 is also a p-removing operator for L.*

3. *There exists a p-removing operator P' with $\operatorname{ord}(P') = \operatorname{ord}(P)$ and with $p\sigma^{-d_P}(\operatorname{lc}(P'L)) = \operatorname{lc}(L)$, i.e. a p-removing operator that neither removes nor adds any other factors.*

Proof. Let $v, w \in \mathbb{D}$ be as in Definition 4.1.6, i.e. $\gcd(p, w) = \gcd(v, w) = 1$ and $vp\sigma^{-d_P}(\operatorname{lc}(PL)) = w \operatorname{lc}(L)$.
1. Since PL is an operator with polynomial coefficients, so is UPL. Furthermore, with $u = \operatorname{lc}(U)$ we have

$$vp\sigma^{-d_P-d_U}(\operatorname{lc}(UPL)) = \sigma^{-d_P-d_U}(u)w \operatorname{lc}(L).$$

Since $\gcd(u, \sigma^{d_P+d_U}(p)) = 1$, we have $\gcd(\sigma^{-d_P-d_U}(u)w, p) = 1$, as required.
2. Clearly, $P_2 \in \mathbb{D}[X; \sigma, \delta]$ implies $P_2L \in \mathbb{D}[X; \sigma, \delta]$. Since also $PL \in \mathbb{D}[X; \sigma, \delta]$, it follows that

$$P_1L = (P - P_2)L = PL - P_2L \in \mathbb{D}[X; \sigma, \delta].$$

If $\operatorname{ord}(P_2) < \operatorname{ord}(P)$, then we have $\operatorname{lc}(PL) = \operatorname{lc}(P_1L)$, so there is nothing else to show. If $\operatorname{ord}(P_2) = \operatorname{ord}(P)$, then $\operatorname{lc}(P_1L) = \operatorname{lc}(PL) - \operatorname{lc}(P_2L)$ and therefore

$$\begin{aligned} vp\sigma^{-d_P}(\operatorname{lc}(P_1L)) &= vp\sigma^{-d_P}(\operatorname{lc}(PL) - \operatorname{lc}(P_2L)) \\ &= (w - vp\sigma^{-d_P}(\operatorname{lc}(P_2))) \operatorname{lc}(L). \end{aligned}$$

Since $\gcd(p, w - vp\sigma^{-d_P}(\operatorname{lc}(P_2))) = \gcd(p, w) = 1$, the claim follows.
3. By the extended Euclidean algorithm we can find $s, t \in \mathbb{D}$ with $1 = sw + tpv$. Then $\sigma^{d_P}(s)P$ is p-removing of order $\operatorname{ord}(P)$ by part 1 ($\sigma^{d_P}(s)$ is obviously coprime to $\sigma^{d_P}(p)$), and its leading coefficient is

$$\sigma^{d_P}\left(\frac{sw}{pv}\right) = \frac{1}{\sigma^{d_P}(pv)} - \sigma^{d_P}(t).$$

By part 2 we may discard the fraction free part $\sigma^{d_P}(t)$, obtaining another p-removing operator P' with $\operatorname{ord}(P') = \operatorname{ord}(P)$ and $p\sigma^{-d_P}(\operatorname{lc}(P'L)) = (1/v) \operatorname{lc}(L)$. Using part 1, we can obtain from here an operator with the desired property. □

Now we can state a normal form for p-removing operators and give a constructive proof for it.

Corollary 4.2.2. *Let $L \in \mathbb{D}[X; \sigma, \delta]$ and $p \in \mathbb{D}$. If p^k is removable from L for $k \in \mathbb{N}$ then there exits a p^k-removing operator P for L of the form*

$$P = \frac{p_0}{\sigma^n(p)^{e_0}} + \frac{p_1}{\sigma^n(p)^{e_1}}X + \cdots + \frac{p_{n-1}}{\sigma^n(p)^{e_{n-1}}}X^{n-1} + \frac{1}{\sigma^n(p)^k}X^n, \quad (4.2.1)$$

with $n, e_0, \ldots, e_{n-1} \in \mathbb{N}$, and $p_0, \ldots, p_{n-1} \in \mathbb{D}$ with $\deg(p_i) < e_i \deg(\sigma^n(p))$.

Proof. Let P' be a p^k-removing operator for L with $\operatorname{ord}(P') = n$ such that for each $i \in \mathbb{N}$, the numerator and the denominator of the ith coefficient are coprime. By Lemma 4.2.1 part 1, we can clear any factors in the denominators of the coefficients of P' that are not of the form $\sigma^n(p)^{e_i}$. Next, we need to reduce the numerator p_n of the leading coefficient to 1 and lower the degrees of the other numerators. To this extent, we first use Lemma 4.2.1 part 3 to get the appropriate leading coefficient. Then, Lemma 4.2.1 part 2 allows us to reduce all the numerators by the corresponding denominator which yields the desired operator. □

Example 4.2.3. Consider $L \in \mathbb{Q}[n][S; s_n, 0]$ with

$$L = (-15n^2 + n + 2)S + (15n^2 + 29n + 12).$$

Here, $p = 3n + 4$ can be removed by the operator

$$P = \frac{-20800}{(15n^2 + 29n + 12)}S - n(n+2)(1515n + 2209)\frac{15n^4 + 89n^3 + 158n^2 + 76n - 20}{15n^2 + 29n + 12}.$$

P can be brought into normal form. First we remove all unnecessary factors in the denominators by multiplying P with $(5n + 3)$. We get the operator

$$\frac{-20800}{5(3n+4)}S - n(n+2)(1515n + 2209)\frac{15n^4 + 89n^3 + 158n^2 + 76n - 20}{5(3n+4)}.$$

Next we lower the degree of the numerators by reducing the numerators with the denominators. We get the normal form p-removing operator

$$\frac{-21840}{5(3n+4)}S - \frac{3360}{5(3n+4)}.$$

Note that in a normal form p-removing operator, the numerator degrees are strictly smaller than the denominator degrees, so the maximal coefficient degree of the p-removed operator will be lower than the maximal coefficient degree of L.

Given $L \in \mathbb{K}[y][X; \sigma, \delta]$ where $\mathbb{K}$ is a field, $p \in \mathbb{K}[y]$ and $k \in \mathbb{N}$, we are now able to construct a p^k-removing operator for L by solving a linear system, provided that we can find an upper bound E for the e_i and an upper bound N for n as in Corollary 4.2.2. Starting from an Ore polynomial P of the form (4.2.1) with undetermined numerator coefficients, we set $P' = \sigma^N(p)^E P$. If P ought to be a p^k-removing operator, the equation $P'L \equiv 0 \bmod \sigma^N(p)^E$ has to hold. This gives a linear system in terms of the undetermined coefficients of the numerators in P and any non-trivial

solution then gives rise to a p^k-removing operator for L. If there doesn't exist any non-trivial solution, then p^k is not removable from L.

Algorithm 4.2.1: Desingularization

Input: $L \in \mathbb{K}[y][X;\sigma,\delta]$, $p \in \mathbb{K}[y]$ irreducible, $k, E, N \in \mathbb{N}$.
Output: A p^k-removing operator for L of order at most N and coefficients with denominators dividing $\sigma^N(p)^E$ or $\perp$ if no such operator exists.

IF $p^k \nmid \mathrm{lc}(L)$: RETURN $\perp$
$P' \leftarrow \sum_{i=0}^{N}(\sum_{j=0}^{\deg(\sigma^N(p))E-1} p_{i,j}y^j)X^i$ with $p_{i,j}$ undetermined
SOLVE : $P'L \equiv 0 \mod \sigma^N(p)^E$
IF there is no non-zero solution: RETURN $\perp$
$P \leftarrow \frac{1}{\sigma^N(p)^E}P'$
RETURN P

If we want to apply Algorithm 4.2.1 in practice, we need to derive a bound E for the denominator and a bound N for the order of the output. While until now we considered general Ore algebras, at this point we need to specialize to certain kinds of Ore polynomial rings.

4.3 Order and Denominator Bounds

4.3.1 Shift Case

We first consider Ore algebras where the pseudo-derivation is the zero-map, as in the case of recurrence operators presented in Section 3.2.1 or q-shift operators as in Example 3.1.3.

The key for deriving order and denominator bounds for p-removing operators lies in the notion of *p-bordered* operators, where the leading and the trailing coefficient share common factors (up to shifts). We can assume without loss of generality that $\mathrm{tc}(L) = l_0$ by dividing L by powers of X from the right

Definition 4.3.1. ([3]) Let $L \in \mathbb{D}[X;\sigma,0]$ and $p \in \mathbb{D}$. L is called *p-bordered* if p divides $\mathrm{lc}(L)$ and there exists a $k \in \mathbb{N}$ such that $\sigma^k(p)$ divides l_0.

The maximal $k \in \mathbb{N}$ for which the kth shift of a factor p of the leading coefficient of an operator divides the trailing coefficient is often called the *dispersion* of p in L. It turns out that the set of p-removable operators is a subset of the p-bordered operators. In [3], this is shown in terms of solutions of L. We give an alternative proof based on the fact that we can reduce the coefficients of a p-extracting operator by a shift of p.

Theorem 4.3.2. *Let $p \in \mathbb{D}$ be an irreducible and removable factor of the leading coefficient of $L \in \mathbb{D}[X;\sigma,0]$. Then L is p-bordered.*

Proof. Let P be a primitive p-extracting operator for L with $\mathrm{tc}(P) = p_m$ for some $m \in \mathbb{N}$ and $\sigma^i(p) \mid \mathrm{cont}(PL)$ for $i \geq m$ as in Theorem 4.1.2. Assume by Lemma 4.1.5 without loss of generality that the maximal coefficient degree of P is strictly less than $\deg(\sigma^i(p))$. We have that

$$\mathrm{tc}(PL) = \mathrm{tc}(P)\sigma^m(l_0),$$

so l_0 has to be divisible by $\sigma^{i-m}(p)$. □

It is this difference in shifts of common factors in the leading and the trailing coefficient that leads to a bound for the order of a p-removing operator and a bound for the denominator exponents of a p-removing operator. We first prove the former, which is a less technically involved matter than the latter.

Lemma 4.3.3. *Let $L \in \mathbb{D}[X;\sigma,0]$ with $l_0 \neq 0$, and let p be an irreducible factor of $\mathrm{lc}(L)$ such that p^k is removable from L for some $k \geq 1$. Let $n \in \mathbb{N}$ be such that $\gcd(\sigma^n(p), l_0) \neq 1$ and $\gcd(\sigma^m(p), l_0) = 1$ for all $m > n$. Then p^k is removable at order n from L.*

Proof. By assumption on L, there exists a p^k-removing operator P, say of order m, and by Corollary 4.2.2 we may assume that

$$P = \frac{p_0}{\sigma^m(p)^{e_0}} + \frac{p_1}{\sigma^m(p)^{e_1}}X + \cdots + \frac{p_m}{\sigma^m(p)^{e_m}}X^m,$$

for $e_i \in \mathbb{N}$ and $p_i \in \mathbb{D}$ with $\deg(p_i) < e_i \deg(\sigma^m(p))$ $(i = 0, \ldots, m)$. We may further assume $\gcd(\sigma^m(p), p_i) = 1$ for $i = 0, \ldots, m$ (viz. that the e_i are chosen minimally).
Suppose that $m > n$. We show by induction that then $e_0 = e_1 = \cdots = e_{m-n-1} = 0$, so that $p_i = 0$ for $i = 0, \ldots, m-n-1$, i.e., the operator P has in fact the form

$$P = \frac{p_{m-n}}{\sigma^m(p)^{e_{m-n}}}X^{m-n} + \cdots + \frac{p_m}{\sigma^m(p)^{e_m}}X^m.$$

Thus $X^{n-m}P \in \mathbb{K}[X;\sigma,0]$ is a p^k-removing operator of order n.
Consider the operator $T := PL \in \mathbb{D}[X;\sigma,0]$. From $\frac{p_0}{\sigma^m(p)^{e_0}}l_0 = t_0 \in \mathbb{D}$ it follows that $e_0 = 0$, because

$$\gcd(\sigma^m(p), p_0) = \gcd(\sigma^m(p), l_0) = 1,$$

by the choice of p_0 and the assumption in the lemma, respectively, and this leaves no possibility for cancellation.
Assume now, as induction hypothesis, that $e_0 = e_1 = \cdots = e_{i-1} = 0$ for some $i < m - n$. Then from

$$\begin{aligned} t_i &= \frac{p_i}{\sigma^m(p)^{e_i}}\sigma^i(l_0) + \frac{p_{i-1}}{\sigma^m(p)^{e_{i-1}}}\sigma^{i-1}(l_1) + \cdots + \frac{p_0}{\sigma^m(p)^{e_0}}l_i \\ &= \frac{p_i}{\sigma^m(p)^{e_i}}\sigma^i(l_0), \end{aligned}$$

it follows that $\sigma^m(p)^{e_i} \mid p_i\sigma^i(l_0)$. By the choice of p_i we have that $\sigma^m(p)$ and p_i are coprime and by the assumption in the lemma we also have $\gcd(\sigma^{m-i}(p), l_0) = 1$ (because $m - i > n$), so it follows that $e_i = 0$. Inductively, we obtain $e_0 = e_1 = \cdots = e_{m-n-1} = 0$, which completes the proof. □

For the proof of the denominator exponent bound, we need to generalize the notion of the multiplicity of a factor of an element of $\mathbb{D}$, where shifts of this factor are taken into account.

Definition 4.3.4. We call $p, q \in \mathbb{D} \setminus \{0\}$ equivalent if there exists an $n \in \mathbb{Z}$ such that $\sigma^n(p)/q$ is a unit in $\mathbb{D}$. We write $[p]$ for the equivalence class of $p \in \mathbb{D} \setminus \{0\}$. If p, q are equivalent in this sense, we write $p \leq q$ if $\sigma^n(p)/q$ is a unit for some $n \geq 0$, and $p > q$ otherwise.
For any irreducible factor p of $u \in \mathbb{D}$, let $v_u(p)$ denote the multiplicity of p in u, and define

$$v_u^<(p) := \max\{\, v_u(q) \mid q \in [p] : p > q \,\}.$$

Example 4.3.5. For $u \in \mathbb{Q}[y]$ as below, the irreducible factors can be grouped into three equivalence classes, $[y], [2y+3]$ and $[y^2+5y+1]$.

$$u = \underbrace{(y-4)(y-1)^3y(y+1)^2}_{\in[y]}\underbrace{(2y-5)(2y+3)^2(2y+9)}_{\in[2y+3]} \times \underbrace{(y^2+5x+1)(y^2+11y+25)^3}_{\in[y^2+5y+1]}.$$

The values $v_u(p)$ and $v_u^<(p)$ for different factors p of u are $v_u(y-4) = 1$, $v_u^<(y-4) = 0$, $v_u^<(y+1) = 3$, and so on.

In Theorem 4.3.6 we now can give a denominator exponent bound for p-removing operators. We summarize the results of this section that are necessary to apply Algorithm 4.2.1 in a setting of Ore algebras with a trivial pseudo-derivation.

Theorem 4.3.6. *Let $L \in \mathbb{D}[X; \sigma, 0]$ with $l_0 \neq 0$ be of order r and let p be an irreducible factor of $\mathrm{lc}(L)$ such that p^k is removable from L for some $k \geq 1$. Let $n \in \mathbb{N}$ be such that $\gcd(\sigma^n(p), l_0) \neq 1$ and $\gcd(\sigma^m(p), l_0) = 1$ for all $m > n$. Then there exists a p^k-removing operator P for L of the form*

$$P = \frac{p_0}{\sigma^n(p)^{e_0}} + \frac{p_1}{\sigma^n(p)^{e_1}}X + \cdots + \frac{p_n}{\sigma^n(p)^{e_n}}X^n,$$

for some $e_i \in \mathbb{N}$ and $p_i \in \mathbb{D}$ with

1. $\deg(p_i) < e_i \deg(\sigma^n(p))$ *and* $\gcd(\sigma^n(p), p_i) = 1$, *and*

2. $e_i \leq k + n\, v^{<}_{\mathrm{lc}(L)}(p)$,

for $i = 0, \ldots, n-1$, *and* $p_n = 1$, $e_n = k$.

Proof. Lemmas 4.2.1 and 4.3.3 imply the existence of an operator P with all the required properties except possibly the exponent estimate. Let P be such an operator, and consider the operator $T := \sum_{i=0}^{r+n} t_i X^i := PL \in \mathbb{D}[X; \sigma, 0]$. Let $e = \max\{e_1, \ldots, e_n\}$ and $\bar{P} := \sum_{i=0}^{n} \bar{p}_i X^i := \sigma^n(p)^e P$. Then $\bar{p}_i = \sigma^n(p)^{e-e_i} p_i$ $(i = 0, \ldots, n)$ and $\sigma^n(p)^e T = \bar{P}L$ and $\gcd(\bar{p}_0, \ldots, \bar{p}_n, \sigma^n(p)) = 1$. Abbreviating $v := v^{<}_{\mathrm{lc}(L)}(p)$, assume that $e > k + n\, v$. We will show by induction that then $\bar{p}_i$ contains $\sigma^n(p)$ with multiplicity more than $i\, v$ for $i = n, n-1, \ldots, 0$, which is inconsistent with $\gcd(\bar{p}_0, \ldots, \bar{p}_n, \sigma^n(p)) = 1$.
First, it is clear that $\bar{p}_n = \sigma^n(p)^{e-e_n} p_n \sigma^n(l_r)$ contains $\sigma^n(p)$ with multiplicity $\geq e - k > nv$, because P is p^k-removing. Suppose now as induction hypothesis that there is an $i \geq 0$ such that $\sigma^n(p)^{j\, v+1} \mid \bar{p}_j$ for $j = n, n-1, \ldots, i+1$. Consider the equality

$$\sigma^n(p)^e t_{i+r} = \bar{p}_i \sigma^i(l_r) + \bar{p}_{i+1} \sigma^{i+1}(l_{r-1}) + \cdots + \bar{p}_n \sigma^n(l_{r-n}),$$

where we use the convention $l_j := 0$ for $j < 0$. The induction hypothesis implies that $\sigma^n(p)^{(i+1)v+1} \mid \bar{p}_j$ for $j = n, n-1, \ldots, i+1$. Furthermore, since $(i+1)v \leq nv < e$, we have $\sigma^n(p)^{(i+1)v+1} \mid \sigma^n(p)^e t_{i+r}$. Both facts together imply $\sigma^n(p)^{(i+1)v+1} \mid \bar{p}_i \sigma^i(l_r)$. The definition of v ensures that $\sigma^n(p)$ is contained in $\sigma^i(l_r)$ with multiplicity at most v, so it must be contained in $\bar{p}_i$ with multiplicity more than $(i+1)v - v = i\, v$, as claimed. □

Example 4.3.7. In the leading coefficient of $L \in \mathbb{Q}[n][S; s_n, 0]$ with

$$L = -(n-2)(n+1)^2 S^2 + (n^3 + 2n^2 + n - 4)S - (n+1)(n+5),$$

the factor $p = (n+1)$ appears. The dispersion of p in L is 4 and $v^{<}_{\mathrm{lc}(L)}(p) = 1$. If there exists a p-removing operator, we are guaranteed to find it by running Algorithm 4.2.1 with input $k = 1$, $N = 4$ and $E = 1 + 4 \cdot 1 = 5$. A possible output is

$$P = \frac{840}{n+5} S^4 + \frac{840}{n+5} S^3 + \frac{252}{n+5} S^2 + \frac{28}{n+5} S + \frac{1}{n+5}.$$

Here, the multiplicity of $\sigma^4(p)$ in the denominators of the coefficients is smaller than the bound E.
Similarly, we can try to remove p from

$$L_2 = (n+1)nS^2 + (3n+2)S - (n+6).$$

When running the algorithm with input $k = 1$, $N = 5$ and $E = 1 + 5 \cdot 0 = 1$, the output is $\perp$, so p_2 cannot be removed from L_2.

4.3.2 Differential Case

Desingularization of differential operators is classical and well-known (see for example [47] and [27]). We include it for the sake of completeness and describe how the classical desingularization method yields the necessary bounds for Algorithm 4.2.1. For simplicity, we only consider the case where a linear factor can be completely removed from the leading coefficient of an operator in $\mathbb{C}[y][\partial; 1, \frac{d}{dy}]$. In [52], more general results can be found that also cover the case where full desingularization is not possible but the multiplicity of a factor can be reduced. With the possible exception of the bound for the exponents in Theorem 4.3.13, the theory in this section can also be found in [47, 27] and [1], on which this summary is based.

As was already indicated in Section 4.1, there is a strong connection between the solutions of a differential operator and its removable factors. We now investigate this connection in more detail. In the context of differential equations, roots of removable factors are called *apparent singularities*. To be more precise, the term 'apparent singularity' is defined in terms of solutions of several different kinds of operators and for differential operators in $\mathbb{C}[y][\partial; 1, \frac{d}{dy}]$, every apparent singularity $\gamma \in \mathbb{C}$ of an operator corresponds to a removable factor $(y - \gamma)$ of its leading coefficient and vice versa. One also distinguishes between *regular* and *irregular* singularities of an operator. For our purpose it is enough to know that this distinction exists and it is not necessary to know the formal definitions, which can be found in [27]. Points in the complex plane that are not roots of the leading coefficient of a given operator are called *ordinary points*.

When considering expansions at an ordinary point or an apparent singularity, the solution space of a given operator is spanned by formal power series solutions.

Lemma 4.3.8. *Let $L \in \mathbb{C}[y][\partial; 1, \frac{d}{dy}]$ and $\gamma \in \mathbb{C}$. Then the following are equivalent:*

1. *γ is either an ordinary point or an apparent singularity.*
2. *L has $\operatorname{ord}(L)$ linearly independent solutions of pairwise different orders in $\mathbb{C}[[y - \gamma]]$, the ring of formal power series in $(y - \gamma)$. This implies that γ is not an irregular singular point of L.* □

From this, a necessary condition for a singularity to be apparent can be derived that does not require the computation of the formal solutions. Let $L \in \mathbb{C}[y][\partial; 1, \frac{d}{dy}]$ and let $f = \sum_{z=-\infty}^{\infty} f_z y^z$ be a formal Laurent series with undetermined coefficients, i.e. we assume there is an unknown minimal index $m \in \mathbb{Z}$ such that $f_m \neq 0$ and $f_i = 0$ for $i < m$. The ith derivative of f is

$$\frac{\partial^i}{\partial y^i} f = \sum_{z=-\infty}^{\infty} f_{z+i}(z+i)^{\underline{i}} y^z.$$

When substituting ∂^i in L by the ith derivative of f, the resulting expression is a sum of the form

$$\sum_{z=-\infty}^{\infty} P(f)y^z,$$

where P is a linear recurrence operator with polynomial coefficients. Let $p_0, \ldots, p_{-k} \in \mathbb{C}[z]$ be such that

$$P(f) = p_0(z)f_z + p_{-1}(z)f_{z-1} + \cdots + p_{-k}(z)f_{z-k}.$$

Suppose that f is a power series solution of L of some order r. Then by plugging in r for z in $P(f)$ one sees that $p_0(r) = 0$ has to hold. So only integer roots of p_0 qualify as orders of power series solutions of L. This approach can be generalized to series expansions at other points in the complex plane by setting $f = \sum_{z=-\infty}^{\infty} f_z p^z$ where p is an irreducible polynomial in $\mathbb{C}[y]$. We then call $\operatorname{ind}_L(p) := p_0 \in \mathbb{C}[z]$ the *indicial polynomial* of L at p, where p_0 is obtained in the same way as above.

Lemma 4.3.9. *Let $L \in \mathbb{C}[y][\partial; 1, \frac{d}{dy}]$ and $\gamma \in \mathbb{C}$. If L has a solution in $\mathbb{C}[[y-\gamma]]$ of order $r \in \mathbb{N}$, then r is a root of $\operatorname{ind}_L(y-\gamma)$.* □

Example 4.3.10. Consider

$$L = (y+3)\partial - 1 \text{ and } p = y + 3.$$

We substitute ∂^i in L by the ith derivative of $f = \sum_{z=-\infty}^{\infty} f_z p^z$ and get

$$L(f) = (y+3)\sum_{z=-\infty}^{\infty} f_{z+1}(z+1)p^z - \sum_{z=-\infty}^{\infty} f_z p^z.$$

Writing this as a series expanded at p, we get $L(f) = \sum_{z=-\infty}^{\infty} P(f)p^z$ with

$$P(f) = (z-1)f_z.$$

So the indicial polynomial of L at p is

$$\operatorname{ind}_L(p) = z - 1.$$

By Lemma 4.3.9, L has no solution in $\mathbb{C}[[y+3]]$ of order 0.

For an ordinary point $\gamma \in \mathbb{C}$, the orders of the formal power series solutions in $\mathbb{C}[[y-\gamma]]$ and hence also the roots of the indicial polynomial form a sequence of consecutive integers.

Lemma 4.3.11. *Let $L \in \mathbb{C}[y][\partial; 1, \frac{d}{dy}]$ and $\gamma \in \mathbb{C}$. Then the following are equivalent:*

1. *γ is not an irregular singularity of L, the formal solutions of L at γ are in $\mathbb{C}[[y-\gamma]]$ and their orders are $0, 1, \ldots, d_L - 1$.*
2. *γ is an ordinary point of L.* □

By combining Lemmas 4.3.8, 4.3.9 and 4.3.11, we get an easy way to desingularize a differential operator L. We construct a left multiple of L with a solution space that contains power series solutions whose orders are the 'missing' roots of the indicial polynomial of L.

Lemma 4.3.12. *Let $L \in \mathbb{C}[y][\partial; 1, \frac{d}{dy}]$ and let $p = y - \gamma$ be an irreducible factor of $\mathrm{lc}(L)$ such that p is desingularizable from L. Let $m \in \mathbb{N}$ be such that $(z - m) \mid \mathrm{ind}_L(p)$ and $(z - m') \nmid \mathrm{ind}_L(p)$ for all $m' > m$. Set*

$$n = \deg\left(\frac{z^{\underline{m+1}}}{\gcd(\mathrm{ind}_L(p), z^{\underline{m+1}})}\right).$$

Then p is desingularizable at order n from L.

Proof. Let $m_1, \ldots, m_n \in \mathbb{N}$ be such that

$$\gcd(\mathrm{ind}_L(p), z^{\underline{m+1}}) \prod_{i=1}^{n} (z - m_i) = z^{\underline{m+1}}.$$

According to Lemma 4.3.8, since p is desingularizable from L, there are $\mathrm{ord}(L)$ linearly independent solutions of L in $\mathbb{C}[[y-\gamma]]$. By Lemma 4.3.9, L has no solutions of order m_i in $\mathbb{C}[[y - \gamma]]$ for $1 \leq i \leq n$. According to Example 3.2.8 part 1, for each p^{m_i} there is an order 1 annihilating operator $L_i \in \mathbb{C}[y][\partial; 1, \frac{d}{dy}]$. We set

$$L' = \mathrm{lclm}(L_n, \mathrm{lclm}(L_{n-1}, \mathrm{lclm}(\ldots, \mathrm{lclm}(L_1, L)\ldots))).$$

L' then is of order at most $n + \mathrm{ord}(L)$ and has $n + \mathrm{ord}(L)$ many linearly independent solutions in $\mathbb{C}[[y - \gamma]]$: The $\mathrm{ord}(L)$ many linearly independent solutions in $\mathbb{C}[[y - \gamma]]$ of L and one solution from each L_i, $1 \leq i \leq n$. By Lemma 4.3.8, γ is not an irregular singularity of L', the formal solutions of L' at γ are in $\mathbb{C}[[y - \gamma]]$ and their orders are $0, 1, \ldots, \mathrm{ord}(L') - 1$. Thus by Lemma 4.3.11, γ is an ordinary point of L'. □

While the proof of Lemma 4.3.12 gives rise to a desingularization algorithm for differential operators, we can also use the order bound for Algorithm 4.2.1. The necessary bound for the exponents in the denominators of the coefficients of a desingularizing operator can be obtained in a way similar to the shift case.

Theorem 4.3.13. *Let $L \in \mathbb{C}[y][\partial; 1, \frac{d}{dy}]$ be of order r and let p be an irreducible factor of $\mathrm{lc}(L)$ such that p is desingularizable from L. Furthermore, let k be the multiplicity of p in L and let $n \in \mathbb{N}$ be as in Lemma 4.3.12. Then there exists a p-desingularizing operator P for L of the form*

$$P = \frac{p_0}{p^{e_0}} + \frac{p_1}{p^{e_1}}\partial + \cdots + \frac{p_n}{p^{e_n}}\partial^n,$$

for some $e_i \in \mathbb{N}$ and $p_i \in \mathbb{C}[y]$ with

1. $\deg(p_i) < e_i \deg(p)$ *and* $\gcd(p, p_i) = 1$, *and*

2. $e_i \leq (n+1)k$,

for $i = 0, \ldots, n-1$, *and* $p_n = 1$, $e_n = k$.

Proof. Part 1 and the form of P follow from Corollary 4.2.2. The order of P follows from Lemma 4.3.12. We prove part 2 in the same way as part 2 of Theorem 4.3.6. Consider the operator $T := \sum_{i=0}^{r+n} t_i X^i := PL \in \mathbb{C}[y][\partial; 1, \frac{d}{dy}]$. Let $e = \max\{e_1, \ldots, e_n\}$ and $\bar{P} := \sum_{i=0}^{n} \bar{p}_i X^i := p^e P$. Then $\bar{p}_i = p^{e-e_i} p_i$ $(i = 0, \ldots, n)$ and $p^e T = \bar{P} L$ and $\gcd(\bar{p}_0, \ldots, \bar{p}_n, p) = 1$.
Assume $e > (n+1)k$. We show by induction that then $\bar{p}_i$ contains p with multiplicity more than ik for $i = n, n-1, \ldots, 0$, therefore contradicting $\gcd(\bar{p}_0, \ldots, \bar{p}_n, p) = 1$.
Since P is a p^k-removing operator in normal form, its leading coefficient is $1/p^k$. Thus $\bar{p}_n$ contains p with multiplicity $e - k > nk$.
Suppose now as induction hypothesis that there is an $i \geq 0$ such that $p^{jk+1} \mid \bar{p}_j$ for $j = n, n-1, \ldots, i+1$. Consider the equality

$$p^e t_{i+r} = \bar{p}_i l_r + \bar{p}_{i+1}(\ldots) + \cdots + \bar{p}_n(\ldots),$$

where the cofactors of the $\bar{p}_i$ are linear combinations of some (derivatives of) coefficients of L. The induction hypothesis implies that $p^{jk+1} \mid \bar{p}_j$ for $j = n, n-1, \ldots, i+1$. Furthermore, , since $(i+1)k \leq nk < e$, we have $p^{(i+1)k+1} \mid p^e t_{i+r}$. Both facts together imply $p^{(i+1)k+1} \mid \bar{p}_i l_r$. The multiplicity of p in l_r is k, so p must be contained in $\bar{p}_i$ with multiplicity more than $(i+1)k - k = ik$, as claimed. □

Example 4.3.14. We try to remove the factor $p = (y-1)$ from the operator

$$L = (y-1)(-5y^2 - 2y + 21)\partial^2 + (16y^2 - 12y - 18)\partial - 20.$$

To get an order bound for the desingularizing operator, we compute the indicial polynomial:

$$\mathrm{ind}_L(p) = 14(z-2)z.$$

In $\mathrm{ind}_L(p)$, the factor $(z-1)$ is missing to complete the factorial $z^{\underline{3}}$. This suggests the order bound $N = 1$. The multiplicity of p in L is $k = 1$, so as the bound for the exponents in the denominators of the coefficients of a desingularizing operator we get $E = 2$. Running Algorithm 4.2.1 with this input yields as possible output

$$P = -\frac{22}{y-1}\partial.$$

p is desingularizable from L at order 1.

Chapter 5

Order-Degree Bounds for Annihilator Ideals

5.1 Degree-Reduction by Desingularization

A holonomic sequence or function is not only annihilated by one, but infinitely many operators of different orders and maximal coefficient degrees. Usually, it is possible to find an operator of relatively low degree if the order is chosen high enough and vice versa. Depending on the context, operators of certain order-degree combinations might be more useful than others. An operator of lowest order has the smallest solution space, an operator of lowest degree gives information about the non-removable factors and the singularities of the solutions, an operator with balanced order and degree is likely to be fast to compute, and so on. In this chapter we investigate which properties of a generator of an annihilator ideal can be used to predict all possible order-degree pairs (r, d) such that there exists an element in the contraction of the ideal with order r and degree d.

We have seen that we can easily reduce the degree of a given operator if we can remove some singularities from its leading coefficient. The normal form of a removing operator suggests that the numerator degree is strictly less than the denominator degree for each of its coefficients and so, the degree in the removed operator will drop by at least 1. The main idea behind getting good order-degree bounds is a trade-off between the leading coefficient degree – which is minimal when considering a removing operator for all removable factors – and the degree of all the other coefficients. We modify removing operators in a way that allows the leading coefficient to be bigger and in return reduce the maximal degree. The problem of order-degree bounds was already considered in [16] for recurrence operators and in [17] for differential operators. The new results presented here were found in collaboration with S. Chen, M. Kauers and M. Singer and have been published in [15]. In Section 5.2 we provide a comparison of the old and the new results for some examples.

Example 5.1.1. Assume we are given a finite sequence of rational numbers that comes from a sequence $(t_n)_{n\in\{0,1,\dots\}}$ which admits a linear recurrence equation with polynomial coefficients. If the amount of data is sufficiently large, we are able to guess recurrence operators of some fixed order and maximal coefficient degree that annihilate $(t_n)_{n\in\{0,1,\dots\}}$. For details on guessing and implementations of the method, see [29, 26]. For example, consider

$$t_n = \sum_{k=0}^{n} \left(\binom{2n+4}{k} + (2n-k)! + k^3 \right).$$

Depending on the number of terms we have given, we can guess operators of different orders and coefficient degrees. The gray area and the green dots in Figure 5.1.1 indicate the order-degree-pairs for which we can find recurrence operators for the sequence t_n. For the order-degree pair $(6, 21)$ represented by the leftmost green dot we can find a generator L of the annihilating ideal of t_n whose leading coefficient contains a removable factor of degree 17. By using Algorithm 4.2.1 we can construct a left multiple of L of order 7 where the degree of the leading coefficient is reduced to 4 (indicated by the blue dot) and the other coefficients have degrees up to 20. (indicated by the red dot and the yellow line). The goal is to balance the degrees such that the red and the blue dot meet at $(7, 12)$.

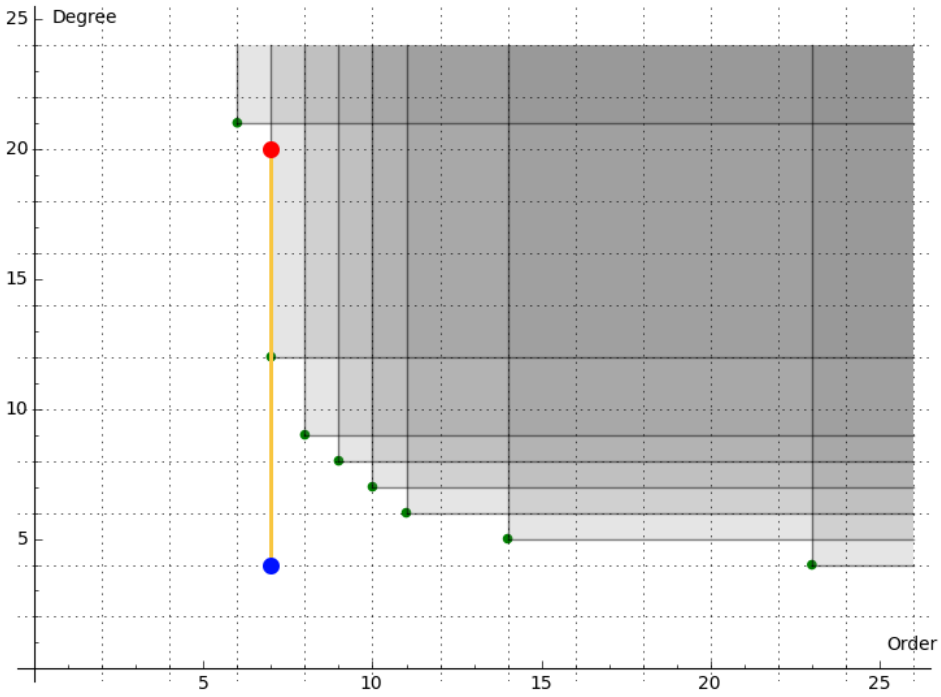

Figure 5.1.1: Order-Degree pairs in the annihilating ideal from Example 5.1.1.

We describe our approach of balancing degrees in two ways. First we give a general overview of the method and then illustrate it in a feasible example.

Let L be an Ore polynomial in $\mathbb{K}[y][X;\sigma,\delta]$ and let $P \in \mathbb{K}(y)[X;\sigma,\delta]$ be a p-removing operator for L in normal form (Figure 5.1.2 top). To balance the degrees in PL, we proceed as follows: Take an operator Q with undetermined coefficients of degree $\deg(p)-1$ and multiply it on P. In the result QP we reduce the numerator degrees so that they are lower than the denominator degrees (Figure 5.1.2 middle). Now, the undetermined coefficients of Q appear in the numerators of the coefficients of QP and we can equate some of the highest degree coefficients to 0. This gives a linear system and by choosing the order of Q and the number of equations in the system carefully, we make sure that it has a non-zero solution. Multiplying QP on L then will reduce the degree in L further than just multiplying P on L. (Figure 5.1.2 bottom)

Example 5.1.2. Consider the recurrence operator

$$L = (2n^3+2n+2)S - (2n^3+6n^2+8n+6) \in \mathbb{Q}[n][S; s_n, 0],$$

Using Algorithm 4.2.1, we can compute an order 1 operator P that removes the factor $p = 2n^3+2n+2$:

$$P = \frac{1}{\sigma(p)}S + \frac{1}{47}\left(\frac{18n^2+102n+109}{\sigma(p)}\right).$$

When we multiply P on L, we see that while the degree of the leading coefficient drops to 0, the degree of the other coefficients only decreases by 1.

$$PL = S^2 + \frac{2}{47}(9n^2+24n-68)S - \frac{1}{47}(18n^2-102n-109).$$

By computing the dispersion of p in L, one can see that L is of the form

$$L = pS - \sigma(p),$$

so it is an annihilating operator of minimal order for the sequence $t_n = p(n)$. We have seen in Example 3.2.3 part 1 that sequences given by a polynomial term in $\mathbb{Q}[n]$ admit a recurrence equation with coefficients in $\mathbb{Q}$, and so, there exists a left multiple of L where all coefficients are of degree $= 0$. We aim at modifying the p-removing operator P in such a way that we can get two left multiples of L with maximum degree 1 and 0 respectively. By this we illustrate the proof of the main theorem of this chapter, Theorem 5.1.5, even though in this case there are easier ways to find a recurrence with coefficients in $\mathbb{Q}$ for p.

As was shown in Lemma 4.2.1 part 1, certain left multiples of p-removing operators are also p-removing, so we can multiply P with some element from $\mathbb{Q}[n]$ coprime to p. Furthermore, Lemma 4.2.1 part 2 allows us to remove polynomial parts in the coefficients of p-removing operators. This means by taking $Q_1 \in \mathbb{Q}[n]$ of degree $< \deg(p)$ with undetermined coefficients and removing the polynomial parts in Q_1P, we get a p-removing operator P_2 for L such that the degree maximum of P_2L is ≤ 2 and the coefficients contain the undetermined coefficients of Q_1. This allows us to equate some of the higher degree coefficients to zero, solve the linear systems in terms of the coefficients of Q_1 and thereby reduce the degree of P_2L.
In this particular example, we get for Q_1

$$Q_1 = 3n - 8,$$

and for this choice P_2 becomes

$$P_2 = \frac{3n-8}{\sigma(p)}S + \frac{-15n-22}{\sigma(p)}.$$

Multiplying P_2 to L then gives a left multiple of L of order 2 with maximal coefficient degree 1:

$$P_2L = (3n-8)S^2 + (-18n+22)S + (15n+22).$$

To further reduce the degree, one needs to increase the number of equations in the linear system while preserving the solvability, which means having more variables than equations. To do so, we can set Q_2 to be an operator of higher order (note that Q is an operator of order 0) with indeterminate polynomial coefficients of degree $< \deg(p)$. As before, we then can multiply Q_2 to P, remove the polynomial parts to get P_3 and equate some high degree coefficients to zero.
Here, we get Q_2 of the form

$$Q_2 = S^2 + (\dots \text{degree } 9 \dots)S + (\dots \text{degree } 18 \dots),$$

and after multiplying it to P and reducing the numerators of the coefficients by the respective denominators, P_3 is

$$\begin{aligned} P_3 =& \frac{1}{\sigma^3(p)}S^3 + \frac{-6n^3-48n^2-126n-110}{\sigma^2(p)^{[2]}}S^2 \\ &+ \frac{6n^3+24n^2+30n+22}{\sigma(p)^{[2]}}S - \frac{1}{\sigma(p)}. \end{aligned}$$

The product P_3L then is a left multiple of L with constant coefficients.

$$P_3L = S^4 - 4S^3 + 6S^2 - 4S + 1.$$

Following the same strategy with Q_3 of order 1, one ends up with a linear system that has no non-zero solution. Thus it is not possible to find Q_3 of order 1 such that Q_3PL has constant coefficients.

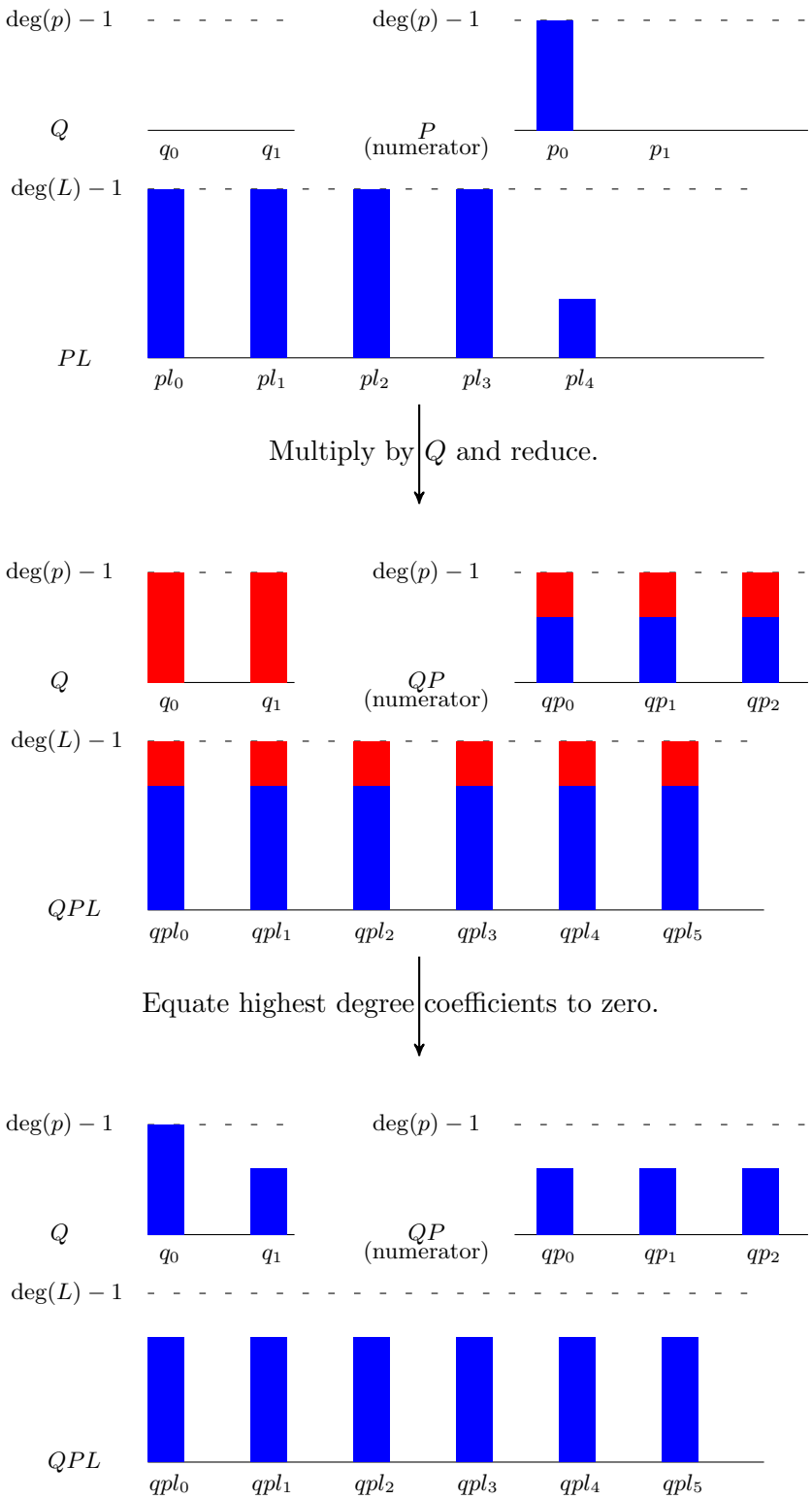

Figure 5.1.2: Balancing degrees by a modified removing operator.

Before we can formalize this approach, we prove two technical lemmas. The first generalizes the Bézout relation to more than two polynomials and will be used in the proof of the main theorem to show that the new operator with balanced coefficient degrees is not zero.

Lemma 5.1.3. *Let $u_1, \dots, u_m \in \mathbb{K}[y]$ be pairwise coprime polynomials and $u = u_1 u_2 \cdots u_m$, and let $v_1, \dots, v_m \in \mathbb{K}[y]$ be such that $\deg(v_i) < \deg(u_i)$ $(i = 1, \dots, m)$. If*

$$\sum_{i=1}^{m} v_i \frac{u}{u_i} = 0,$$

then $v_1 = v_2 = \cdots = v_m = 0$.

Proof. Since the u_i are pairwise coprime, $u_i \nmid (u/u_i)$ for all i. However, $u_i \mid (u/u_j)$ for all $j \neq i$. Both facts together with $\sum_{i=1}^{m} v_i u/u_i = 0$ imply that $u_i \mid v_i$ for all i. Since $\deg(v_i) < \deg(u_i)$, the claim follows. □

The next lemma gives a characterization of removability which is more convenient in our context.

Lemma 5.1.4. *A factor $p \in \mathbb{D}$ is removable from $L \in \mathbb{D}[X; \sigma, \delta]$ at order n if and only if there exists $P \in \mathbb{D}[X; \sigma, \delta]$ with $\operatorname{ord}(P) = n$ and $PL \in \sigma^n(p) \operatorname{lc}(P) \mathbb{D}[X; \sigma, \delta]$.*

Proof. First, let $P \in \mathbb{D}[X; \sigma, \delta]$ be of order n and such that PL is an element of $\sigma^n(p) \operatorname{lc}(P) \mathbb{D}[X; \sigma, \delta]$. Then $P' = \frac{1}{\sigma^n(p) \operatorname{lc}(P)} P$ is a p-removing operator. Conversely, start from a p-removing operator of the form

$$P' = \sum_{i=0}^{n-1} \frac{p_i}{\sigma^n(p)^{e_i}} X^i + \frac{1}{\sigma^n(p)} X^n,$$

and set $P = \sigma^n(p)^e P'$ where $e = \max\{e_0, \dots, e_{n-1}, 1\} \geq 1$. Because of $P'L \in \mathbb{D}[X; \sigma, \delta]$ it follows that

$$PL \in \sigma^n(p)^e \mathbb{D}[X; \sigma, \delta] = \sigma^n(p) \operatorname{lc}(P) \mathbb{D}[X; \sigma, \delta]. \qquad \square$$

We are ready to state the main result of this chapter, a lower bound for the degree of left multiples of a given operator as a function of the order.

Theorem 5.1.5. *Let $L \in \mathbb{K}[y][X; \sigma, \delta]$, and let $p_1, \dots, p_m \in \mathbb{K}[y]$ be factors of $\operatorname{lc}(L)$ which are removable at orders $n_1, \dots, n_m$, respectively, so that the $\sigma^{n_i}(p_i)$ are pairwise coprime. Let $r \geq \operatorname{ord}(L)$ and*

$$d \geq \deg(L) - \left\lceil \sum_{i=1}^{m} \Big(1 - \frac{n_i}{r - \operatorname{ord}(L) + 1}\Big)^+ \deg(p_i) \right\rceil,$$

where we use the notation $(x)^+ := \max\{x, 0\}$. Then there exists an operator $Q \in \mathbb{K}(y)[X; \sigma, \delta] \setminus \{0\}$ such that $QL \in \mathbb{K}[y][X; \sigma, \delta]$ and $\operatorname{ord}(QL) = r$ and $\deg(QL) = d$.

Proof. Set $s := r - \operatorname{ord}(L)$ so that $s = \operatorname{ord}(Q)$. We may assume without loss of generality that s is such that $1 - \frac{n_i}{r-\operatorname{ord}(L)+1} = 1 - \frac{n_i}{s+1} > 0$ for all i by simply removing all the p_i for which $1 - \frac{n_i}{s+1} \leq 0$ from consideration. We thus have $s \geq n_i$ for all i.

Lemma 5.1.4 yields operators $P_i \in \mathbb{K}[y][X;\sigma,\delta]$ of order n_i with $P_iL \in \sigma^{n_i}(p_i)\operatorname{lc}(P_i)\mathbb{K}[y][X;\sigma,\delta]$. Set

$$q = \prod_{i=1}^{m}\prod_{j=0}^{s-n_i} \sigma^{j+n_i}(p_i)\sigma^j(h_i),$$

where $h_i = \operatorname{lc}(P_i)$. Consider the ansatz

$$Q_1 = \sum_{i=1}^{m}\sum_{j=0}^{s-n_i} q_{i,j}\frac{q}{\sigma^{j+n_i}(p_i)\sigma^j(h_i)}X^jP_i,$$

for undetermined polynomial coefficients $q_{i,j}$ $(i = 1,\dots,m;\ j = 0,\dots,s-n_i)$ of degree less than $\deg(p_i)$. Regardless of the choice of these coefficients, we will always have $Q_1 \in \mathbb{K}[y][X;\sigma,\delta]$ and $Q_1L \in q\mathbb{K}[y][X;\sigma,\delta]$. Also, for arbitrary $R \in \mathbb{K}[y][X;\sigma,\delta]$ and $Q_2 = Q_1 - qR$ we have $Q_2 \in \mathbb{K}[y][X;\sigma,\delta]$ and $Q_2L \in q\mathbb{K}[y][X;\sigma,\delta]$. This means that we can replace the coefficients in Q_1 by their remainders upon division by q without violating any of the mentioned properties of Q_1.

Also observe that any operator Q_2 obtained in this way is nonzero unless all the $q_{i,j}$ are zero, because if k is maximal such that at least one of the $q_{i,k}$ is nonzero, then

$$\operatorname{lc}(Q_1) = \sum_{i=1}^{m} q_{i,k}\frac{q}{\sigma^{k+n_i}(p_i)\sigma^k(h_i)}\sigma^k(h_i) = \sum_{i=1}^{m} q_{i,k}\frac{q}{\sigma^{k+n_i}(p_i)},$$

is nonzero by Lemma 5.1.3. Furthermore, we have $\operatorname{lc}(Q_1) \not\equiv 0 \bmod q$, because $\deg(q_{i,k}) < \deg(p_i)$ implies $\deg(\operatorname{lc}(Q_1)) < \deg(q)$.

The ansatz for the $q_{i,j}$ gives $\sum_{i=1}^{m}(s - n_i + 1)\deg(p_i)$ variables. Plug this ansatz into Q_1 and reduce all the polynomial coefficients modulo q to obtain an operator Q_2 of degree less than $\deg(q) = \sum_{i=1}^{m}(s - n_i + 1)(\deg(p_i) + \deg(h_i))$. Then for each of the $s+1$ polynomial coefficients in Q_2 equate the coefficients of the terms y^j for

$$j > \sum_{i=1}^{m}\Big((s-n_i)\deg(p_i) + (s-n_i+1)\deg(h_i)\Big) + \left\lfloor \frac{\sum_{i=1}^{m} n_i\deg(p_i)}{s+1} \right\rfloor,$$

to zero. This gives altogether

$$\begin{aligned}
&(s+1)\Bigg(\sum_{i=1}^{m}(s-n_i+1)\big(\deg(p_i)+\deg(h_i)\big)\\
&\quad-\sum_{i=1}^{m}\Big((s-n_i)\deg(p_i)+(s-n_i+1)\deg(h_i)\Big)\\
&\quad-\left\lfloor\frac{\sum_{i=1}^{m}n_i\deg(p_i)}{s+1}\right\rfloor-1\Bigg)\\
&=(s+1)\Bigg(\sum_{i=1}^{m}\deg(p_i)-\left\lfloor\frac{\sum_{i=1}^{m}n_i\deg(p_i)}{s+1}\right\rfloor-1\Bigg),
\end{aligned}$$

equations. The resulting linear system has a nontrivial solution because

$$\begin{aligned}
&\#\text{vars}-\#\text{eqns}\\
=\;&\sum_{i=1}^{m}(s-n_i+1)\deg(p_i)-(s+1)\Bigg(\sum_{i=1}^{m}\deg(p_i)-\left\lfloor\frac{\sum_{i=1}^{m}n_i\deg(p_i)}{s+1}\right\rfloor-1\Bigg)\\
=\;&-\sum_{i=1}^{m}n_i\deg(p_i)-(s+1)\Bigg(-\left\lfloor\frac{\sum_{i=1}^{m}n_i\deg(p_i)}{s+1}\right\rfloor-1\Bigg)\\
>\;&-\sum_{i=1}^{m}n_i\deg(p_i)+\frac{s+1}{s+1}\sum_{i=1}^{m}n_i\deg(p_i)=0.
\end{aligned}$$

By construction, the solution gives rise to an operator $Q_2 \in \mathbb{K}[y][X;\sigma,\delta]$ of order at most s with polynomial coefficients of degree at most

$$\sum_{i=1}^{m}\big((s-n_i)\deg(p_i)+(s-n_i+1)\deg(h_i)\big)+\left\lfloor\frac{\sum_{i=1}^{m}n_i\deg(p_i)}{s+1}\right\rfloor,$$

for which $Q_2L \in q\mathbb{K}[y][X;\sigma,\delta]$. Thus if we set $Q=\frac{1}{q}Q_2 \in \mathbb{K}(y)[X;\sigma,\delta]$, we have $\operatorname{ord}(QL)=\operatorname{ord}(L)+s=r$ and $\deg(QL)$ is at most

$$\begin{aligned}
&\deg(L)+\deg(Q_2)-\deg(q)\\
&\le\deg(L)+\sum_{i=1}^{m}\big((s-n_i)\deg(p_i)+(s-n_i+1)\deg(h_i)\big)\\
&\quad+\left\lfloor\frac{\sum_{i=1}^{m}n_i\deg(p_i)}{s+1}\right\rfloor-\sum_{i=1}^{m}(s-n_i+1)(\deg(p_i)+\deg(h_i))\\
&=\deg(L)-\sum_{i=1}^{m}\deg(p_i)+\left\lfloor\frac{\sum_{i=1}^{m}n_i\deg(p_i)}{s+1}\right\rfloor\\
&=\deg(L)-\left\lceil\sum_{i=1}^{m}\Big(1-\frac{n_i}{s+1}\Big)\deg(p_i)\right\rceil,
\end{aligned}$$

as required. The final step uses the facts $\lfloor -x\rfloor=-\lceil x\rceil$ and $\lceil x+n\rceil=\lceil x\rceil+n$ for $x\in\mathbb{R}$ and $n\in\mathbb{Z}$. □

5.2 Examples and Applications

We compare the order-degree bound of Theorem 5.1.5 with the real order-degree areas and older bounds in several specially constructed examples and examples coming from applications. The bound in Theorem 5.1.5 turns out to be sharp in the vast majority of the cases and we only know of one class of examples (Example 5.2.6) that was provided by Mark van Hoeij where it overshoots.

Example 5.2.1. (Example 5.1.1 cont.) Applying the result given in Theorem 5.1.5 to the operator L in Example 5.1.1, we see that the order-degree area in the left ideal generated by L is bounded by a curve given by (the floor function applied to) a hyperbola:

$$\left\lfloor \frac{4r-3}{r-5} \right\rfloor, \quad \text{for } r > 5.$$

In Figure 5.2.1, it appears that for some values of r, the bound is too low, but this only happens for non-integer values of r which are irrelevant.

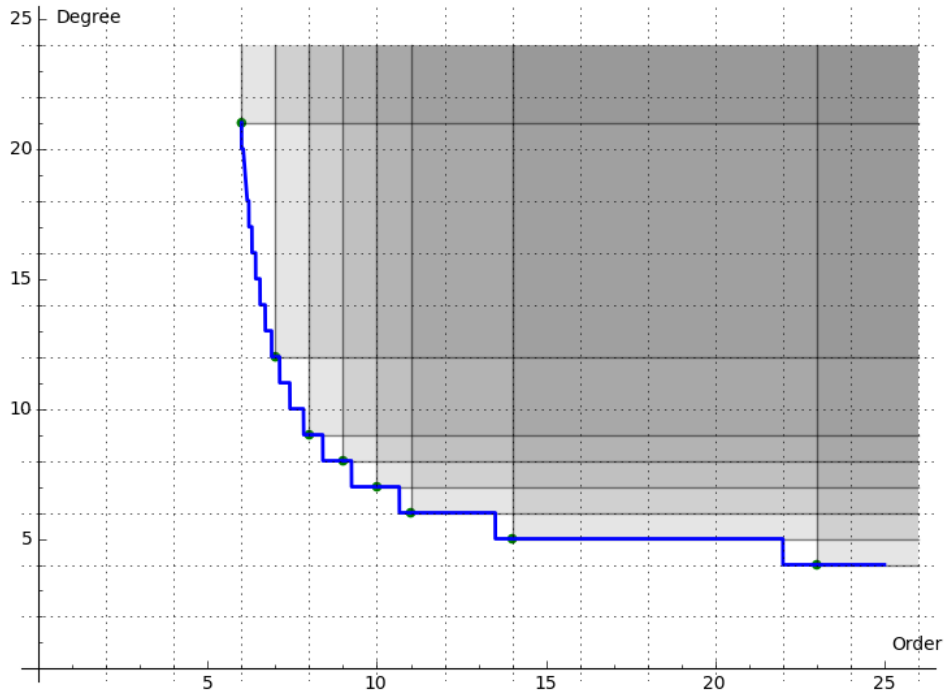

Figure 5.2.1: Order-degree bounds for Example 5.2.1.

Example 5.2.2. To obtain a recurrence operator in $\mathbb{Q}[n][S; s_n, 0]$ with removable factors with dispersion (see Section 4.3.1) greater than 1, we start from a hypergeometric term. As mentioned in Example 3.2.3, any sequence given by

$$t_n = p(n)\frac{(c_1 n)!^{k_1}}{(c_2 n)!^{k_2}},$$

with $p \in \mathbb{Q}[n]$ and $c_1, c_2, k_1, k_2 \in \mathbb{N} \setminus \{0\}$, is hypergeometric and is annihilated by the order 1 recurrence

$$L = r_{\text{den}}(n)S - r_{\text{num}}(n),$$

where $r = r_{\text{num}}/r_{\text{den}}$ is the shift quotient of t_n. The shift quotient can be written in the form

$$r(n) = \frac{p(n+1)}{p(n)} \frac{(c_1 n + c_1)(c_1 n + c_1 - 1) \dots (c_1 n + 1)}{(c_2 n + c_2)(c_2 n + c_2 - 1) \dots (c_2 n + 1)}.$$

Assume that p is such that it does not contain a factor of the form $(c_1 n + i)$ or $(c_2 n + i)$ for $i \in \mathbb{Z}$. It follows that the roots of p that are not roots of $\sigma(p)$ appear in the leading coefficient of L. We show that these are removable. To this end, we construct an annihilating operator for t_n whose leading coefficient does not contain p. Observe that for all $i \in \mathbb{N}$ with $i \geq 0$, the quotient $\sigma^i(t_n)/t_n$ is a rational function:

$$\frac{\sigma^i(t_n)}{t_n} = \frac{p(n+i)}{p(n)} \frac{(c_1 n + i c_1)!}{(c_1 n)!} \frac{(c_2 n)!}{(c_2 n + i c_2)!} = \frac{p(n+i)}{p(n)} r_i(n),$$

for some rational function r_i with numerator and denominator coprime to p. Next, let P be an annihilating operator for the C-finite sequence $p(n)$ of order $\operatorname{ord}(P) =: m$ with coefficients p_i in $\mathbb{Q}$ and set

$$L' = p_m \frac{1}{r_m} S^m + p_{m-1} \frac{1}{r_{m-1}} S^{m-1} + \dots + p_1 \frac{1}{r_1} S + p_0.$$

Then

$$\frac{1}{t_n} L'(t_n) = P(p) = 0.$$

and clearing denominators in L' will give the desired annihilator of t_n whose leading coefficient is coprime to any shift of p. Consequently, p is removable from L.

If we choose p to be a σ-factorial, we can control the dispersion of the removable singularities: Let $p = q^{[k]}$ where $q \in \mathbb{Q}[y]$ is irreducible and $k \in \mathbb{N}$. The leading coefficient of L contains the denominator of $\sigma(p^{[k]})/p^{[k]}$ and the trailing coefficient of L contains the numerator. We have

$$\frac{\sigma(p^{[k]})}{p^{[k]}} = \frac{\sigma^k(p)}{p}.$$

So p is removable at order k from L.

As a concrete example, consider

$$t_n = \left((7n-9)^{10}\right)^{[4]} \frac{(2n)!^3}{(5n)!^2}.$$

Then the shift quotient is

$$r(n) = \frac{(7n+19)^{10}}{(7n-9)^{10}} \frac{8(n+1)(2n+1)^3}{25(5n+1)^2(5n+2)^2(5n+3)^2(5n+4)^2},$$

and the factor $(7n-9)^{10}$ appears with dispersion 4 in L. The lowest order desingularizing operator is of order 4. In Figure 5.2.2 it can be seen that the order-degree curve obtained from Theorem 5.1.5 consists of a line parallel to the order axis and a translated hyperbola given by

$$\left\lfloor \frac{8(5+r)}{r} \right\rfloor, \quad \text{for } r > 3.$$

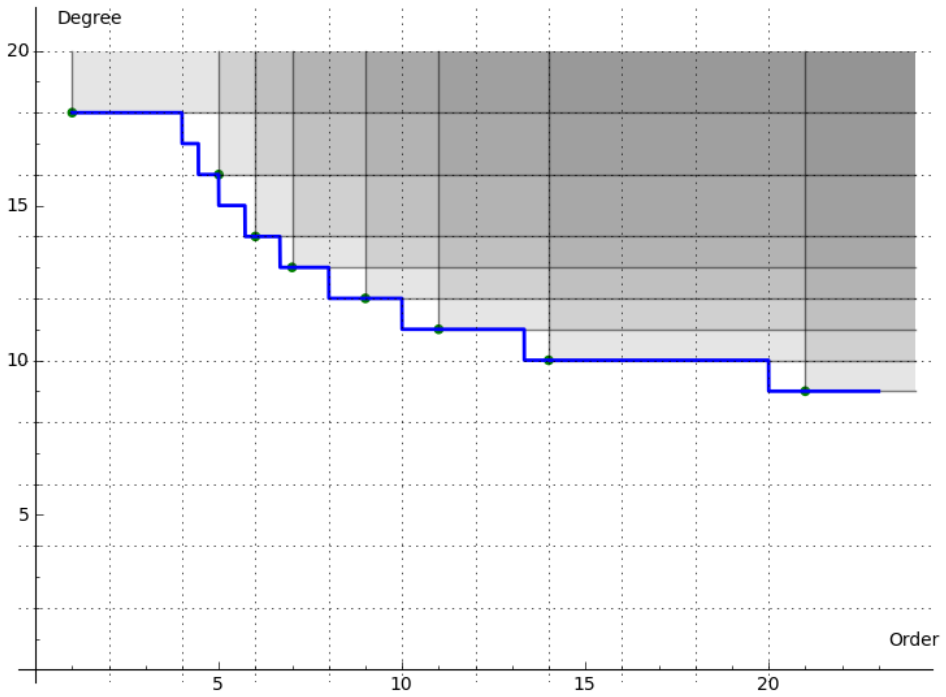

Figure 5.2.2: Order-degree bounds for Example 5.2.2.

Example 5.2.3. Similar to the construction explained in Example 5.2.2, we can obtain a recurrence operator whose leading coefficient contains two coprime factors which are removable at two different orders. Consider the hypergeometric sequence

$$t_n = \left((5n^3+3n^2+7n+5)(n+1/5)^{[11]}\right)^7 \frac{(2n)!^3}{(3n)!^2}.$$

Here, $p_1 = (5n^3+3n^2+7n+5)$ is removable at order 1 while $p_2 = (n+1/3)$ is removable at order 11. Theorem 5.1.5 suggests that the order-degree curve is given by the minimum of two hyperbolas, one emerging from the

desingularizing operator for p_1 (the red hyperbola in Figure 5.2.3) and the other one from the desingularizing operator for both, p_1 and p_2 (the blue hyperbola in Figure 5.2.3). The superposition of these two hyperbolas (the purple curve in Figure 5.2.3) then describes the exact order-degree area of the annihilator ideal.

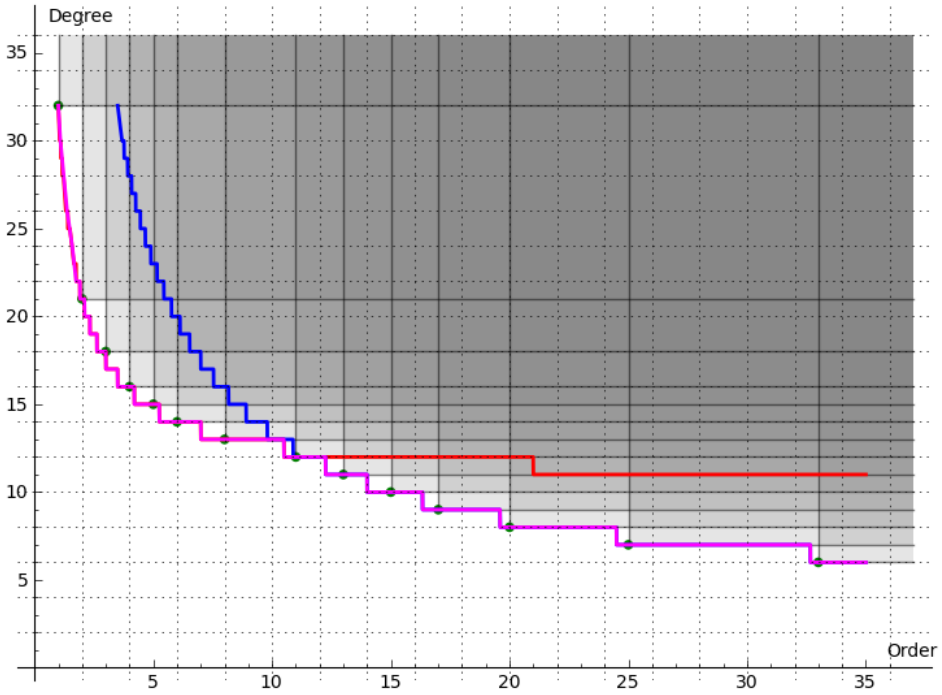

Figure 5.2.3: Order-degree bounds for Example 5.2.3.

In [16] and [17], the authors derive order-degree bounds for ideals generated by operators that come from applying hypergeometric/hyperexponential creative telescoping to summation and integration problems. In this context, the information necessary to compute the bounds come from hypergeometric and hyperexponential terms and no information about the least order operator in the ideal is required. One of the major drawbacks of Theorem 5.1.5 is that the least order operator is usually not known. There are, however, Examples where the bound presented here performs significantly better than the bounds in [16] and [17].

Example 5.2.4. Consider the minimal order telescoper L for the hypergeometric term

$$h = \frac{\Gamma(2n+k)\Gamma(n-k+2)}{\Gamma(2n-k)\Gamma(n+2k)},$$

from Example 6.2 of [16]. L is of the form

$$\begin{aligned} L = &-10n(8+5n)(9+5n)(11+5n)(12+5n)p(n)S^3 \\ &+ (\dots \text{degree } 15\dots)S^2 + (\dots \text{degree } 16\dots)S \\ &+ 9(n+1)(3n+1)(3n+2)^2(3n+4)p(n+1), \end{aligned}$$

where p is a certain irreducible polynomial of degree 10. This polynomial is removable at order 1. Therefore, by Theorem 5.1.5, we expect left multiples of L of order r and degree bounded by

$$\left\lfloor \frac{6r-2}{r-2} \right\rfloor, \quad r > 2.$$

In Figure 5.2.4 the curve $\lfloor (6r-2)/(r-2) \rfloor$ (blue) is contrasted with the estimate $\lfloor (8r-1)/(r-2) \rfloor$ (red) derived in [16] for this example. The new curve matches precisely the boundary of the gray region, even including the very last degree drop (which is not clearly visible on the figure): for $r = 12$ we have $(6r-2)/(r-2) = 7$ and for $r = 13$ we have $(6r-2)/(r-2) \approx 6.9 < 7$.

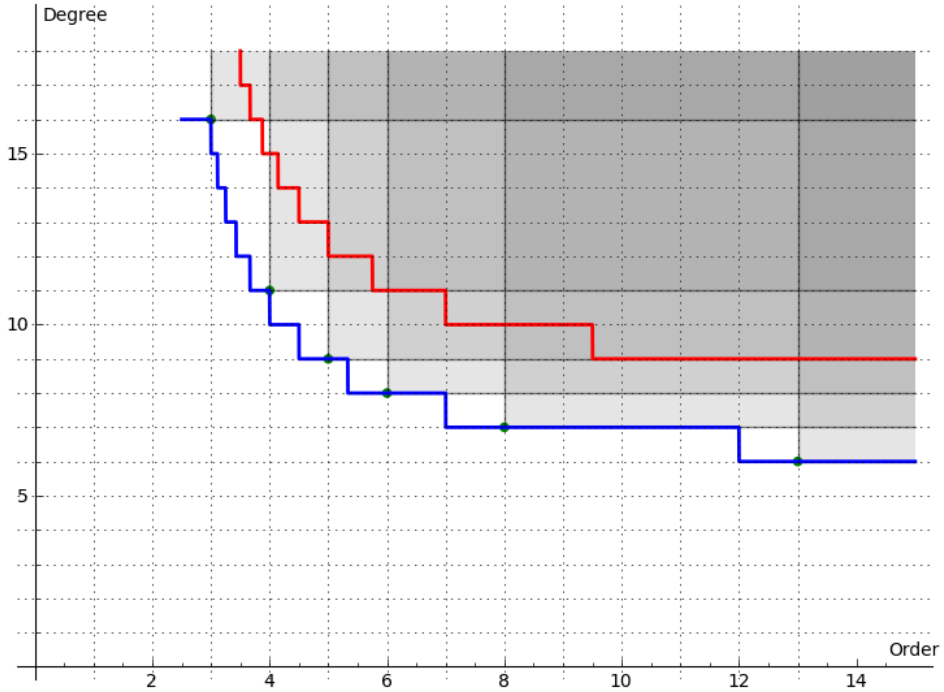

Figure 5.2.4: Order-degree bounds for Example 5.2.4.

Example 5.2.5. For the hyperexponential term $h = \frac{e^u}{v}$ with

$$\begin{aligned} u &= 4y^2z^2 + 7y^2z + 9y^2 + 5yz^2 + 2yz + 3y + 5z^2 + z + 6, \\ v &= 6y^2z^2 + 10y^2z + 6y^2 + 9yz^2 + 5yz + 8y + 8z^2 + 10z + 8, \end{aligned}$$

from Example 15.2 in [17], the minimal order telescoper L has order 3 and degree 40. The leading coefficient contains an irreducible polynomial p of degree 23 at order 1 and otherwise only non-removable factors. Theorem 5.1.5 therefore predicts left multiples of L of order r and degree

$$\left\lfloor \frac{17r-11}{r-2} \right\rfloor, \quad r > 2.$$

Again, this estimate (blue curve in Figure 5.2.5) is accurate, while the estimate $\lfloor (24r-9)/(r-2) \rfloor$ derived in [17] (red curve in Figure 5.2.5) overshoots.

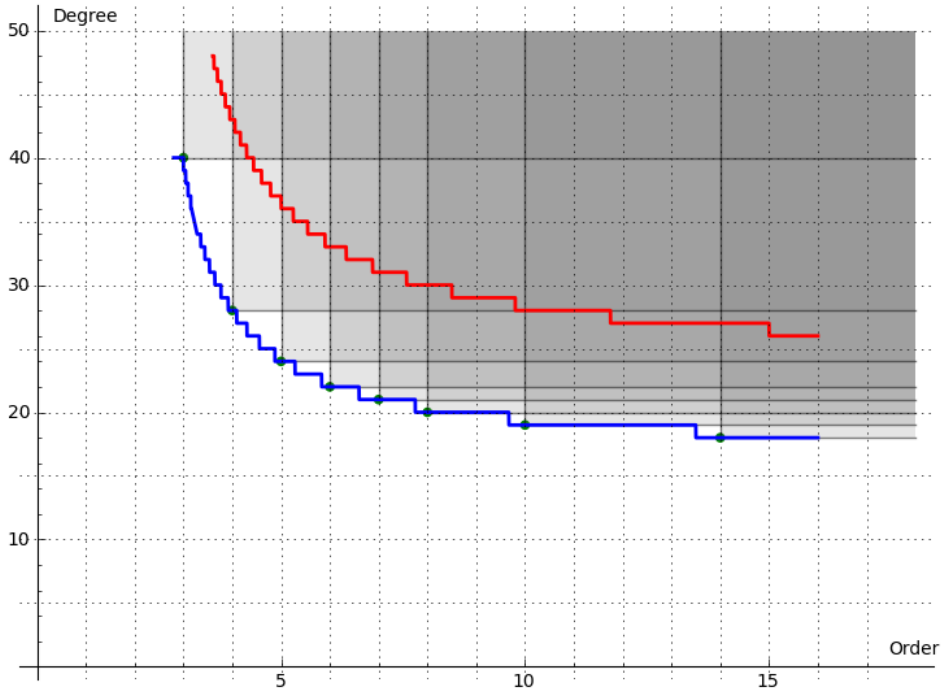

Figure 5.2.5: Order-degree bounds for Example 5.2.5.

Example 5.2.6. (M. van Hoeij, personal communication) Although the bound of Theorem 5.1.5 appears to be tight in many cases, it is not always tight. The operator

$$\begin{aligned} &n^2(n+2)^2(n+4)^2(n+6)(2n-3)S \\ &\quad -(n+1)^2(n+3)^2(n+5)^2(2n-1), \end{aligned}$$

is an example: It has a left multiple of order 2 and degree 3 although according to Theorem 5.1.5 we would expect a multiple of order 2 to have degree at least $8-(1-\frac{1}{2-1})^+4 = 4$. (Figure 5.2.6)

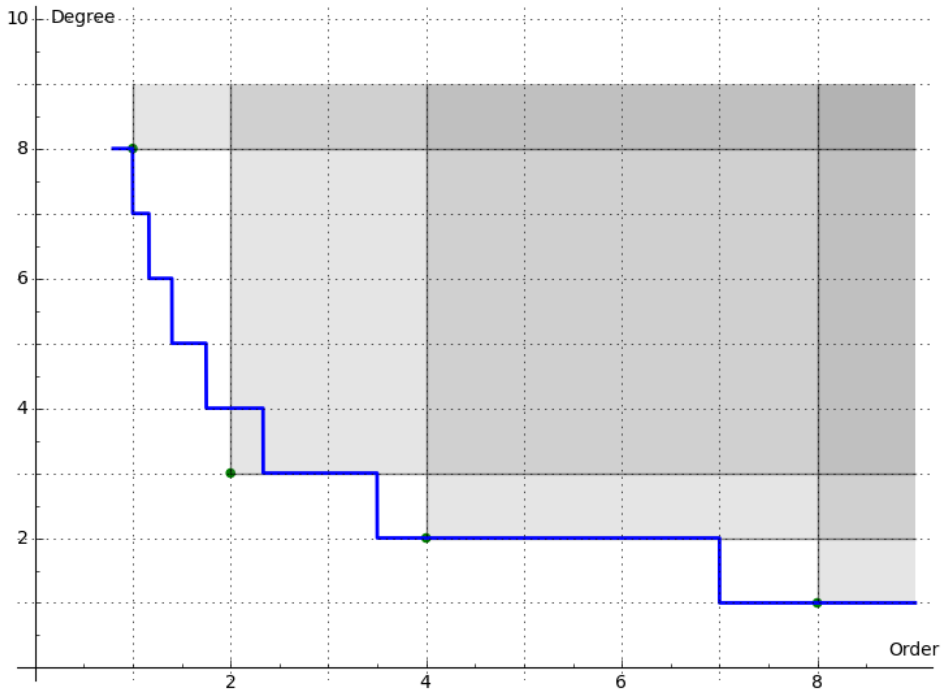

Figure 5.2.6: Order-degree bounds for Example 5.2.6.

Example 5.2.7. ([8]) Consider the following 3D-lattice walks problem for a fixed stepset in $\mathbb{Z}^3$. For $n \in \mathbb{N}$, count all the lattice walks in the octant $\mathbb{N}^3$ that start from $(0,0,0)$ and that perform exactly n steps without leaving the octant. We denote this number by t_n. This problem is studied in [8] and for a certain stepset, the authors guessed a recurrence operator $L \in \mathbb{Z}_{90017}[n][S; s_n, 0]$ that annihilates the sequence $(t_n \bmod 90017)_{n\in\mathbb{N}}$. L is of order 95 with maximal coefficient degree 3740 and its leading coefficient contains a factor of degree 3685 which is removable at order 1.
The order-degree bound (see Figure 5.2.7) predicted by Theorem 5.1.5 suggests that guessing an operator with order slightly larger than 95 is significantly faster than guessing the lowest order operator. The bound is

$$\left\lfloor \frac{55(r-27)}{r-94} \right\rfloor, \quad \text{for } r > 94.$$

Example 5.2.8. ([6]) The evaluation of Feynman diagrams in elementary particle physics leads to sequences that can be expressed in terms of generalized harmonic sums. Some examples require hundreds of different harmonic sums. All these sequences are D-finite, but of very high order. The example shown in Figure 5.2.8 was taken from [6]. The minimal order operator has order 35 and degree 938. Its leading coefficient contains a factor of degree 893 which is removable at order 1. In [6], the authors guessed two operators of order 53 and degree 92 and then computed their GCRD to get the minimal order operator. This is a point on the curve given by $\left\lfloor \frac{45r-637}{r-34} \right\rfloor$, for $r > 34$.

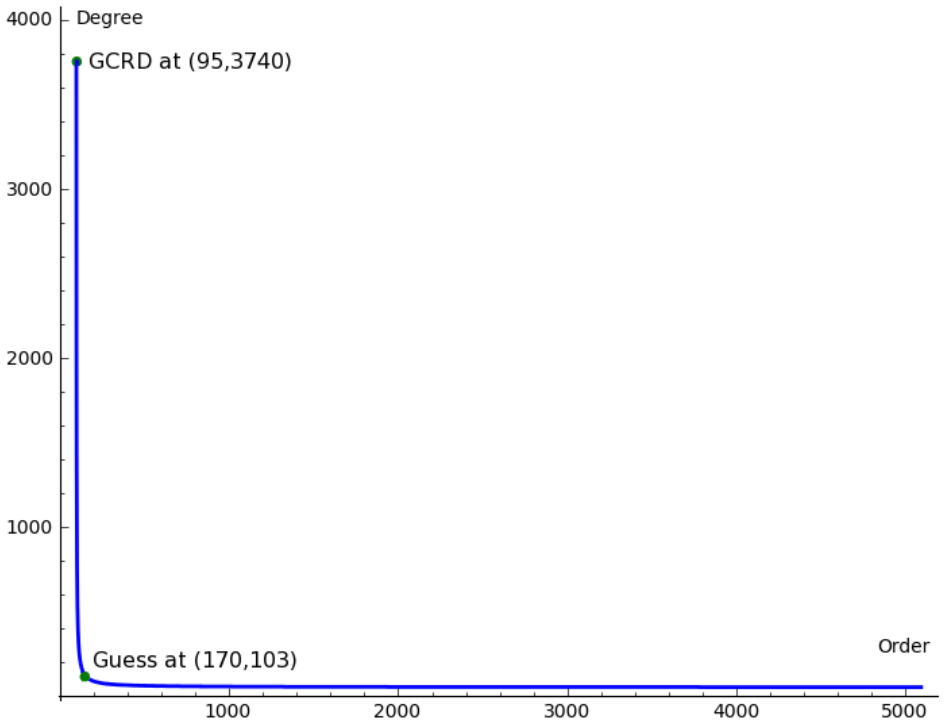

Figure 5.2.7: Order-degree bound for Example 5.2.7.

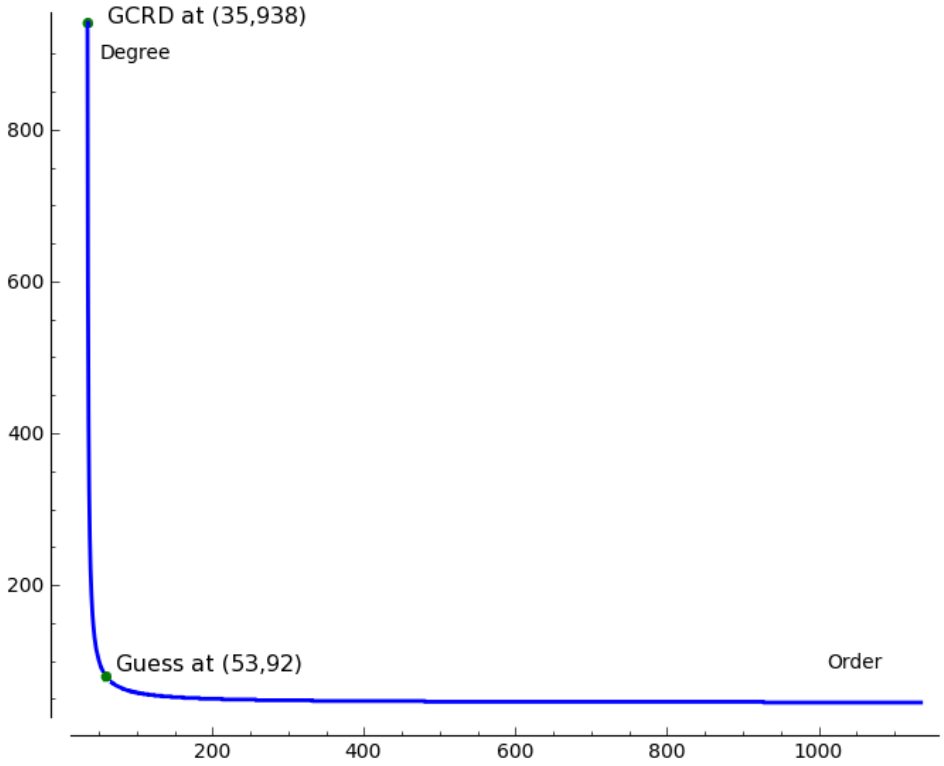

Figure 5.2.8: Order-degree bound for Example 5.2.8.

Chapter 6

Improved Polynomial Remainder Sequences for Ore Polynomials

6.1 Polynomial Remainder Sequences

We have seen that, given two operators in an Ore algebra $\mathbb{D}[X;\sigma,\delta]$, we are able to compute their greatest common right divisor using the Euclidean algorithm provided that $\mathbb{D}$ is a field. If the base ring is merely a domain, the computations will in general have to be carried out in its quotient field $\mathbb{K}$. The output will have coefficients in the quotient field, but by making use of the fact that any $\mathbb{K}\setminus\{0\}$-left multiple of a GCRD is again a greatest common right divisor of the input operators, we can clear any denominators appearing in the result and still obtain a GCRD, now with coefficients in $\mathbb{D}$. As we will see, it is possible to extend this idea and multiply also the remainders that appear during the execution of the algorithm by a sufficiently large, easy to predict factor to avoid denominators and carry out all the division steps in $\mathbb{D}[X;\sigma,\delta]$. An introduction to this technique in the commutative case can be found in [24] and [41] and for Ore operators, it is stated in [40].

Avoiding computations in $\mathbb{K}$ can significantly improve the running time of the algorithm, but careless multiplication by base ring elements might result in remainders with extraordinarily large content, outweighing the speed-up achieved by the fraction free division. To optimize the running time, we want to make sure that no non-trivial denominators appear in the remainder coefficients and at the same time divide out as much content as possible. In this chapter we derive a new way of doing so where we also try to reduce the additional costs for identifying factors of the content of the remainders to a minimum. Before stating our own contribution, we provide in this and the following section an overview over polynomial remainder sequences and subresultant theory for Ore algebras. The key results of this

theory were first given and proved by Ziming Li in [40]. We elaborate the theory by also proving some further theorems analogous to the commutative case which were not needed by Li.

Like in Chapter 4, we consider the following situation throughout the chapter. We would like to stress again that this covers many Ore algebras relevant in applications:

Setting. Let $\mathbb{D}$ be a Euclidean domain with degree function deg and let $\mathbb{D}[X;\sigma,\delta]$ be an Ore polynomial ring where σ is an automorphism. We denote the quotient field of $\mathbb{D}$ by $\mathbb{K}$ and fix operators $A, B \in \mathbb{D}[X;\sigma,\delta]$, $B \neq 0$ with $\operatorname{ord}(A) \geq \operatorname{ord}(B)$. Furthermore we let $G \in \mathbb{D}[X;\sigma,\delta]$ be the GCRD of A and B in $\mathbb{K}[X;\sigma,\delta]$. As stated in Section 4.1, the maximal coefficient degree of an operator L is denoted by $\deg(L)$. In order to simplify the analysis of the size of the intermediate results in the Euclidean algorithm, we assume that $\deg(ab) \leq \deg(a) + \deg(b)$ for all $a, b \in \mathbb{D}$.

Recall that the unit normal greatest common right divisor G of A and B by definition has coefficients in $\mathbb{D}$, is primitive in $\mathbb{D}[X;\sigma,\delta]$ and its leading coefficient is unit normal in $\mathbb{D}$. Even though G has coefficients in $\mathbb{D}$, it is not necessarily a GCRD in $\mathbb{D}[X;\sigma,\delta]$ but in $\mathbb{K}[X;\sigma,\delta]$. As was established in Chapter 4, the left quotients $\operatorname{lquo}(A,G)$ or $\operatorname{lquo}(B,G)$ can have coefficients in $\mathbb{K}$ if G contains removable factors.

In order to put optimizations like the ones outlined above into practice, we need to slightly modify the division with remainder process by introducing two base ring elements α and β as factors in the remainder formula (2.1.1). The first one, α, is necessary for clearing possible denominators while β is used for dividing out known parts of the content of the new remainder.

Example 6.1.1. Let $A, B \in \mathbb{Z}[X]$ with

$$A = 4X^3 + 7X^2 + 9X + 9, \quad B = 2X^2 + 3.$$

Division with remainder in $\mathbb{Q}[X]$ gives

$$A = (2X + \frac{7}{2})B + 3X - \frac{3}{2}. \tag{6.1.1}$$

We can clear the denominators of the coefficients of the remainder by multiplying (6.1.1) by $\alpha = 2$:

$$\alpha A = (4X + 7)B + 6X - 3.$$

The new remainder now has coefficients in $\mathbb{Z}$, but also content that can be divided out. So with $\beta := 3$ we get

$$\alpha A = (4X + 7)B + \beta(2X - 1),$$

and one can proceed in the GCRD computation by dividing B by $2X - 1$.

In general, for two operators A and B, the remainder formula (2.1.1) changes into

$$\alpha A = QB + \beta R, \quad \text{with } \operatorname{ord}(R) < \operatorname{ord}(B).$$

We allow this refined division in each iteration of the Euclidean algorithm and also modify the computation of the Bézout coefficients accordingly such that (2.1.2) still holds.

Algorithm 6.1.1: Refined extended Euclidean algorithm

Input: $A, B \in \mathbb{D}[X; \sigma, \delta]$ and two sequences $(\alpha_i)_{i\in\{1,\dots,\ell\}}$, $(\beta_i)_{i\in\{1,\dots,\ell\}}$ in $\mathbb{K} \setminus \{0\}$

Output: G, S, T such that $G = u \cdot \operatorname{gcrd}(A, B)$ for some $u \in \mathbb{K}$ and $G = SA + TB$.

$(R_0, R_1) \leftarrow (A, B)$
$(S_0, T_0, S_1, T_1) \leftarrow (1, 0, 0, 1)$
$i \leftarrow 1$
WHILE $R_i \neq 0$:
  $(R_{i+1}, Q_i) \leftarrow (\beta_i^{-1} \operatorname{lrem}(\alpha_i R_{i-1}, R_i), \operatorname{lquo}(\alpha_i R_{i-1}, R_i))$
  $(S_{i+1}, T_{i+1}) \leftarrow (\beta_i^{-1}(\alpha_i S_{i-1} - Q_i S_i), \beta_i^{-1}(\alpha_i T_{i-1} - Q_i T_i))$
  $i \leftarrow i + 1$
RETURN $(R_{i-1}, S_{i-1}, T_{i-1})$

In order to show that Algorithm 6.1.1 is correct and to derive good choices for the α_i and β_i, a thorough investigation of all the intermediate results in the execution of the algorithm is necessary. Formally, we treat these as sequences of operators and base ring elements.

Definition 6.1.2. Let $(R_i)_{i\in\{0,\dots,\ell+1\}}$, $(Q_i)_{i\in\{1,\dots,\ell\}}$, $(S_i)_{i\in\{0,\dots,\ell+1\}}$ as well as $(T_i)_{i\in\{0,\dots,\ell+1\}}$ be sequences in $\mathbb{K}[X; \sigma, \delta]$, $(d_i)_{i\in\{0,\dots,\ell\}}$ a sequence in $\mathbb{N}$ and let $(\alpha_i)_{i\in\{1,\dots,\ell\}}$ and $(\beta_i)_{i\in\{1,\dots,\ell-1\}}$ be sequences in $\mathbb{K}$ such that

$$\begin{aligned}
&R_0 = A, \quad R_1 = B, \quad d_i = \operatorname{ord}(R_i),\\
&\alpha_i R_{i-1} = Q_i R_i + \beta_i R_{i+1}, \quad d_{i+1} < d_i,\\
&R_i = S_i A + T_i B, \quad \operatorname{ord}(S_i) = d_1 - d_{i-1}, \ \operatorname{ord}(T_i) = d_0 - d_{i-1},
\end{aligned}$$

and all R_i are non-zero except for $R_{\ell+1}$. We call the sequence $(R_i)_{i\in\{0,\dots,\ell+1\}}$ a *polynomial remainder sequence* (PRS) for A and B. A PRS is called *normal* if $d_i = d_{i-1} - 1$ for $1 \leq i \leq \ell$.

Whenever we talk about a PRS $(R_i)_{i\in\{0,\dots,\ell+1\}}$, we allow ourselves to refer to the related sequences $(Q_i)_{i\in\{1,\dots,\ell\}}$, $(d_i)_{i\in\{0,\dots,\ell\}}$ etc. as in the above definition without explicitly introducing them.

Before we get into any further analysis of possible advantages of this refined division approach, we show that we are indeed free to choose the α_i

and β_i and still get a GCRD in the second to last division step. This proves the correctness of Algorithm 6.1.1. (The correctness of the new formulas for the Bézout coefficients can be shown easily by hand calculation.)

Theorem 6.1.3. *Let $(R_i)_{i\in\{0,\dots,\ell+1\}}$ and $(\tilde{R}_i)_{i\in\{0,\dots,\tilde{\ell}+1\}}$ be two PRSs for A and B. Then $\ell = \tilde{\ell}$ and there exist $\gamma_2, \dots, \gamma_{\ell+1} \in \mathbb{K}\setminus\{0\}$ such that*

$$R_i = \gamma_i \tilde{R}_i \text{ for all } 2 \le i \le \ell+1.$$

Also, for each choice of $\gamma'_2, \dots, \gamma'_{\ell+1} \in \mathbb{K}\setminus\{0\}$ and $\gamma'_0 = \gamma'_1 = 1$, the sequence $(\gamma'_i R_i)_{i\in\{0,\dots,\ell+1\}}$ is a PRS for A and B.

Proof. It suffices to show that for any two operators $A, B \in \mathbb{K}[X;\sigma,\delta]$ and base field elements $\alpha, \beta \in \mathbb{K}\setminus\{0\}$, there exists $\gamma \in \mathbb{K}\setminus\{0\}$ with $\operatorname{lrem}(A,B) = \gamma \cdot \operatorname{lrem}(\alpha A, \beta B)$. Set $\gamma = \alpha^{-1}$. Then there is a $Q \in \mathbb{K}[X;\sigma,\delta]$ such that:

$$\gamma \cdot \operatorname{lrem}(\alpha A, \beta B) = \gamma(\alpha A - Q\beta B) = A - \underbrace{\left(\frac{1}{\alpha} Q \beta\right)}_{=:\tilde{Q}} B.$$

By the uniqueness of the left quotient of two operators, $\tilde{Q}$ is equal to $\operatorname{lquo}(A,B)$ and thus $\gamma \cdot \operatorname{lrem}(\alpha A, \beta B) = \operatorname{lrem}(A,B)$.
The second part of the theorem follows by defining a PRS $(R'_i)_{i\in\{0,\dots,\ell+1\}}$ for A and B with $\alpha_i = 1$ and $\beta_i = \frac{\operatorname{lc}(R'_{i-1} - Q'_i R'_i)}{\gamma_i \operatorname{lc}(R_i)}$. □

A PRS for A and B is uniquely determined by specifying the α_i and β_i, which is an immediate consequence of the uniqueness of the quotient and the remainder of two Ore operators. Next we will study how to choose these factors in order to improve the running time of the Euclidean algorithm.

An upper bound for the possible denominators in the remainder coefficients and thus a suitable choice for the α_i can be found easily: From the non-commutative analog of (2.2.1) it follows that the common denominator of the coefficients of the remainder of two operators A and B can be at most $\operatorname{lc}(B)^{[d_A - d_B + 1]}$.

Definition 6.1.4. Set $\alpha = \operatorname{lc}(B)^{[d_A - d_B + 1]}$. Then the *pseudo-remainder* $\operatorname{prem}(A,B)$ and the *pseudo-quotient* $\operatorname{pquo}(A,B)$ of A and B are defined as

$$\operatorname{prem}(A,B) := \operatorname{lrem}(\alpha A, B), \qquad \operatorname{pquo}(A,B) := \operatorname{lquo}(\alpha A, B). \tag{6.1.2}$$

Both, the pseudo-remainder and the pseudo-quotient of A and B have coefficients in $\mathbb{D}$. It can happen that α as in Definition 6.1.4 contains too many factors which then appear as content in the pseudo-remainder. In implementations of the refined Euclidean algorithm, these factors should be removed from α – provided that they are known – before it is multiplied

to A. In the development of the theory however, we are free to include such factors in our choice of β and thus we will always set

$$\alpha_i = \mathrm{lc}(R_i)^{[d_{i-1}-d_i+1]}, \tag{6.1.3}$$

in any PRS with remainders in $\mathbb{D}[X;\sigma,\delta]$. It should be noted that most of the content generated by pseudo-remaindering usually is not a result of choosing the α_i too big.

Example 6.1.5. Let α_i be as in (6.1.3) and set

1. $\beta_i = 1$. This is called the pseudo PRS for A and B. Here, no content will be divided out.

2. $\beta_i = \mathrm{cont}(\alpha_i R_{i-1} - Q_i R_i)$. This is called the primitive PRS for A and B. The coefficients of the remainders will be as small as possible, but it is necessary to compute the GCD of the coefficients of each remainder in order to get the β_i.

While in both of the above PRSs all the remainders are elements of $\mathbb{D}[X;\sigma,\delta]$, the degrees of the coefficients can differ drastically, as illustrated in the following example. It can be observed that the degrees of the coefficients in the pseudo PRS typically grow exponentially with i, which renders this PRS practically useless. (See [53] for an analysis of the coefficient growth in case of commutative polynomials.) The growth in the primitive PRS is linear in i, if $\deg(\sigma(a)) \leq \deg(a)$ and $\deg(\delta(a)) \leq \deg(a)$ for all $a \in \mathbb{D}$ (Theorem 6.3.15).

Example 6.1.6. We have seen in Example 5.1.1 that the method of guessing can be used to get annihilating operators of different orders and degrees for a holonomic sequence of which we just know finitely many terms. The cost of guessing is proportional to order×degree and hence, the (most often) hyperbolic shape of the order-degree bound derived in Chapter 5 suggests that guessing a minimal order operator is usually more expensive than guessing an operator with balanced order and degree. To get a reasonable candidate for the lowest order operator, we can use the Euclidean algorithm, since the greatest common right divisor of two annihilators guessed at different orders and degrees has a high chance of being the generator of the whole annihilator ideal. Consider the sequence from Example 5.1.1,

$$t_n = \sum_{k=0}^{n} \left(\binom{2n+4}{k} + (2n-k)! + k^3 \right).$$

Given the first 300 terms of this sequence, we can find two operators A and B in $\mathbb{Q}[n][S;s_n,0]$ with $d_A = 14$, $d_B = 13$ and maximal coefficient degree $\deg(A) = 5$, $\deg(B) = 6$ respectively. Both operators annihilate the

given sequence, but none of them is of minimal order. To get an annihilating minimal order operator, we compute the GCRD of A and B in $\mathbb{Q}(n)[S; s_n, 0]$. Table 6.1.1 shows the maximal coefficient degrees of the remainders for different PRSs for A and B.

PRS	R_2	R_3	R_4	R_5	R_6	R_7	R_8
pseudo	11	22	49	114	271	650	1565
primitive	9	12	15	18	21	24	21

Table 6.1.1: Maximal coefficient degrees for different PRSs in Example 6.1.6.

The example confirms that the degrees in the pseudo PRS grow exponentially. This behavior is typical for generic input as well as for input coming from applications. While the primitive PRS only has linear growth in the degrees, the GCD of the coefficients of each remainder has to be computed.

Our goal is to find a choice for the β_i that reduces the computational overhead to a minimum while still determining most if not all of the content of the remainders. The improvements presented in this work are based on the subresultant PRS. In this PRS, the content that is generated systematically by pseudo-remaindering will be cleared from the remainders, resulting in linear coefficient growth.

6.2 Subresultant Theory

In this section we aim to provide a comprehensible and coherent introduction to the theory of subresultants in the non-commutative case, that also gives enough insight into the motivation behind the ideas of this rather technical but well-understood topic. A deep understanding is crucial for the proofs in Section 6.3 and we advise the reader to be henceforth exceedingly attentive to the distinction between operators in $\mathbb{D}[X; \sigma, \delta]$ and operators in $\mathbb{K}[X; \sigma, \delta]$. The basic outline of the next two subsections follows the texts on resultants and subresultants in the commutative case in [53] and [24]. Many of the main ideas that are used for subresultants in Section 6.2.2 already emerge in a less technical fashion in Section 6.2.1, where we deal with the concept of the resultant of two Ore polynomials. For commutative polynomials, the theory of subresultants was intensively studied in [13, 14, 22, 41].

6.2.1 Resultant

Given two Ore polynomials A and B, is there a way to tell whether they have a non-trivial GCRD without actually computing it? This question is the first step towards the definition of the resultant of A and B and our main motivation behind it. An answer can be found by taking a closer look at the Bézout relation and syzygys of A and B.

Theorem 6.2.1. *A and B have a non-trivial GCRD if and only if there exist non-zero $S, T \in \mathbb{K}[X;\sigma,\delta]$ such that*

$$SA + TB = 0, \quad d_S < d_B \text{ and } d_T < d_A. \tag{6.2.1}$$

Proof. If the GCRD G of A and B is non-trivial, the last iteration in the extended Euclidean algorithm gives $S, T \in \mathbb{K}[X;\sigma,\delta]$ with $SA + TB = 0$ and $d_S = d_B - d_G < d_B$ and $d_T = d_A - d_G < d_A$.
Conversely, let $S, T \in \mathbb{K}[X;\sigma,\delta]$ satisfy (6.2.1) and assume $G = 1$. Then again the EEA will give $\tilde{S}, \tilde{T} \in \mathbb{K}[X;\sigma,\delta]$ with $\tilde{S}A + \tilde{T}B = 0$ and $d_{\tilde{S}} = d_B$ and $d_{\tilde{T}} = d_A$. Since $SA = -TB$, we get that SA is a common left multiple of A and B. On the other hand $\tilde{S}A$ is the least common left multiple of A and B, and it follows that $d_S \geq d_{\tilde{S}} = d_B$, which contradicts the order-bound given in (6.2.1). □

We can restate the result of Theorem 6.2.1 in terms of linear algebra. For that purpose, let $\mathbb{K}[X;\sigma,\delta]_d$ be the set of all Ore polynomials in $\mathbb{K}[X;\sigma,\delta]$ with order strictly less than $d \in \mathbb{N}$. We regard $\mathbb{K}[X;\sigma,\delta]_d$ as a const$(\mathbb{K}[X;\sigma,\delta])$-vector space. Any $\mathbb{K}[X;\sigma,\delta]$-linear combination of A and B of the form

$$SA + TB, \quad d_S < d_B \text{ and } d_T < d_A, \tag{6.2.2}$$

can be expressed by the linear map

$$\begin{aligned} \varphi_{A,B} : \mathbb{K}[X;\sigma,\delta]_{d_B} \times \mathbb{K}[X;\sigma,\delta]_{d_A} &\to \mathbb{K}[X;\sigma,\delta]_{d_A+d_B}, \\ (S,T) &\mapsto SA + TB. \end{aligned}$$

If S and T are as in Theorem 6.2.1, it means that (S,T) is an element of the kernel of $\varphi_{A,B}$. Thus, A and B have a non-trivial greatest common right divisor if and only if the kernel of $\varphi_{A,B}$ is non-zero. For $\mathbb{K}[X;\sigma,\delta]_d$, we fix the ordered basis $\mathcal{B}_d = (X^{d-1}, X^{d-2}, \ldots, X^0)$ and for the product space $\mathbb{K}[X;\sigma,\delta]_{d_1} \times \mathbb{K}[X;\sigma,\delta]_{d_2}$, we fix the ordered basis $\mathcal{B}_{d_1,d_2} = ((X^{d_1-1},0),(X^{d_1-2},0),\ldots,(X^0,0),(0,X^{d_2-1}),(0,X^{d_2-2}),\ldots,(0,X^0))$. The matrix representation of $\varphi_{A,B}$ with respect to the bases B_{d_A,d_B} and $B_{d_A+d_B}$ is given by the transpose of the Sylvester matrix.

Definition 6.2.2. The *Sylvester matrix* $\mathrm{Syl}(A,B)$ is defined to be the matrix of size $(d_A + d_B) \times (d_A + d_B)$ with the following entries: If $1 \leq i \leq d_B$ and $1 \leq j \leq d_A + d_B$, the entry in the ith row and jth column is the $(d_A + d_B - j)$th coefficient of $X^{d_B - i}A$. If $d_B + 1 \leq i \leq d_A + d_B$ and $1 \leq j \leq d_A + d_B$, the entry in the ith row and jth column is the $(d_A + d_B - j)$th coefficient of $X^{d_A-(i-d_B)}B$.
The determinant $\det(\mathrm{Syl}(A,B))$ is called the *resultant* $\mathrm{res}(A,B)$ of A and B.

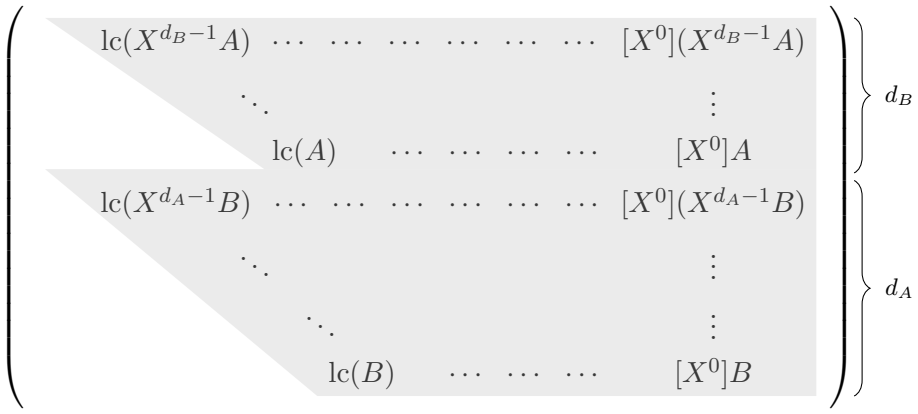

Figure 6.2.1: The form of the Sylvester matrix of A and B. Entries outside of the gray area are zero.

Corollary 6.2.3. *The GCRD of A and B is non-trivial if and only if* $\mathrm{res}(A,B)=0$. □

In the next theorem we will see that the resultant can be written in the form (6.2.2) and in the proof we make use of the central technique to connect the resultant (and later subresultants) to other linear combinations of A and B.

Theorem 6.2.4. *There exist non-zero $S,T\in\mathbb{D}[X;\sigma,\delta]$ such that*

$$SA+TB=\mathrm{res}(A,B),\quad d_S<d_B,\quad d_T<d_A. \tag{6.2.3}$$

Proof. If the resultant is zero, then the existence of S and T follows by clearing denominators of the cofactors in $\mathbb{K}[X;\sigma,\delta]$, which exist because of Theorem 6.2.1 and Corollary 6.2.3. Let $\mathrm{res}(A,B)\neq 0$. By Corollary 6.2.3, the GCRD of A and B is 1 and so there are $\tilde{S}=\sum_{i=0}^{d_B-1}\tilde{s}_iX^i$ and $\tilde{T}=\sum_{i=0}^{d_A-1}\tilde{t}_iX^i$ with coefficients in $\mathbb{K}$ such that

$$\tilde{S}A+\tilde{T}B=1.$$

This equation can be written as

$$\mathrm{Syl}(A,B)^{\mathsf{T}}\begin{pmatrix}\tilde{s}_{d_B-1}\\ \vdots\\ \tilde{s}_0\\ \tilde{t}_{d_A-1}\\ \vdots\\ \tilde{t}_0\end{pmatrix}=\begin{pmatrix}0\\ \vdots\\ 0\\ 1\end{pmatrix},$$

and by Cramer's rule, the $\tilde{s}_i$ and $\tilde{t}_i$ are of the form $\frac{p_i}{\mathrm{res}(A,B)}$ with the $p_i\in\mathbb{D}$ being the determinants of some submatrices of $\mathrm{Syl}(A,B)$. Thus, setting $S=\mathrm{res}(A,B)\tilde{S}$ and $T=\mathrm{res}(A,B)\tilde{T}$ gives $S,T\in\mathbb{D}[X;\sigma,\delta]$ for which (6.2.3) holds. □

If $\operatorname{res}(A,B)$ is non-zero, it is an element of $\mathbb{D}\setminus\{0\}$ and the GCRD of A and B is 1. Therefore, by Theorem 6.1.3 there exists a PRS such that its last non-zero element, the result of the GCRD computation, is equal to $\operatorname{res}(A,B)$ and the extended Euclidean algorithm gives S and T as in Theorem 6.2.4.

Example 6.2.5. Let $A, B \in \mathbb{Z}_{11}[n][S; s_n, 0]$ with

$$A = (9n+1)S^3 + (9n+3)S^2 + (8n+6)S + (8n+1),$$

$$B = (2n+3)S^2 + (10n+2)S + (5n+6).$$

Running the extended Euclidean algorithm on A and B gives $\tilde{S}$ and $\tilde{T}$ in $\mathbb{Z}_{11}[n][S; s_n, 0]$ such that $\tilde{S}A + \tilde{T}B = 0$ with

$$\tilde{S} = (6n^4 + 9n^3 + 4n^2 + 6n + 2)S + (9n^4 + 7n^2 + 4n + 2),$$

$$\tilde{T} = (6n^4+2n^3+7n^2+5)S^2+(7n^4+7n^3+9n^2+4n+8)S+(n^4+8n^3+10n^2+7).$$

The Sylvester matrix of A and B is

$$\begin{pmatrix} 9n+10 & 9n+1 & 8n+3 & 8n+9 & 0 \\ 0 & 9n+1 & 9n+3 & 8n+6 & 8n+1 \\ 2n+7 & 10n & 5n+5 & 0 & 0 \\ 0 & 2n+5 & 10n+1 & 5n & 0 \\ 0 & 0 & 2n+3 & 10n+2 & 5n+6 \end{pmatrix},$$

and by writing $\tilde{S}$ and $\tilde{T}$ as the vector $v = (\tilde{s}_1, \tilde{s}_0, \tilde{t}_2, \tilde{t}_1, \tilde{t}_0)$, we get

$$\operatorname{Syl}(A,B)^{\mathsf{T}} v = 0 = \operatorname{res}(A,B).$$

6.2.2 Subresultants

The GCRD of two Ore polynomials is a $\mathbb{K}$-multiple of the last non-zero element in any of their polynomial remainder sequences, which is the remainder of lowest finite order. The results from the previous subsection can be generalized to any other finite order, giving access to all the remainders in a polynomial remainder sequence. Again, we start by looking at Bézout relations.

Theorem 6.2.6. *Let $(R_i)_{i\in\{0,\dots,\ell+1\}}$ be the PRS for A and B with $\alpha_i = \beta_i = 1$ and let $n \in \mathbb{N}$ with $n \le d_B$. There exists no $i \in \mathbb{N}$ with $d_i = n$ if and only if there are non-zero S, T such that*

$$\operatorname{ord}(SA+TB) < n, \quad d_S < d_B - n \text{ and } d_T < d_A - n. \tag{6.2.4}$$

Proof. First, let there be no i such that $n = d_i$. Unless $n < d_\ell$, we let $j \in \mathbb{N}$ be such that $d_{j-1} > n > d_j$ and otherwise we let $j = \ell + 1$. Then we can take $S = S_j$ and $T = T_j$, because $\operatorname{ord}(S_jA + T_jB) = d_j < n$ and $\operatorname{ord}(S_j) = d_A - d_{j-1} < d_A - n$ and $\operatorname{ord}(T_j) = d_B - d_{j-1} < d_B - n$.

Coversely, let S and T be such that (6.2.4) holds and assume there is an i such that $d_i = n$. Following the constructive proof of the LCLM existence in [12], we set

$$C_0 = T, \quad C_1 = -S,$$
$$C_{j+1} = C_{j-1} - C_j Q_j \text{ for } 1 \leq j \leq i.$$

Assume that the following holds for $1 \leq j \leq i+1$:

$$\operatorname{ord}(C_{j-1}R_j - C_j R_{j-1}) < n, \tag{6.2.5}$$

$$C_{j-1}S_j - C_j S_{j-1} = (-1)^{j-1}S. \tag{6.2.6}$$

Setting $j = i+1$ in (6.2.5) gives

$$\operatorname{ord}(C_i \underbrace{R_{i+1}}_{\text{order} < n} - C_{i+1} \underbrace{R_i}_{\text{order} = n}) < n,$$

so we get

$$\operatorname{ord}(C_i) > \operatorname{ord}(C_{i+1}), \tag{6.2.7}$$

and setting $j = i+1$ in (6.2.6) gives

$$C_i \underbrace{S_{i+1}}_{\text{order} = d_B - n} - C_{i+1} \underbrace{S_i}_{\text{order} < d_B - n} = (-1)^i \underbrace{S}_{\text{order} < d_B - n},$$

and so

$$\operatorname{ord}(C_i) < \operatorname{ord}(C_{i+1}),$$

which contradicts (6.2.7). To finish the proof, it remains to show that (6.2.5) and (6.2.6) hold. We do this by induction on j. For $j = 1$, we get:

$$\operatorname{ord}(C_{j-1}R_j - C_j R_{j-1}) = \operatorname{ord}(TB + SA) < n,$$

and

$$C_{j-1}S_j - C_j S_{j-1} = T0 + S1 = S.$$

Now assume (6.2.5) and (6.2.6) hold for $j-1$ for a fixed $2 \leq j \leq i+1$. Then

$$\begin{aligned}
&\operatorname{ord}(C_{j-1}R_j - C_j R_{j-1}) = \\
&\quad \operatorname{ord}(C_{j-1}(R_{j-2} - Q_{j-1}R_{j-1}) - (C_{j-2} - C_{j-1}Q_{j-1})R_{j-1}) = \\
&\quad \operatorname{ord}(C_{j-1}R_{j-2} - C_{j-2}R_{j-1}) < n,
\end{aligned}$$

and

$$\begin{aligned}
&C_{j-1}S_j - C_j S_{j-1} = \\
&\quad C_{j-1}(S_{j-2} - Q_{j-1}S_{j-1}) - (C_{j-2} - C_{j-1}Q_{j-1})S_{j-1} = \\
&\quad C_{j-1}S_{j-2} - C_{j-2}S_{j-1} = (-1)(-1)^{j-2}S = (-1)^{j-1}S.
\end{aligned}$$

This completes the proof. □

Theorem 6.2.1 is a special case of Theorem 6.2.6 when taking $n = 0$. As before, we express the result of Theorem 6.2.6 in terms of linear algebra. This time we are not interested in the actual result of the linear combination $SA + TB$, but only whether or not the order is less than some given n. For this reason, we modify the linear map that was described in the previous section in a way such that lower order terms are ignored. We do this by taking the left quotient of the linear combination and X^n. While the result will live in the vector space $\mathbb{K}[X;\sigma,\delta]_{d_A+d_B-2n}$, it actually represents the higher order part of the linear combination, namely the coefficients with index greater than or equal to n.

Any pair of cofactors S, T of a linear combination of A and B satisfying

$$\operatorname{ord}(SA + TB) < n, \quad d_S < d_B - n \text{ and } d_T < d_A - n, \tag{6.2.8}$$

lies in the kernel of the linear map

$$\begin{aligned}\varphi_{A,B,n} : \mathbb{K}[X;\sigma,\delta]_{d_B-n} \times \mathbb{K}[X;\sigma,\delta]_{d_A-n} &\to \mathbb{K}[X;\sigma,\delta]_{d_A+d_B-2n},\\ (S,T) &\mapsto \operatorname{lquo}(SA + TB, X^n).\end{aligned}$$

The matrix representation of this map is given by the transpose of a submatrix of the Sylvester matrix.

Definition 6.2.7. For $n \in \mathbb{N}$ with $0 \le n \le d_B$, the matrix $\operatorname{Syl}_n(A,B)$ of size $(d_A + d_B - 2n) \times (d_A + d_B - 2n)$ is obtained from $\operatorname{Syl}(A,B)$ by removing the rows 1 to n, the rows $d_B + 1$ to $d_B + n$, the columns 1 to n and the last n columns. We call its determinant the nth *principal subresultant* of A and B.

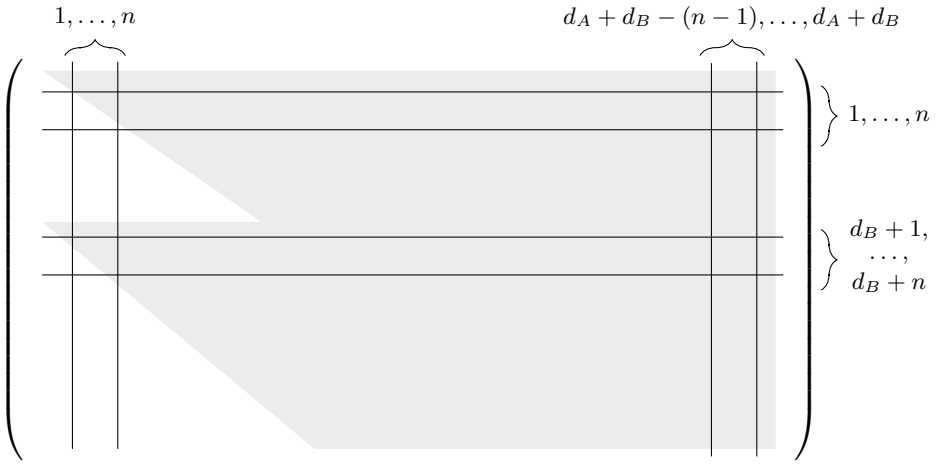

Figure 6.2.2: Sketch of $\operatorname{Syl}_n(A,B)$.

Corollary 6.2.8. *No remainder sequence for A and B contains a remainder of order n if and only if* $\det(\operatorname{Syl}_n(A,B)) = 0$. □

In Theorem 6.2.4 we have seen that the resultant of A and B can always be expressed as a $\mathbb{D}[X;\sigma,\delta]$-linear combination of A and B where the cofactors satisfy a certain order bound and if the GCRD is trivial, there is a PRS in which the last non-zero element is equal to the resultant. A similar statement is true for the principal subresultants. Let $n \in \mathbb{N}$ with $0 \leq n \leq d_B$. We will see in Corollary 6.2.13 that there exist non-zero $S, T \in \mathbb{D}[X;\sigma,\delta]$ such that for $R := SA + TB$ with the nth coefficient r_n we have

$$\operatorname{ord}(R) \leq n, \quad r_n = \operatorname{Syl}_n(A,B), \quad d_S < d_B - n, \quad d_T < d_A - n,$$

and there is a PRS that contains R. The question arises if not only the nth coefficient but also any of the other coefficients of R can be expressed as a Sylvester submatrix determinant. Like we were able to set up a linear system for the nth coefficient, we can do the same for all the lower order coefficients.

Definition 6.2.9. For $n, m \in \mathbb{N}$ with $0 \leq m \leq n \leq d_B$, the matrix $\operatorname{Syl}_{n,m}(A,B)$ of size $(d_A+d_B-2n)\times(d_A+d_B-2n)$ is obtained from $\operatorname{Syl}(A,B)$ by removing the rows 1 to n, the rows d_B+1 to d_B+n, the columns 1 to n and the last $n+1$ columns except for the column d_A+d_B-m. Note that if $n = m$, then $\operatorname{Syl}_{n,m}(A,B) = \operatorname{Syl}_n(A,B)$.

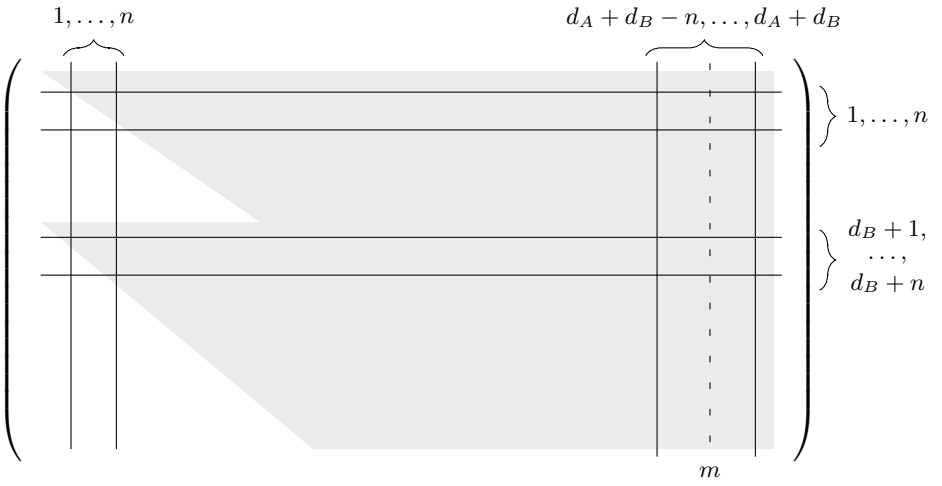

Figure 6.2.3: Sketch of $\operatorname{Syl}_{n,m}(A,B)$. The lines indicate the removed rows and columns. The column under the dotted line is added again.

For fixed n, all the $\operatorname{Syl}_{n,m}(A,B)$ agree except for the last column. This together with Cramer's rule allows us to construct a PRS such that all the coefficients of the remainders in the sequence can be expressed in terms of determinants of matrices of the form given in Definition 6.2.9.

Definition 6.2.10. For $0 \leq n \leq d_B$, the polynomial

$$\operatorname{sres}_n(A,B) := \sum_{m=0}^{n} \det(\operatorname{Syl}_{n,m}(A,B))X^m,$$

is called the nth *(polynomial) subresultant* of A and B. If the order of $\operatorname{sres}_n(A,B)$ is strictly less than n, the nth subresultant of A and B is called *defective*, otherwise it is called *regular*.

Some of these subresultants will be the elements of the subresultant polynomial remainder sequence for A and B.

Theorem 6.2.11. *Let $(R_i)_{i\in\{0,\dots,\ell+1\}}$ be the monic PRS for A and B, i.e. $\alpha_i = 1$ and $\beta_i = 1/\operatorname{lc}(R_{i+1})$, and let $i, n \in \mathbb{N}$ be such that R_i is of order n. If $j \in \mathbb{N}$ is such that $\operatorname{sres}_j(A,B)$ is of order n as well, then*

$$\operatorname{sres}_j(A,B) = \det(\operatorname{Syl}_{j,n}(A,B))R_i.$$

Proof. For $\operatorname{sres}_j(A,B)$ to be of order n, j has to be greater than or equal to n and $\operatorname{Syl}_{j,n}(A,B)$ has to be regular. Similar to the proof of Theorem 6.2.4, we use Cramer's rule to get $v \in \mathbb{D}^{d_A+d_B-2j}$ such that

$$\operatorname{Syl}_{j,n}(A,B)^{\mathsf{T}} v = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ \det(\operatorname{Syl}_{j,n}(A,B)) \end{pmatrix}, \tag{6.2.9}$$

We show that v is a solution of

$$\operatorname{Syl}_{j,l}(A,B)^{\mathsf{T}} v = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ \det(\operatorname{Syl}_{j,l}(A,B)) \end{pmatrix}, \tag{6.2.10}$$

for any $0 \le l \le j$. First, assume $\det(\operatorname{Syl}_{j,l}(A,B)) = 0$. For $1 < k \le d_A + d_B - 2j =: m$, denote the the kth row of $\operatorname{Syl}_{j,l}(A,B)^{\mathsf{T}}$ by r_k. Because the matrix is singular, there exist $c_1, \dots, c_m \in \mathbb{K}$ with

$$r_m = c_1 r_1 + \cdots + c_{m-1} r_{m-1}. \tag{6.2.11}$$

Furthermore, since the first $k-1$ rows of $\operatorname{Syl}_{j,l}(A,B)$ are the same as the first $k-1$ rows of $\operatorname{Syl}_{j,n}(A,B)$, we conclude from (6.2.9) that:

$$r_1 v = r_2 v = \cdots = r_{m-1} v = 0.$$

Combining this and (6.2.11) yields

$$\begin{aligned} r_m v = (c_1 r_1 + \cdots + c_{m-1} r_{m-1}) v = \\ c_1 r_1 v + \cdots + c_{m-1} r_{m-1} v = \\ 0 = \det(\operatorname{Syl}_{j,l}(A,B)). \end{aligned}$$

This shows (6.2.10) in the case that $\det(\mathrm{Syl}_{j,l}(A,B)) = 0$.
Now let $\det(\mathrm{Syl}_{j,l}(A,B)) \neq 0$. Then equation (6.2.10) has a unique solution and by Cramer's rule, every component of the solution is the determinant of some submatrix of $\mathrm{Syl}_{j,l}(A,B)$. In each of these submatrices, the last column of $\mathrm{Syl}_{j,l}(A,B)$ is removed and therefore, they don't depend on l. This means that we get the same solution to (6.2.10) for all l, in particular for $l = n$. This proves (6.2.10) for all $0 \leq l \leq j$.
Next, we set $v' \in \mathbb{D}^{d_A+d_B-2n}$ to be the vector one gets by adding zeros in v at the places corresponding to the rows that have to be added when going from $\mathrm{Syl}_j(A,B)$ to $\mathrm{Syl}_n(A,B)$. Then

$$\mathrm{Syl}_n(A,B)^{\mathsf{T}} v' = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ \det(\mathrm{Syl}_{j,n}(A,B)) \end{pmatrix},$$

holds. Since by Corollary 6.2.8, $\mathrm{Syl}_n(A,B)$ is regular, this solution is unique and therefore its components have to be the coefficients of the operators $\det(\mathrm{Syl}_{j,n}(A,B))S_i$ and $\det(\mathrm{Syl}_{j,n}(A,B))T_i$, where S_i and T_i are the unique cofactors such that $S_iA + T_iB = R_i$. This completes the proof. □

Not all the subresultants of A and B are regular and in both the regular and the defective case, a subresultant carries information about the order of subresultants with lower index. In [40], Li proves the *subresultant block structure*: For $i \in \mathbb{N}$, the ith subresultant is either regular or defective. If it is regular, it is of order i and all other subresultants with lower index are of strictly lower order. If it is defective with the $(i+1)$st subresultant being regular, its order is equal to the order of the next regular subresultant with index $j < i$, provided that such a j exists. In that case, all the subresultants with indices $j < k < i$ are zero. If there is no regular subresultant with an index lower than i, then the ith and all subsequent subresultants are zero.

Example 6.2.12. We investigate the subresultants of A and B, both elements in the $\mathbb{Z}_{11}[n][S; s_n, 0]$ with

$$\begin{aligned} A = {} & (10n^6 + 8n^5 + 5n^4 + n^3 + 6n^2 + n + 2)S^4 \\ & + (n^6 + 2n^5 + 3n^4 + 8n^3 + 4n + 4)S^3 \\ & + (2n^6 + 7n^4 + n^3 + 10n^2 + 2)S^2 \\ & + (8n^5 + 5n^4 + 8n^3 + n^2 + 5n + 4)S + (9n^5 + 3n^4 + 8n^3 + 8), \end{aligned}$$

and

$$\begin{aligned} B = {} & (2n^5 + 9n^4 + 8n^3 + 8n^2 + 8n + 2)S^3 \\ & + (7n^5 + 5n^4 + 7n^2 + 5n + 4)S^2 \\ & + (2n^4 + 7n^3 + 6n^2 + 2n + 5)S + (4n^4 + 7n^3 + 4n^2 + n + 7). \end{aligned}$$

In any polynomial remainder sequence for A and B we get the order sequence $(4, 3, 1, 0)$. The 2nd coefficient of $\mathrm{sres}_2(A, B)$ is the determinant of the matrix $\mathrm{Syl}_{2,2}(A, B)$ which consists of the rows r_1, r_2, r_3 with:

$$\begin{aligned}
r_1 &= (10n^6 + 8n^5 + 5n^4 + n^3 + 6n^2 + n + 2,\\
&\qquad 2n^5 + 8n^4 + 9n^3 + 7n^2 + 6n + 4, 0),\\
r_2 &= (n^6 + 2n^5 + 3n^4 + 8n^3 + 4n + 4,\\
&\qquad 7n^5 + 7n^4 + 2n^3 + 8n^2 + 8n + 6, 2n^5 + 9n^4 + 8n^3 + 8n^2 + 8n + 2),\\
r_3 &= (2n^6 + 7n^4 + n^3 + 10n^2 + 2,\\
&\qquad 2n^4 + 4n^3 + 6n^2 + 10n, 7n^5 + 5n^4 + 7n^2 + 5n + 4).
\end{aligned}$$

This determinant is 0. So the 2nd subresultant is defective and accordingly, there is no remainder of order 2 in any PRS for A and B. The next regular subresultant is $\mathrm{sres}_1(A, B)$, so $\mathrm{sres}_2(A, B)$ is of order 1.

In Figure 6.2.4, we illustrate an example of a sequence of subresultants where all the effects that are described in the subresultant block structure appear. There, the 6th subresultant is defective and all the coefficients of the next two subresultants, $\mathrm{sres}_5(A, B)$ and $\mathrm{sres}_4(A, B)$, turn out to be zero, because the next regular subresultant is of order 3.

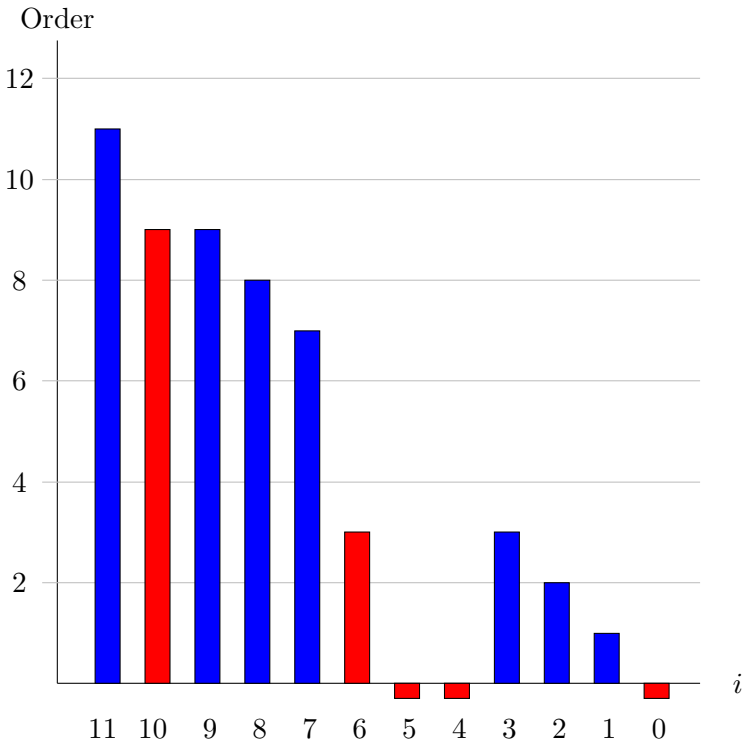

Figure 6.2.4: Orders for different $\mathrm{sres}_i(A, B)$. Blue bars represent the order of regular, red bars the order of defective subresultants.

It is easy to compute A and B in $\mathbb{Q}[y][\partial; 1, \frac{d}{dy}]$ such that their subresultants are as in this example, but their coefficients are usually to big for stating them here.

With the subresultant block structure, we can now show that in a PRS that consists of subresultants, also the intermediate results of the Bézout coefficients are fraction free.

Corollary 6.2.13. *Let $i \in \mathbb{N}$. Then there exist $S_i, T_i \in \mathbb{D}[X; \sigma, \delta]$ such that*

$$S_i A + T_i B = \operatorname{sres}_i(A, B), \quad d_{S_i} < d_B - i \text{ and } d_{T_i} < d_A - i.$$

Proof. First consider the case $\operatorname{sres}_i(A, B) = 0$. Then $\operatorname{Syl}_i(A, B)$ is singular and there exists a non-zero solution $v \in \mathbb{D}^{d_A + d_B - 2i}$ of the equation $\operatorname{Syl}_i(A, B)^{\mathsf{T}} v = 0$. Since all the $\det(\operatorname{Syl}_{i,j}(A, B))$ with $j < i$ are zero as well, it can be shown as in the proof of Theorem 6.2.11 that v is also a solution to $\operatorname{Syl}_{i,j}^{\mathsf{T}}(A, B)v = 0$. The components of v correspond to the coefficients of some S_i and T_i that are as required.
Now suppose $\operatorname{sres}_i(A, B)$ is of order $n \in \mathbb{N}$. By the subresultant block structure, there is a remainder R in the monic PRS for A and B of order n. Then S_i and T_i can be constructed as in the proof of Theorem 6.2.11. □

As stated in Corollary 6.2.8, if there is a remainder of order n in any PRS for A and B, then there is at least one subresultant of that order. On the other hand, the subresultant block structure suggests that there can be two subresultants of the same order. If one wants to construct a PRS that only contains subresultants, a decision has to be made for either of the two. The fact that the size of the $\operatorname{Syl}_i(A, B)$ increases with decreasing i suggests choosing the subresultant with higher index.

Definition 6.2.14. The *subresultant sequence of A and B of the first kind* is the subsequence of

$$(A, B, \operatorname{sres}_{d_B - 1}(A, B), \operatorname{sres}_{d_B - 2}(A, B), \ldots, \operatorname{sres}_0(A, B), 0),$$

that contains A, B, the trailing zero and all non-zero $\operatorname{sres}_i(A, B)$ for which $\operatorname{sres}_{i+1}(A, B)$ is regular.

Example 6.2.15. If the order of the subresultants of A and B are as in Figure 6.2.4, the subresultant sequence for A and B of the first kind contains the subresultants with indices $11, 10, 8, 7, 6, 2, 1$.

From Theorem 6.2.11, Theorem 6.1.3 and the subresultant block structure, it is clear that there exists a PRS for A and B that is equal to the subresultant sequence for A and B of the first kind, but it is not clear how to choose α_i and β_i in the refined Euclidean algorithm without having to compute the determinants of the $\operatorname{Syl}_i(A, B)$. In the non-commutative case, this problem was solved by Z. Li in [40].

Theorem 6.2.16 ([40]). *The polynomial remainder sequence given by*

$$\alpha_i = \operatorname{lc}(R_i)^{[d_{i-1}-d_i+1]},$$
$$\beta_i = \begin{cases} -\sigma(\psi_1)^{[d_0-d_1]}, & \text{if } i = 1, \\ -\operatorname{lc}(R_{i-1})\sigma(\psi_i)^{[d_{i-1}-d_i]}, & \text{if } 2 \leq i \leq \ell - 1, \end{cases}$$

where

$$\psi_i = \begin{cases} -1, & \text{if } i = 1, \\ \dfrac{(-\operatorname{lc}(R_{i-1}))^{[d_{i-2}-d_{i-1}]}}{\sigma(\psi_{i-1})^{[d_{i-2}-d_{i-1}-1]}}, & \text{if } 2 \leq i \leq \ell - 1. \end{cases}$$

is equal to the subresultant sequence for A and B of the first kind. □

We call the PRS in Theorem 6.2.16 the *subresultant polynomial remainder sequence* for A and B. The degrees of the remainders in the subresultant PRS grow linearly with i, provided that $\deg(\sigma(a)) \leq \deg(a)$ and $\deg(\delta(a)) \leq \deg(a)$ for all $a \in \mathbb{D}$.

Theorem 6.2.17. *Let $(R_i)_{i\in\{0,\ldots,\ell+1\}}$ be the subresultant PRS for A and B. Fix $i \in \{2, \ldots, \ell\}$ and let $b_i \in \mathbb{N}$ be such that*

$$\max_{k \in \{0,\ldots,d_B - d_{i-1} - 2\}}(\deg(X^k A)) \leq b_i \quad \text{and} \quad \max_{k \in \{0,\ldots,d_A - d_{i-1} - 2\}}(\deg(X^k B)) \leq b_i.$$

Then

$$\deg(R_i) \leq (d_A + d_B - 2(d_{i-1} - 1))b_i.$$

Proof. Let $\mathcal{S}_m$ be the symmetric group of degree $m \in \mathbb{N}$. By our assumption on the degree function deg and the formula

$$\det(A) = \sum_{f\in\mathcal{S}_m} \operatorname{sgn}(f) \prod_{k=1}^{m} a_{k,f(k)},$$

the degree of the determinant of an $m \times m$ matrix A with entries $a_{k,l} \in \mathbb{D}$ is bounded by md where d is the maximal degree of the entries.
Suppose now that R_i is the jth subresultant of A and B. Then, by the definition of the subresultant sequence of the first kind and the definition of the subresultant PRS, the $(j+1)$st subresultant of A and B is regular. Because of this and the subresultant block structure, R_{i-1} is of order $j+1$ and so j is equal to $d_{i-1} - 1$. The bound for R_i then follows from the determinant bound above with $m = d_A + d_B - 2(d_{i-1} - 1)$ and $d = b_i$. □

Example 6.2.18. (Example 6.1.6 cont.) Running the GCRD computation of Example 6.1.6 with the α_i and β_i from the subresultant PRS gives the following maximal coefficient degrees:

PRS	R_2	R_3	R_4	R_5	R_6	R_7	R_8
subresultant	11	16	21	26	31	36	41
primitive	9	12	15	18	21	24	21

Table 6.2.5: Maximal coefficient degrees for different PRSs in Exmaple 6.2.18.

Like the primitive PRS, the subresultant PRS shows linear growth. At the same time, the degrees in the subresultant PRS are not as small as possible. While this usually cannot be observed for randomly chosen input, it is very common for operators coming from applications. For randomly generated operators, the subresultant PRS and the primitive PRS usually coincide. Our next goal is to understand the difference between randomly generated input and the operators A and B as above and to identify the source of some (and most often all) of the additional content in the subresultant PRS.

6.3 Improved Polynomial Remainder Sequences

To derive improvements of the subresultant PRS, we proceed in two stages: First we identify the source of the additional content that appears systematically when computing the GCRD of operators coming from applications. To make use of this knowledge, we will then adjust the formulas for α_i and β_i from Theorem 6.2.16 so that we get a PRS with smaller degrees without having to compute the content of every remainder.

In contrast to the theory in Sections 6.1 and 6.2, the results of this section present original research by the author that was first published in [28].

6.3.1 Sources of Additional Content

In the case of commutative polynomials, some results are known for detecting additional content. An approach worth pursuing when looking for content is to make use of the representation of subresultants in terms of determinants of the matrices $\mathrm{Syl}_{i,j}(A, B)$. By exploiting the special form of these matrices as well as the correspondence between rows of the Sylvester matrix and monomial multiples of A and B, we generalize two known improvements in the commutative case to the Ore setting. The first, Theorem 6.3.1, is a generalization of an observation mentioned in [13], which carries over quite easily to the Ore case. The second, Theorem 6.3.5, usually performs better in terms of coefficient size of the remainders, but a heuristic argument is necessary to use it algorithmically (see Section 6.3.2).

We have a closer look at the structure of the Sylvester matrix. Its first column only contains two non-zero entries, shifts of the leading coefficients of A and B. This structure carries over to the $\mathrm{Syl}_{i,j}(A, B)$, so any common factor of these shifts appears as content in the subresultants (in a shifed version).

Theorem 6.3.1. *With* $t := \gcd(\sigma^{d_B-1}(\mathrm{lc}(A)), \sigma^{d_A-1}(\mathrm{lc}(B)))$ *and* $\gamma_i := \sigma^{-i}(t)$ *for* $0 \leq i \leq d_B - 1$*, we get:*

$$\gamma_i \mid \mathrm{cont}(\mathrm{sres}_i(A, B)). \tag{6.3.1}$$

Proof. Let i be fixed. The coefficients of $\mathrm{sres}_i(A, B)$ are the determinants of the matrices $\mathrm{Syl}_{i,j}(A, B)$ for $0 \leq j \leq i$. The first column of all of these matrices is

$$(\sigma^{d_B-1-i}(\mathrm{lc}(A)), 0, \ldots, 0, \sigma^{d_A-1-i}(\mathrm{lc}(B)), 0, \ldots, 0)^{\mathsf{T}}.$$

Laplace expansion along this column proves the claim. □

Not every subresultant of A and B is an element of the subresultant PRS for A and B. To make use of Theorem 6.3.1 for a new PRS, we specialize the statement to the subresultant sequence of the first kind and restate formula (6.3.1) for this sequence in order to be able to compute the γ_i inductively.

Corollary 6.3.2. *Let* $(R_i)_{i\in\{0,\ldots,\ell+1\}}$ *be the subresultant PRS for* A *and* B *(not necessarily normal). If we choose*

$$t = \gcd(\sigma^{d_B-1}(\mathrm{lc}(A)), \sigma^{d_A-1}(\mathrm{lc}(B))), \quad \gamma_2 = \sigma^{-d_B+1}(t),$$
$$\gamma_i = \sigma^{d_{i-2}-d_{i-1}}(\gamma_{i-1}) \text{ for } 2 < i \leq \ell,$$

then $\gamma_i \mid \mathrm{cont}(R_i)$ *for* $2 \leq i \leq \ell$.

Proof. Suppose R_i is the jth subresultant of A and B. As in the proof of Theorem 6.2.17, we have that j is equal to $d_{i-1}-1$. Then, by Theorem 6.3.1, the content of R_i is divisible by $\sigma^{-d_{i-1}+1}(t)$. It is easy to see that $\sigma^{-d_{i-1}+1}(t)$ is equal to γ_i. □

By the result in Theorem 6.3.1, it is possible to reduce the size of the coefficients of any non-zero subresultant of A and B by a value independent of the index of the particular subresultant. Comparing the degrees in the subresultant PRS and the primitive PRS in Table 6.2.5, however, we see that the degree of the content in the subresultant PRS in this example increases with the index of the remainder. (And so it increases with a decreasing index of the subresultant.) This means that the factors identified in this first improvement do not cover all the content that may appear in applications.

In the commutative case, a second source of additional content was determined, although this result does not seem to be widely known. Assume that A, B are commutative polynomials. A factor that certainly appears in the leading coefficient of both A and B is the leading coefficient of their GCD G. To be more precise, it not only appears in A and B but in all the elements of the contraction of the ideal generated by G, which includes all

subresultants of A and B and also all intermediate results a_i in the division with remainder process described by (2.2.1). This means that in the pseudo-remainder formula, the choice for α_i in (6.1.3) contains the leading coefficient of G as an extraneous factor that then appears as content in the subresultants. In [33], D. Knuth proves the following theorem.

Theorem 6.3.3. *([33]) Let $A, B \in \mathbb{D}[X]$ be such that the subresultant PRS for A and B is normal, i.e. $d_{i-1} = d_i + 1$ for $1 \leq i \leq \ell$, and let G be the GCD of A and B. Then $\mathrm{lc}(G)^{2(i-1)} \mid \mathrm{cont}(R_i)$ for $2 \leq i \leq \ell$.* □

Adapting this theorem to Ore operators is not straightforward. From now on, we denote by $\mathcal{I}$ the contraction of the left ideal generated by G in $\mathbb{K}[X; \sigma, \delta]$. We have seen that the leading coefficient of a left multiple of G of order $n \in \mathbb{N}$ does not necessarily contain all the factors of $\mathrm{lc}(G)$ but only the essential part of $\mathcal{I}$ at order n.

Example 6.3.4. (Example 6.2.18 cont.) If we take A and B as in Example 6.2.18, then the leading coefficient of the GCRD of A and B is $(n+9)p(n)$, where $p(n)$ is a polynomial of degree 17 and $(n+9)$ is the minimal essential part of $\mathcal{I}$ in a shifted version. The subresultant PRS for A and B turns out to be normal and R_2 is of order $d_2 = 12$. By Theorem 6.3.3, if the polynomials were elements of $\mathbb{D}[X]$, $\mathrm{cont}(R_2)$ would be divisible by $\mathrm{lc}(G)^2$ and a naive translation of the theorem to the non-commutative case suggests divisibility by a polynomial of degree at least 36. The (monic) content of R_2, though, is only $(n+16)(n+17)$, which is equal to $\sigma^7(n+9)^{[2]}$.

Again in the commutative case, let Q_A, $Q_B \in \mathbb{D}[X]$ be such that $A = Q_A G$ and $B = Q_B G$. Knuth proves Theorem 6.3.3 by showing that if $(R_i)_{i \in \{0,\ldots,\ell+1\}}$ is the subresultant PRS of A and B and $(\tilde{R}_i)_{i \in \{0,\ldots,\ell+1\}}$ is the subresultant PRS for Q_A, Q_B, then

$$Q_i = \mathrm{lc}(G)^{2(i-1)} \tilde{R}_i. \tag{6.3.2}$$

This approach is problematic for Ore polynomials, because there the Q_i's and the $\tilde{R}_i$'s have coefficients in $\mathbb{K}$ and not necessarily in $\mathbb{D}$. This means that even after showing that a σ-factorial analog of Equation (6.3.2) holds for Ore polynomials (which can be easily done by induction) the left factor $\mathrm{lc}(G)^{2[i-1]}$ and the denominators in the coefficients of $\tilde{R}_i$ might not be coprime and thus lead to cancellation. In order to see which essential parts of $\mathcal{I}$ appear as content and why they do not cancel out, we again investigate the linear map defined by the $\mathrm{Syl}_{i,j}(A, B)$ as well as the effects of the structure of the Sylvester matrix on the determinant. This new approach not only allows us to generalize Theorem 6.3.3 to the Ore case, but also to remove the restriction to normal remainder sequences.

Theorem 6.3.5. *Let $i \in \{0, \dots, d_B - 1\}$ and $\Delta := d_A + d_B - 2i$. If t_k is the kth shift of the essential part of $\mathcal{I}$ at order k for $i < k \leq \Delta + i - 1$, then*

$$\left(\prod_{k=i+1}^{\Delta+i-1} t_k \right) \mid \operatorname{cont}(\operatorname{sres}_i(A, B)).$$

Proof. For any $j \in \{0, \dots, i\}$, $\operatorname{Syl}_{i,j}(A, B)$ is of size $\Delta \times \Delta$ and if the last column is removed, the resulting matrix does not depend on j anymore. For $n \in \{1, \dots, \Delta - 1\}$, let $\mathcal{M}_{i,n}$ be the set of all $n \times n$ matrices obtained by removing the last $\Delta - n$ columns and any $\Delta - n$ rows from $\operatorname{Syl}_{i,j}(A, B)$. The jth coefficient of $\operatorname{sres}_i(A, B)$ is the determinant of $\operatorname{Syl}_{i,j}(A, B)$ and Laplace expansion along the last column shows that it is a $\mathbb{D}$-linear combination of the elements of $\mathcal{M}_{i,\Delta-1}$. By induction on n we show that the determinant of any element of $\mathcal{M}_{i,n}$ is divisible by $t_{\Delta+i-n} t_{\Delta+i-(n-1)} \cdots t_{\Delta+i-1}$. The theorem is then proven by setting $n = \Delta - 1$.
For $n = 1$, the only entry in a matrix in $\mathcal{M}_{i,1}$ is either zero or the leading coefficient of a monomial left multiple of A or B of order $\Delta + i - 1$, so the claim follows from Theorem 4.1.7.
Now suppose the claim is true for $1 \leq n < \Delta - 1$ and let M be any element of $\mathcal{M}_{i,n+1}$. If the determinant of M is zero, then there is nothing to show. Consider the case where $\det(M) \neq 0$. Then there is a $v \in \mathbb{K}^{n+1}$ such that $M^{\mathsf{T}} v = (0, \dots, 0, 1)^{\mathsf{T}}$. By Cramer's rule, the jth component v_j of v is of the form $p_j / \det(M)$ where $p_j \in \mathbb{D}$ is the determinant of some element of $\mathcal{M}_{i,n}$. By induction hypothesis, p_j is divisible by $t_{\Delta+i-n} t_{\Delta+i-(n-1)} \cdots t_{\Delta+i-1}$. Every row in M corresponds to an operator of the form $X^k A$ or $X^k B$ for $k \in \mathbb{N}$, minus some of the lower order terms. For the jth row, $1 \leq j \leq n+1$, we denote the corresponding operator by L_j. By the definition of v, the operator $\sum_{j=0}^{n+1} v_j L_j \in \mathbb{K}[X; \sigma, \delta]$ will have order $\Delta + i - (n+1)$ and leading coefficient 1. So if we set

$$v' := \frac{\det(M)}{t_{\Delta+i-n} t_{\Delta+i-(n-1)} \cdots t_{\Delta+i-1}} v \in \mathbb{D}^{n+1},$$

and $L = \sum_{j=0}^{n+1} v'_j L_j$, then L is an element in $\mathcal{I}$ with order $\operatorname{ord}(L) = \Delta + i - (n+1)$ and its leading coefficient is

$$\det(M) / (t_{\Delta+i-n} t_{\Delta+i-(n-1)} \cdots t_{\Delta+i-1}) \in \mathbb{D}.$$

Theorem 4.1.7 yields that $\operatorname{lc}(L)$ is divisible by $t_{\Delta+i-(n+1)}$, so we get in total $t_{\Delta+i-(n+1)} t_{\Delta+i-n} \cdots t_{\Delta+i-1} \mid \det(M)$. □

We have shown in Corollary 6.2.13 that the non-zero subresultants are elements of the ideal generated by A and B in $\mathbb{D}[X; \sigma, \delta]$. The same is true for the subresultants with the content identified in Theorem 6.3.5 being cleared.

Corollary 6.3.6. *Fix $i \in \mathbb{N}$ with $0 \leq i \leq d_B - 1$ and $\operatorname{sres}_i(A, B)$ being non-zero. Let t_k be as in Theorem 6.3.5 for $i < k \leq \Delta + i - 1$. Then there exist non-zero $S_i, T_i \in \mathbb{D}[X; \sigma, \delta]$ such that*

$$S_i A + T_i B = \frac{1}{\prod_{k=i+1}^{\Delta+i-1} t_k} \operatorname{sres}_i(A, B), \quad d_S < d_B - i, \ d_T < d_A - i.$$

Proof. Suppose $\operatorname{sres}_i(A, B)$ is of order $n \in \mathbb{N}$. By Corollary 6.2.13, there are operators $\tilde{S}_i = \sum_{j=0}^{d_B-(i+1)} \tilde{s}_j X^j$ and $\tilde{T}_i = \sum_{j=0}^{d_A-(i+1)} \tilde{t}_j X^j$ with $\tilde{s}_j, \tilde{t}_j \in \mathbb{D}$ such that

$$\tilde{S}_i A + \tilde{T}_i B = \operatorname{sres}_i(A, B),$$

and so

$$\operatorname{Syl}_{i,n}(A, B)^{\mathsf{T}} \underbrace{(\tilde{s}_{d_B-(i+1)}, \ldots, \tilde{s}_0, \tilde{t}_{d_A-(i+1)}, \ldots, \tilde{t}_0)^{\mathsf{T}}}_{=:v} = (0, \ldots, 0, \det(\operatorname{Syl}_{i,n}(A, B)))^{\mathsf{T}},$$

with $\det(\operatorname{Syl}_{i,n}(A, B)) \neq 0$. By Cramer's rule, the jth component v_j of v is of the form

$$\det(\operatorname{Syl}_{i,n}(A, B)) \frac{p_j}{\det(\operatorname{Syl}_{i,n}(A, B))} = p_j,$$

where $p_j \in \mathbb{D}$ is the determinant of some element of $\mathcal{M}_{i,\Delta-1}$ (as in Theorem 6.3.5). Therefore, by what was shown in the proof of Theorem 6.3.5, the v_j are divisible by $\prod_{k=i+1}^{\Delta+i-1} t_k$. Setting

$$S_i = \frac{1}{\prod_{k=i+1}^{\Delta+i-1} t_k} \tilde{S}_i, \quad T_i = \frac{1}{\prod_{k=i+1}^{\Delta+i-1} t_k} \tilde{T}_i,$$

completes the proof. □

As was already noted in Chapter 4, all removable singularities can usually be removed by an order 1 operator if the ideal generator G comes from applications. In the context of Theorem 6.3.5, this means that the essential part of $\mathcal{I}$ is the same at every order $n > \operatorname{ord}(G)$: the minimal essential part introduced in Definition 4.1.10. When only considering one essential part, the statement of the theorem simplifies in a way that makes it more useful for the Euclidean algorithm. We only have to obtain information about one essential part instead of several essential parts at different orders.

Corollary 6.3.7. *Let $i \in \{0, \ldots, d_B - 1\}$ and $\Delta := d_A + d_B - 2i$. If t is the essential part of $\mathcal{I}$ at order $d_A + d_B - 1$, then*

$$\sigma^{i+1}(t)^{[\Delta-1]} \mid \operatorname{cont}(\operatorname{sres}_i(A, B)).$$

Proof. According to Theorem 4.1.7, t divides the essential part of $\mathcal{I}$ at order j for any $d_G \leq j \leq d_A + d_B - 1$. Theorem 6.3.5 yields that $\operatorname{cont}(\operatorname{sres}_i(A, B))$ is divisible by

$$\sigma^{i+1}(t)\sigma^{i+2}(t)\dots\sigma^{\Delta+i-1}(t) = \sigma^{i+1}(t)^{[\Delta-1]}. \qquad \square$$

As for Theorem 6.3.1, an adjustment of Corollary 6.3.7 to the subresultant sequence of the first kind is needed in order to construct a new PRS.

Corollary 6.3.8. *Let $(R_i)_{i\in\{0,\dots,\ell+1\}}$ be the subresultant PRS for A and B (not necessarily normal) and let t be the essential part of $\mathcal{I}$ at order $d_A + d_B - 1$. If we set $\gamma_2 = \sigma^{d_B}(t)^{[d_A-d_B+1]}$ and*

$$\gamma_i = \sigma^{d_{i-1}}(t)^{[d_{i-2}-d_{i-1}]}\gamma_{i-1}\sigma^{d_A+d_B-d_{i-2}+1}(t)^{[d_{i-2}-d_{i-1}]} \text{ for } 2 < i \leq \ell,$$

then $\gamma_i \mid \operatorname{cont}(R_i)$ for $2 \leq i \leq \ell$.

Proof. Suppose R_i is the jth subresultant of A and B. As in the proof of Theorem 6.2.17, we have that j is equal to $d_{i-1}-1$. So by Corollary 6.3.7, the content of R_i is divisible by $\sigma^{d_{i-1}}(t)^{[d_A+d_B-2d_{i-1}+1]}$. Simple hand calculation shows that this is equal to γ_i. $\square$

6.3.2 Algorithm and Examples

To incorporate the results of the preceding section into the Euclidean algorithm, we derive new formulas for the α_i and β_i for PRSs that contain the elements of the subresultant sequence of the first kind with the additional content found in Theorems 6.3.1 and 6.3.5 divided out.

We start with a technical lemma to connect the pseudo-quotient of two operators to the pseudo-quotient of $\mathbb{K}$-multiples of the same operators.

Lemma 6.3.9. *For $\gamma_1, \gamma_2 \in \mathbb{K} \setminus \{0\}$, we get:*

$$\operatorname{pquo}(\gamma_1 A, \gamma_2 B)\gamma_2 = \gamma_1\gamma_2^{[d_A-d_B+1]} \operatorname{pquo}(A, B).$$

Proof. By Lemma 2.3 in [40], the pseudo-remainder of $\gamma_1 A$ and $\gamma_2 B$ is the $(d_B - 1)$st subresultant of $\gamma_1 A$ and $\gamma_2 B$ (up to sign). Consequently, its coefficients are determinants of submatrices of $\operatorname{Syl}(\gamma_1 A, \gamma_2 B)$ that contain one row corresponding to the operator $\gamma_1 A$ and $d_A - d_B + 1$ rows corresponding to operators of the form $X^i\gamma_2 B$, $0 \leq i \leq d_A - d_B$. Thus, by Lemma 2.2 in [40], it follows that

$$\operatorname{prem}(\gamma_1 A, \gamma_2 B) = \gamma_1\gamma_2^{[d_A-d_B+1]} \operatorname{prem}(A, B). \tag{6.3.3}$$

The pseudo-remainder formula (6.1.2) applied to $\gamma_1 A$ and $\gamma_2 B$ gives

$$\operatorname{lc}(\gamma_2 B)^{[d_A-d_B+1]}\gamma_1 A = \operatorname{pquo}(\gamma_1 A, \gamma_2 B)\gamma_2 B + \operatorname{prem}(\gamma_1 A, \gamma_2 B).$$

Combining this with (6.3.3) and then dividing the resulting equation by $\gamma_1\gamma_2^{[d_A-d_B+1]}$ from the left yields the desired result. $\square$

This now allows us to state α_i and β_i for improved polynomial remainder sequences, based on the formulas for the subresultant PRS given in Theorem 6.2.16:

Theorem 6.3.10. *Let $(R_i)_{i\in\{0,\dots,\ell+1\}}$ be the subresultant PRS for A and B and let $(\gamma_i)_{i\in\{0,\dots,\ell+1\}}$ be any sequence in $\mathbb{K}\setminus\{0\}$ with $\gamma_0=\gamma_1=1$. Set $\tilde{R}_i=\frac{1}{\gamma_i}R_i$. Then $(\tilde{R}_i)_{i\in\{0,\dots,\ell+1\}}$ is a PRS for A and B with:*

$$\tilde{\alpha}_i = \operatorname{lc}(\tilde{R}_i)^{[d_{i-1}-d_i+1]},$$
$$\tilde{\beta}_i = \begin{cases} -\sigma(\tilde{\psi}_1)^{[d_0-d_1]}\gamma_2, & \text{if } i=1,\\ \dfrac{-\operatorname{lc}(\tilde{R}_{i-1})\sigma(\tilde{\psi}_i)^{[d_{i-1}-d_i]}}{\gamma_i{}^{[d_{i-1}-d_i+1]}}\gamma_{i+1}, & \text{if } 2\le i\le \ell-1,\end{cases}$$

where

$$\tilde{\psi}_i = \begin{cases} -1, & \text{if } i=1,\\ \dfrac{(-\gamma_{i-1}\operatorname{lc}(\tilde{R}_{i-1}))^{[d_{i-2}-d_{i-1}]}}{\sigma(\tilde{\psi}_{i-1})^{[d_{i-2}-d_{i-1}-1]}}, & \text{if } 2\le i\le \ell-1.\end{cases}$$

Proof. From the definition of $\tilde{R}_i$ and the equations

$$\alpha_i R_{i-1} = Q_i R_i + \beta_i R_{i+1} \qquad \text{and} \qquad \alpha_i = \gamma_i^{[d_{i-1}-d_i+1]}\tilde{\alpha}_i,$$

it follows that

$$\gamma_i^{[d_{i-1}-d_i+1]}\gamma_{i-1}\tilde{\alpha}_i\tilde{R}_{i-1} = Q_i\gamma_i\tilde{R}_i + \beta_i\gamma_{i+1}\tilde{R}_{i+1}. \tag{6.3.4}$$

For the first summand on the right hand side, Lemma 6.3.9 yields

$$Q_i\gamma_i = \gamma_i^{[d_{i-1}-d_i+1]}\gamma_{i-1}\tilde{Q}_i. \tag{6.3.5}$$

For the second summand, observe that since $\gamma_i\operatorname{lc}(\tilde{R}_i)$ equals $\operatorname{lc}(R_i)$, we have that ψ_i equals $\tilde{\psi}_i$ for all $1\le i\le\ell$. Thus

$$\beta_i\gamma_{i+1} = \gamma_i^{[d_{i-1}-d_i+1]}\gamma_{i-1}\tilde{\beta}_i. \tag{6.3.6}$$

The proof is concluded by combining (6.3.4), (6.3.5) and (6.3.6) and dividing the resulting equation by $\gamma_i^{[d_{i-1}-d_i+1]}\gamma_{i-1}$ from the left. □

Based on these new α_i and β_i, we present two new polynomial remainder sequences for Ore polynomials.

Definition 6.3.11. Let t be the essential part of $\mathcal{I}$ at order d_A+d_B-1. In Definition 6.1.2, set

1. $\gamma_2=\gcd(\operatorname{lc}(A),\sigma^{d_A-d_B}(\operatorname{lc}(B)))$, $\gamma_i=\sigma^{d_{i-2}-d_{i-1}}(\gamma_{i-1})$ and α_i and β_i as in Theorem 6.3.10. This is the *simple improved polynomial remainder sequence* for A and B.

2. $\gamma_2 = \sigma^{d_B}(t)^{[d_A-d_B+1]}$ and

$$\gamma_i = \sigma^{d_{i-1}}(t)^{[d_{i-2}-d_{i-1}]}\gamma_{i-1}\sigma^{d_A+d_B-d_{i-2}+1}(t)^{[d_{i-2}-d_{i-1}]},$$

and α_i and β_i as in Theorem 6.3.10. This is the *essential polynomial remainder sequence* for A and B.

By Corollaries 6.3.2 and 6.3.8, the remainders in the simple improved PRS and the essential PRS for A and B have coefficients in $\mathbb{D}$.

Computing the simple improved PRS is straightforward, but in order to compute the essential polynomial remainder sequence for A and B with the refined Euclidean algorithm, one needs to know the essential part at order $d_A + d_B - 1$ of $\mathcal{I}$. This knowledge is usually not available and there is no known way to compute it without considerable computational overhead. To bypass this problem, we give a reasonable guess for the essential part. By Theorem 4.1.7 shifts of the essential part t at order $d_A + d_B - 1$ divide the leading coefficients of all operators in $\mathcal{I}$ of order $\leq d_A + d_B - 1$, in particular the leading coefficient of A and the leading coefficient of B. So we get

$$\sigma^{d_A}(t) \mid \gcd(\mathrm{lc}(A), \sigma^{d_A-d_B}(\mathrm{lc}(B))). \tag{6.3.7}$$

In practice, it is most often the case that $\mathrm{lc}(A)$ and $\sigma^{d_A-d_B}(\mathrm{lc}(B))$ share no other factors, so the GCD on the right hand side of (6.3.7) will be equal to the d_Ath shift of t. We recommend to use this guess in implementations of the refined Euclidean algorithm to compute the essential PRS for A and B. Also, if the guess is correct (or too small), then all the content that is detected in the simple improved PRS is also detected in the essential PRS. Otherwise, if the guess is too big, this can be fixed during the execution of the algorithm (see Example 6.3.13 below).

Example 6.3.12. (Example 6.2.18 cont.) We now will use Theorem 6.3.10 and Corollaries 6.3.2 and 6.3.8 to compute new PRSs for A and B as in Example 6.1.6. The essential part of $\mathcal{I}$ at order $d_A + d_B - 1$ is $(n+3)$, so $\sigma^{d_A}(n+3) = (n+17)$, which is also the guess given by the right hand side of (6.3.7). Applying Corollary 6.3.2 yields the factors

$$\gamma_2 = n+17, \quad \gamma_3 = n+18, \quad \ldots \quad \gamma_i = n+16+i-1, \quad \ldots$$

whereas Corollary 6.3.8 gives

$$\gamma_2 = (n+16)^{[2]}, \quad \gamma_3 = (n+15)^{[4]}, \quad \ldots \quad \gamma_i = (n+16-i+2)^{[2(i-1)]}, \quad \ldots$$

The improvements in the simple improved PRS are marginal, while the degrees in the essential PRS are equal to the degrees in the primitive PRS, except for the very last step:

PRS	R_2	R_3	R_4	R_5	R_6	R_7	R_8
subresultant	11	16	21	26	31	36	41
simple improved	10	15	20	25	30	35	40
essential	9	12	15	18	21	24	27
primitive	9	12	15	18	21	24	21

Table 2: Maximal coefficient degrees for the subresultant, simple improved, essential and primitive PRS in Example 6.3.12.

Example 6.3.13. Although the remainders in the essential polynomial remainder sequence are usually primitive when starting from randomly generated operators or operators that come from some applications, it is not guaranteed that this is always the case. As an example, consider

$$\begin{aligned} &A, B \in \mathbb{Q}[y][X], \\ &A = X^4 + yX^2 + yX + y, \\ &B = X^3 + yX^2. \end{aligned}$$

The second subresultant of A and B is $\operatorname{sres}_2(A, B) = (y + y^2)X^2 + yX + y$, so $\operatorname{cont}(\operatorname{sres}_2(A, B)) = y$, but in the essential PRS, no content will be found. As mentioned, it may also happen that the guess for the essential part of $\mathcal{I}$ at order $d_A + d_B - 1$ is too large, for example:

$$\begin{aligned} &A, B \in \mathbb{Q}[y][D, 1, \tfrac{d}{dy}], \\ &A = (y+1)D^4 + D^3 + D^2 + yD + 1, \\ &B = (y+1)D^3 + D^2 + 1. \end{aligned}$$

Here, $\operatorname{cont}(R_3)$ in the subresultant PRS is $(y + 1)$, but a factor $(y + 1)^2$ is predicted. The mistake in predicting the essential part can be noticed on the fly during the execution of the algorithm as soon as a remainder with coefficients in $\mathbb{Q}(y) \setminus \mathbb{Q}[y]$ appears. It is then possible to either switch to another PRS or to refine the guess of the essential part. One strategy to do so is to remove all the factors from the guess that could be responsible for the occurance of denominators. Let t be the guess for the essential part of $\mathcal{I}$ at order $d_A + d_B - 1$ and let c be the non-trivial common denominator of the coefficients of a remainder R_i in the essential PRS. Furthermore let M be the set of all integers m such that $\gcd(\sigma^m(c), t) \neq 1$. Update R_i, γ_i and t with

$$\begin{aligned} R_i &\leftarrow cR_i, \\ \gamma_i &\leftarrow \frac{\gamma_i}{c}, \\ t &\leftarrow \frac{t}{\gcd(t, \prod_{m \in M} \sigma^m(c))}, \\ \gamma_{i+1} &\leftarrow \sigma^{d_i - d_B}(t)^{[d_A + d_B - 2d_i + 1]}, \text{ (see the proof of Cor. 6.3.8)} \end{aligned}$$

and continue the computation with these new values. For differential operators in $\mathbb{C}[y][D; 1, \frac{d}{dy}]$, we have $M = \{0\}$ and for recurrence operators in $\mathbb{C}[n][S_n; s_n, 0]$, M contains all the integer roots of $\operatorname{res}_n(c(n+m), t) \in \mathbb{Q}[m]$.

The assumption that it is sufficient to consider only one essential part usually holds, but we have seen in Example 5.2.3 that it can happen that different factors of the leading coefficient of a generator of an operator ideal are removable at different orders. This leads to different essential parts at different orders and hence, not all the content will be detected in the essential PRS. It is highly unlikely that this happens for operators that are not specially designed for this purpose.

Example 6.3.14. We can guess two operators A and B in $\mathbb{Q}[n][S; s_n, 0]$ of order $d_A = 16$, $d_B = 14$, respectively that annihilate the sequence

$$t_n = (7n^3 + 5n^2 + n + 1)^7((n + 1/7)^{\overline{12}})^7 \frac{(2n)!^3}{(3n)!^2}.$$

The GCRD of A and B is of order 1 and the essential part of $\mathcal{I}$ at order $d_A + d_B - 1$ is of degree 4. The essential part of $\mathcal{I}$ at order 11, however, is of degree 11, so here we are in the rare case where the essential part of $\mathcal{I}$ at order $d_A + d_B - 1$ is only contained but not equal to the essential part at lower orders. Formula (6.3.7) only predicts the essential part of $\mathcal{I}$ at order $d_A + d_B$ and during the GCRD computation, content that comes from lower order essential parts emerges.

PRS	R_2	R_3	R_4	R_5	R_6	R_7	R_8
essential	31	44	57	70	83	96	109
primitive	31	44	50	56	62	68	74

Table 3: Maximal coefficient degrees for the first few remainders in the essential and primitive PRS in Example 6.3.14.

It is possible to also guess the essential part of $\mathcal{I}$ at lower orders and then use Theorem 6.3.5 to get the primitive remainders, but like in the direct computation of the primitive PRS, GCD computations in the base ring would be necessary after each division step.

Besides the practical use of the improvements presented in this chapter for the computation of the greatest common right divisor of Ore polynomials, we can also give a new upper bound for the maximal coefficient degree of the remainders in the primitive PRS in terms of the essential parts of $\mathcal{I}$.

Theorem 6.3.15. *Let $(R_i)_{i\in\{0,\dots,\ell+1\}}$ be the primitive PRS for A and B. Fix $i \in \{2, \dots, \ell\}$ and let $b_i \in \mathbb{N}$ be such that*

$$\max_{k \in \{0,\dots,d_B - d_{i-1} - 2\}}(\deg(X^k A)) \le b_i \quad \text{and} \quad \max_{k \in \{0,\dots,d_A - d_{i-1} - 2\}}(\deg(X^k B)) \le b_i.$$

If t_k denotes the kth shift of the essential part of $\mathcal{I}$ at order $k \in \mathbb{N}$, then

$$\deg(R_i) \leq (d_A + d_B - 2(d_{i-1} - 1))b_i - \sum_{k=d_{i-1}}^{d_A+d_B-d_{i-1}+1} \deg(t_k).$$

Proof. The bound is an immediate consequence of Theorem 6.2.17 and Corollary 6.3.8. □

Appendix A

The Ore Algebra Package for Sage

The group for algorithmic combinatorics at RISC offers a software package for the mathematics software system Sage (see [51]) developed by Manuel Kauers, Fredrik Johansson and the author. It is available for free download together with an extensive documentation from

http://www.risc.jku.at/research/combinat/software/ore_algebra/

Among many other features, the packages allows to desingularize recurrence and differential operators as described in Chapter 4 and to compute the GCRD of two Ore polynomials by using different polynomial remainder sequences, including the essential PRS as introduced in Chapter 6. Here are some use cases where we desingularize a recurrence operator and compute the GCRD of two differential operators.

First, we load the package and define the Ore rings.

```
sage: # Load the package.
sage: from ore_algebra import *
sage: # Define the base rings for the Ore algebras.
sage: Abase.<y> = PolynomialRing(QQ)
sage: Bbase.<n> = PolynomialRing(QQ)
sage: # Define a differential Ore algebra
sage: # and set Dy to be its generator.
sage: A.<Dy> = OreAlgebra(Abase)
sage: # Define a recurrence Ore algebra.
sage: # and set Sn to be its generator.
sage: B.<Sn> = OreAlgebra(Bbase)
```

To get an Ore polynomial with a removable factor in the leading coefficient, we take a polynomial in $\mathbb{Q}[n]$ and its order 1 annihilator.

```
sage: p = 2*n^3 - 8*n^2 + 1
sage: L = p*Sn-p(n+1)
sage: L
 (2*n^3 - 8*n^2 + 1)*Sn - 2*n^3 + 2*n^2 + 10*n + 5
sage: # Check that L is an annihilator of p.
sage: L(p)
                          0
```

Desingularization then yields an operator with a leading coefficient in $\mathbb{Q}$. The trailing coefficient, however, is not as small as possible.

```
sage: L2 = L.desingularize()
sage: # L2 is also an annihilator of p.
sage: L2(p)
                          0
sage: # The leading coefficient of L2 has degree 0.
sage: L2.leading_coefficient().degree()
                          0
sage: # But the trailing coefficient is of degree >0.
sage: L2.coeffs()[0].degree()
                          9
```

Next we take two differential operators and compute their greatest common right divisor and their Bézout coefficients.

```
sage: # Create two Ore polynomials L1 and L2
sage: # with non-trivial GCRD G.
sage: G = A.random_element(2)
sage: L1, L2 = A.random_element(7), A.random_element(5)
sage: while L1.gcrd(L2) != 1: L2 = A.random_element(5)
sage: L1, L2 = L1*G, L2*G
sage: # Compute the GCRD of L1 and L2 and compare it
sage: # to unit normal G.
sage: L1.gcrd(L2).normalize() == G.normalize()
                        True
sage: # Compute the GCRD of L1 and L2 and
sage: # the corresponding Bezout coefficients.
sage: (L3, S, T) = L1.xgcrd(L2)
sage: S*L1 + T*L2 == L3
                        True
```

Different polynomial remainder sequences can be used to compute the GCRD. Note that the output will always be the unit normal GCRD and therefore it won't be visible that different PRSs are used:

```
sage: # Create random differential operators
sage: L1, L2 = A.random_element(3), A.random_element(2)
sage: # Compute the GCRD with various PRSs which
sage: # can be specified via different keywords.
sage: algs = ["improved", "classic", "monic",
       "subresultant"]
sage: [L1.gcrd(L2, prs=a) for a in algs]
                      [1,1,1,1]
```

For a comprehensive tutorial on how to use many of the features provided by the package, see [31].

Appendix B

Notation

The table given below contains explanations and references to the definitions of the mathematical notation and symbols used throughout the thesis in order of appearance.

Chapter 2	
$a \mid b$, $a \mid_r b$, $a \mid_l b$	a divides b (on the right or left). → Section 2.1.
$\gcd(a,b)$, $\mathrm{gcrd}(a,b)$, $\mathrm{gcld}(a,b)$	The unit normal greatest common (right or left) divisor of a and b. → Definition 2.1.1.
$\mathrm{quo}(a,b)$, $\mathrm{rquo}(a,b)$, $\mathrm{lquo}(a,b)$	The (right or left) quotient of a and b. → Definition 2.1.3.
$\mathrm{rem}(a,b)$, $\mathrm{rrem}(a,b)$, $\mathrm{lrem}(a,b)$	The (right or left) remainder of a and b. → Definition 2.1.3.
$\mathrm{lcm}(a,b)$, $\mathrm{lcrm}(a,b)$, $\mathrm{lclm}(a,b)$	The unit normal least common (right or left) multiple of a and b. → Definition 2.1.4.
$a^{\underline{n}}$	The nth falling factorial of a: $\prod_{i=0}^{n-1}(a-i)$. → Section 2.1.
$a^{\overline{n}}$	The nth rising factorial of a: $\prod_{i=0}^{n-1}(a+i)$. → Section 2.1.
$\mathbb{D}[x]$	Commutative polynomial ring in x over $\mathbb{D}$. → Section 2.2.
$\mathrm{lc}(p)$, $\mathrm{tc}(p)$, $[x^i]p$	The leading, the trailing and the ith coefficient of a polynomial p in x. → Section 2.2.

$\deg(p)$	The degree of a commutative polynomial p. → Section 2.2.
$\operatorname{cont}(p)$	The content of a polynomial p. → Section 2.2.
$\operatorname{pp}(p)$	The primitive part of a polynomial p. → Section 2.2.
Chapter 3	
$\mathbb{D}[X;\sigma,\delta]$	Ore polynomial ring in X over $\mathbb{D}$ with endomorphism σ and pseudo-derivation δ. → Definition 3.1.1.
$\operatorname{const}(\mathbb{D}[X;\sigma,\delta])$	The set of constants of the Ore Algebra $\mathbb{D}[X;\sigma,\delta]$. → Definition 3.1.1.
$\operatorname{ord}(A), d_A$	The order of $A \in \mathbb{D}[X;\sigma,\delta]$, i.e. the degree of A in X. → Section 3.1.1.
$\sigma^n(a)$	The nth shift of a. → Section 3.1.1.
$a^{[n]}$	The nth σ-factorial of a: $a\sigma(a)\dots\sigma^{n-1}(a)$. → Definition 3.1.2.
s_n	Shift function in n: $p(n) \mapsto p(n+1)$. → Example 3.1.3.
$s_{q,y}$	q-Shift in y: $p(y) \mapsto p(qy)$. → Example 3.1.3.
$A(f)$	The image of the action of an operator A applied to a function f. → Definition 3.1.4.
$V(A), V(A)_{\mathcal{G}}$	Set of solutions of an operator A (in $\mathcal{G}$). → Section 3.1.2.
Chapter 4	
$\deg(L)$	The maximum of all the degrees of the coefficients of an operator L. → Section 4.1.
$v_u(p)$	The multiplicity of an irreducible element p in u. → Definition 4.3.4.

$v_u^<(p)$	The backward-shift multiplicity of an irreducible element p in u. → Definition 4.3.4.
$\mathrm{ind}_L(p)$	The indicial polynomial of $L \in \mathbb{K}[y][\partial; 1, \frac{d}{dy}]$ at $p \in \mathbb{K}[y]$. → Section 4.3.2.

Chapter 6

$\mathrm{prem}(A, B)$, $\mathrm{pquo}(A, B)$	The pseudo-remainder and the pseudo-quotient of two operators A and B. → Definition 6.1.4.
$\mathrm{Syl}(A, B)$	The Sylvester matrix of A and B. → Definition 6.2.2.
$\mathrm{res}(A, B)$	The resultant of A and B. → Definition 6.2.2.
$\mathrm{Syl}_i(A, B)$, $\mathrm{Syl}_{i..j}(A, B)$	Submatrices of the Sylvester matrix of A and B. → Definition 6.2.7.
$\mathrm{sres}_i(A, B)$	The ith polynomial subresultant of A and B. → Definition 6.2.9.

Bibliography

[1] S. A. Abramov, M. A. Barkatou, and M. van Hoeij. Apparent singularities of linear difference equations with polynomial coefficients. *Appl. Algebra Eng., Commun. Comput.*, 17(2):117–133, June 2006.

[2] S. A. Abramov, H. Q. Le, and Z. Li. Univariate Ore polynomial rings in computer algebra. *Journal of Mathematical Sciences*, 131(5):5885–5903, 2005.

[3] S. A. Abramov and M. van Hoeij. Desingularization of linear difference operators with polynomial coefficients. In *Proceedings of ISSAC 1999*, pages 269–275, 1999.

[4] M. Abramowitz and I. A. Stegun. *Handbook of Mathematical Functions: With Formulas, Graphs, and Mathematical Tables*. Applied mathematics series. Dover Publications, 1964.

[5] G. Almkvist and D. Zeilberger. The method of differentiating under the integral sign. *Journal of Symbolic Computation*, 10:571–591, 1990.

[6] J. Blümlein, M. Kauers, S. Klein, and C. Schneider. Determining the closed forms of the O(as3) anomalous dimension and Wilson coefficients from Mellin moments by means of computer algebra. *Computer Physics Communications*, 180(11):2143–2165, November 2009.

[7] A. Bostan, S. Boukraa, S. Hassani, M. van Hoeij, J.-M. Maillard, J.-A. Weil, and N. Zenine. The Ising model: from elliptic curves to modular forms and Calabi-Yau equations. *Journal of Physics A: Mathematical and Theoretical*, 44(4):44pp, 2011.

[8] A. Bostan, M. Bousquet-Mélou, M. Kauers, and S. Melczer. On lattice walks confined to the positive octant. 2013. in preparation.

[9] A Bostan, F. Chyzak, G. Lecerf, B. Salvy, and É. Schost. Differential equations for algebraic functions. In *Proceedings of ISSAC 2007*, pages 25–32, 2007.

[10] A. Bostan, F. Chyzak, Z. Li, and B. Salvy. Fast computation of common left multiples of linear ordinary differential operators. In *Proceedings of ISSAC 2012*, pages 99–106, 2012.

[11] A. Bostan and M. Kauers. The complete generating function for Gessel walks is algebraic. *Proceedings of the American Mathematical Society*, 138(9):3063–3078, September 2010. With an Appendix by Mark van Hoeij.

[12] M. Bronstein and M. Petkovšek. An introduction to pseudo-linear algebra. *Theoretical Computer Science*, 157:3–33, 1996.

[13] W. S. Brown. The subresultant PRS algorithm. *ACM Trans. Math. Softw.*, 4(3):237–249, 1978.

[14] W. S. Brown and J. F. Traub. On Euclid's algorithm and the theory of subresultants. *J. ACM*, 18(4):505–514, 1971.

[15] S. Chen, M. Jaroschek, M. Kauers, and M. Singer. Desingularization explains order-degree curves for Ore operators. In *Proceedings of ISSAC 2013*, pages 157–164, 2013.

[16] S. Chen and M. Kauers. Order-degree curves for hypergeometric creative telescoping. In *Proceedings of ISSAC 2012*, pages 122–129, 2012.

[17] S. Chen and M. Kauers. Trading order for degree in creative telescoping. *Journal of Symbolic Computation*, 47(8):968–995, 2012.

[18] F. Chyzak. An extension of Zeilberger's fast algorithm to general holonomic functions. *Discrete Mathematics*, 217(1-3):115–134, 2000.

[19] F. Chyzak, M. Kauers, and B. Salvy. A non-holonomic systems approach to special function identities. In *Proceedings of ISSAC 2009*, pages 111–118, 2009.

[20] F. Chyzak and B. Salvy. Non-commutative elimination in ore algebras proves multivariate holonomic identities. *Journal of Symbolic Computation*, 26(2):187–227, August 1998.

[21] P.M. Cohn. *Free rings and their relations*. L.M.S. monographs. Academic Press, 1971.

[22] G. E. Collins. Subresultants and reduced polynomial remainder sequences. *J. ACM*, 14(1):128–142, 1967.

[23] P. Flajolet and R. Sedgewick. *Analytic Combinatorics*. Cambridge University Press, New York, NY, USA, 1 edition, 2009.

[24] K.O. Geddes, S.R. Czapor, and G. Labahn. *Algorithms for Computer Algebra*. Kluwer Academic Publishers, 1992.

[25] R. L. Graham, D. E. Knuth, and O. Patashnik. *Concrete Mathematics: A Foundation for Computer Science*. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 2nd edition, 1994.

[26] W. Hebisch and M. Rubey. Extended rate, more gfun. *Journal of Symbolic Computation*, 46(8):889–903, August 2011.

[27] E. L. Ince. *Ordinary Differential Equations*. Dover Books on Science. Dover Publications, 2012.

[28] M. Jaroschek. Improved polynomial remainder sequences for Ore polynomials. *Journal of Symbolic Computation*, 58:64–76, 2013.

[29] M. Kauers. Guessing handbook. *Technical Report, RISC, Johannes Kepler University Linz*, 09-07, 2009.

[30] M. Kauers, M. Jaroschek, and F. Johansson. *Ore algebra package for Sage*, 2013. `https://www.risc.jku.at`.

[31] M. Kauers, M. Jaroschek, and F. Johansson. Ore polynomials in Sage. *ArXiv 1306.4263*, June 2013.

[32] M. Kauers and P. Paule. *The Concrete Tetrahedron*. Text and Monographs in Symbolic Computation. Springer Wien, 1st edition, 2011.

[33] D. E. Knuth. *The Art of Computer Programming, Volume II: Seminumerical Algorithms, 2nd Edition*. Addison-Wesley, 1981.

[34] C. Koutschan. *Advanced Applications of the Holonomic Systems Approach*. PhD thesis, RISC, Johannes Kepler University Linz, September 2009.

[35] C. Koutschan. HolonomicFunctions (User's Guide). Technical Report 10-01, RISC Report Series, Johannes Kepler University Linz, January 2010.

[36] C. Koutschan, M. Kauers, and D. Zeilberger. Proof of George Andrews's and David Robbins's q-TSPP conjecture. *Proceedings of the National Academy of Sciences*, 108(6):2196–2199, 2011.

[37] T.Y. Lam. *A First Course in Noncommutative Rings*. Graduate Texts in Mathematics. Springer, 2001.

[38] E. Landau. Ein Satz über die Zerlegung homogener linearer Differentialausdrücke in irreducible Factoren. *Journal für die reine und angewandte Mathematik*, 124:115–120, 1902.

[39] Z. Li. *A Subresultant Theory for Linear Differential, Linear Difference, and Ore Polynomials with Applications*. PhD thesis, RISC, Johannes Kepler University Linz,, 1996.

[40] Z. Li. A subresultant theory for Ore polynomials with applications. In *Proceedings of ISSAC 1998*, pages 132–139, 1998.

[41] R. Loos. Generalized polynomial remainder sequences. In *Computer Algebra, Symbolic and Algebraic Computation. B. Buchberger, G. Collins, R. Loos (eds)*, pages 115–137. Springer-Verlag, Wien-New York, 1982.

[42] Ø. Ore. Theory of non-commutative polynomials. *Annals of Mathematics*, 34(3):480–508, 1933.

[43] M. Petkovšek, H.S. Wilf, and D. Zeilberger. $A = B$. Ak Peters Series. Peters, 1996.

[44] M. Petkovšek. Hypergeometric solutions of linear recurrences with polynomial coefficients. *Journal of Symbolic Computation*, 14(2–3):243 – 264, 1992.

[45] B. Salvy. D-finiteness: algorithms and applications. In *Proceedings of ISSAC 2005*, pages 2–3, 2005.

[46] B. Salvy and P. Zimmermann. Gfun: a Maple package for the manipulation of generating and holonomic functions in one variable. *ACM Transactions on Mathematical Software*, 20(2):163–177, 1994.

[47] L. Schlesinger. *Handbuch der Theorie der linearen Differentialgleichungen*. Number 1 in Handbuch der Theorie der linearen Differentialgleichungen. B. G. Teubner, 1895.

[48] M. F. Singer. Liouvillian solutions of n-th order homogeneous linear differential equations. *American Journal of Mathematics*, 103(4):pp. 661–682, 1981.

[49] N. Sloane et al. *The On-Line Encyclopedia of Integer Sequences*. `http://oeis.org`.

[50] R. P. Stanley. *Enumerative combinatorics*, volume 2. Wadsworth Publ. Co., Belmont, CA, USA, 1986.

[51] W. A. Stein et al. *Sage Mathematics Software (Version 5.11)*. The Sage Development Team, 2013. `http://www.sagemath.org`.

[52] H. Tsai. Weyl closure of a linear differential operator. *Journal of Symbolic Computation*, 29(4-5):747–775, 2000.

[53] J. von zur Gathen and J. Gerhard. *Modern Computer Algebra*. Cambridge University Press, New York, NY, USA, 2nd edition, 2003.

[54] H. S. Wilf and D. Zeilberger. An algorithmic proof theory for hypergeometric (ordinary and "q") multisum/integral identities. *Inventiones mathematicae*, 108(1):575–633, 1992.

[55] J. Wimp and D. Zeilberger. Resurrecting the asymptotics of linear recurrences. *J. Math. Anal. Appl.*

[56] D. Zeilberger. A fast algorithm for proving terminating hypergeometric identities. *Discrete Mathematics*, 80(2):207 – 211, 1990.

[57] D. Zeilberger. A holonomic systems approach to special functions identities. *Journal of Computational and Applied Mathematics*, 32(3):321 – 368, 1990.

[58] D. Zeilberger. The method of creative telescoping. *Journal of Symbolic Computation*, 11(3):195 – 204, 1991.

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, 12. November 2013 Maximilian Jaroschek

Curriculum Vitae

Maximilian Jaroschek
Research Institute for Symbolic Computation
Johannes Kepler University
Altenberger Straße 69
4040 Linz, Austria

mjarosch@risc.jku.at
www.risc.jku.at/mjarosch

Education

PhD in Technical Sciences (2010 – present)
Research Institute for Symbolic Computation
Johannes Kepler University Linz
Adviser: PD Dr. Manuel Kauers

Diploma in Computer Science (2004 – 2009)
Department of Informatics
University of Passau
Adviser: Prof. Dr. Thomas Müller-Gronbach
Diploma-Thesis: Multi-Level Monte Carlo Verfahren zur Bewertung von Optionen

Scientific Work

Refereed Publications

M. Jaroschek. Improved Polynomial Remainder Sequences for Ore Polynomials, Journal of Symbolic Computation, 58:64 – 76, 2013.

S. Chen, M. Jaroschek, M. Kauers, and M. Singer. Desingularization explains order-degree curves for Ore operators. In *Proceedings of ISSAC 2013*: 157 – 164, 2013.

M. Kauers, M. Jaroschek, and F. Johansson. Ore polynomials in

Sage
Technical report, ArXiv 1306.4263, to appear, June 2013.

Software

M. Kauers, M. Jaroschek, and F. Johansson. Ore algebra package for Sage, 2013. https://www.risc.jku.at.

Talks

Desingularization Explains Order-Degree Curves for Ore Operators (August 2013)
SIAM Conference on Applied Algebraic Geometry 2013, Fort Collins, CO, USA.

Desingularization Explains Order-Degree Curves for Ore Operators (June 2013)
38th International Symposium on Symbolic and Algebraic Computation, Boston, MA, US.

Improved Polynomial Remainder Sequences for Ore Polynomials (October 2012)
Tenth Asian Symposium on Computer Mathematics, Beijing, China.

Posters

Improved Polynomial Remainder Sequences for Ore Polynomials (July 2012)
37th International Symposium on Symbolic and Algebraic Computation, Grenoble, France.

Teaching

Lecture: Number Sequences (August 2012)
Nesin Mathematics Village, Şirince, Turkey.

Lecture: Fast Algorithms for Polynomial Arithmetic (August 2011)
Nesin Mathematics Village, Şirince, Turkey.

Exercise lecture: Analysis (WS 2011/2012)
Johannes Kepler University, Linz, Austria.

Exercise lecture: Analysis (WS 2010/2011)
Johannes Kepler University, Linz, Austria.

Other

Organizer: Gröbner Bases, Resultants and Linear Algebra Workshop (September 2013)
RISC, Johannes Kepler University, Linz, Austria.

Talk: Na Servus – Auch in Bayern Sind sie ein Wenig Deutsch (May 2013)
Muğla Sıtkı Koçman Üniversitesi, Muğla, Turkey.