J. Symbolic Computation (1997) **11**, 1–000

Factorization of Differential Operators with Rational Functions Coefficients

Mark van Hoeij

(Received December 12, 1995)

In this paper we will give a new efficient method for factorizing differential operators with rational functions coefficients. This method solves the main problem in Beke's factorization method, which is the use of splitting fields and/or Gröbner basis.

1. Introduction

A differential equation

$$y^{(n)} + a_{n-1}y^{(n-1)} + \cdots + a_1y' + a_0y = 0$$

corresponds to a differential operator

$$f = \partial^n + a_{n-1}\partial^{n-1} + \cdots + a_0\partial^0$$

acting on y. In this paper the coefficients a_i are elements of the differential field $k(x)$ and ∂ is the differentiation d/dx. The field k is the field of constants. It is assumed to have characteristic 0. $\overline{k}$ is the algebraic closure of k. The differential operator f is an element of the non-commutative ring $k(x)[\partial]$. This is an example of an Ore ring (Ore, 1933). A factorization $f = LR$ where $L, R \in \overline{k}(x)[\partial]$ is useful for computing solutions of f because solutions of the right-hand factor R are solutions of f as well.

The topic in this paper is factorization in the ring $\overline{k}(x)[\partial]$. Multiplication in $\overline{k}(x)[\partial]$ is not commutative. However, some properties of are independent of the order of the multiplication, for example the Newton polygons of fg and gf at a point p are the same. The non-commutativity is one of the reasons that factorization in $\overline{k}(x)[\partial]$ is difficult. To handle this difficulty we will extract the *commutative part* $\mu_*(f)$ of an operator f. We will first try to find local properties of differential operators which do not depend on the order of multiplication and then we will define the commutative part of f as the collection of those properties. For this purpose we will first define *exponential parts* and their multiplicities for local differential operators in section 3. Then $\mu_*(f)$ will be defined as the collection of all exponential parts and their multiplicities at all singularities of f.

Let $f = LR$ where $f \in k(x)[\partial]$ is given and where $L, R \in \overline{k}(x)[\partial]$ is a factorization that we want to compute. The commutative part μ_* has the following property

$$\mu_*(f) = \mu_*(L) + \mu_*(R).$$

This equation leaves only a finite number of possibilities for $\mu_*(R)$. Beke's method (cf.

0747–7171/90/000000 + 00 \$03.00/0

(Beke, 1894) and also section 4) for computing first order right-hand factors R of f can be explained in terms of μ_* as follows. Try all possible $\mu_*(R)$ and for each $\mu_*(R)$ the problem of finding R is reduced to computing the rational solutions of a certain differential operator. Computing rational solutions of a differential operator can be done quickly (cf. (Abramov, Bronstein and Petkovšek, 1995)) but the number of possible $\mu_*(R)$ one needs to check depends exponentially (worst case) on the number of singularities. So Beke's method performs well on examples with few singularities, but for operators with many singularities "try all possibilities" is not a good answer to the question which $\mu_*(R)$ need to be considered. Furthermore this method involves computing in algebraic extensions over k which can be of exponentially large degree. Most previous factorization algorithms (except (Singer, 1996)) are based on Beke's algorithm for computing first order factors, and use the exterior power method for computing higher order factors.

This paper is organized as follows:

- Sections 5 and 6 contain the main result of this paper: An algorithm, that does not use computations with exponentially large algebraic extensions nor Gröbner bases, for factorizing differential operators. This algorithm can produce (first order or higher order) factors, or irreducibility proofs, for a large class (specified in section 5) of differential operators. However, not every operator is in this class, so not every operator can be handled.
- Section 7. A supplemental algorithm, that makes our algorithm complete for first order right-hand factors.
- Section 8. The exterior power method. This is another supplemental algorithm, obtained from the literature, to make the algorithm complete for higher order factors. The exterior power method is not efficient; only small operators (low order and small coefficients) can be handled this way. So we want to avoid it whenever possible.
- Section 4. Beke's algorithm for computing factors of order 1, reformulated in our terminology.

In section 7 we use the algorithm of sections 5 and 6 to compute a set S with at most order(f) elements such that $\mu_*(R) \in S$ for all first order right-hand factors R. When such S is computed, the problem of computing all first order right-hand factors is practically solved because the number of possibilities that need to be checked is now linear instead of exponential like in Beke's algorithm, and the algebraic extensions that we need to work with are of much lower degree than in Beke's algorithm. As already mentioned, Beke's algorithm, section 4, sometimes performs well but it can also be extremely slow if there are many singularities. For such cases the algorithm obtained by combining sections 5, 6 and 7 is an good alternative.

Computing left-hand factors and computing right-hand factors are equivalent problems. They can be reduced to each other by applying the adjoint. The adjoint is a $\overline{k}(x)$-anti-automorphism of $\overline{k}(x)[\partial]$ given by $\partial \mapsto -\partial$. It interchanges the role of left and right. Using the adjoint and the algorithm in sections 5, 6 and 7 we can compute all first order left and right-hand factors so every operator of order ≤ 3 can either be factored or proven to be irreducible. The method given in sections 5 and 6 can also compute higher order factors (or produce irreducibility proofs) for many (see section 5 for a more precise description) operators of order > 3. Tests show that this method can handle large examples; operators in $\mathbb{Q}(x)[\partial]$ of order > 10 with > 10 singularities are often still feasible if the bound that is computed in section 9.1 is not too high. This would be impossible with previous factorization algorithms that use the exterior power method for computing higher order factors; computing exterior powers of such large operators will cause the computer to run out of memory. Note that in a few cases, namely the operators which do not belong in the class specified in section 5, we have to use the exterior power method as well, in which case factorizing operators of order 10 is impossible as well.

If the bound in section 9.1 is very high then even small operators are hard to factor. We can not hope to solve this problem; for example the factorization of $\partial^2 - \frac{1}{n}\partial + \frac{n}{x}$ with $n = 10^{10}$ is not feasible no matter which method we use because the result will not fit in any existing computer.

2. Preliminaries

The reader is assumed to be familiar with sections 3, 6 and 8 (except for the algorithm) of (vH, Formal Solutions). From section 3 the preliminaries: Newton polygon/polynomial, differential field, Ore ring, the ring $k((x))[\delta]$ where $\delta = x\partial$, LCLM (Least Common Left Multiple), algebraic extensions of $k((x))$ and the universal extension. From section 6: exponential parts and from section 8 the relation between exponential parts and formal solutions. In the next section we will give a different introduction to exponential parts which is hopefully easier to understand than section 6 in (vH, Formal Solutions).

Note that many results similar to the ones in (vH, Formal Solutions) are found (in a different terminology) elsewhere as well, references are given in (vH, Formal Solutions). The notations in this paper are the same as in (vH, Formal Solutions).

We assume that the characteristic of the constants field k is 0. If $f \in k(x)[\partial]$ then f has finitely many coefficients in $k(x)$ and each of these coefficients has finitely many coefficients in k. So without loss of generality we can restrict ourselves to a coefficients field k and a differential operator $f \in k(x)[\partial]$ where k is finitely generated over $\mathbb{Q}$.

3. Exponential parts of local differential operators

This section gives a short introduction of exponential parts. For proofs of the statements in this section see (vH, Formal Solutions) (or the references therein).

3.1. A description in terms of the solution space

Let V be the universal extension (called R in lemma 2.1.1 in (Hendriks and van der Put, 1995)) of $k((x))$. This is a differential ring extension of $\overline{k((x))}$ consisting of all solutions of all $f \in k((x))[\delta]$.

Let $f \in k((x))[\delta] \setminus \{0\}$ be a differential operator. The action of f defines a $\overline{k}$-linear surjective map

$$f : V \to V.$$

The kernel of this map, denoted as $V(f)$, is the solution space of f. V contains all solutions of f. Hence the dimension of the kernel of f on V is maximal

$$\text{order}(f) = \dim(V(f)).$$

This number $\dim(V(f))$ is useful for factorization because it is independent of the order of the multiplication, i.e. $\dim(V(fg)) = \dim(V(gf))$. To obtain more of such useful numbers we will split $V(f)$ in a direct sum and look at the dimensions of the components (V_e, E and $\sim$ are defined in (vH, Formal Solutions), and are described below as well)

$$V = \bigoplus_{e \in E/\sim} V_e.$$

The V_e are $\overline{k}$-vector spaces and also $k((x))[\delta]$-modules. So $f(V_e) \subset V_e$ for all non-zero $f \in k((x))[\delta]$. Then $f(V_e) = V_e$ because f is surjective on V. The kernel of f on V_e is denoted by $V_e(f) = V(f) \bigcap V_e$. Denote

$$\mu_e(f) = \dim(V_e(f)).$$

This is consistent with the definition of $\mu_e(f)$ in (vH, Formal Solutions) because of theorem 8.1 in (vH, Formal Solutions). These μ_e are useful for factorization because they are independent of the order of the multiplication, i.e. if $f, g \in k((x))[\delta] \setminus \{0\}$ then

$$\mu_e(gf) = \mu_e(fg) = \mu_e(f) + \mu_e(g).$$

This equation is lemma 6.3 in (vH, Formal Solutions). It also follows from the fact that the dimension of the kernel of the composition of two surjective linear maps equals the sum of the dimensions of the kernels.

Recall the following definitions from (vH, Formal Solutions). These definitions were done in such a way that the subspaces V_e of V are as small as possible (more precisely: V_e is an indecomposable $\overline{k} \cdot k((x))[\delta]$-module) because then the integers $\mu_e(f)$ give as much as possible information about f. Denote the set

$$E = \bigcup_n \overline{k}[x^{-1/n}]$$

and the map

$$\mathrm{Exp} : E \to V$$

as $\mathrm{Exp}(e) = \exp(\int \frac{e}{x} dx)$. To define $\mathrm{Exp}(e)$ without ambiguity one can use the construction of the universal extension, cf. (Hendriks and van der Put, 1995). Then $\mathrm{Exp}(e_1 + e_2) = \mathrm{Exp}(e_1)\mathrm{Exp}(e_2)$ so Exp behaves like an exponential function. For rational numbers q we have $\mathrm{Exp}(q) = x^q \in \overline{k((x))}$. Denote (see also section 8.3 in (vH, Formal Solutions))

$$V_e = \mathrm{Exp}(e) \cdot (\overline{k} \cdot k((x))[e])[\log(x)] \subset V.$$

Note that $\overline{k} \cdot k((x))[e] = \overline{k} \cdot k((x^{1/n}))$ where n is the ramification index of e. Define $\sim$ on E as follows: $e_1 \sim e_2$ if and only if $e_1 - e_2$ is an integer divided by the ramification index of e_1. $V_{e_1} = V_{e_2}$ if and only if $e_1 \sim e_2$ so V_e is defined for $e \in E/\sim$. Hence $\mu_e(f)$ is defined for $e \in E/\sim$ as well.

$$V(f) = \bigoplus_{e \in E/\sim} V_e(f)$$

An element $e \in E/\sim$ is called an *exponential part* of f if $\mu_e(f) > 0$. The number $\mu_e(f) = \dim(V_e(f))$ is called the *multiplicity* of e in f. The sum of the multiplicities of all exponential parts of f equals the order of f.

3.2. Exponential parts and semi-regular parts

We now give the definition of $\mu_e(f)$ as it appears in (vH, Formal Solutions). Let $e \in \overline{k((x))}$. Then the *substitution map*

$$S_e : \overline{k((x))}[\delta] \to \overline{k((x))}[\delta]$$

is the $\overline{k((x))}$-automorphism given by

$$S_e(\delta) = \delta + e.$$

The following gives the relation between the solution spaces

$$\mathrm{Exp}(e) \cdot V(S_e(f)) = V(f).$$

Let $f \in k((x))[\delta]\backslash\{0\}$ and $e \in E$. Let n be the ramification index of e. Let $P = N_0(S_e(f))$ be the Newton polynomial corresponding to slope 0 in the Newton polygon of $S_e(f) \in \overline{k}((x^{1/n}))[\delta]$. Now $\mu_e(f)$ is defined as the number of roots (counted with multiplicity) of P in $\frac{1}{n}\mathbb{Z}$. If $e_1 \sim e_2$ then $\mu_{e_1}(f) = \mu_{e_2}(f)$ for all $f \in k((x))[\delta] \setminus \{0\}$ hence $\mu_e(f)$ is defined for $e \in E/\sim$ as well.

Let L be a finite algebraic extension of $k((x))$ and let $f \in L[\delta]$. Then f is called *semi-regular* over L if f has a fundamental system of solutions in $L[\log(x)]$. According to (vH, Formal Solutions) this is equivalent with the following two conditions

- f is regular singular (regular operators are regular singular as well).
- The roots of the Newton polynomial $N_0(f)$ are integers divided by the ramification index of L over $k((x))$.

Note that the definition of semi-regular depends on the field L. For $f \in k((x))[\delta]$ we have $\mu_0(f) = \mathrm{order}(f)$ if and only if all solutions of f are elements of $V_0 = \overline{k} \cdot k((x))[\log(x)]$ if and only if f is semi-regular over $k((x))$. A regular operator is semi-regular as well.

Semi-regular operators are "easy" differential operators. It is easy to compute the formal solutions (cf. (vH, Formal Solutions)) for such operators. One of the benefits of exponential parts and semi-regular parts is that we can use them to split up a "difficult" differential operator f as an LCLM of "easier" parts. More precisely: an operator f can be written as an LCLM of operators which are of the form $S_{-e}(R_e)$ for some $e \in E$ and semi-regular $R_e \in k((x))[e,\delta]$.

Let $e \in E$, $f \in k((x))[\delta]$ and $\mu_e(f) > 0$. Then the *semi-regular part* R_e of f for $e \in E$ is defined in (vH, Formal Solutions) as the highest order monic right-hand factor of $S_e(f)$ in $k((x))[e,\delta]$ which is semi-regular over $k((x))[e]$. The order of R_e is $\mu_e(f)$. $S_{-e}(R_e)$ is a right-hand factor of f. If f is monic and $e_1, \ldots, e_d \in E$ is a list of representatives of all exponential parts of f, then (cf. section 6.1 in (vH, Formal Solutions))

$$f = \mathrm{LCLM}(S_{-e_1}(R_{e_1}), \ldots, S_{-e_d}(R_{e_d})). \tag{3.1}$$

This LCLM factorization of f corresponds to the direct sum splitting (cf. sections 8.2 and 8.3 in (vH, Formal Solutions))

$$V(f) = V_{e_1}(f) \bigoplus \cdots \bigoplus V_{e_d}(f). \tag{3.2}$$

The solution space of $S_{-e_i}(R_{e_i})$ is $V_{e_i}(f)$.

3.3. Generalized exponents

In some applications (section 9.1, (van Hoeij and Weil, 1997) and (van Hoeij, 1996)) the use of the equivalence $\sim$ erases useful information about the differential operator. We would like to make a canonical choice of representatives in E for the exponential parts (which are in $E/\sim$), and call these the generalized exponents†.

In (vH, Formal Solutions) we first defined exponential parts using the map S_e and the Newton polynomial N_0 (because such a definition is convenient for computing the exponential parts) and afterwards related the exponential parts to the formal solutions (because that makes exponential parts easier to understand). We will do the same for the generalized exponents, first define them using N_0 and S_e, and then relate them to the formal solutions by introducing the notion of the *valuation* of a formal solution.

Definition 3.1. *Let $e \in E$ and $f \in \overline{k((x))}[\delta] \setminus \{0\}$. Define the number $\nu_e(f)$ as the multiplicity of the root 0 in $N_0(S_e(f))$.*

$e \in E$ is called a generalized exponent of f if $\nu_e(f) > 0$. The number $\nu_e(f)$ is called the multiplicity of this generalized exponent.

For a given $\overline{e} \in E/\mathbb{Q}$ the sum of $\nu_e(f)$ taken over all $e \in E$ for which $\overline{e}$ is e mod $\mathbb{Q}$ equals $\overline{\mu}_{\overline{e}}(f)$. Hence by theorem 6.1 in (vH, Formal Solutions) it follows that

$$\sum_{e \in E} \nu_e(f) = \mathrm{order}(f). \tag{3.3}$$

Definition 3.2. *Let $f \in \overline{k((x))}[\delta]$ be of order n. The list $e_1, \ldots, e_n \in E$ is called a* list of generalized exponents *of f if for all $e \in E$ the number of e_i which equal e is $\nu_e(f)$.*

Two lists of generalized exponents are equivalent if they are a permutation of each other. Up to this equivalence a list of generalized exponents is uniquely defined for every $f \in \overline{k((x))}[\delta]$. If f is regular singular then the list of generalized exponents is the list of roots of the Newton polynomial $N_0(f)$ of f.

Lemma 3.1. *If $e \in E$, $f \in \overline{k((x))}[\delta]$ and $e_1, \ldots, e_n \in E$ is the list of generalized exponents of f then $e_1 - e, \ldots, e_n - e$ is the list of generalized exponents of $S_e(f)$.*

Proof: This follows from the fact that $S_{e_i - e}(S_e(f)) = S_{e_i}(f)$.

□

Lemma 3.2. *If R is a right-hand factor of f then the list of generalized exponents of R is a sublist of the list of generalized exponents of f. In other words: $\nu_e(R) \leq \nu_e(f)$ for all $e \in E$.*

† In an older version of this text a generalized exponent was called *canonical exponential part* (meaning: a canonical choice of a representative in E for an exponential part in $E/\sim$) and the list of generalized exponents was called *canonical list.* To give a better indication of the purpose of this notion the name was changed to generalized exponent in (van Hoeij and Weil, 1997).

Proof: If R is a right-hand factor of f then $S_e(R)$ is a right hand factor of $S_e(f)$. So the Newton polynomial $N_0(S_e(R))$ is a factor of $N_0(S_e(f))$, cf. (vH, Formal Solutions).

□

The lemma does not hold for left-hand factors of f. Take for example $f = \delta \cdot (\delta - 3/x^5)$. The list of generalized exponents is $5, 3/x^5$ and the list of generalized exponents of δ is 0.

LEMMA 3.3. *If $f_1, \ldots, f_d \in \overline{k((x))}[\delta]$ have no generalized exponents in common then the list of generalized exponents of $f = \mathrm{LCLM}(f_1, \ldots, f_d)$ is the concatenation of the lists of generalized exponents of the f_i.*

Proof: Denote l as the list of generalized exponents of f and m as the concatenation of the lists of generalized exponents of the f_i. The lists of generalized exponents of the f_i are sublists of l and since they have no elements in common it follows that m is a sublist of l. The number of elements of m is the sum of the orders of the f_i. Hence this number is $\geq \mathrm{order}(f)$, and this equals the number of elements of l. Hence l is m (up to a permutation).

□

Note that if the f_i do have generalized exponents in common then not every generalized exponent of f needs to be a generalized exponent of one of the f_i. Take for example f_1 such x is a basis of $V(f_1)$ and take f_2 such that $x + x^{10}$ is a basis of $V(f_2)$. Then the lists of generalized exponents of f_1 and f_2 are both 1, but the list of generalized exponents of $\mathrm{LCLM}(f_1, f_2)$ is $1, 10$.

Consider the set

$$\overline{V}_0 = \overline{k((x))}[\log(x)]$$

cf. section 8.3 in (vH, Formal Solutions). We can define a valuation

$$v : \overline{V}_0 \longrightarrow \mathbb{Q} \bigcup \{\infty\}$$

where $v(0) = \infty$ and $v(a)$ with $a \neq 0$ is the smallest exponent of x in a with a non-zero coefficient. So $x^{-v(a)} a \in \overline{k}[[x^{1/n}]][\log(x)]$ for some n and $v(a)$ is maximal with this property.

$\overline{V}_e \subset V$ is defined as $\mathrm{Exp}(e) \cdot \overline{V}_0$. Define the set

$$V_* = (\bigcup_e \overline{V}_e) \setminus \{0\}$$

where the union is taken over all $e \in E$. Notice that V_* is closed under multiplication. We can extend the valuation v to V_*

$$v : V_* \longrightarrow E$$

as follows: let $y \in V_*$. Then $y = \mathrm{Exp}(e) r$ for some $e \in E$ (which is determined modulo $\mathbb{Q}$ by y) and $r \in \overline{V}_0$. Now define $v(y) = e + v(r)$. This $v(y)$ does not depend on the choice of e and r. For all $e \in E$ we have $v(\mathrm{Exp}(e)) = e$. If $v(y_1)$ and $v(y_2)$ are both defined (i.e. $y_1, y_2 \in V_*$) then $v(y_1 y_2) = v(y_1) + v(y_2)$.

THEOREM 3.1. *Let $f \in \overline{k((x))}[\delta]$ be of order m. There exists a basis $y_1, \ldots, y_m \in V_*$ of $V(f)$ such that $v(y_1), \ldots, v(y_m)$ is the list of generalized exponents of f. Conversely, for any solution y of f in V_* the valuation $v(y)$ is a generalized exponent.*

Proof: We will first prove the theorem for operators $f \in \overline{k}((x^{1/n}))[\delta]$ which are semi-regular over $\overline{k}((x^{1/n}))$. Note that $v(\int \frac{a_i}{x} dx) = v(a_i)$ (take the coefficient of the term $x^0 \log(x)^0$ in the integral equal to 0). From this it follows by induction that the algorithm in section 8.1 in (vH, Formal Solutions) produces a basis of solutions for which the valuations are the roots of the Newton polynomial (and hence these valuations form the list of generalized exponents). Now suppose $y \in \overline{k}((x^{1/n}))[\log(x)]$ is a solution of this semi-regular f. Factor f (cf. section 5 and 8.1 in (vH, Formal Solutions)) as $f = L \cdot (\delta - q + a)$ where $q \in \frac{1}{n}\mathbb{Z}$, $a \in x^{1/n} \cdot \overline{k}[[x^{1/n}]]$ and $L \in \overline{k}((x^{1/n}))[\delta]$ is semi-regular. If $v(y) = q$ then $v(y)$ is a generalized exponent of $\delta - q + a$ and hence of f as well. If $v(y) \neq q$ then write $y = \sum_{i,j} c_{i,j} x^i \log(x)^j$. Here the sum is taken over $i \in \frac{1}{n}\mathbb{Z}$ and $j \in \mathbb{N}$. Take j maximal such that $c_{v(y),j} \neq 0$. Then the coefficient of $x^{v(y)} \log(x)^j$ in $(\delta - q + a)(y) = xy' - qy + ay$ is $c_{v(y),j}(v(y) - q) \neq 0$. So $v((\delta - q + a)(y)) \leq v(y)$. Furthermore all terms in $xy' - qy + ay$ have valuation $\geq v(y)$ hence $v((\delta - q + a)(y)) = v(y)$. Now $(\delta - q + a)(y)$ is a solution of the semi-regular operator L and hence by induction $v(y)$ is a root of the Newton polynomial of L. Because f is regular singular the Newton polynomial of L is a factor of the Newton polynomial of f and hence $v(y)$ is a root of the Newton polynomial of f. So the theorem holds for any semi-regular $f \in \overline{k}((x^{1/n}))[\delta]$.

To prove the theorem for any $f \in \overline{k((x))}[\delta]$ write f as

$$f = \mathrm{LCLM}(S_{-e_1}(\overline{R}_{e_1}), \ldots, S_{-e_q}(\overline{R}_{e_q})) \tag{3.4}$$

as in section 6.1 in (vH, Formal Solutions). For a definition of $\overline{R}_e$ for $e \in E$ and $f \in \overline{k((x))}[\delta]$ see also section 6.1 in (vH, Formal Solutions). It follows from the definition that the order of $\overline{R}_e$ is $\overline{\mu}_e(f)$. The solutions of $S_{-e}(\overline{R}_e)$ are in $\overline{V}_e(f)$, cf. section 8.2 in (vH, Formal Solutions). The dimension of the solution space of $S_{-e}(\overline{R}_e)$ is $\mathrm{order}(\overline{R}_e) = \overline{\mu}_e(f)$ which equals the dimension of $\overline{V}_e(f)$ by theorem 8.1 in (vH, Formal Solutions). Hence $V(S_{-e}(\overline{R}_e)) = \overline{V}_e(f)$ and equation (3.4) corresponds to the following direct sum

$$V(f) = \overline{V}_{e_1}(f) \bigoplus \cdots \bigoplus \overline{V}_{e_q}(f).$$

Theorem 3.1 holds for the $\overline{R}_{e_i}$ because these are semi-regular over $\overline{k}((x^{1/n}))$ for some n. So we have a basis of solutions (computed by the method of section 8.1 in (vH, Formal Solutions)) $y_{i,j}$, $j = 1, \ldots, \overline{\mu}_{e_i}(f)$ of $\overline{R}_{e_i}$ such that the valuations of this basis form the list of generalized exponents of $\overline{R}_{e_i}$. So $\mathrm{Exp}(e_i) y_{i,j}$, $j = 1, \ldots, \overline{\mu}_{e_i}(f)$ is a basis of solutions of $S_{-e_i}(\overline{R}_{e_i})$ and according to lemma 3.1 the valuations of these $\mathrm{Exp}(e_i) y_{i,j}$ form the list of generalized exponents of $S_{-e_i}(\overline{R}_{e_i})$. Then from equation (3.4) it follows that $\mathrm{Exp}(e_i) y_{i,j}$, $j = 1, \ldots, \overline{\mu}_{e_i}(f)$, $i = 1, \ldots, q$ is a basis of solutions of f and according to lemma 3.3 the valuations of this basis is the list of generalized exponents.

To prove the second statement take $y \in V(f)$ with $y \in V_*$. Then y is a non-zero element of $\overline{V}_e(f)$ for some $e \in E$. So y is a solution of $S_{-e}(\overline{R}_e)$, and hence $\mathrm{Exp}(-e)y$ is a solution of $\overline{R}_e$. Theorem 3.1 is true for $\overline{R}_e$ because it is semi-regular over $\overline{k}((x^{1/n}))$ for some n. So $v(\mathrm{Exp}(-e)y) = v(y) - e$ is a generalized exponent of $\overline{R}_e$. Then by lemma 3.1 it follows that $v(y)$ is a generalized exponent of $S_{-e}(\overline{R}_e)$ and hence by lemma 3.2 $v(y)$ is a generalized exponent of f.

□

The following lemma gives a relation between factorizations in $\overline{k((x))}[\delta]$ and generalized exponents.

LEMMA 3.4. *Let* $r_1, \ldots, r_n \in \overline{k((x))}$ *and* $f = \delta^n + a_{n-1}\delta^{n-1} + \cdots + a_0\delta^0 \in \overline{k((x))}[\delta]$ *such that* $f = (\delta - r_1)\cdots(\delta - r_n)$. *Define* $v'(r) \in \mathbb{Q}$ *for* $r \in \overline{k((x))}$ *as the minimum of* 0 *and* $v(r)$. *Let*

$$e_i = \mathrm{pp}(r_i) - \sum_{j>i} v'(r_i - r_j).$$

Then $e_1, \ldots, e_n$ *is the list of generalized exponents of* f. *Furthermore*

$$\mathrm{pp}(a_{n-1}) = -\sum_i (e_i + \sum_{j>i} v'(e_i - e_j)). \tag{3.5}$$

Recall that for $r \in \overline{k((x))}$ the *principal part* $\mathrm{pp}(r) \in E$ is defined in section 6 in (vH, Formal Solutions) by the condition that $v(r - \mathrm{pp}(r)) > 0$.

Proof: Let $v_0(a)$ for non-zero $a \in \overline{k((x))}[\delta]$ be the smallest exponent of x in a with a non-zero coefficient in $\overline{k}[\delta]$, and $v_0(0) = \infty$, which generalizes the definition of v_0 in section 2 in (vH, Formal Solutions). Then v_0 is a valuation on $\overline{k((x))}[\delta]$ and $v'(r) = v_0(\delta - r)$ for $r \in \overline{k((x))}$. Now the following relation for the Newton polynomials holds for all non-zero $L, R \in \overline{k((x))}[\delta]$

$$N_0(LR) = N_0(S_{v_0(R)}(L)) \cdot N_0(R)$$

which is a generalization of the formula in section 3.4 in (vH, Formal Solutions) to $\overline{k((x))}[\delta]$. Let $L = \delta - r_1$ and $R = (\delta - r_2)\cdots(\delta - r_n)$ so $f = LR$. By induction we know that $e_2, \ldots, e_n$ is the list of generalized exponents of R. The list of generalized exponents of f is the list of generalized exponents of R plus one more element. To show that this element is e_1 we must show that the multiplicity of the root 0 in the polynomial $N_0(S_{e_1}(f))$ equals the multiplicity of the root 0 in $N_0(S_{e_1}(R))$ plus one, in other words $N_0(S_{e_1}(f))/N_0(S_{e_1}(R)) = T$ (here T is the variable used to denote the Newton polynomial, as in (vH, Formal Solutions)). $S_{e_1}(f) = S_{e_1}(L) \cdot S_{e_1}(R)$ and $v_0(S_{e_1}(R)) = v_0(S_{e_1}(\delta - r_2)) + \cdots + v_0(S_{e_1}(\delta - r_n)) = v_0(\delta - r_2 + e_1) + \cdots + v_0(\delta - r_n + e_1) = v_0(\delta - r_2 + r_1) + \cdots + v_0(\delta - r_n + r_1) = \mathrm{pp}(r_1) - e_1$. Hence

$$\frac{N_0(S_{e_1}(f))}{N_0(S_{e_1}(R))} = N_0(S_{v_0(S_{e_1}(R))}(S_{e_1}(L))) = N_0(S_{\mathrm{pp}(r_1)}(L)) = T.$$

Equation (3.5) follows from the fact that $r_1 + \cdots + r_n = -a_{n-1}$ (note that $v'(r_i - r_j) = v'(e_i - e_j)$).

□

Summary: The generalized exponents are the valuations of the solutions (of those solutions for which the valuation is defined, i.e. which are in V_*). The exponential parts are the generalized exponents modulo the equivalence $\sim$. Generalized exponents of right-hand factors of f (but not of left-hand factors) are generalized exponents of f as well. For exponential parts we have this property for all factors.

3.4. Localization and exponential parts

For a point $p \in P^1(\overline{k}) = \overline{k} \bigcup \{\infty\}$ we can define a $\overline{k}$-automorphism $l_p : \overline{k}(x) \to \overline{k}(x)$ as follows. If $p = \infty$ then $l_p(x)$ is defined as $1/x$ and if $p \in \overline{k}$ then $l_p(x) = x + p$. We can extend l_p to a ring automorphism of $\overline{k}(x)[\partial]$ by defining $l_p(\partial) = \partial$ if p is finite (i.e. $p \in \overline{k}$) and $l_p(\partial) = -x^2\partial$ if p is infinity. For a differential operator $f \in \overline{k}(x)[\partial]$ we call $l_p(f)$ the *localization* of f at the point $x = p$. The operator $l_p(f)$ is viewed as an element of $\overline{k}((x))[\delta]$ instead of $\overline{k}(x)[\partial]$.

Definition 3.3. *Let $e \in E/\sim$, $f \in k(x)[\partial]$ and $p \in P^1(\overline{k})$. Define*

$$\mu_{e,p}(f) = \mu_e(l_p(f)).$$

Now e is called an exponential part *of f at the point p if $\mu_{e,p}(f) > 0$. The number $\mu_{e,p}(f)$ is called the* multiplicity *of e in f at the point p.*

If p is a semi-regular point of f then f has only a trivial (i.e. zero modulo $\sim$) exponential part at p.

The following notation $\mu_*(f) \in \mathbb{N}^{(E/\sim)\times P^1(\overline{k})}$ formalizes all exponential parts and their multiplicities at all points in $P^1(\overline{k})$

$$\mu_*(f) : (E/\sim) \times P^1(\overline{k}) \to \mathbb{N}$$

which maps (e, p) to $\mu_{e,p}(f)$. For $f, g \in \overline{k}(x)[\partial]$ we have

$$\mu_*(fg) = \mu_*(gf) = \mu_*(f) + \mu_*(g).$$

A remark on the implementation: Localizing a rational function at the point $x = 0$ is a mathematically trivial operation because $\overline{k}(x) \subset \overline{k}((x))$. On a computer this is not a trivial operation, it is a conversion of data types. Computations with infinite power series are done by *lazy evaluation*. Note that substitutions like l_p in polynomials or rational functions can be costly. So even for polynomials, which are only finite series, one should implement the map l_p with lazy evaluation, so that no more terms than needed will be computed. Since higher powers of x tend to have larger coefficients this can make a significant difference in computation time.

3.5. The type of an operator

In this section we will examine the relation between μ_* and the so-called type of a differential operator.

Definition 3.4. *Let $f, g \in \overline{k}(x)[\partial]$. Now f and g are said to be of the same* type *if there exist $r_1, r_2 \in \overline{k}(x)[\partial]$ such that*

$$r_1(V(f)) = V(g) \quad \text{and} \quad r_2(V(g)) = V(f)$$

This notion is called *Art-begriff* in (Ore, 1932). Four different characterizations of this notion are given in (Singer, 1996), corollary 2.6. Verifying if f and g are of the same type can be done by computing the set $\mathcal{E}_{\mathcal{D}}(g, f)$ (cf. (van Hoeij, 1996) and (Singer, 1996)) and checking if it contains an r_1 for which $r_1 : V(f) \to V(g)$ is bijective. If such r_1 exists then an operator $r_2 \in \overline{k}(x)[\partial]$ with $r_2(V(g)) = V(f)$ exists as well (for properties like these and for a quick introduction to this topic see also (Tsarev, 1996)). r_2 can be found by solving the equation $r_2 r_1 + lf = 1$ via the extended Euclidean algorithm (cf. (Ore, 1933)). This equation has a solution $r_2, l \in \overline{k}(x)[\partial]$ because r_1 is injective on $V(f)$ and hence $\mathrm{GCRD}(f, r_1) = 1$ (GCRD stands for greatest common right divisor).

Define the following equivalence $\sim_*$ on $\overline{k}(x)$.

$$r_1 \sim_* r_2 \Longleftrightarrow \exists_{y \in \overline{k}(x)} \quad r_1 - r_2 = y'/y.$$

Define for $r \in \overline{k}(x)$ the $\overline{k}(x)$-automorphism

$$S_r^* : \overline{k}(x)[\partial] \to \overline{k}(x)[\partial]$$

by $S_r^*(\partial) = \partial + r$. Note that this is not the same (∂ instead of δ) as the previously defined S_r. For $f, g \in \overline{k}(x)[\partial]$ if $\mu_*(f) = \mu_*(g)$ then $\mu_*(S_r^*(f)) = \mu_*(S_r^*(g))$. Similarly if $\mathrm{type}(f) = \mathrm{type}(g)$ then $\mathrm{type}(S_r^*(f)) = \mathrm{type}(S_r^*(g))$.

LEMMA 3.5. *Let $a, b \in \overline{k}(x)$. Then $\mu_*(\partial) = \mu_*(\partial - a)$ if and only if $\partial - a$ has a non-zero solution y in $\overline{k}(x)$. Furthermore $\mu_*(\partial - a) = \mu_*(\partial - b)$ if and only if $a \sim_* b$.*

Note that $\mu_*(\partial) = \mu_*(\partial - a)$ means $\partial - a$ is semi-regular at all points $p \in P^1(\overline{k})$.

Proof: If $\partial - a$ has a rational solution y then $l_p(\partial - a)$ has a solution $l_p(y) \in V_0$. Hence $\mu_0(l_p(\partial - a)) > 0$ for all p. Since the order is 1 there are no other exponential parts hence $l_p(\partial - a)$ is semi-regular. Conversely if $\partial - a$ is semi-regular at all points p then one can verify that

$$y = \prod_{p \in \overline{k}} (x - p)^{a_p} \in \overline{k}(x)$$

is a non-zero rational solution of $\partial - a$, where $a_p \in \mathbb{Z}$ is the exponent of $\partial - a$ at p. Hence the first statement follows. The second statement is reduced to the first statement by applying S_a^*.

□

LEMMA 3.6. *Let $f = \partial^n + a_{n-1}\partial^{n-1} + \cdots + a_0\partial^0$ and $g = \partial^n + b_{n-1}\partial^{n-1} + \cdots + b_0\partial^0$ be in $\overline{k}(x)[\partial]$. Let $a_{i,p}, b_{i,p} \in \overline{k}((x))$ for $i = 0, \ldots, n-1$ and $p \in P^1(\overline{k})$ such that $l_p(f) = \delta^n + a_{n-1,p}\delta^{n-1} + \cdots + a_{0,p}\delta^0$ and $l_p(g) = \delta^n + b_{n-1,p}\delta^{n-1} + \cdots + b_{0,p}\delta^0$. Then $a_{n-1} \sim_* b_{n-1}$ if and only if $\mathrm{pp}(a_{n-1,p} - b_{n-1,p})$ is an integer for all $p \in P^1(\overline{k})$.*

Note: For convenience of notation $l_p(f) \in \overline{k}((x))[\delta]$ has been multiplied on the left by an element of $\overline{k}((x))$ so that it can be represented as a monic element of $\overline{k}((x))[\delta]$. For the definition of the principal part pp see lemma 3.5.

Proof: Denote $f_1 = \partial + a_{n-1}$ and $g_1 = \partial + b_{n-1}$. One can verify (for a similar but more detailed computation see also lemma 9.1 in section 9.1) that $l_p(f_1) = \delta + a_{n-1,p} + m_p$ for some $m_p \in \mathbb{Z}$. Now $a_{n-1,p} - b_{n-1,p} \in \mathbb{Z} + x \cdot \overline{k}[[x]]$ if and only if $\delta + a_{n-1,p}$ and $\delta + b_{n-1,p}$ in $\overline{k}((x))[\delta]$ have the same exponential part $e \in E/\sim$. So $a_{n-1,p} - b_{n-1,p} \in \mathbb{Z} + x \cdot \overline{k}[[x]]$ for all $p \in P^1(\overline{k})$ if and only if $\mu_*(f_1) = \mu_*(g_1)$. Now the lemma follows from the previous lemma.

□

PROPOSITION 3.1. *Let* $f = \partial^n + a_{n-1}\partial^{n-1} + \cdots + a_0\partial^0$ *and* $g = \partial^n + b_{n-1}\partial^{n-1} + \cdots + b_0\partial^0$ *be in* $\overline{k}(x)[\partial]$. *Then*

$$\mathrm{type(f)} = \mathrm{type}(g) \Longrightarrow \mu_*(f) = \mu_*(g). \tag{3.6}$$

Furthermore

$$\mu_*(f) = \mu_*(g) \Longrightarrow a_{n-1} \sim_* b_{n-1}. \tag{3.7}$$

If $n = 1$ *then the two implication arrows can be reversed.*

For $n > 1$ these arrows can not be reversed. Take for example $\partial^2 + x^5$ and $\partial^2 + x^5 + x$. These two operators have the same μ_* but not the same type. The second arrow can not be reversed either if $n > 1$, as almost any random example will show: $\mu_*(\partial^2) \neq \mu_*(\partial^2 - x)$; the exponential parts are different at $x = \infty$.

Proof: Suppose $\mathrm{type}(f) = \mathrm{type}(g)$. By definition $r(V(f)) = V(g)$ for some operator r. We need to show that $\mu_{e,p}(f) = \mu_{e,p}(g)$ for all e and p. We may assume (after having applied the map l_p) that $p = 0$. Recall from section 3 that $r(V_e) = V_e$, $V_e(f) = V_e \bigcap V(f)$ and $\mu_e(f) = \dim(V_e(f))$. From $r(V_e(f)) = r(V_e \bigcap V(f)) \subset r(V(f)) \bigcap r(V_e) = V(g) \bigcap V_e = V_e(g)$ it follows that $\mu_e(f) \leq \mu_e(g)$. In the same way one shows that $\mu_e(f) \geq \mu_e(g)$ and so (3.6) is proven.

If $n = 1$ then (3.7) follows from lemma 3.5. The fact that $a_{n-1} \sim_* b_{n-1}$ implies $\mathrm{type}(f) = \mathrm{type}(g)$ if $n = 1$ follows directly from the definitions. What remains to be shown is (3.7) for the case $n > 1$.

Consider two lists $e_1, \ldots, e_n$ and $e'_1, \ldots, e'_n$ of elements of $\overline{k}[x^{-1/r}] \subset E$, such that $e_i \sim e'_i$ for all i. Denote $d = (e_1 + \cdots + e_n) - (e'_1 + \cdots + e'_n)$. Then $d \in \frac{1}{r}\mathbb{Z}$ but not necessarily $d \in \mathbb{Z}$. However, if both lists are invariant (up to permutations) under the Galois action of the field extension $\overline{k}(x) \subset \overline{k}(x^{1/r})$ then one can conclude $d \in \mathbb{Z}$.

Let $p \in P^1(\overline{k})$. Let $a_{i,p}, b_{i,p}$ be elements of $\overline{k}((x))$ such that $l_p(f) = \delta^n + a_{n-1,p}\delta^{n-1} + \cdots + a_{0,p}\delta^0$ and $l_p(g) = \delta^n + b_{n-1,p}\delta^{n-1} + \cdots + b_{0,p}\delta^0$ (note: here $l_p(f)$ and $l_p(g)$ have been multiplied on the left by an element of $\overline{k}((x))$ to make them monic). Let $e_1, \ldots, e_n$ resp. $e'_1, \ldots, e'_n$ be the lists of generalized exponents of $l_p(f)$ and $l_p(g)$. Assume that $\mu_*(f) = \mu_*(g)$. Then, after a permutation, we have $e_i \sim e'_i$ for $i = 1, \ldots, n$. Then $v'(e_i - e_j) = v'(e'_i - e'_j)$ where v' is defined in lemma 3.4. Because the lists of generalized exponents are invariant under the Galois action of $\overline{k}(x) \subset \overline{k}(x^{1/r})$ it follows that $\sum_i (e_i - e'_i)$ is an integer. Then by equation (3.5) it follows that $\mathrm{pp}(a_{n-1,p} - b_{n-1,p})$ is an integer. This holds for all $p \in P^1(\overline{k})$ hence (3.7) follows from lemma 3.6.

□

DEFINITION 3.5. *Let* $f \in \overline{k}(x)[\partial]$ *then* $\gamma_1(f)$ *is the set of all* $\mu_*(R)$ *for all first order right-hand factors* $R \in \overline{k}(x)[\partial]$ *of* f.

Because of lemma 3.5 the set $\gamma_1(f)$ can be identified with a subset of $\overline{k}(x)[\partial]/\sim_*$. We can also view it as the set of types of all first order right-hand factors. In the next section we will see that once $\gamma_1(f)$ is known, then computing all first order right-hand factors is not difficult anymore. This is in fact more general: Given an operator f and an irreducible operator R, one can compute all right-hand factors of f that are of the same type as R by solving a mixed equation. This follows from work of Loewy and Ore, see (Tsarev, 1996) for an introduction to this topic. Solving the mixed equation is the topic of (van Hoeij, 1996). So one can find all irreducible right-hand factors of f if one can find the set of types (this set is finite) of all irreducible right-hand factors of f.

The fact that for order $n = 1$ the type of an operator corresponds to μ_* (which is a collection of local data, i.e. data that we can compute) is the reason that computing factors of order 1 is theoretically easier than computing higher order factors. For higher order factors R the type is not determined by $\mu_*(R)$ which makes the situation more complicated. However, the coefficient a_{n-1} of $R = \partial^n + a_{n-1}\partial^{n-1} + \cdots + a_0\partial^0$ is determined modulo $\sim_*$ by $\mu_*(R)$, in other words type$(\partial + a_{n-1})$ is determined by $\mu_*(R)$. Hence it is not surprising that in Beke's method for higher order factors of f one first computes a differential equation $\wedge^n f$, such that for any right-hand factor $R = \partial^n + a_{n-1}\partial^{n-1} + \cdots + a_0\partial^0$ of f the operator $\partial + a_{n-1}$ is as a right-hand factor of $\wedge^n f$ (see also section 8 on this).

4. Beke's method for finding first order factors

In this section we will describe Beke's factorization method in (Beke, 1894). His method is a good illustration how to use exponential parts. Previous implementations for factorization in $\overline{k}(x)[\partial]$ are based on his method. For example, the factorizer in the Kovacic algorithm (cf. Section 3.1 in (Kovacic, 1986)) is based on Beke's method. Note that Beke only uses this method for regular singular operators, for the more general case he uses polynomial equations. However, equipped with the terminology of exponential parts, the regular singular case is not harder nor easier than the general case. We only need to replace the word exponent in Beke's text by exponential part. Though the method in this section is not precisely the same as in (Beke, 1894), the difference is small enough to call it Beke's method.

Let $f \in k(x)[\partial]$. Assume f has a first order right-hand factor factor $\partial - r$ where $r \in \overline{k}(x)$ and we want to compute such a factor. This is done in 2 steps

1 Determine $\mu_*(\partial - r)$, i.e. determine the exponential part of $\partial - r$ at all singularities.

2 Compute r.

When $\mu_*(\partial - r)$ is known then r is determined up to the equivalence $\sim_*$. So we can take a representative $r_0 \in \overline{k}(x)$ such that $r_0 \sim_* r$, in other words $r - r_0 = y'/y$ for some $y \in \overline{k}(x)$. Now r is easily found as follows. y is a rational solution of $S^*_{r_0}(\partial - r)$ and hence a rational solution of $S^*_{r_0}(f)$. Any rational solution of $S^*_{r_0}(f)$ gives a right factor $\partial - r = \partial - r_0 - y'/y$ of f.

Beke's method does not give a real answer to how to do the first step, except by trying all possibilities. Suppose order$(f) = N$ and f has M singularities. At every singularity there are at most N different exponential parts so the number of possibilities to check is $\leq N^M$. Another reason that checking all possibilities is very costly is because it can introduce large algebraic extensions. Localizing at all singularities costs at most an algebraic extension of degree $M!$ over k. Computing an exponential part at one singularity costs at most an extension of degree N so Beke's method uses an algebraic extension of degree $\leq M! \cdot N^M$. If the set $\gamma_1(f)$ were known then the algebraic extensions one needs to compute with would be much smaller. *Computing all first order right-hand factors of f and computing $\gamma_1(f)$ are equivalent problems.*

Note that Beke's method implies a method for computing the radical solutions (i.e. solutions y for which $y^n \in \overline{k}(x)$ for some integer n). For this we need to adapt the algorithm such that it only tries exponential parts in $\mathbb{Q}$ modulo $\mathbb{Z}$ instead of all exponential parts.

5. The main idea of the algorithm

Let $f \in k(x)[\partial]$ and suppose a non-trivial factorization $f = LR$ exists with $L, R \in \overline{k}(x)[\partial]$. We want to determine a right-hand factor of f. This could be done if we knew a non-zero subspace $W \subset V(R)$, cf. section 6. However, a priori we only know that $V(R) \subset V(f)$ but this does not give any non-zero element of $V(R)$.

For any exponential part e of f at a point $p \in P^1(\overline{k})$ we have (after replacing f, L, R by $l_p(f), l_p(L), l_p(R)$ we may assume that $p = 0$) $V_e(R) \subset V_e(f)$ and $\mu_e(L) + \mu_e(R) = \mu_e(f)$. Suppose that we are in a situation where $\mu_e(L) = 0$. Then the dimensions of $V_e(R)$ and $V_e(f)$ are the same and hence we have found a subspace $V_e(f) = V_e(R)$ of $V(R)$. Then we can factor f (cf. section 6). Note that we do not necessarily find the factorization LR, it is possible that instead of R a right-hand factor of R is found.

So now we search for situations where we may assume $\mu_e(L) = 0$. There are several instances of this:

1 Suppose that order$(L) = 1$ and that f has more than 1 exponential part at the point p. Let $e_1 \not\sim e_2$ be two different exponential parts of f. Then $\mu_{e_1}(L) = 0$ or $\mu_{e_2}(L) = 0$ because the sum of the multiplicities $\mu_e(L)$ for all exponential parts $e \in E/\sim$ is the order of L which is 1. So we need to distinguish two separate cases and in at least one of these cases we will find a non-trivial factorization of f.

2 More generally suppose order$(L) = d$ and that at a point p the operator f has at least $d+1$ different exponential parts $e_1, \ldots, e_{d+1}$. Then for at least one of these e_i we have $\mu_{e_i}(L) = 0$. Hence by distinguishing $d+1$ cases $i = 1, \ldots, d+1$ we will find a non-trivial factorization of f.

So we can factor any reducible operator which has:

1 A first order left-hand factor and a singularity with more than 1 exponential part.

2 Or more generally: an operator with a left-hand factor of order d and a singularity at which there are more than d different exponential parts.

3 By using the adjoint we can also factor operators which have a right-hand factor of order d and a point p with more than d different exponential parts.

4 An operator which has a singularity with an exponential part e of multiplicity 1. Then we can distinguish two cases $\mu_e(L) = 0$ or $\mu_e(R) = 0$. The latter case is reduced to the former case using the adjoint. We call the minimum of the multiplicities taken over all exponential parts of all singularities the *minimum multiplicity*. By checking both cases $\mu_e(L) = 0$ or $\mu_e(R) = 0$ any operator f with minimum multiplicity 1 is either irreducible or it is factored by our method.

Note on computing first order factors: If a first order left or right-hand factor exists, then our approach can compute a factorization whenever there is a singularity with at least two different exponential parts. This reduces the problem of finding all first order factors, cf. section 7. The only case that remains is when each singularity has only 1 exponential part. However, this special case is a trivial case for Beke's method because we need to check only one possibility in Beke's method. We can proceed as follows: Compute (if it exists) an $r \in k(x)$ such that $\partial - r$ has the same exponential part as f at all singularities. Then $S_r^*(f)$ is semi-regular at all singularities. For computing the first order right-hand factors of such an operator the only thing one needs to do in Beke's method is to compute the rational solutions.

Note on computing higher order factors: An operator with minimum multiplicity 1 is either irreducible or factored by our algorithm. If the minimum multiplicity is > 1 we can often still factor f by constructing irreducible local factors for the different exponential parts and trying to construct right-hand factors $R \in \overline{k}(x)[\partial]$ from these local factors in the same way as in section 6. However, in this case our algorithm is a incomplete because we can not guarantee irreducibility if no factorization is obtained. Currently our implementation will print a warning message in such cases. To make the algorithm complete for these cases we will have to use the rather inefficient exterior power method, cf. section 8.

Note that it is possible that a factor of a minimum multiplicity 1 operator has minimum multiplicity > 1.

6. Computing a right-hand factor R

After having applied the map l_p of section 3.4 (and a field extension of k if $p \in \overline{k} \setminus k$) we may assume that the singularity p in the previous section is the point $p = 0$.

The assumption from section 5 was that an $e \in E$ is known for which $\mu_e(f) > 0$ and $\mu_e(L) = 0$. From this we concluded that $V_e(f) \subset V(R)$. In other words $S_{-e}(R_e) \in k((x))[e, \delta]$ is a right-hand factor of R, where R_e is the semi-regular part of f, cf. section 6.1 in (vH, Formal Solutions). R_e and hence $S_{-e}(R_e)$ can be computed by local factorization (cf. section 8.4 in (vH, Formal Solutions)). We want to have a local right-hand factor r of R. There are several strategies: We can take $r = S_{-e}(R_e)$, or we can take a first order right-hand factor in $k((x))[e, \delta]$ of $S_{-e}(R_e)$. Another strategy, to speed up the algorithm, is first to try to factor f in $k(x)[\partial]$ instead of $\overline{k}(x)[\partial]$. If no factorization in $k(x)[\partial]$ is obtained, then we can redo the computation afterwards to search a factorization in $\overline{k}(x)[\partial]$. If we want to factor f in $k(x)[\partial]$ then we can take $r \in k((x))[\delta]$ of minimal order such that $S_{-e}(R_e)$ is a right-hand factor of r. So, depending on whether we want to factor f in $k(x)[\partial]$ or in $\overline{k}(x)[\partial]$, we have a right-hand factor $r \in k((x))[\delta]$ or $r \in k((x))[e, \delta]$ of R. Note that to find r we do not need to compute formal solutions, we only need the factorization algorithm in (vH, Formal Solutions). From now on we will assume that $r \in k((x))[\delta]$, the other case works precisely the same (just replace k by $\overline{k}$).

Let $n = \mathrm{order}(f)$. The goal is to compute an operator $R = a_d\partial^d + \cdots + a_0\partial^0 \in k[x, \partial]$ that has r as a right-hand factor. Here d should be minimal. Because r divides both f and R on the right it also divides $\mathrm{GCRD}(f, R)$. (greatest common right divisor, cf. (Ore, 1933)) Then $\mathrm{GCRD}(f, R) = R$ because d is minimal. We conclude that R is a right-hand factor of f. If $d < n$ a non-trivial factorization is obtained this way.

There are two ways of choosing the number d. The first is to try all values $d = 1, 2, \ldots, n - 1$. Suppose that for a certain d we find an R that has r as a right-hand factor and for numbers smaller than d such R could not be found. Then d is minimal and hence R is a right-hand factor of f. The second approach to take $d = n - 1$. If we find $R = a_d\partial^d + \cdots + a_0\partial^0$ that has r as a right-hand factor we can compute $\mathrm{GCRD}(R, f)$. This way we also find a right-hand factor of f. Sometimes it is possible to conclude a priori that there is no right-hand factor of order $n-1$. If for instance all irreducible local factors have order ≥ 3 then the order of a right-hand factor is $\leq n-3$ and so we can take $d = n-3$ instead of $d = n-1$.

We can compute a bound N (cf. section 9) for the degrees of the a_i. So the problem now is

> Are there polynomials $a_i \in k[x]$ of degree $\leq N$, not all equal to 0, such that r is a right-hand factor of $R = a_d\partial^d + \cdots + a_0\partial^0$?

Let m be the order of r. Write $D = k((x))[\partial]$. The D-module D/Dr is a $k((x))$-vector space of dimension m with a basis $\partial^0, \partial^1, \ldots, \partial^{m-1}$. Write $\partial^0, \partial^1, \ldots, \partial^d$ on this basis as vectors $v_0, \ldots, v_d$ in $k((x))^m$. Now multiply $v_0, \ldots, v_d$ with a suitable power of x such that the v_i become elements of $k[[x]]^m$. r is a right factor of R if and only if

$$a_0v_0 + \cdots + a_dv_d = 0$$

in $k[[x]]^m$. This is a system of linear equations with coefficients in $k[[x]]$ which should be solved over $k[x]$. One way of solving this is to convert it to a system of linear equations over k using the bound N. A much faster way is the Beckermann-Labahn algorithm which was found first by Labahn and Beckermann, and later independently by Derksen (Derksen, 1994; Beckermann and Labahn, 1994). Their method is as follows

Sketch of the Beckermann-Labahn algorithm

- Let $M_i \subset k[x]^{d+1}$ be the $k[x]$-module of all sequences $(a_0, a_1, \ldots, a_d)$ for which $v(a_0v_0 + \cdots + a_dv_d) \geq i$. The "valuation" v of a vector is defined as the minimum of the valuations of its entries. The valuation of 0 is infinity.
- Choose a basis (as $k[x]$-module) of M_0.
- For $i = 1, 2, 3, \ldots$ compute a basis for M_i using the basis for M_{i-1}.

This sketch looks easy and the algorithm is short (Derksen's implementation is only a few kilobytes) but it is absolutely non-trivial. The difficult part is how to construct a basis for M_i from a basis for M_{i-1} in an efficient way. Labahn, Beckermann and Derksen give an elegant solution for this problem by computing a basis with a certain extra property. Given a basis for M_{i-1} with this property they are able to compute a basis for M_i in a very efficient way. Again this basis has this special property which allows the computation of M_{i+1} so one can continue this way.

Define the degree of a vector of polynomials as the maximum of the degrees of these polynomials. From the basis for M_i we can find a non-zero $A_i \in M_i$ with minimal degree. Suppose there exists a non-zero $R = a_d\partial^d + \cdots + a_0\partial^0 \in k[x, \partial]$ having r as a right-hand factor. Then there exists such R with all $\deg(a_i) \leq N$ where N is a bound we can compute, cf. section 9. So then there is a non-zero $(a_0, \ldots, a_d)$ of degree $\leq N$ which is an element of every M_i. Because of the minimality of $\deg(A_i)$ it follows that then $\deg(A_i) \leq N$ for all i. So whenever $\deg(A_i) > N$ for any i we know that there is no $R \in k(x)[\partial]$ of order d which has r as a right-hand factor.

Algorithm Construct R
For $i = 0, 1, 2, \ldots$ do

- Compute M_i and $A_i \in M_i$ of minimal degree.

- If $\deg(A_i) > N$ then RETURN "R does not exist".
- If $\deg(A_i) = \deg(A_{i-3})$ then

  Comment: the degree did not increase 3 steps in a row so it is likely that a right-hand factor is found.

  If $A_i = (a_0, \ldots, a_d)$ then write $R = a_d\partial^d + \cdots + a_0\partial^0$. Divide by a_d to make R monic. Test if R and f have a non-trivial right-hand factor in common. If so, return this right-hand factor, otherwise continue with the next i.

Suppose the algorithm does not terminate. Then $\deg(A_i) = B_1$ for all $i \geq B_2$ for some integers B_1 and B_2. Define $D_i \subset M_i$ as the k-vector space generated by all A_j with $j \geq i$. These D_i are finite dimensional k-vector spaces and $D_{i+1} \subset D_i$ for each i. Then there must be an integer i such that D_i is the intersection of all D_j. Let $(a_0, \ldots, a_d) = A_i$. This A_i is an element of every $D_j \subset M_j$ so the valuation of $a_0v_0 + \cdots + a_dv_d$ is $\geq j$ for any j. Then $a_0v_0 + \cdots + a_dv_d = 0$ so r is a right-hand factor of $a_d\partial^d + \cdots + a_0\partial^0$. Then we have a contradiction because this means that the algorithm will find a right-hand factor in step i. So the algorithm terminates.

In our implementation we use modular arithmetic to replace the computations in $\mathbb{Q}$ by computations modulo some prime power p^n. This works for sufficiently large p. If it appears during the computation that p is not high enough the computation will be re-done with a larger prime number. Rational numbers can be reconstructed from their modular images if we have taken sufficiently many and sufficiently large prime powers (the algorithm is called iratrecon in Maple, unfortunately no reference is given in the help page). If k is an algebraic extension of $\mathbb{Q}$ then elements of k are represented as polynomials over $\mathbb{Q}$ in one or more variables with a bounded degree. Then this modular arithmetic avoids the so-called "intermediate expression swell". If the transcendence degree of k over $\mathbb{Q}$ is more than 0 then modular arithmetic does not avoid intermediate expression swell. If we then still want to avoid expression swell we would need to substitute values in $\mathbb{Q}$ for transcendental elements of k to reduce the transcendence degree. For factors of order > 1 it is not clear if this will work, for the case of order 1 factors see the comments at the end of the next section.

7. Computing all first order right-hand factors

Our algorithm in sections 5 and 6 can find a non-trivial factorization for any operator which has a first order right-hand factor. However, it may not compute all first order right-hand factors. In this section we show how to combine Beke's method with our factorization method. With this combination we can:

1 Like Beke's algorithm compute all first order right-hand factors R.

2 Avoid checking an exponential number of different $\mu_*(R)$. In fact we will need to check at most order(f) different $\mu_*(R)$.

LEMMA 7.1. *If $f, L, R \in \overline{k}(x)[\partial]$ and $f = LR$ then $\gamma_1(f) \subset \gamma_1(L) \bigcup \gamma_1(R)$.*

Proof: Let $\partial - r$ be a right factor of f and let $y \neq 0$ be a solution of $\partial - r$. Then y is a solution of f. We must prove that $\mu_*(\partial - r)$ is in $\gamma_1(L)$ or $\gamma_1(R)$. If y is a solution of R then $\partial - r$ is a factor of R so $\mu_*(\partial - r) \in \gamma_1(R)$. If y is not a solution of R then $R(y)$ is a non-zero solution of L. Using the fact $y' = ry$ we can write derivatives of

y as multiples of y and hence $R(y) = ty$ for some $t \in \overline{k}(x)$. Now ty is a solution of L so $\partial - (ty)'/(ty) = \partial - t'/t - y'/y = \partial - t'/t - r$ is a right-hand factor of L. So $\mu_*(\partial - t'/t - r) \in \gamma_1(L)$ and $\mu_*(\partial - t'/t - r) = \mu_*(\partial - r)$ (cf. section 3.5).

□

LEMMA 7.2. *If* $f = \mathrm{LCLM}(f_1, \ldots, f_d)$ *and* $\mathrm{order}(f) = \sum_i \mathrm{order}(f_i)$ *with* $f, f_1, \ldots, f_d \in \overline{k}(x)[\partial]$ *then* $\gamma_1(f) = \bigcup_i \gamma_1(f_i)$.

Without the condition $\mathrm{order}(f) = \sum_i \mathrm{order}(f_i)$ the lemma need not hold. For example $f_1 = \partial \cdot (\partial - x)$ and $f_2 = (\partial - 1/(x-1)) \cdot (\partial - x)$.

Proof: $\bigcup_i \gamma_1(f_i) \subset \gamma_1(f)$ because every right-hand factor of every f_i is a right-hand factor of f. So we only need to show that $\gamma_1(f) \subset \bigcup_i \gamma_1(f_i)$.

First suppose $d = 2$. Suppose $\partial - r$ is a right-hand factor of f. We must show that $\mu_*(\partial - r)$ is in $\gamma_1(f_1)$ or in $\gamma_1(f_2)$. From the condition $\mathrm{order}(\mathrm{LCLM}(f_1, f_2)) = \mathrm{order}(f_1) + \mathrm{order}(f_2)$ it follows that f_1 and f_2 have no common right-hand factor. Then we can write $1 = g_1 f_1 + g_2 f_2$ for some $g_1, g_2 \in \overline{k}(x)[\partial]$ using the extended Euclidean algorithm. The solution space of f is a direct sum $V(f) = V(f_1) \bigoplus V(f_2)$. $g_1 f_1 + g_2 f_2$ is the identity and $g_2 f_2$ acts like the zero map on $V(f_2)$ hence $g_1 f_1$ acts like the projection map of $V(f)$ to $V(f_2)$. Similarly, if $y \in V(f)$ then $g_2 f_2(y) \in V(f_1)$ is the projection of y on the component $V(f_1)$. Let $y \in V(f)$ be a non-zero solution of the right-hand factor $\partial - r$ of f. $(g_1 f_1 + g_2 f_2)(y) = y$ so $g_1 f_1(y) \neq 0$ or $g_2 f_2(y) \neq 0$. Assume $g_1 f_1(y) \neq 0$, in the other case the proof works in the same way. Like in the proof of the previous lemma we can write $g_1 f_1(y) = ty$ for some rational function t. Then ty is a solution of f_2 and so $\partial - r - t'/t$ is a right-hand factor of f_2. $\mu_*(\partial - r) = \mu_*(\partial - r - t'/t) \in \gamma_1(f_2)$.

If $d > 2$ write $f = \mathrm{LCLM}(f_1, \mathrm{LCLM}(f_2, \ldots, f_d))$ and apply induction.

□

Algorithm compute the possible $\mu_*(R)$
Input: An operator $f \in k(x)[\partial]$.
Output: A set S with at most $\mathrm{order}(f)$ elements such that $\gamma_1(f) \subset S$.

1 If $\mathrm{order}(f) = 1$ then the problem is trivial.
2 If $\mathrm{order}(f) > 1$ then apply the factorization algorithm of section 5.

   (a) If no non-trivial factorization is found then f has no first order right factors so return the empty set.
   (b) If a factorization $f = LR$ is found then apply recursion on L and R and use lemma 7.1.
   (c) If a factorization of the form $f = L \cdot \mathrm{LCLM}(R_1, \ldots, R_d)$ is found then apply recursion on L and apply step 2d on $\mathrm{LCLM}(R_1, \ldots, R_d)$.
   (d) If an LCLM factorization $f = \mathrm{LCLM}(R_1, \ldots, R_d)$ is found then

      i If $\mathrm{order}(f) = \sum_i \mathrm{order}(R_i)$ then apply lemma 7.2. Note that if the $R_i \in \overline{k}(x)[\partial]$ are conjugated over k then it suffices to apply recursion on only R_1 because γ_1 of the other factors $R_2, \ldots, R_d$ can be obtained from $\gamma_1(R_1)$ by conjugation.

ii If $\mathrm{order}(f) < \sum_i \mathrm{order}(R_i)$ then compute the greatest common right divisor G_1 of R_1 and $\mathrm{LCLM}(R_2, \ldots, R_d)$. If G_1 is a non-trivial factor of R_1 then let $G_1, \ldots, G_n$ be the conjugates of G_1 over k. Then $f = L \cdot \mathrm{LCLM}(G_1, \ldots, G_n)$ for some L and so we can proceed as in case 2c. This recursion terminates because $\mathrm{order}(G_1) < \mathrm{order}(R_1)$. If G_1 is not a non-trivial factor then compute operators $\tilde{R}_i$, $i = 2, \ldots, d$ such that $V(\tilde{R}_i) = R_1(V(R_i))$. Then $f = \mathrm{LCLM}(\tilde{R}_2, \ldots, \tilde{R}_d) \cdot R_1$ and we can apply recursion.

Algorithm first order factors
Input: An operator $f \in k(x)[\partial]$.
Output: All first order right-hand factors $R \in \overline{k}(x)[\partial]$ of f.

1 Compute the set S from "algorithm compute the possible $\mu_*(R)$"
2 For each element of $s \in S$ do

(a) Construct an $r \in \overline{k}(x)$ such that $\mu_*(\partial - r) = s$. Note that this requires no computation because a factor $\partial - r$ with $\mu_*(\partial - r) = s$ has already been computed in a factorization that was done in "algorithm compute the possible $\mu_*(R)$".
(b) Compute a basis $y_1, \ldots, y_d$ of rational solutions of $S_r^*(f)$ and write the general rational solution as $c_1 y_1 + \cdots + c_d y_d$ where the c_i are undetermined constants.
(c) If $d \neq 0$ then $\partial - r - (c_1 y_1 + \cdots + c_d y_d)'/(c_1 y_1 + \cdots + c_d y_d)$ are right-hand factors of f parametrized by $(c_1, \ldots, c_d) \in P^{d-1}(\overline{k})$.

It follows that the set of $r \in \overline{k}(x)$ for which $\partial - r$ is a right-hand factor of f is a disjoint union of at most $\mathrm{order}(f)$ projective spaces.

The algorithm in sections 5, 6 only avoids intermediate expression swell if $k \subset \overline{\mathbb{Q}}$. If the transcendence degree of k is > 0 then the algorithm still works, but then it is much less efficient. We will explain below that finding first order factors of operators in $k(x)[\partial]$ can be reduced to finding first order factors of operators in $\overline{\mathbb{Q}}(x)[\partial]$. This is important for the efficiency because in this way intermediate expression swell can be avoided.

Suppose k is a field, finitely generated over $\mathbb{Q}$, of transcendence degree $d > 0$. We will briefly describe in the rest of this section how computing all first order right-hand factors over k can be reduced to the same problem over a field of transcendence degree $d-1$. We will only give the idea and skip the details. Suppose k is an algebraic function field $k = l(s,t)$, where l is of transcendence degree $d-1$, s is transcendental over l and t is algebraic over $l(s)$. Then there exists a regular point $(s,t) = (s_0, t_0) \in (\overline{l})^2$ on the corresponding curve such that the coefficients of f are in the local ring at this point. A regular point corresponds to a valuation v on k. For elements $c \in k$ we have $v(c) \geq 0$ if and only if c is in the local ring at this point. Such elements can be evaluated at the point (s_0, t_0). Denote this evaluation map by τ. If $c \in k$ with $v(c) \geq 0$ then $\tau(c) \in l(s_0, t_0) \subset \overline{l}$.

This valuation v can be extended to a (non-discrete) valuation on $\overline{k}$. It can be further extended to a valuation on $\overline{k}[x]$ by defining the valuation of an element of $\overline{k}[x]$ as the minimum of the valuations of its coefficients in $\overline{k}$. Then v can be extended to $\overline{k}(x)$ because this is the field of fractions of $\overline{k}[x]$. Now v can be extended to $\overline{k}(x)[\partial]$ by defining the valuation of an operator in $\overline{k}(x)[\partial]$ as the minimum of the valuations of its coefficients in $\overline{k}(x)$. One can verify that this is indeed a valuation, i.e. that for operators $f, g \in \overline{k}(x)[\partial]$ we have $v(f \cdot g) = v(f) + v(g)$. The evaluation map τ can be extended as well, if $g \in \overline{k}(x)[\partial]$

and $v(g) \geq 0$ then $\tau(g) \in \bar{l}(x)[\partial]$ can be defined (first extend τ to $\overline{k}[x]$, then to $\overline{k}(x)$ and then to $\overline{k}(x)[\partial]$).

Without loss of generality we may assume that f is monic (i.e. the coefficient of the highest power of ∂ in f is 1) and we only consider monic factors of f. We can choose the point (s_0, t_0) in such a way that the valuation of f is 0. A monic operator has valuation ≤ 0 because the valuation of the leading coefficient is $v(1) = 0$. If $f = LR$ with $L, R \in \overline{k}(x)[\partial]$ and L, R are monic then $v(f) = v(L) + v(R)$ and since the valuations of L and R are ≤ 0 we have $v(R) = 0$. So any monic right-hand factor R of f can be evaluated at the point $(s,t) = (s_0, t_0)$. In other words: if $f = LR$ with L, R monic then this factorization can be evaluated at the point (s_0, t_0) which gives the factorization $\tau(f) = \tau(L)\tau(R)$. Now we can reduce the problem of computing all first order right factors of f as follows: compute the right factors of $\tau(f)$, this gives $\gamma_1(\tau(f))$ (cf. section 3.5 for a definition). Now for any first order right-hand factor R of f we have a right-hand factor $\tau(R)$ of $\tau(f)$ so $\tau(\gamma_1(f)) \subset \gamma_1(\tau(f))$. Choose the point (s_0, t_0) in such a way that for any two different exponential parts of f the images under τ do not coincide. Then we can reconstruct $\gamma_1(f)$ from $\tau(\gamma_1(f))$. We do not know $\tau(\gamma_1(f))$, however. But we know that $\tau(\gamma_1(f))$ is a subset of $\gamma_1(\tau(f))$ so we can check each element of $\gamma_1(\tau(f))$ to see if it yields a factor of f. This way we find all first order right factors of f.

8. Several strategies for completing the algorithm

Suppose $f \in k(x)[\partial]$ and our factorization algorithm in sections 5, 6 and 7 produces no non-trivial factorization. Can we then stop the computation and conclude that f is irreducible? If order$(f) < 4$ or if there exist e, p such that $\mu_{e,p}(f) = 1$ (the algorithm computes all $\mu_{e,p}(f)$ so it knows when this case occurs) then the answer is yes. In the remaining cases we can apply the following approach that we will call the *exterior power method.* It is obtained from (Beke, 1894) combined with significant improvements (namely steps 3 and 4) given in (Tsarev, 1994; Bronstein, 1994).

1 Compute an operator $\wedge^d f \in k(x)[\partial]$ with the property that if $y_1, \ldots, y_d \in V(f)$ then the Wronskian of $y_1, \ldots, y_d$ is in $V(\wedge^d f)$. We will call $\wedge^d f$ the d-th exterior power of f (called Differentialresolvente in (Beke, 1894). These equations are often also called associated equations). The important property is that if

$$\partial^d + a_{d-1}\partial^{d-1} + \cdots + a_0\partial^0$$

is a right-hand factor of f then $\partial + a_{d-1}$ is a right-hand factor of $\wedge^d f$.

2 Compute all first order right-hand factors in $\overline{k}(x)[\partial]$ of $\wedge^d f$.

3 In (Tsarev, 1994) a method (based on Plücker relations) is given for deciding which order 1 factors of $\wedge^d f$ correspond to order d right-hand factors of f.

4 Use these first order factors to compute the factors of f of order d. An efficient way to do this step is given in (Bronstein, 1994).

For operators of order 4 this approach works quite well, for order 5 it is already quite costly, and for higher order it is usually infeasible unless the coefficients are very small. Step 2 can be done by section 7, or by Beke's method (cf. section 4 and (Beke, 1894), see (Bronstein, 1992; Grigor'ev, 1990; Schwarz, 1989) for variations on Beke's method). We will give a number of strategies to speed up step 2.

First we apply the factorization method from (van Hoeij, 1996) on f. If this produces a non-trivial factorization then we have gained something, we can apply recursion on the factors. But if no factorization is found we gain something as well, because then we can conclude by lemma 8.1 below that if f is reducible in $\overline{k}(x)[\partial]$ then it is reducible in $k(x)[\partial]$ as well. Hence we only need to compute first order factors of $\wedge^d$ in $k(x)[\partial]$ instead of $\overline{k}(x)[\partial]$. This information removes the main bottleneck (which is splitting field computations) of Beke's method for computing factors of order 1. But we can gain even more as follows. We first try our algorithm in section 6 on all singularities p and all exponential parts e. Note that such computations are usually cheaper than computations with $\wedge^d f$ because $\wedge^d f$ is a much larger expression than f. If we are lucky and find a factorization, then we can apply recursion. But if no factorization was found, then we gain something as well, namely then we know that for all e, p if $\mu_{e,p}(f) > 0$ then $\mu_{e,p}(L) > 0$ (otherwise a factorization would have been found) and in the same way $\mu_{e,p}(R) > 0$ (by applying the adjoint). Hence for every e, p we have $\mu_{e,p}(L) > 0$ if and only if $\mu_{e,p}(R) > 0$. The number of possible μ_* in section 4 that need to be considered in Beke's algorithm can be very large. However, with our information on the exponential parts of L and R we can skip a lot of different μ_*. The best case is if order$(f) = 4$. In this case L and R must be irreducible and have order 2 and furthermore $\mu_*(L) = \mu_*(R)$ (otherwise f would already have been factored). Then $\mu_*(R)$ is known, and hence by proposition 3.1 the type of $\partial + a_{d-1}$ is known (we had $R = \partial^d + a_{d-1}\partial^{d-1} + \cdots + a_0\partial^0$ and $d = 2$). We want to find $\partial + a_{d-1}$ as a right-hand factor of $\wedge^d f$, and since we know the only possible value of $\mu_*(\partial + a_{d-1})$ we can find $\partial + a_{d-1}$ by checking only 1 possibility in Beke's algorithm. So computing $\partial + a_{d-1}$ has been reduced to finding rational solutions. If order$(f) > 4$ then we can still significantly reduce the number of cases in Beke's algorithm in this way, but we can not reduce this number to 1 anymore.

LEMMA 8.1. *If $f \in k(x)[\partial]$ is irreducible in $k(x)[\partial]$ then it is completely reducible in $\overline{k}(x)[\partial]$.*

An operator is called *completely reducible* if it is an LCLM of irreducible (in $\overline{k}(x)[\partial]$) operators. So any irreducible (in $\overline{k}(x)[\partial]$) operator is completely reducible as well.

Proof: Let f_1 be an irreducible right factor of f in $\overline{k}(x)[\partial]$. Let $f_1, \ldots, f_r$ be the conjugates (over the field extension $k \subset \overline{k}$) of f_1. Because conjugation commutes with differentiation we see that $f_1, \ldots, f_r$ are irreducible right factors of f. The Galois group of the extension $k \subset \overline{k}$ permutes the f_i hence LCLM$(f_1, \ldots, f_r)$ is invariant under this group. Then this LCLM is a factor of f in $k(x)[\partial]$ and hence equal to f because f is irreducible in this ring.

□

9. A bound for the degrees

Let $f \in k(x)[\partial]$ be given. Let $R = \partial^n + a_{n-1}\partial^{n-1} + \cdots + a_0\partial^0 \in \overline{k}(x)[\partial]$ be a right-hand factor of f. The topic of this section is to compute bounds for the degrees of the numerators and denominators of the a_i. These bounds are known when

- For every a_i and for every singularity p of f and the point $p = \infty$ we have a lower bound for the valuation of $l_p(a_i) \in \overline{k}((x))$.

- We have an upper bound for the number of *extra singularities*. A point $p \in \overline{k}$ is called an extra singularity of the factorization $f = LR$ if f is regular at p and R is singular at p.

The bounds in the first item are obtained from the relation $N(f) = N(L) + N(R)$ (cf. section 3.3 in (vH, Formal Solutions)). The valuation of the a_i at the extra singularities is also bounded by this relation. So all that is still needed is an upper bound for the number of extra singularities.

9.1. The number of extra singularities

It is known that the number of extra singularities can be bounded using *Fuchs' relation*. This relation says that the sum of the residues is zero (cf. lemma 9.2). In this section we will relate these residues to the list of generalized exponents. The list of generalized exponents of a right-hand factor R of f is a sublist of the list of generalized exponents of f. This gives us a method to bound the residues of R at the singular points of f. The residues at the extra singularities are negative integers. Hence, since the sum of the residues is zero, the number of extra singularities is bounded by the sum of the residues of R at the singularities of f. Note that the result in this section is similar to (Bertrand and Beukers, 1985). A difference is that we have a precise equation instead of a bound for $\mathrm{lres}(f)$ in lemma 9.3, resulting in a sharper bound for the number of extra singularities.

Definition 9.1. *Let* $f = a_n\partial^n + a_{n-1}\partial^{n-1} + \cdots + a_0\partial^0 \in k(x)[\partial]$ *with* $a_n \neq 0$. *Let* $p \in \overline{k}$. *Then the* residue $\mathrm{res}_p(f)$ *of* f *at the point* p *is defined as the residue of* a_{n-1}/a_n *at the point* p. *The residue* $\mathrm{res}_\infty(f)$ *of* f *at* ∞ *is defined as the residue of* $-x^2 a_{n-1}/a_n$ *at the point* ∞.

Let $f = a_n\delta^n + a_{n-1}\delta^{n-1} + \cdots + a_0\delta^0 \in k((x))[\delta]$ *with* $a_n \neq 0$. *Define the* local residue $\mathrm{lres}(f)$ *as the constant coefficient of* $a_{n-1}/a_n \in k((x))$.

Lemma 9.1. *Let* $f \in k(x)[\partial]$. *Let* n *be the order of* f. *If* $p \in \overline{k}$ *then* $\mathrm{res}_p(f) = \mathrm{lres}(l_p(f)) + 1 + 2 + \cdots + (n-1)$ *and if* $p = \infty$ *then* $\mathrm{res}_p(f) = \mathrm{lres}(l_p(f)) - (1 + 2 + \cdots + (n-1))$.

Proof: Without loss of generality we may assume that f is monic. Write $f = \partial^n + a_{n-1}\partial^{n-1} + \cdots + a_0\partial^0$. Suppose $p \in \overline{k}$. Then $l_p(f) = \partial^n + l_p(a_{n-1})\partial^{n-1} + \cdots + l_p(a_0)\partial^0 = (\frac{1}{x}\delta)^n + l_p(a_{n-1})(\frac{1}{x}\delta)^{n-1} + \cdots + l_p(a_0)$. The coefficient of δ^n in this expression is $1/x^n$ and the coefficient of δ^{n-1} is $l_p(a_{n-1})/x^{n-1} - (1 + 2 + \cdots + (n-1))/x^n$. So $\mathrm{lres}(l_p(f))$ is the residue at $x = 0$ of $l_p(a_{n-1})$ (which is the same as the residue at $x = p$ of a_{n-1}) minus $1 + 2 + \cdots + (n-1)$ and hence the lemma holds for $p \in \overline{k}$.

Now suppose $p = \infty$. $l_p(f) = (-x\delta)^n + l_p(a_{n-1})(-x\delta)^{n-1} + \cdots$. The coefficient of δ^n in this expression is $(-x)^n$ and the coefficient of δ^{n-1} is $(-x)^{n-1}l_p(a_{n-1}) + (-x)^n(1 + 2 + \cdots + (n-1))$. So the local residue is -1 times the coefficient of x^1 in $l_p(a_{n-1}) \in k((x))$ (this coefficient equals the residue of $l_p(a_{n-1})/x^2$ at $x = 0$ and this equals the residue of $x^2 a_{n-1}$ at $x = \infty$) plus $1 + 2 + \cdots + (n-1)$.

□

LEMMA 9.2. *Let* $f, g \in k(x)[\partial]$ *be monic and* $p \in P^1(\overline{k})$. *Then* $\mathrm{res}_p(fg) = \mathrm{res}_p(f) + \mathrm{res}_p(g)$. *If* $p \in \overline{k}$ *and* f *is regular at the point* p *then* $\mathrm{res}_p(f) = 0$. *Furthermore*

$$\sum_{p \in P^1(\overline{k})} \mathrm{res}_p(f) = 0$$

Proof: The proof of the first two statements is easy, we will skip it. Let $f = \partial^n + a_{n-1}\partial^{n-1} + \cdots + a_0\partial^0$. The third statement is easy to prove if a_{n-1} is of the form $(x-p)^m$ for some $p \in \overline{k}$ and $m \in \mathbb{Z}$. Now the statement follows because every $a_{n-1} \in \overline{k}(x)$ is a $\overline{k}$-linear combination of such expressions $(x-p)^m$.

□

Note that the relation $\mathrm{res}_p(fg) = \mathrm{res}_p(f) + \mathrm{res}_p(g)$ need not hold without the restriction that g is monic (take for example $f = \partial$, $g = x^5\partial$ and $p = 0$).

Let $e_1, \ldots, e_n \in E$. Define $B(e_1, \ldots, e_n)$ as the constant term in the expression $\sum_i e_i + \sum_{j>i} v'(e_i - e_j)$, where v' is defined in lemma 3.4.

LEMMA 9.3. *Let* $f \in k((x))[\delta]$ *and* $e_1, \ldots, e_n$ *the list of generalized exponents of* f. *Then* $\mathrm{lres}(f) = -B(e_1, \ldots, e_n)$.

Proof: $\mathrm{pp}(a_{n-1}) = -\sum_i \left(e_i + \sum_{j>i} v'(e_i - e_j)\right)$, cf. lemma 3.4. The local residue is the constant term of a_{n-1}. This equals the constant term of $\mathrm{pp}(a_{n-1})$, which is $-B(e_1, \ldots, e_n)$.

□

LEMMA 9.4. *Suppose* $f, L, R \in \overline{k}(x)[\partial]$ *are monic,* $f = LR$ *and* f *is regular at the point* $p \in \overline{k}$. *Then* R *is singular at* p *if and only if* $\mathrm{res}_p(R)$ *is a negative integer.*

Proof: We may assume $p = 0$. Let v be the usual valuation on $\overline{k}((x))$. Let n be the order of R and $b_1, \ldots, b_n \in \overline{k}[[x]]$ be a basis of formal solutions of R such that the valuations $v(b_1), \ldots, v(b_n)$ is the list of generalized exponents of R. Because f is regular the list of generalized exponents of f is $0, 1, \ldots, \mathrm{order}(f) - 1$. The list of generalized exponents $v(b_1), \ldots, v(b_n)$ of R is a sublist of this. Hence $B(v(b_1), \ldots, v(b_n))$ is an integer $\geq 0 + 1 + \cdots + (n-1)$. If R is regular then $B(v(b_1), \ldots, v(b_n)) = 0 + 1 + \cdots + (n-1)$. Conversely, if $B(v(b_1), \ldots, v(b_n)) = 0 + 1 + \cdots + (n-1)$ then (after a permutation) we have $v(b_i) = i - 1$, $i = 1, \ldots, n$. Furthermore $b_i \in V(f) \subset \overline{k}((x))$. Hence by lemma 9.2 in (vH, Formal Solutions) it follows that R is regular.

So R is singular if and only if $B(v(b_1), \ldots, v(b_n)) > 0 + 1 + \cdots + (n-1)$. $\mathrm{res}_0(R) = 1 + \cdots + (n-1) - B(v(b_1), \ldots, v(b_n))$ hence this is a negative integer if and only if R is singular.

□

Let $f \in k(x)[\partial]$ and R a right-hand factor of order d. Let S be the set of singularities of f and the point ∞. Let T be the set of extra singularities of R. So R is regular outside $S \bigcup T$ and hence the residue of R is 0 outside $S \bigcup T$. We want to find an upper bound for the number $\#T$ of extra singularities. Since the sum of the residues of R is zero we have

$$\sum_{p \in S}(\mathrm{res}_p(R)) = -\sum_{p \in T}(\mathrm{res}_p(R)) \geq \#T.$$

$\mathrm{res}_p(R)$ is determined by the list of generalized exponents of R at p which is a sublist of the list of generalized exponents of f at the point p. So for every p we have finitely many possibilities for $\mathrm{res}_p(R)$.

We search for a bound for the integer values that $\sum_{p \in S}(\mathrm{res}_p(R))$ can have. This is a rather difficult problem if k is a complicated field. To simplify the problem we will substitute values for the parameters appearing in k to reduce the transcendence degree of k to 0. Then the problem is the following: for each point p we have lists of generalized exponents of f in $\overline{\mathbb{Q}}[x^{-1/n}]$ for some n. Each sublist determines one of the residues that R can have in the point p. Every combination of the possible residues at all $p \in S$ must be added to see if the result happens to be an integer and we must find a bound that integer. This can require computing in algebraic field extensions over $\mathbb{Q}$ of an enormous degree. So we must further simplify the problem (note that this simplification can lead to a possibly higher bound, so the step we will make is not always the best thing to do). This simplification can be done in several ways. One way to eliminate these algebraic numbers is to replace each algebraic number by its image under the following $\mathbb{Q}$-linear map:

$$\Psi : \overline{\mathbb{Q}} \to \mathbb{Q}.$$

$\Psi(a)$ is defined as the trace of a over the field extension $\mathbb{Q} \subset \mathbb{Q}(a)$ divided by the degree of this extension (one should take into account the fact that this may alter the $v'(e_i - e_j)$). Another way is to compute with floating point approximations.

Now we need not compute in complicated constants fields anymore, but one problem remains, namely we must check a large number of different possibilities. To reduce this number we can bound each residue (which is a rational number after having applied Ψ) separately, add all these rational numbers and take the largest integer which is $\leq$ this sum. Similarly one can compute a bound for the image of the residue under Ψ without checking all sublists of the list of generalized exponents.

10. Factorization in other rings

The Labahn-Beckermann algorithm can be used to factor in other rings as well. For example the commutative ring $\overline{k}(x)[y]$. An element f in this ring can be factored by computing an irreducible local factor $l \in \overline{k}((x))[y]$ of f and constructing an $R \in \overline{k}(x)[y]$ of minimal degree such that l is a factor of R, in the same way as in section 6.

Another example is the ring of difference operators $\overline{k}(x)[\tau]$ where $\tau \cdot x = (x+1) \cdot \tau$. The only place on $P^1(\overline{k})$ where we can study the difference operators locally is $x = \infty$ because all other places on $P^1(\overline{k})$ (a place on $P^1(\overline{k})$ is a valuation on $\overline{k}(x)$) are not invariant under τ. One can compute local factorizations and define exponential parts and generalized exponents for difference operators in a very similar way as for differential operators. So we can apply the method from section 6 to the ring $\overline{k}(x)[\tau]$ as well. In the differential case the completeness of our algorithm in section 7 depends on the fact that we can choose a suitable singularity to apply our method from section 5 to. However, for the ring $\overline{k}(x)[\tau]$ we can not always choose a suitable singularity because $x = \infty$ is the only point we can take. As a consequence, our factorization algorithm for $\overline{k}(x)[\tau]$ is incomplete, even for factors of order 1.

References

Abramov A., Bronstein M., Petkovšek M., *On polynomial solutions of linear operator equations.* Proceedings ISSAC 95, ACM Press, 290-296, (1995).

Beckermann B., Labahn G., *A uniform approach for Hermite Padé and simultaneous Padé Approximants and their Matrix-type generalizations*, Numerical Algorithms, **3**, p. 45-54, (1992).

Beckermann B., Labahn G., *A uniform approach for the fast computation of Matrix-type Padé approximants*, SIAM J. Matrix Analysis and Applications, p. 804-823, (1994).

Beke E., *Die Irreduzibilität der homogenen linearen Differentialgleichungen*, Math. Ann. **45**, p. 278-294, (1894).

Bertrand D., Beukers F., *Équations différentielles linéaires et majorations de multiplicités*, Ann. scient. Éc. Norm. Sup. 4 série, t. 18, p. 181-192, (1985).

Bronstein M., *Linear Ordinary Differential Equations: breaking through the order two barrier.* Proceedings ISSAC 92, ACM Press, p. 42-48, (1992).

Bronstein M., *An improved algorithm for factoring linear ordinary differential operators.* Proceedings ISSAC 94, Oxford, U.K., ACM Press, p. 336-340, (1994).

Derksen H., *An algorithm to compute generalized Padé-Hermite forms* Manuscript. Available by ftp at daisy.math.unibas.ch in /pub/hderksen/pade.dvi (1994).

Grigor'ev D.Y., *Complexity of Factoring and Calculating the GCD of Linear Ordinary Differential Operators.* J. Symb. Comp. **10**, 7-37, (1990).

Hendriks P.A., van der Put M., *Galois action on solutions of a differential equation*, J. Symb. Comp. (1995).

van Hoeij M., *Formal Solutions and Factorization of Differential Operators with Power Series Coefficients*, to appear in J. Symb. Comp.

van Hoeij M., Weil J.A., *An algorithm for computing invariants of differential Galois groups*, to appear in J. of Pure and Applied Algebra.

van Hoeij M., *Rational Solutions of the Mixed Differential Equation and its Application to Factorization of Differential Operators*, Proceedings ISSAC'96, 219-225, (1996).

Kovacic J., *An algorithm for solving second order linear homogeneous differential equations*, J. Symb. Comp **2** p. 3-43 (1986)

Loewy A., *Über vollständig reduzible lineare homogene Differentialgleichungen*, Math. Ann., **62**, 89-117, (1906).

Ore O., *Formale Theorie der linearen Differentialgleichungen (Zweiter Teil)*, J. für d. Reine u. angew. Math., **168**, p. 233-252, (1932).

Ore O., *Theory of non-commutative polynomial rings*, Ann. of Math. **34** p. 480-508, (1933).

Schwarz F., *A factorization Algorithm for Linear Ordinary Differential Equations.* Proceedings of ISSAC 89, ACM Press, p. 17-25, (1989).

Singer M.F., *Liouvillian solutions of n-th order homogeneous linear differential equations.* Amer.J.Mat. **103**, p. 661-682, (1981).

Singer M.F., *An outline of differential Galois theory* In *Computer Algebra and Differential Equations*, Ed. E. Tournier, New York: Academic Press, (1990).

Singer M.F., *Liouvillian Solutions of Linear Differential Equations with Liouvillian Coefficients*, J. Symb. Comp. **11**, p. 251-273, (1991).

Singer M.F., *Testing Reducibility of Linear Differential Operators: A Group Theoretic Perspective*, Appl. Alg. in Eng. Comm. and Comp., **7**, p. 77-104, (1996).

Singer M.F., Ulmer F., *Galois groups for second and third order linear differential equations* J.Symb.Comp **16**, No. 1, p. 9-36. (1993)

Sommeling R., *Characteristic classes for irregular singularities*, Ph.D. thesis, University of Nijmegen. (1993).

Tsarev S.P., *On the problem of factorization of linear ordinary differential operators*, Programming & computer software, v. 20, **1**, p. 27-29, (1994).

Tsarev S.P., *An Algorithm for Complete Enumeration of All Factorizations of a Linear Ordinary Differential Operator*, ISSAC'96 Proceedings, (1996).

Weil J.A., *Constantes et polynômes de Darboux en algèbre différentielle : application aux systèmes différentiels linéaires*, PhD dissertation, École Polytechnique, (1995).