

Desingularization Explains Order-Degree Curves for Ore Operators

Shaoshi Chen^{*}
Dept. of Mathematics / NCSU
Raleigh, NC 27695, USA

Maximilian Jaroschek[†]
RISC / Joh. Kepler University
4040 Linz, Austria

Manuel Kauers[†]
RISC / Joh. Kepler University
4040 Linz, Austria

Michael F. Singer^{*}
Dept. of Mathematics / NCSU
Raleigh, NC 27695, USA

ABSTRACT

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. An order-degree curve for a given Ore operator 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 give a new proof of a desingularization result by Abramov and van Hoeij for the shift case, and show how desingularization implies order-degree curves which are extremely accurate in examples.

Categories and Subject Descriptors

I.1.2 [Computing Methodologies]: Symbolic and Algebraic Manipulation—*Algorithms*

General Terms

Algorithms

Keywords

Ore Operators, Singular Points

1. INTRODUCTION

We consider linear operators of the form

$$L = \ell_0 + \ell_1 \partial + \dots + \ell_r \partial^r,$$

where ℓ_0, \dots, ℓ_r are polynomials or rational functions in x , and ∂ denotes, for instance, the derivation $\frac{d}{dx}$ or the shift

^{*}Supported by the National Science Foundation (NSF) grant CCF-1017217.

[†]Supported by the Austrian Science Fund (FWF) grant Y464-N18.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

Copyright 20XX ACM X-XXXXX-XX-X/XX/XX ...\$10.00.

operator $x \mapsto x + 1$. (Formal definitions are given later.) Operators act in a natural way on functions. They are used in computer algebra to represent the functions f which they annihilate, i.e., $L \cdot f = 0$.

Multiplication of operators is defined in such a way that the product of two operators acts on a function like the two operators one after the other: $(PL) \cdot f = P \cdot (L \cdot f)$. Therefore, if L is an annihilating operator for some function f , and if P is any other operator, then PL is also an annihilating operator for f .

We are interested in turning a given operator L into a “nicer” one by multiplying it from the left by a suitable P , for two different flavors of “nice”. First, we consider the problem of removing factors from the leading coefficient ℓ_r of L . This is known as desingularization and it is needed for computing the values of f at the roots of ℓ_r (provided it is defined there). Desingularization of differential operators is classical [9], and for difference operators, Abramov and van Hoeij [2, 1] give an algorithm for doing it. We give below a new proof of (a slightly generalized version of) their results.

Secondly, we consider the problem of producing left multiples with polynomial coefficients of low degree. Unlike the situation for commutative polynomials, a left multiple PL of L may have polynomial coefficients even if P has rational function coefficients with nontrivial denominators and the polynomial coefficients of L have no common factors. In such situations, it may happen that the degrees of the polynomial coefficients in PL are strictly less than those in L . This phenomenon can be exploited in the design of fast algorithms because a small increase of the order can allow for a large decrease in degree and therefore yield a smaller total size of the operator (“trading order for degree”). Degree estimates supporting this technique have been recently given for a number of different computational problems [4, 7, 6, 3]. Although limited to special situations, these estimates can overshoot by quite a lot. Below we derive a general estimate for the relation between orders and degrees of left multiples of a given operator L from the results about desingularization. This estimate is independent of the context from which the operator L arose, and it is fairly accurate in examples.

2. OVERVIEW

Before discussing the general case, let us illustrate the concepts of desingularization and trading order for degree

on a concrete example. Consider the differential operator

$$\begin{aligned} L &= -(45 + 25x - 35x^2 - x^3 + 2x^4) \\ &\quad + 2(33 - 9x - 3x^2 - x^3)\partial \\ &\quad (1+x)(23 - 20x - x^2 + 2x^3)\partial^2 \in \mathbb{Q}[x][\partial], \end{aligned}$$

where $\partial = \frac{d}{dx}$. That L is desingularizable at (a root of) $p := 23 - 20x - x^2 + 2x^3$ means that there is some other operator $P \in \mathbb{Q}(x)[\partial]$ such that PL has coefficients in $\mathbb{Q}[x]$ and its leading coefficient no longer contains p as factor. Such a P is called a desingularizing operator for L at p and PL the corresponding desingularized operator. In our example,

$$P = \frac{299}{p}\partial + \frac{1035 - 104x - 136x^2}{p} \in \mathbb{Q}(x)[\partial]$$

is a desingularizing operator for L at p , the desingularized operator is

$$\begin{aligned} PL &= (-2350 - 2055x + 104x^2 + 136x^3) \\ &\quad + (2151 + 281x + 136x^2)\partial \\ &\quad + (1932 + 931x - 240x^2 - 136x^3)\partial^2 + 299(1+x)\partial^3. \end{aligned}$$

A desingularizing operator need not exist. For example, it is impossible to remove the factor $x + 1$ from the leading coefficient of L by means of desingularization. In Section 3 we explain how to check for a given operator L and a factor p of its leading coefficient whether a desingularizing operator exists, and if so, how to compute it.

Desingularization causes a degree drop in the leading coefficient but may affect the other coefficients of the operator in an arbitrary fashion. However, a desingularizing operator can be turned into an operator which lowers the degrees of all the coefficients. To this end, multiply P from the left by some polynomial $q \in \mathbb{Q}[x]$ for which the coefficients of qP have low degree modulo p , i.e., for which $qP = \frac{1}{p}P_1 + P_2$ where $P_1, P_2 \in \mathbb{Q}[x][\partial]$ and P_1 has low degree coefficients. In our example, a good choice is $q = (-43 + 34x)/299$, i.e.

$$P_1 = (-22x + 29) + (-43 + 34x)\partial, \quad P_2 = -\frac{2312}{299}.$$

Since PL has polynomial coefficients, so does

$$\begin{aligned} \frac{1}{p}P_1L &= qPL - P_2L \\ &= (-10 - 165x + 22x^2) + (201 + 65x - 34x^2)\partial \\ &\quad + (-100 + 109x - 22x^2)\partial^2 - (1+x)(43 - 34x)\partial^3. \end{aligned}$$

This operator has degree $\deg_x(L) + \deg_x(P_1) - \deg_x(p) = 2$, compared to $\deg_x(L) + \deg_x(P) = 3$ achieved with the original desingularizing operator. There is no left multiple of L of order 3 and degree less than 2. There is also none of order 4, but there does exist a left multiple of degree 1 and order 5. It can be obtained from P by multiplying from the left by an operator $q_0 + q_1\partial + q_2\partial^2 \in \mathbb{Q}[x][\partial]$ of order 2 for which the coefficients of $p^3(q_0 + q_1\partial + q_2\partial^2)P$ have low degrees modulo p^3 : Taking

$$q_0 = \frac{633+64x-88x^2}{89401}, \quad q_1 = \frac{8(17x^2+13x-92)}{89401}, \quad q_2 = \frac{1}{299}$$

we have $(q_0 + q_1\partial + q_2\partial^2)P = \frac{1}{p^3}Q_1 + Q_2$, where

$$\begin{aligned} Q_1 &= (841 + 580x - 436x^2 - 148x^3 + 59x^4 + 12x^5 - 4x^6) \\ &\quad + (1697 - 528x - 752x^2 + 120x^3 + 127x^4 - 12x^5 \\ &\quad - 4x^6)\partial + (x-7)(-9+x+2x^2)p\partial^2 + p^2\partial^3, \\ Q_2 &= \frac{16(779+374x)}{89401} - \frac{272(69+34x)}{89401}\partial. \end{aligned}$$

Set $Q := \frac{1}{p^3}Q_1$. Then, since PL has polynomial coefficients, so does

$$\begin{aligned} QL &= (q_0 + q_1\partial + q_2\partial^2)PL - Q_2L \\ &= (2+x) + (-3+x)\partial - (8+2x)\partial^2 \\ &\quad + (2-2x)\partial^3 + (6+x)\partial^4 + (1+x)\partial^5. \end{aligned}$$

Its degree is $\deg_x(L) + \deg_x(Q_1) - 3\deg_x(p) = 1$.

As the factor $x + 1$ cannot be removed from L , we cannot hope to reduce the degree even further. We have thus found that the region of all points $(r, d) \in \mathbb{N}^2$ such that there is a left $\mathbb{Q}(x)[\partial]$ -multiple of L of order r and with polynomial coefficients of degree at most d is given by $((2, 4) + \mathbb{N}^2) \cup ((3, 2) + \mathbb{N}^2) \cup ((5, 1) + \mathbb{N}^2)$.

In Section 4 we explain the construction of the operators Q that turn a desingularizing operator into one that lowers all the degrees as far as possible, and we give a formula that describes the points (r, d) for which such a Q exists.

3. PARTIAL DESINGULARIZATION

In this section we discuss under which circumstances an operator L admits a left multiple PL in which a factor of the leading coefficient of L is removed. This is of interest in its own right, and will also serve as the starting point for the construction described in the following section. In view of this latter application, we cover here a slightly generalized variant of desingularization, which not only applies to the case where a factor can be completely removed, but also cases where only the multiplicity of the factor can be lowered.

Example 1. In the shift case (i.e., $\partial x = (x+1)\partial$), consider the operator

$$\begin{aligned} L &= (3+x)(9+7x+x^2) - (33+70x+47x^2+12x^3+x^4)\partial \\ &\quad + (2+x)^2(3+5x+x^2)\partial^2. \end{aligned}$$

The factor $(x+2)^2$ in the leading coefficient cannot be removed completely. Yet we can find a multiple in which $x+2$ appears in the leading coefficient (in shifted form) with multiplicity one only. One such left multiple of L is

$$\begin{aligned} &(402 + 208x + 25x^2) - (514 + 743x + 258x^2 + 25x^3)\partial \\ &\quad + (233 + 378x + 183x^2 + 25x^3)\partial^2 - 9(3+x)\partial^3. \end{aligned}$$

We speak in this case of a partial desingularization. The general definition is as follows. We formulate it for operators in an arbitrary Ore algebra $\mathbb{O} := A[\partial] := A[\partial; \sigma, \delta]$ where A is a \mathbb{K} -algebra (in our case typically $A = \mathbb{K}[x]$ or $A = \mathbb{K}(x)$), \mathbb{K} is a field, $\sigma: A \rightarrow A$ is an automorphism and $\delta: A \rightarrow A$ a σ -derivation, i.e., a \mathbb{K} -linear map satisfying the skew Leibniz rule $\delta(pq) = \delta(p)q + \sigma(p)\delta(q)$ for $p, q \in A$. For any $f \in A$, the multiplication rule in $A[\partial; \sigma, \delta]$ is $\partial f = \sigma(f)\partial + \delta(f)$. We write $\deg_{\partial}(L)$ for the order of $L \in A[\partial]$, and if $A = \mathbb{K}[x]$, we write $\deg_x(L)$ for the maximum degree among the

polynomial coefficients of L . For general information about Ore algebras, see [5].

Definition 2. Let $L \in \mathbb{K}[x][\partial; \sigma, \delta]$ and let $p \in \mathbb{K}[x]$ be such that $p \mid \text{lc}_\partial(L) \in \mathbb{K}[x]$. We say that p is removable from L at order n if there exists some $P \in \mathbb{K}(x)[\partial]$ with $\deg_\partial(P) = n$ and some $w, v \in \mathbb{K}[x]$ with $\gcd(p, w) = 1$ such that $PL \in \mathbb{K}[x][\partial]$ and $\sigma^{-n}(\text{lc}_\partial(PL)) = \frac{w}{vp} \text{lc}_\partial(L)$. 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 $\gcd(p, \text{lc}_\partial(L)/p) = 1$, we say desingulariz[able]ing[ed] instead of remov[able]ing[ed], respectively.

The backwards shift σ^{-n} in the definition above is introduced in order to compensate the effect of the term ∂^n in P on the leading coefficient on L (i.e., $\text{lc}_\partial(\partial^n L) = \sigma^n(\text{lc}_\partial(L))$.) Moreover, observe that in this definition, removing a polynomial p does not necessarily mean that the p -removed operator has no roots of (some shift of) p in its leading coefficient. If L contains some factors of higher multiplicity, as in the example above, then removal of a polynomial is defined so as to respect multiplicities. Also observe that in the definition we allow that some new factors w are introduced when p is removed. This is only a matter of convenience. We will see below that we may always assume $v = w = 1$, i.e., if something can be removed at the cost of introducing new factors into the leading coefficient, then it can also be removed without introducing new factors. The justification rests on the following lemma.

Lemma 3. Let $L \in \mathbb{K}[x][\partial; \sigma, \delta]$, let $p \in \mathbb{K}[x]$ with $p \mid \text{lc}_\partial(L)$ be removable from L , and let $P \in \mathbb{K}(x)[\partial; \sigma, \delta]$ be a p -removing operator for L with $\deg_\partial(P) = n$.

1. If $U \in \mathbb{K}[x][\partial]$ with $\gcd(\text{lc}_\partial(U), \sigma^{n+\deg_\partial(U)}(p)) = 1$, then UP is also a p -removing operator for L .
2. If $P = P_1 + P_2$ for some $P_1 \in \mathbb{K}(x)[\partial]$ with $\deg_\partial(P_1) = n$ and $P_2 \in \mathbb{K}[x][\partial]$, then P_1 is also a p -removing operator for L .
3. There exists a p -removing operator P' with $\deg_\partial(P') = n$ and with $p\sigma^{-n}(\text{lc}_\partial(P'L)) = \text{lc}_\partial(L)$.

Proof. Let $v, w \in \mathbb{K}[x]$ be as in Definition 2, i.e., $\gcd(p, w) = 1$ and $vp\sigma^{-n}(\text{lc}_\partial(PL)) = w \text{lc}_\partial(L)$.

1. Since PL is an operator with polynomial coefficients, so is UPL . Furthermore, with $u = \text{lc}_\partial(U)$ and $m = \deg_\partial(U)$ we have

$$vp\sigma^{-n-m}(\text{lc}_\partial(UPL)) = \sigma^{-n-m}(u)w \text{lc}_\partial(L).$$

Since $\gcd(u, \sigma^{n+m}(p)) = 1$, we have $\gcd(\sigma^{-n-m}(u)w, p) = 1$, as required.

2. Clearly, $P_2 \in \mathbb{K}[x][\partial]$ implies $P_2L \in \mathbb{K}[x][\partial]$. Since also $PL \in \mathbb{K}[x][\partial]$, it follows that

$$P_1L = (P - P_2)L = PL - P_2L \in \mathbb{K}[x][\partial].$$

If $\deg_\partial(P_2) < n$, then we have $\text{lc}_\partial(PL) = \text{lc}_\partial(P_1L)$, so there is nothing else to show. If $\deg_\partial(P_2) = n$, then $\text{lc}_\partial(P_1L) = \text{lc}_\partial(PL) - \text{lc}_\partial(P_2L)$ and therefore

$$\begin{aligned} vp\sigma^{-n}(\text{lc}_\partial(P_1L)) &= vp\sigma^{-n}(\text{lc}_\partial(PL) - \text{lc}_\partial(P_2L)) \\ &= (w - vp\sigma^{-n}(\text{lc}_\partial(P_2))) \text{lc}_\partial(L). \end{aligned}$$

Since $\gcd(p, w - vp\sigma^{-n}(\text{lc}_\partial(P_2))) = \gcd(p, w) = 1$, the claim follows.

3. By the extended Euclidean algorithm we can find $s, t \in \mathbb{K}[x]$ with $1 = sw + tpv$. Then $\sigma^n(s)P$ is p -removing of order n by part 1 ($\sigma^n(s)$ is obviously coprime to $\sigma^n(p)$), and its leading coefficient is

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

By part 2 we may discard the polynomial part $\sigma^n(t)$, obtaining a p -removing operator P' with the desired property. ■

The lemma implies that if there is a p -removing operator at all, then there is also one in which all the denominators are powers of $\sigma^n(p)$ (because any factors coprime with p can be cleared according to part 1), and where all numerators have smaller degree than the corresponding denominators (because polynomial parts can be removed according to part 2).

Similarly as in the proof of part 3, we can also reduce the problem of removing a composite polynomial to the problem of removing powers of irreducible polynomials. For example, if $p = p_1p_2$ is removable from L , where $p_1, p_2 \in \mathbb{K}[x]$ are coprime, then obviously both p_1 and p_2 are removable. Conversely, if p_1 and p_2 are removable, and if P_1, P_2 are removing operators of orders n_1, n_2 with $\text{lc}_\partial(P_1) = 1/\sigma^{n_1}(p_1)$ and $\text{lc}_\partial(P_2) = 1/\sigma^{n_2}(p_2)$, then for $n = \max\{n_1, n_2\}$ and $u_1, u_2 \in \mathbb{K}[x]$ with

$$u_1\sigma^n(p_2) + u_2\sigma^n(p_1) = \gcd(\sigma^n(p_1), \sigma^n(p_2)) = 1$$

the operator $P := u_1\partial^{n-n_1}P_1 + u_2\partial^{n-n_2}P_2 \in \mathbb{K}(x)[\partial]$ is such that $PL \in \mathbb{K}[x][\partial]$ and $\text{lc}_\partial(PL) = \text{lc}_\partial(L)/\sigma^n(p)$.

In summary, in order to determine whether a polynomial $p = p_1^{k_1}p_2^{k_2}\dots p_m^{k_m}$ is removable from an operator L , it suffices to be able to check for an irreducible polynomial p_i and a given $k_i \geq 1$ whether $p_i^{k_i}$ is removable. Let now p be an irreducible polynomial and $k \geq 1$. If there exists a p^k -removing operator, then it can be assumed to be of the form

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

for some $e_0, \dots, e_{n-1} \in \mathbb{N}$, and $p_0, \dots, p_{n-1} \in \mathbb{K}[x]$ with $\deg_x(p_i) < e_i \deg_x(p)$. In order to decide whether such an operator exists, it is now enough to know a bound on n as well as a bound e on the exponents e_i , for if n and e are known, we can make an ansatz $p_i = \sum_{j=0}^{e_i-1} p_{i,j}x^j$ with undetermined coefficients $p_{i,j}$, then calculate PL and rewrite all its coefficients in the form $a/\sigma^n(p)^e + b$ for some polynomials a, b depending linearly on the undetermined $p_{i,j}$, then compare the coefficients of the various a 's with respect to x to zero and solve the resulting linearly system for the $p_{i,j}$.

How the bounds on n and e are derived depends on the particular Ore algebra at hand. In this paper, we give a complete treatment of the shift case ($(\sigma p)(x) = p(x+1)$, $\delta = 0$) and make some remarks about the differential case ($\sigma = \text{id}$, $\delta = \frac{d}{dx}$). For other cases, see the preprint [8].

3.1 Shift Case

In this section, let $\mathbb{K}[x][\partial]$ denote the Ore algebra of recurrence operators, i.e., σ is the automorphism mapping x to $x+1$ and δ is the zero map. This case was studied by

Abramov and van Hoeij [2, 1]. We give below a new proof of their result, and extend it to the case of partial desingularization. For consistency with the differential case, we formulate the result for the leading coefficients, while Abramov and van Hoeij consider the analogous for the trailing coefficients. Of course, this difference is immaterial.

We proceed in two steps. First we give a bound on the order of a removing operator (Lemma 4), and then, in a second step, we provide a bound on the exponents in the denominators (Theorem 5). As explained above, it is sufficient to consider the case of removing powers of irreducible polynomials, and we restrict to this case.

Lemma 4. *Let $L = \ell_0 + \ell_1\partial + \dots + \ell_r\partial^r \in \mathbb{K}[x][\partial]$ with $\ell_0, \ell_r \neq 0$, and let p be an irreducible factor of $\text{lc}_\partial(L)$ such that p^k is removable from L for some $k \geq 1$. Let $n \in \mathbb{N}$ be s.t. $\gcd(\sigma^n(p), \ell_0) \neq 1$ and $\gcd(\sigma^m(p), \ell_0) = 1$ 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 the observations following Lemma 3 we may assume that

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

for $e_i \in \mathbb{N}$ and $p_i \in \mathbb{K}[x]$ with $\deg_x(p_i) < e_i \deg_x(p)$ ($i = 0, \dots, m$). We may further assume $\gcd(\sigma^m(p), p_i) = 1$ for $i = 0, \dots, m$ (viz. that the e_i are chosen minimally).

Suppose that $m > n$. We show by induction that then $e_0 = e_1 = \dots = e_{m-n-1} = 0$, so that $p_i = 0$ for $i = 0, \dots, m-n-1$, i.e., the operator P has in fact the form

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

Thus $\partial^{n-m}P \in \mathbb{K}(x)[\partial]$ is a p^k -removing operator of order n .

Consider the operator $T := \sum_{i=0}^{r+m} t_i \partial^i := PL \in \mathbb{K}[x][\partial]$. From $\frac{p_0}{\sigma^m(p)^{e_0}}\ell_0 = t_0 \in \mathbb{K}[x]$ it follows that $e_0 = 0$, because

$$\gcd(\sigma^m(p), p_0) = \gcd(\sigma^m(p), \ell_0) = 1$$

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 $e_0 = e_1 = \dots = e_{i-1} = 0$ for some $i < m-n$. Then from

$$\begin{aligned} t_i &= \frac{p_i}{\sigma^m(p)^{e_i}}\sigma^i(\ell_0) + \frac{p_{i-1}}{\sigma^m(p)^{e_{i-1}}}\sigma^{i-1}(\ell_1) + \dots + \frac{p_0}{\sigma^m(p)^{e_0}}\ell_i \\ &= \frac{p_i}{\sigma^m(p)^{e_i}}\sigma^i(\ell_0) \end{aligned}$$

it follows that $\sigma^m(p)^{e_i} \mid p_i \sigma^i(\ell_0)$. By the choice of p_i we have $\gcd(\sigma^m(p), p_i) = 1$ and by the assumption in the lemma we have $\gcd(\sigma^{m-i}(p), \ell_0) = 1$ (because $m-i > n$), so it follows that $e_i = 0$. Inductively, we obtain $e_0 = e_1 = \dots = e_{m-n-1} = 0$, which completes the proof. ■

It can be shown that p cannot be removed from L if $\sigma^n(p)$ is coprime with the trailing coefficient of L for all $n \in \mathbb{N}$ by a variant of [2, Lemma 3.], so the above lemma covers all situations where removing of a factor is possible.

In order to formulate the result about the possible exponents in the denominator, it is convenient to first introduce some notation. Let us call two irreducible polynomials $p, q \in \mathbb{K}[x] \setminus \{0\}$ *equivalent* if there exists $n \in \mathbb{Z}$ such that $\sigma^n(p)/q \in \mathbb{K}$. We write $[q]$ for the equivalence class

of $q \in \mathbb{K}[x] \setminus \{0\}$. If p, q are equivalent in this sense, we write $p \leq q$ if $\sigma^n(p)/q \in \mathbb{K}$ for some $n \geq 0$, and $p > q$ otherwise.

The irreducible factors of a polynomial $u \in \mathbb{K}[x]$ can be grouped into equivalence classes, for example

$$\begin{aligned} u &= \underbrace{(x-4)(x-1)^3 x(x+1)^2 (2x-5)(2x+3)^2 (2x+9)} \\ &\quad \times \underbrace{(x^2+5x+1)(x^2+11x+25)^3}. \end{aligned}$$

For any monic irreducible factor p of $u \in \mathbb{K}[x]$, let $v_p(u)$ denote the multiplicity of p in u , and define

$$v_{<p}(u) := \max\{v_q(u) \mid q \in [p] : p > q\}.$$

For example, for the particular u above we have $v_{x-4}(u) = 1$, $v_{<x-4}(u) = 0$, $v_{<x+1}(u) = 3$, and so on.

Besides being applicable not only to desingularization but also removal of any factors, the following theorem also refines the corresponding result of Abramov and van Hoeij in so far as their version only covers the case of desingularizing L at some p with $v_{>p}(\text{lc}_\partial(L)) = 0$ whereas we do not need this assumption.

Theorem 5. *Let $L = \ell_0 + \ell_1\partial + \dots + \ell_r\partial^r \in \mathbb{K}[x][\partial]$ with $\ell_0, \ell_r \neq 0$, and let p be an irreducible factor of ℓ_r such that p^k is removable from L for some $k \geq 1$. Let $n \in \mathbb{N}$ be such that $\gcd(\sigma^n(p), \ell_0) \neq 1$ and $\gcd(\sigma^m(p), \ell_0) = 1$ for all $m > n$. Then there exists a p^k -removing operator P for L and p of the form*

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

for some $e_i \in \mathbb{N}$ and $p_i \in \mathbb{K}[x]$ with

1. $\deg_x(p_i) < e_i \deg_x(p)$ and $\gcd(\sigma^n(p), p_i) = 1$, and
2. $e_i \leq k + n v_{<p}(\text{lc}_\partial(L))$

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

Proof. Lemmas 3 and 4 imply the existence of an operator P with all the required properties except possibly the exponent estimate in item 2. Let P be such an operator, and consider the operator $T := \sum_{i=0}^{r+n} t_i \partial^i := PL \in \mathbb{K}[x][\partial]$.

Let $e = \max\{e_1, \dots, e_n\}$ and $\bar{P} := \sum_{i=0}^n \bar{p}_i \partial^i := \sigma^n(p)^e P$. Then $\bar{p}_i = \sigma^n(p)^{e-e_i} p_i$ ($i = 0, \dots, n$) and $\sigma^n(p)^e T = \bar{P}L$ and $\gcd(\bar{p}_0, \dots, \bar{p}_n, \sigma^n(p)) = 1$.

Abbreviating $v := v_{<p}(\text{lc}_\partial(L))$, 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 $i = n, n-1, \dots, 0$, which is inconsistent with $\gcd(\bar{p}_0, \dots, \bar{p}_n, \sigma^n(p)) = 1$.

First it is clear that $\bar{p}_n = \sigma^n(p)^e p_n \sigma^n(\ell_r)$ contains $\sigma^n(p)$ with multiplicity $\geq e - k > n v$, 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 $j = n, n-1, \dots, i+1$. Consider the equality

$$\sigma^n(p)^e t_{i+r} = \bar{p}_i \sigma^i(\ell_r) + \bar{p}_{i+1} \sigma^{i+1}(\ell_{r-1}) + \dots + \bar{p}_n \ell_{r-n},$$

where we use the convention $\ell_j := 0$ for $j < 0$. The induction hypothesis implies that $\sigma^n(p)^{(i+1)v+1} \mid \bar{p}_j$ for $j = n, n-1, \dots, i+1$. Furthermore, since $(i+1)v \leq n v < e$, we have $\sigma^n(p)^{(i+1)v+1} \mid \sigma^n(p)^e t_{i+r}$. Both facts together imply $\sigma^n(p)^{(i+1)v+1} \mid \bar{p}_i \sigma^i(\ell_r)$. The definition of v ensures that $\sigma^n(p)$ is contained in $\sigma^i(\ell_r)$ 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. ■

“ \Rightarrow ”: Start from a p -removing operator of the form

$$P_0 = \sum_{i=0}^{n-1} \frac{p_i}{\sigma^n(p)^{e_i}} \partial^i + \frac{1}{\sigma^n(p)} \partial^n,$$

and set $P = \sigma^n(p)^e P_0$ where $e = \max\{e_0, \dots, e_{n-1}, 1\} \geq 1$. Because of $P_0 L \in \mathbb{K}[x][\partial]$ it follows that

$$PL \in \sigma^n(p)^e \mathbb{K}[x][\partial] = \sigma^n(p) \text{lc}_\partial(P) \mathbb{K}[x][\partial]. \quad \blacksquare$$

The next lemma is a generalization of Bezout’s relation to more than two coprime polynomials, which we will also need in the proof.

Lemma 8. *Let $u_1, \dots, u_m \in \mathbb{K}[x]$ be pairwise coprime and $u = u_1 u_2 \cdots u_m$, and let $v_1, \dots, v_m \in \mathbb{K}[x]$ be such that $\deg_x(v_i) < \deg_x(u_i)$ ($i = 1, \dots, m$). 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 $\deg_x(v_i) < \deg_x(u_i)$, the claim follows. \blacksquare

Theorem 9. *Let $L \in \mathbb{K}[x][\partial]$, and let $p_1, \dots, p_m \in \mathbb{K}[x]$ be factors of $\text{lc}_\partial(L)$ which are removable at orders n_1, \dots, n_m , respectively, so that the $\sigma^{n_i}(p_i)$ are pairwise coprime. Let $r \geq \deg_\partial(L)$ and*

$$d \geq \deg_x(L) - \left[\sum_{i=1}^m \left(1 - \frac{n_i}{r - \deg_\partial(L) + 1} \right)^+ \deg_x(p_i) \right],$$

where we use the notation $(x)^+ := \max\{x, 0\}$. Then there exists an operator $Q \in \mathbb{K}(x)[\partial] \setminus \{0\}$ such that $QL \in \mathbb{K}[x][\partial]$ and $\deg_\partial(QL) = r$ and $\deg_x(QL) = d$.

Proof. Let $r \geq \deg_\partial(L)$, and set $s := r - \deg_\partial(L)$ so that $s = \deg_\partial(Q)$. We may assume without loss of generality that s is such that $1 - \frac{n_i}{r - \deg_\partial(L) + 1} = 1 - \frac{n_i}{s+1} > 0$ 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 7 yields operators $P_i \in \mathbb{K}[x][\partial]$ of order n_i with $P_i L \in \sigma^{n_i}(p_i) \text{lc}_\partial(P_i) \mathbb{K}[x][\partial]$. Set

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

where $l_i = \text{lc}_\partial(P_i)$. Consider the ansatz

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

for undetermined polynomial coefficients $q_{i,j}$ ($i = 1, \dots, m$; $j = 0, \dots, n_i$) of degree less than $\deg_x(p_i)$. Regardless of the choice of these coefficients, we will always have $Q_1 \in \mathbb{K}[x][\partial]$ and $Q_1 L \in q \mathbb{K}[x][\partial]$. Also, for arbitrary $R \in \mathbb{K}[x][\partial]$ and $Q_2 = Q_1 - qR$ we have $Q_2 \in \mathbb{K}[x][\partial]$ and $Q_2 L \in q \mathbb{K}[x][\partial]$. 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

$$\text{lc}_\partial(Q_1) = \sum_{i=1}^m q_{i,k} \frac{q}{\sigma^{k+n_i}(p_i) \sigma^k(l_i)} \sigma^k(l_i) = \sum_{i=1}^m q_{i,k} \frac{q}{\sigma^{k+n_i}(p_i)}$$

is nonzero by Lemma 8. Furthermore, $\text{lc}_\partial(Q_1) \not\equiv 0 \pmod{q}$ because $\deg_x(q_{i,k}) < \deg_x(p_i)$ implies $\deg_x(\text{lc}_\partial(Q_1)) < \deg_x(q)$.

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

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

to zero. This gives altogether

$$\begin{aligned} & (s + 1) \left(\sum_{i=1}^m ((s - n_i + 1)(\deg_x(p_i) + \deg_x(l_i)) - 1 - \deg_x(l_i)) \right. \\ & \left. - \sum_{i=1}^m (s - n_i)(\deg_x(p_i) + \deg_x(l_i)) - \left\lfloor \frac{\sum_{i=1}^m n_i \deg_x(p_i)}{s + 1} \right\rfloor \right) \\ & = (s + 1) \left(\sum_{i=1}^m \deg_x(p_i) - 1 - \left\lfloor \frac{\sum_{i=1}^m n_i \deg_x(p_i)}{s + 1} \right\rfloor \right) \end{aligned}$$

equations. The resulting linear system has a nontrivial solution because

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

By construction, the solution gives rise to an operator $Q_2 \in \mathbb{K}[x][\partial]$ of order at most n with polynomial coefficients of degree at most

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

for which $Q_2 L \in q \mathbb{K}[x][\partial]$. Thus if we set $Q = \frac{1}{q} Q_2 \in \mathbb{K}(x)[\partial]$, we have $\deg_\partial(QL) = \deg_\partial(L) + s = r$ and $\deg_x(QL)$

is at most

$$\begin{aligned}
& \deg_x(L) + \deg_x(Q_2) - \deg_x(q) \\
& \leq \deg_x(L) + \sum_{i=1}^m (s - n_i)(\deg_x(p_i) + \deg_x(l_i)) \\
& \quad + \left\lfloor \frac{\sum_{i=1}^m n_i \deg_x(p_i)}{s+1} \right\rfloor \\
& \quad - \sum_{i=1}^m (s - n_i + 1)(\deg_x(p_i) + \deg_x(l_i)) \\
& \leq \deg_x(L) - \sum_{i=1}^m \deg_x(p_i) + \left\lfloor \frac{\sum_{i=1}^m n_i \deg_x(p_i)}{s+1} \right\rfloor \\
& = \deg_x(L) - \left\lfloor \sum_{i=1}^m \left(1 - \frac{n_i}{s+1}\right) \deg_x(p_i) \right\rfloor,
\end{aligned}$$

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 $n \in \mathbb{Z}$.) ■

Example 10. 1. Consider again the example from Section 2. There we started from an operator $L \in \mathbb{K}[x][\partial]$ of order 2 and degree 4 for which there exists a desingularizing operator P of order 1 which removes a polynomial p of degree 3. According to the theorem, for every $r \geq 2$ exists an operator $Q \in \mathbb{K}[x][\partial]$ with $QL \in \mathbb{K}[x][\partial]$, $\deg_\partial(QL) \leq r$ and

$$d := \deg_x(QL) \leq 4 - \left(1 - \frac{1}{r-2+1}\right)^+ 3 = \frac{r+2}{r-1}.$$

This hyperbola precisely predicts the order-degree pairs we found in Section 2:

r	2	3	4	5	6	7	8	9
d	4	2	2	1	1	1	1	1

2. Consider the sequence $(a_n)_{n=0}^\infty$ defined by

$$a_n = \sum_k \frac{\Gamma(2n+k)\Gamma(n-k+2)}{\Gamma(2n-k)\Gamma(n+2k)} \quad (n \in \mathbb{N}).$$

Zeilberger's algorithm finds an annihilating operator L of the form

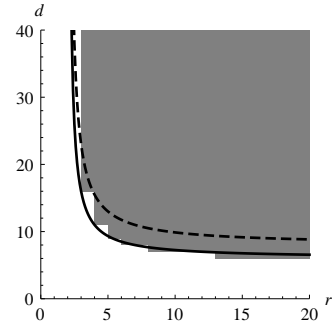
$$\begin{aligned}
& 9(1+n)(1+3n)(2+3n)^2(3n+4)p(n+1) \\
& + (\dots \text{degree } 16 \dots) \partial + (\dots \text{degree } 15 \dots) \partial^2 \\
& - 10n(8+5n)(9+5n)(11+5n)(12+5n)p(n) \partial^3,
\end{aligned}$$

where ∂ represents the shift operator and p is a certain irreducible polynomial of degree 10. This polynomial is removable of order 1. Therefore, by the theorem, we expect left multiples of L of order r and degree bounded by

$$16 - \left(1 - \frac{1}{r-3+1}\right)^+ 10 = \frac{6r-2}{r-2}.$$

In the figure below, the curve $d = \frac{6r-2}{r-2}$ (solid) is contrasted with the estimate $d = \frac{8r-1}{r-2}$ (dashed) derived last year for this example [6] as well as the region of all points (r, d) for which a left multiple of L of order r and degree d exists (gray). The new curve matches precisely the boundary of the gray region, even including the very last degree drop (which is not clearly visible

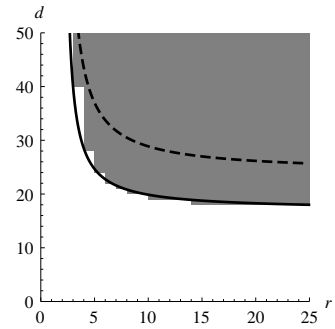
on the figure): for $r = 12$ we have $\frac{6r-2}{r-2} = 7$ and for $r = 13$ we have $\frac{6r-2}{r-2} \approx 6.9 < 7$.



3. Consider the minimal order telescoper L for the hyper-exponential term in Example 15.2 in [7]. It 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 9 therefore predicts left multiples of L of degree r and degree

$$40 - \left(1 - \frac{1}{r-3+1}\right)^+ 23 = \frac{17r-11}{r-2}$$

for all $r \in \mathbb{N}$. Again, this estimate is accurate, while the estimate $\frac{24r-9}{r-2}$ derived in [7] overshoots.



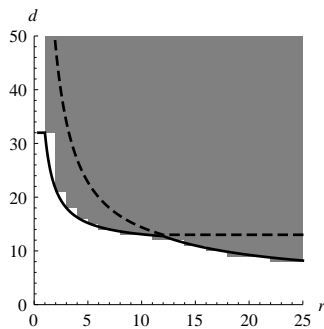
4. Operators coming from applications tend to have leading coefficients that contain a single irreducible polynomial of large degree which can be removed at order 1, besides factors that are not removable. But Theorem 9 also covers the more general situation of factors that are only removable of higher order, and even the case of several polynomials that are removable at several orders. As an example for this general situation, consider the operator

$$\begin{aligned}
L &= 8(1+x)(1+2x)^3(37+3z)^7(14+32x+26x^2+7x^3)^7 \\
&\quad - 9(1+3x)^9(2+3x)^2(1+x+5x^2+7x^3)^7 \partial,
\end{aligned}$$

where ∂ represents the shift operator. From its leading coefficient, the polynomial $(1+x+5x^2+7x^3)^7$ is removable at order 1, and in addition, $(1+3x)^7$ is removable at order 12. The remaining factors are not removable. According to Theorem 9 we expect that L admits left multiples of order r and degree

$$32 - 21\left(1 - \frac{1}{r}\right)^+ - 7\left(1 - \frac{3}{1}\right)^+,$$

for all $r \in \mathbb{N}$. It turns out that this prediction is again accurate for every r . Observe that in this example the curve is a superposition of two hyperbolas.



In conclusion, we believe that removable factors provide a universal explanation for all the order-degree curves that have been observed in recent years for various different contexts. We have derived a formula for the boundary of the gray region associated to a fixed operator L , which, although formally only a bound, happens to be exact in all the examples we considered. This does not immediately imply better complexity estimates or faster variants of algorithms exploiting the phenomenon of order-degree curves, because usually L is not known in advance but rather the desired output of a calculation, and therefore we usually have no information about the removable factors of $\text{lc}_\partial(L)$. However, we now know what we have to look at: in order to improve algorithms based on trading order for degree, we need to develop a theory which provides a priori information about the removable factors of $\text{lc}_\partial(L)$. In other words, our result reduces the task of better understanding order-degree curves to the task of better understanding what causes the appearance of removable factors in operators coming from applications.

5. REFERENCES

- [1] Sergei A. Abramov, Moulay A. Barkatou, and Mark van Hoeij. Apparent singularities of linear difference equations with polynomial coefficients. *AAECC*, 17:117–133, 2006.
- [2] Sergei A. Abramov and Mark van Hoeij. Desingularization of linear difference operators with polynomial coefficients. In *Proceedings of ISSAC'99*, pages 269–275, 1999.
- [3] Alin Bostan, Frederic Chyzak, Ziming Li, and Bruno Salvy. Fast computation of common left multiples of linear ordinary differential operators. In *Proceedings of ISSAC'12*, pages 99–106, 2012.
- [4] Alin Bostan, Frédéric Chyzak, Bruno Salvy, Grégoire Lecerf, and Éric Schost. Differential equations for algebraic functions. In *Proceedings of ISSAC'07*, pages 25–32, 2007.
- [5] Manuel Bronstein and Marko Petkovšek. An introduction to pseudo-linear algebra. *Theoretical Computer Science*, 157(1):3–33, 1996.
- [6] Shaoshi Chen and Manuel Kauers. Order-degree curves for hypergeometric creative telescoping. In *Proceedings of ISSAC'12*, pages 122–129, 2012.
- [7] Shaoshi Chen and Manuel Kauers. Trading order for degree in creative telescoping. *Journal of Symbolic Computation*, 47(8):968–995, 2012.
- [8] Frederic Chyzak, Philippe Dumas, Ha Le, Jose Martin, Marni Mishna, and Bruno Salvy. Taming apparent singularities via Ore closure. in preparation.
- [9] E. L. Ince. *Ordinary Differential Equations*. Dover, 1926.