Rational Solutions of the Mixed Differential Equation and its Application to Factorization of Differential Operators

Mark van Hoeij
Department of mathematics
University of Nijmegen
6525 ED Nijmegen
The Netherlands
e-mail: hoeij@sci.kun.nl

March 27, 1996

Abstract

The topic of this paper is a fast method to compute the rational solutions of a certain differential equation that will be called the mixed differential equation. This can be applied to speed up the factorization of completely reducible linear differential operators with rational functions coefficients.

1 Introduction

A differential equation

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

corresponds to a differential operator of order n

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

acting on y. In the present 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 [12]. The equation $\partial x = x\partial + 1$ holds in this ring. We denote the solution space of f as $V(f)$. It is a $\overline{k}$ vector space of dimension order(f). One way to define $V(f)$ without ambiguity is to define it as a subset of the *universal extension*, cf. [7].

A factorization $f = LR$ where $L, R \in k(x)[\partial]$ is useful for computing solutions of f because the solutions $V(R)$ of the right hand factor R are solutions of f as well. Given L and R we can ask the following question: How can one compute (if it exists) an operator $R_2 \in k(x)[\partial]$ such that $V(f) = V(R) \bigoplus V(R_2)$? In section 3.1 it is shown how this question can be reduced to the mixed equation with $c = 1$. Such an operator R_2 could also be computed by one of the factorization algorithms for differential operators, cf. [4, 5, 9, 13]. However, these factorization algorithms can be quite costly so we want to have an alternative method.

The mixed equation (called *gemischte Gleichung* in [11]) is the following: Let L and R in $k(x)[\partial]$. We will assume that L and R are monic (i.e. the coefficient in $k(x)$ of the highest power of ∂ is 1). Let $c \in k(x)[\partial]$ with $\text{order}(c) < \text{order}(L)$. In the applications c is either 1 (cf. section 3.1) or 0 (cf. section 3.2). Compute the set of all $r \in k(x)[\partial]$ such that there exists an $l \in k(x)[\partial]$ with

$$Rr + lL = c. \tag{1}$$

We call this the mixed equation. An equivalent equation is

$$\text{RRem}(Rr, L) = c. \tag{2}$$

Here RRem stands for the remainder after a right hand division. Note that it is sufficient to compute only solutions r of order smaller than $\text{order}(L)$ because the other solutions are obtained from these by adding elements of $k(x)[\partial]L$. Therefore, we will restrict ourselves to solutions r with

$$\text{order}(r) < \text{order}(L).$$

The set of solutions of the mixed equation in the case $c = 0$ is called $\mathcal{E}_{\mathcal{D}}(R, L)$ in [14]. Singer gives a very interesting application of computing the set $\mathcal{E}_{\mathcal{D}}(f, f)$, namely the following: If $\mathcal{E}_{\mathcal{D}}(f, f)$ contains a non-constant element r then he shows how one can compute a non-trivial factor in $\overline{k}(x)[\partial]$ of f in an efficient way, cf. section 3.1 in [14]. We will give an example of this in section 3.2. If f is completely reducible then either $\mathcal{E}_{\mathcal{D}}(f, f)$ contains a non-constant element (and so f can be factored) or $\mathcal{E}_{\mathcal{D}}(f, f)$ is the set of constants and then f is irreducible. This will be the main application of the mixed equation.

Acknowledgments: I would like to thank J.A. Weil and S.P. Tsarev for useful discussions about these topics. It should also be noted that J.A. Weil has ideas (which have not yet been written down) for similar results about factoring completely reducible operators as well. Both approaches have their own advantages. The advantage of his approach is it can be applied to other problems as well. The advantage of the approach in this paper is that the algorithm is short and, even though the bound we give in proposition 1 is very technical, easier to implement (at least for the most important case $L = R$ and $c = 0$). A proper comparison between the two methods can be done when both methods are implemented. This will be done somewhere in 1996.

Outline of the paper: The part of this paper that is new is section 4. Sections 2 and 3 are not new, see also [11, 14]. These sections are intended as an introduction for section 4 and to give applications. Section 4.1 can be viewed as an introduction for section 4.2 because the result of section 4.1 is re-done more generally in section 4.2. The algorithm in section 4 for solving the mixed equation consists of two parts:

1. For each singularity $p \in P^1(\overline{k})$ compute a bound for the valuation at p of the coefficients in $k(x)$ of r.
2. Solve linear equations over k (a different approach is given in section 4 as well).

Computer algebra systems already have code for solving linear equations, so the only thing that needs to be implemented for solving the mixed equation is the bound in section 4.2.

An implementation of the algorithm (currently only the computation of $\mathcal{E}_{\mathcal{D}}(f, f)$ is implemented, but it is not much work to adapt this code for the case of a more general mixed equation) is available from
`http://www-math.sci.kun.nl/math/compalg/diffop/`

2 Preliminaries

This section lists a few facts that we use about differential operators. For a more complete introduction see [14]. In section 4.2 the reader is assumed to be familiar with section 3 in [9].

The *least common left multiple* $f = \mathrm{LCLM}(R_1, R_2)$ of two operators R_1 and R_2 is defined as the monic operator f with minimal order such that R_1 and R_2 are right hand factors of f. $V(f) = V(R_1) + V(R_2)$.

An operator f is called *completely reducible* if f is the LCLM of irreducible operators $R_1, \ldots, R_n$. Note that an irreducible operator is completely reducible as well.

The *greatest common right divisor* $R = \mathrm{GCRD}(f_1, f_2)$ of two operators f_1 and f_2 is defined as the monic operator R with maximal order such that R is a right hand factor of both f_1 and f_2. $V(R) = V(f_1) \bigcap V(f_2)$. By the Euclidean algorithm (cf. [12]) one can find two operators g_1 and g_2 such that

$$R = g_1 f_1 + g_2 f_2$$

and $\mathrm{order}(g_1) < \mathrm{order}(f_2)$. If $R = 1$ then the pair g_1, g_2 is uniquely determined. This can be shown as follows: If there were two different pairs then the difference h_1, h_2 of these pairs would satisfy the equation $h_1 f_1 + h_2 f_2 = 0$ and $\mathrm{order}(h_1) < \mathrm{order}(f_2)$. Then $V(f_2) \subset V(h_1 f_1)$ so $f_1(V(f_2)) \subset V(h_1)$. However, f_1 is injective on $V(f_2)$ because $V(f_1) \bigcap V(f_2) = V(R) = 0$ so $\mathrm{order}(h_1) = \dim(V(h_1)) \geq \dim(f_1(V(f_2))) = \dim(V(f_2)) = \mathrm{order}(f_2)$ which is a contradiction.

A *valuation* on a ring R is a map $v : R \to \mathbb{Z} \bigcup \{\infty\}$ (other additive groups than $\mathbb{Z}$, such as $\mathbb{Q}$, are allowed as well) such that $v(0) = \infty$, $v(fg) = v(f) + v(g)$ for all $f, g \in R \setminus \{0\}$. Furthermore $v(f+g) \geq \min(v(f), v(g))$ and $v(f+g) = \min(v(f), v(g))$ if $v(f) \neq v(g)$. One can define different valuations on the ring of local (i.e. power series coefficients) differential operators, cf. section 2 in [8]. The valuation of a power series $a \in k((x)) \setminus \{0\}$ is defined as the smallest n for which the coefficient of x^n in a is non-zero. The valuation of a non-zero rational function $a \in k(x) \setminus \{0\}$ at a point $p \in P^1(\overline{k}) = \overline{k} \bigcup \{\infty\}$ is defined as follows: If $p = \infty$ then the valuation of a at p is the degree of the denominator minus the degree of the numerator. If $p \in \overline{k}$ then the valuation of a at p is defined as the integer n for which $b = a/(x-p)^n$ has no pole at p and $b(p) \neq 0$. Suppose that B_p for $p \in P^1(\overline{k})$ are given integers for which $B_p \neq 0$ for only finitely many p and that $N \geq 0$ where $N = \sum B_p$. Then the set of all a in $\overline{k}(x)$

for which the valuation of a at p is $\geq -B_p$ is a $\overline{k}$ vector space of dimension $N+1$. The elements of this vector space are of the form n/D where $D \in \overline{k}(x)$ can be determined from the B_p and where $n \in \overline{k}[x]$ is a polynomial of degree $\leq N$.

In section 3.1 in [14] Singer gives three methods for computing $\mathcal{E}_{\mathcal{D}}(f,f)$. We will write here the first method (this method is computationally very costly, however. That is why we give an alternative method in section 4.) because we can draw two useful conclusions from this method. Let $n = \text{order}(L)$ and $m = \text{order}(R)$. Write $r = r_0\partial^0 + \ldots + r_{n-1}\partial^{n-1}$ where the r_i are indeterminates. Write $c = c_0\partial^0 + \ldots + c_{n-1}\partial^{n-1}$. Now $\text{RRem}(Rr, L)$ is a $k(x)$ linear combination of the r_i and the derivatives of the r_i. The highest derivative of r_i that appears in $\text{RRem}(Rr, L)$ is $r_i^{(m)}$. This $r_i^{(m)}$ only appears in the coefficient of ∂^i in $\text{RRem}(Rr, L)$ and the coefficient of $r_i^{(m)}$ in that expression is 1 (we use that R is monic). So equation 2 is equivalent with the following set of differential equations

$$\{r_i^{(m)} + \ldots = c_i | 0 \leq i \leq n-1\}$$

where the dots stand for $k(x)$ linear expressions in $r_j^{(m')}$, $j \in \{0, \ldots, n-1\}$, $m' \in \{0, \ldots, m-1\}$. If $c \neq 0$ then this system is not homogeneous. To make it homogeneous we add one extra variable z, one equation $z' = 0$, and replace the c_i by zc_i. We can convert this system to a system of first order equations by introducing new indeterminates $r_{i,j}$ for the j'th derivative of r_i and adding the equations $r_{i,j+1} = r'_{i,j}$. This way we obtain a system of equations of the form

$$Ay = y' \tag{3}$$

where A is a $nm+1$ by $nm+1$ matrix (if $c = 0$ then nm instead of $nm+1$ because then z is not needed) over $k(x)$ and y is a vector consisting of the $r_{i,j}$ and z. Such a matrix differential equation can be reduced to a single equation of order $nm+1$ (or nm if $c = 0$) by a cyclic vector computation and can then be solved, see [1] for computing rational solutions of a differential operator. We note the following:

Remark 1. If $p \in \overline{k}$ is a regular point for L, R and the c_i have no pole at p then the matrix A has no pole at the point p. If the vector y would have a pole of order t at the point p then the pole order of y' would be $t+1$, but the pole order of Ay is $\leq t$. This contradicts $Ay = y'$ so y (and hence the r_i as well) have no pole at the point p.

Remark 2. Every basis of the solutions y of equation 3 over $k(x)$ is a basis of solutions y over $\overline{k}(x)$ as well. Hence, for the mixed equation, to compute a basis for the solutions $r \in \overline{k}(x)[\partial]$ it suffices to compute a basis for the solutions $r \in k(x)[\partial]$.

3 Applications of the mixed equation

3.1 Computing a complement of $V(R)$

Let $f = LR$ where $f, L, R \in k(x)[\partial]$ are monic and suppose there exists a different factorization $f = L_2R_2$ in $\overline{k}(x)[\partial]$ such that $V(f) = V(R) \bigoplus V(R_2)$. We assume that the operators f, L, R, L_2 and R_2 are monic. The greatest common right divisor $\text{GCRD}(R, R_2)$ of R and R_2 must be 1 because R and R_2 have no common non-zero solutions. Then, by the Euclidean algorithm, it follows that

$$rR + r_2R_2 = 1$$

for some $r, r_2 \in \overline{k}(x)[\partial]$ which are uniquely determined under the condition order$(r) <$ order(R_2) (note that order(R_2) = order(L)).

The map $rR + r_2R_2 = 1$ is the identity and the map r_2R_2 acts like the zero map on $V(R_2) \subset V(f)$. Hence the map rR acts like the projection of $V(f)$ to $V(R_2)$. So rR acts like the identity on $V(R_2)$. Now R maps $V(f)$ onto $V(L)$, the kernel is $V(R)$ hence R is a bijection from $V(R_2)$ to $V(L)$. So r is the inverse bijection from $V(L)$ to $V(R_2)$. Hence Rr acts like the identity on $V(L)$, then $Rr - 1$ maps $V(L)$ to 0 so L must be a right hand factor of $Rr - 1$. In other words

$$Rr + lL = 1 \tag{4}$$

for some $l \in \overline{k}(x)[\partial]$. R_2 can be constructed from r using the equation $V(R_2) = r(V(L))$ as follows: Write $z = r(y)$. We can write the derivatives of z as vectors over $\overline{k}(x)$ on the basis $y, y', \ldots, y^{(n-1)}$ (the higher order derivatives of y can be simplified using the relation $L(y) = 0$). Here $n =$ order(L). The n'th derivative of z must be $\overline{k}(x)$ linearly dependent on the lower order derivatives $z, z', \ldots, z^{(n-1)}$. Computing this linear dependence gives R_2.

So: *computing the set of monic operators R_2 with the property $V(f) = V(R) \bigoplus V(R_2)$ is equivalent with solving the mixed equation for $c = 1$.* These monic R_2 are in 1-1 correspondence to the solutions r of this mixed equation. Because of remark 2 in section 2 the existence of such an $R_2 \in \overline{k}(x)[\partial]$ is equivalent with the existence of such an $R_2 \in k(x)[\partial]$.

3.2 Singer's Factorization method

In this section we describe a factorization method of Singer (cf. section 3.1 in [14]) and show in an example how to combine Singer's method with the method from section 4. Note that our f and r are called L and R in [14], we call this f and r to be consistent with the rest of our paper.

Suppose the dimension of $\mathcal{E}_{\mathcal{D}}(f, f)$ is more than 1. Then we can take an element $r \in \overline{k}(x)[\partial]$ in $\mathcal{E}_{\mathcal{D}}(f, f)$ which is not a constant (we always take r of order $<$ order(f)).

Now r is a $\overline{k}$ linear map from $V(f)$ to $V(f)$. We can compute a basis of $V(f)$ by computing formal solutions of f at a point (this is easiest at a regular point). Then compute the matrix of the map r in this basis and take an eigenvalue $a \in \overline{k}$. Then GCRD$(f, r - a) \in \overline{k}(x)[\partial]$ is a non-trivial factor of f. Note that for $f \in k(x)[\partial]$ with $\dim(\mathcal{E}_{\mathcal{D}}(f, f)) > 1$ the only algebraic extension that is used over k to compute a right hand factor is the eigenvalue a.

Example: Given is the following differential operator

$$f = \partial^4 + \frac{6}{x}\partial^3 + \frac{2(x^2-1)}{x^4}\partial^2 - \frac{2(3x^2-1)}{x^5}\partial + \frac{1}{x^8}$$

which is the LCLM of two irreducible operators in $\overline{\mathbb{Q}}(x)[\partial]$. The problem is to find a right hand factor of f. $\mathcal{E}_{\mathcal{D}}(f, f)$ is the set of operators r of order $<$ order(f) such that

$$fr + lf = 0$$

for some $l \in \overline{\mathbb{Q}}(x)[\partial]$. In section 4 we will compute the solutions r of order $<$ order(f) of this mixed equation. The solution space is 2 dimensional. Hence we can choose a

non-constant solution:

$$r = -x^5\partial^3 - x^4\partial^2 + 2x^3\partial + x\partial.$$

Now we need a basis for $V(f)$. We choose a basis $b_1, \ldots, b_4 \in \mathbb{Q}((x-1))$ of formal solutions at the point $x = 1$. These b_i are uniquely determined by requiring that $b_i \bmod (x-1)^4$ is $(x-1)^{i-1}$. The operator r acts on this basis as

$$\begin{pmatrix} 0 & 3 & -2 & -6 \\ 1 & 3 & -2 & 0 \\ -3/2 & 1/2 & 2 & -3 \\ 13/6 & -5/3 & 1/3 & 7 \end{pmatrix}.$$

The eigenvalues of this matrix are $3+\sqrt{2}$ and $3-\sqrt{2}$. From the eigenvalue $3+\sqrt{2}$ we obtain the following right hand factor of f

$$\mathrm{GCRD}(f, r - 3 - \sqrt{2}) = \partial^2 + \frac{\sqrt{2}}{x}\partial - \frac{1}{x^4}.$$

The other eigenvalue $3-\sqrt{2}$ gives the conjugate over $\mathbb{Q}$ of this factor.

Note that $\dim(\mathcal{E}_{\mathcal{D}}(f,f)) > 1$ implies that f is reducible but not that f is completely reducible. For example if $f = (\partial + 1/x)\partial$ then $r = x\partial \in \mathcal{E}_{\mathcal{D}}(f,f)$ (giving the right hand factor ∂) but f is not the LCLM of irreducible operators.

4 Solving the mixed equation

Write

$$r = \sum_{i=0}^{\mathrm{order}(L)-1} r_i \partial^i.$$

In section 2 we have seen that the r_i can not have a pole at a point $p \in \overline{k}$ if R, L and c have no pole at p. In section 4.1 (lemma 1) and section 4.2 (proposition 1 and the comments after proposition 1) we show how to compute a bound for the valuation of each r_i in the remaining places (i.e. the point ∞ and the points in $\overline{k}$ where R, L or c has a pole). Then we can write

$$r_i = \frac{n_i}{D_i}$$

with $n_i \in k[x]$ of degree $\leq N_i$ and $D_i \in k(x)$ where N_i and D_i are computed from the bounds. So given the bounds, we only need to determine the polynomials n_i. This can be done in several different ways:

- **Approach 1**. Write the n_i as a polynomials in x of degree N_i with undetermined coefficients. Then substitute r in the mixed equation and find linear equations for these undetermined coefficients. Solving these equations gives the solutions of the mixed equation.
- **Approach 2**.

  Let L_1 be an operator such that $V(L_1) = c(V(L))$. If $c = 0$ then take $L_1 = 1$, if $c = 1$ then $L_1 = L$. In the remaining cases L_1 can be obtained as follows: write $z = c(y)$ where y is a solution of L. Denote $n = \mathrm{order}(L)$. Using $L(y) = 0$ we

write the derivatives of z as $k(x)$ linear expressions in $y, y', \ldots, y^{(n-1)}$. Computing a $k(x)$ linear dependence between $z, z', \ldots, z^{(n)}$ gives L_1.

Compute a basis for $V(L)$ and a basis $z_1, \ldots, z_m$ for $V(L_1 R)$ (for example a basis of formal solutions at a regular point). Let $y \in V(L)$. Then $Rr(y) = c(y) \in V(L_1)$ so $r(y) \in V(L_1 R)$. Assume that all the D_i are equal to one polynomial D (if they are not polynomials we can take the numerator, and if they are not equal we can replace the D_i by the least common multiple). Then

$$r(y) = \frac{1}{D} \sum n_i \partial^i(y) \in V(L_1 R)$$

so

$$\sum n_i y^{(i)} = C_1 D z_1 + \ldots + C_m D z_m. \tag{5}$$

Here the n_i and C_i are polynomials in x with a bounded degree (the degree of the C_i is 0). The $y^{(i)}$ and Dz_i are power series in $x - p$ (if we computed the formal solutions at a regular point p). For each basis element y of $V(L)$ we obtain an equation of this form. The problem of computing all polynomials n_i and C_i satisfying the given conditions on their degrees, such that equation (5) holds up to a given accuracy $a \in \mathbb{N}$ (i.e. modulo $(x-p)^a$) is handled efficiently by the Beckermann-Labahn algorithm, cf. [6, 3]. A good guess for the accuracy a that is required to obtain solutions of the mixed equation is the sum of the degrees of the n_i plus the number of n_i and C_i. If we took the accuracy a too small then we find too many solutions, i.e. we find a basis $b_1, \ldots, b_t$ such that the solutions of the mixed equation form a subspace of the vector space spanned by $b_1, \ldots, b_t$. Then we can pick out the correct solutions from this vector space as follows: Substitute $r = c_1 b_1 + \ldots c_t b_t$, where the c_i are variables, in the mixed equation (2) and solve linear equations to find the right $c_1, \ldots, c_t$.

- **Approach 3**. One can compute the n_i from the formal solutions $r_i \in k((x-p))$ of the mixed equation where p is a regular point, in a way that is similar to the way that the rational solutions of a differential operator are obtained from the formal solutions in [1]. This way we have to solve linear equations over k in $\text{order}(L) \cdot \text{order}(R)$ variables.

4.1 The local bound problem, regular singular case

Define $\delta = x\partial$. The ring $k(x)[\partial]$ is a subring of the ring $k((x))[\partial] = k((x))[\delta]$. We can define a valuation (see also section 2 in [8])

$$v_0 : k((x))[\delta] \to \mathbb{Z} \bigcup \{\infty\}$$

as follows: For non-zero $f = \sum_{i,j} f_{i,j} x^i \delta^j$ the valuation $v_0(f)$ is the smallest i for which $f_{i,j} \neq 0$ for some j. For this f we can define the *Newton polynomial for slope 0* (see also section 3.4 in [8]) using a variable T as follows

$$N_0(f) = \sum_j f_{v_0(f),j} T^j \in k[T].$$

The substitution map

$$S_{T=T+i} : k[T] \to k[T]$$

is a k homomorphism defined by $T \to T + i$.

We recall a few facts about the Newton polynomial N_0

- degree$(N_0(f))$ = order(f) if and only if f is regular singular.
- The roots of $N_0(f)$ in $\overline{k}$ are called the *exponents* of f.
- For all L, R in $k((x))[\delta]$ we have

$$N_0(L \cdot R) = S_{T=T+v_0(R)}(N_0(L)) \cdot N_0(R).$$

Note that we assumed that L and R are monic in $k(x)[\partial]$. Then they are not monic when considered as elements of $k((x))[\delta]$.

The *local bound problem* is the following: Given are R, L and c in $k((x))[\delta]$ with order$(c) <$ order(L). Give a lower bound for $v_0(r)$ (or give for each coefficient of r in $k((x))$ a lower bound separately) for all solutions $r \in k((x))[\delta]$ of the mixed equation, i.e. for all r with order$(r) <$ order(L) for which there exists an $l \in k((x))[\delta]$ such that $Rr + lL = c$.

Lemma 1 Bound for $v_0(r)$ in the regular singular case. *Let R, r, l, L and c in $k((x))[\delta]$ with $Rr + lL = c$,* order$(c) <$ order(L), order$(r) <$ order(L), $R \neq 0$, $L \neq 0$ *and* $r \neq 0$. *Assume that L is regular singular. Then*

$$c \neq 0 \quad \text{and} \quad v_0(r) \geq v_0(c) - v_0(R)$$

or

$$\gcd(S_{T=T+v_0(r)}(N_0(R)), N_0(L)) \neq 1. \tag{6}$$

Proof: If $v_0(r) \geq v_0(c) - v_0(R)$ then $v_0(c)$ must be finite and so $c \neq 0$. Now assume $v_0(r) < v_0(c) - v_0(R)$. Then $v_0(Rr) < v_0(c) = v_0(Rr + lL)$. This is only possible if the lowest power of x in Rr and lL cancel against each other. Hence

$$N_0(Rr) + N_0(lL) = 0.$$

The assumption that L is regular singular means

$$\text{degree}(N_0(L)) = \text{order}(L).$$

Apply the multiplication formula for the Newton polynomials

$$\begin{aligned} 0 &= N_0(Rr) + N_0(lL) \\ &= S_{T=T+v_0(r)}(N_0(R)) \cdot N_0(r) + S_{T=T+v_0(L)}(N_0(l)) \cdot N_0(L). \end{aligned}$$

Because degree$(N_0(r)) <$ order$(L) =$ degree$(N_0(L))$ equation 6 follows.

□

Note that equation 6 can hold for only finitely many integers $v_0(r)$. So the minimum of these integers (and the integer $v_0(c) - v_0(R)$ if $c \neq 0$) is a lower bound for $v_0(r)$. The bound can be computed from $v_0(c)$, $v_0(R)$, $N_0(L)$ and $N_0(R)$.

4.2 The local bound problem, general case

We can generalize the valuation v_0 to $\overline{k((x))}[\delta]$ as follows: If $f \in \overline{k((x))}[\delta]$ then f is an element of $\overline{k}((x^{1/n}))[\delta]$ for some $n \in \mathbb{N}$. Write $f = \sum_i x^i f_i$ where $f_i \in \overline{k}[\delta]$ and where the sum is taken over $i \in \frac{1}{n}\mathbb{Z}$. If $f \neq 0$ then $v_0(f)$ is defined as the smallest i for which $f_i \neq 0$ and the Newton polynomial $N_0(f)$ is defined as this f_i (with δ replaced by the variable T).

Define the set $E = \bigcup_n \overline{k}[x^{-1/n}]$. In section 3.3 in [9] we have defined a valuation from a subset V_* of the universal extension V to the set E

$$v : V_* \to E$$

The map

$$\mathrm{Exp} : E \to V_*$$

is defined as $\mathrm{Exp}(e) = \exp(\int \frac{e}{x} dx)$. We have $v(\mathrm{Exp}(e)) = e$.

For a definition of the canonical list see [9]. The canonical exponential parts are the elements of this list. The multiplicity of a canonical exponential part is the number of times that it appears in the canonical list. For $e \in \overline{k((x))}$ the *substitution map*

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

is defined as the $\overline{k((x))}$ homomorphism given by $S_e(\delta) = \delta + e$.

Definition 1 *Let $e \in E$ and $f \in \overline{k((x))}[\delta] \setminus \{0\}$. Then the multiplicity $\nu_e(f)$ of the canonical exponential part e in f is defined as the multiplicity of the root 0 in $N_0(S_e(f))$.*

Note: $\nu_e(f)$ is not the same as the multiplicity of the exponential part $\mu_e(f)$, cf. section 3 in [9]. The exponential parts are the canonical exponential parts modulo a certain equivalence, hence their multiplicity $\mu_e(f)$ is $\geq$ the multiplicity $\nu_e(f)$ of the canonical exponential part. The sum of $\nu_e(f)$ taken over all $e \in E$ is the number of elements of the canonical list which is order(f).

The canonical exponential parts are a generalization of exponents. The exponents of an operator f are those canonical exponential parts which are in $\overline{k}$. An operator is regular singular if and only if all canonical exponential parts are exponents, i.e. if they are elements of $\overline{k}$.

Our approach for the general (i.e. not necessarily regular singular) case is quite technical. To explain the idea behind this approach we will first reformulate the approach of the previous section into the terminology of exponents instead of Newton polynomials. Then we can generalize by replacing the exponents by canonical exponential parts. If

$$Rr + lL = c \quad \text{and} \quad c = 0$$

and e is an exponent of L then e is an exponent of Rr as well. If the multiplicity of the exponent e in r is smaller than $\nu_e(L)$ then (the proof follows later in the more general case) $v_0(r) + e$ is an exponent of R. This must happen for at least one exponent e of L because if L is regular singular then the number of exponents e (counting with multiplicity) is more than the order of r. By comparing the exponents of R and L, and taking the smallest possible integer difference, we obtain a bound for $v_0(r)$. If $c \neq 0$ we have to consider the possibility $v_0(Rr) \geq v_0(c)$ as well.

If L is not regular singular (L is irregular singular) then the number of exponents e is not necessarily larger than order(r). And so the argument that $v_0(r)+e$ must be an exponent of R for some exponent e of L does not hold anymore. This problem can be fixed by using the canonical exponential parts instead of exponents. We will first relate the multiplicity $\nu_e(f)$ to a property *degl* of formal solutions. Denote

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

as in [8, 9].

Definition 2 *For an element $y \in \overline{V}_0$ define* $\mathrm{degl}(y)$ *as follows: y can be written as $y = \sum_{i,j} a_{ij} x^i \log(x)^j$ where the sum is taken over $j \in \mathbb{N}$ and $i \in \frac{1}{n}\mathbb{Z}$ for some $n \in \mathbb{N}$. Then* $\mathrm{degl}(y)$ *is the maximal j for which $a_{v(y),j} \neq 0$.*

Every element $y \in V_*$ is of the form $\mathrm{Exp}(e)z$ *for some $e \in E$ and $z \in \overline{V}_0$. Then* $\mathrm{degl}(y)$ *is defined as* $\mathrm{degl}(z)$.

Lemma 2 *Let $e \in \overline{k}$, $f = \delta - e + s$ with $s \in \overline{k((x))}$ and $v(s) > 0$ and $y \in \overline{V}_0 \setminus \{0\}$. If $e \neq v(y)$ then*

$$v(f(y)) = v(y) \quad \text{and} \quad \mathrm{degl}(f(y)) = \mathrm{degl}(y).$$

If $e = v(y)$ and $\mathrm{degl}(y) > 0$ *then*

$$v(f(y)) = v(y) \quad \text{and} \quad \mathrm{degl}(f(y)) = \mathrm{degl}(y) - 1$$

and if $e = v(y)$ and $\mathrm{degl}(y) = 0$ *then*

$$v(f(y)) > v(y).$$

The proof of the lemma is easy, we skip it. Note that $f(y) = 0$ is only possible in the case $e = v(y)$ and $\mathrm{degl}(y) = 0$.

Lemma 3 *Let $f \in \overline{k((x))}[\delta] \setminus \{0\}$, $y \in \overline{V}_0 \setminus \{0\}$ and $d = \mathrm{degl}(y)$. Let $e = v(y) \in \mathbb{Q}$ and $d' = \nu_e(f)$. If $d' \leq d$ then*

$$v(f(y)) = v_0(f) + v(y) \quad \text{and} \quad \mathrm{degl}(f(y)) = d - d'.$$

If $d' > d$ then

$$v(f(y)) > v_0(f) + v(y)$$

Note that $f(y) = 0$ is only possible in the case $d' > d$.

Proof: Factor (cf. section 5 in [8]) f as $f = L \cdot (\delta - e_1 + s_1) \cdots (\delta - e_n + s_n)$ where $v(s_i) > 0$, $e_1, \ldots, e_n \in \overline{k}$ are the exponents of f and L has no regular singular factor (i.e. L has no slope 0 in the Newton polygon). Then $v_0(f) = v_0(L)$. Denote $z = (\delta - e_1 + s_1) \cdots (\delta - e_n + s_n)(y) \in \overline{V}_0$. Now either $v(z) \in \mathbb{Q}$ or $z = 0$. d' is the number of i for which $e_i = v(y)$.

Assume $z \neq 0$. Write $L = L_0\delta^0 + \ldots + L_m\delta^m$. Now $v(L_i) > v(L_0)$ for $i > 0$ (because L has no slope 0) and $v(\delta^i(z)) \geq v(z)$ so $v(L_i\delta^i(z)) > v(L_0 \cdot z)$. Hence $v(L(z)) = v(L_0 \cdot z)$ and $\mathrm{degl}(L(z)) = \mathrm{degl}(L_0 \cdot z)$. Now $f(y) = L(z)$ so $v(f(y)) = v(L_0 \cdot z) = v(L_0) + v(z) = v_0(L) + v(z) = v_0(f) + v((\delta - e_1 + s_1) \cdots (\delta - e_n + s_n)(y))$ and $\mathrm{degl}(f(y)) = \mathrm{degl}(L_0 \cdot z) = \mathrm{degl}(z) = \mathrm{degl}((\delta - e_1 + s_1) \cdots (\delta - e_n + s_n)(y))$. Now the lemma follows by repeated use of the previous lemma.

□

Lemma 4 *Let $f \in k((x))[\delta]$. Then f has a solution y in V_* with* $\mathrm{degl}(y) = d$ *and $v(y) = e$ if and only if $e, e, \ldots, e$ ($d+1$ times) is a sublist of the canonical list of f (in other words: $\nu_e(f) > d$).*

The canonical list is defined up to permutations, so we can view it as a set with multiplicities. A solution in V_* with $\mathrm{degl}(y) = d$ means that the multiplicity of $v(y)$ in the canonical list is at least $d+1$, i.e. $\nu_{v(y)}(f) \geq d+1$. Note the following consequence of the lemma: If there exists a solution y with $v(y) = e$ and $\mathrm{degl}(y) > 0$ then there exists a solution z with $v(z) = e$ and $\mathrm{degl}(z) = \mathrm{degl}(y) - 1$. This can easily be shown in a different way as well, take $z = y - S_{\log}(y)$ where $S_{\log}$ is the map that replaces $\log(x)$ by $\log(x) + 1$, cf. section 9 in [8].

Proof: Let $y \in V_*$ with $\mathrm{degl}(y) = d$, $v(y) = e$ and $f(y) = 0$. Write $z = \mathrm{Exp}(-e)y$, so $v(z) = 0$ and $z \in \overline{V}_0 \setminus \{0\}$. We have $V(f) = \mathrm{Exp}(\mathrm{e}) \cdot V(S_e(f))$. So $S_e(f)(z) = 0$ and hence by lemma 3 it follows that $\nu_0(S_e(f)) > \mathrm{degl}(z) = d$. Since $\nu_e(f) = \nu_0(S_e(f))$ one part of the lemma follows.

Now suppose $\nu_e(f) > d$. We must prove that f has a solution in V_* with valuation e and degl d. Let $R \in k((x))[e, \delta]$ be the right hand factor of $S_e(f)$ of maximal order which is semi-regular (cf. section 3.2 in [9]) over $k((x))[e]$. Now $\nu_0(R) = \nu_0(S_e(f)) = \nu_e(f) > d$.

It is sufficient to prove that R has a solution y with valuation 0 and degl d, because then $\mathrm{Exp}(e)y$ is a solution of f with the desired property. Section 8.1 in [8] gives a recursive algorithm for computing a basis of solutions of R. This algorithm makes repeated use of integration $s_i = \int \frac{a_i}{x} dx$. In this integration process (we take the constant term in the integral equal to 0) we have $v(s_i) = v(a_i)$. Furthermore $\mathrm{degl}(s_i) = \mathrm{degl}(a_i)$ if $v(a_i) \neq 0$ and $\mathrm{degl}(s_i) = \mathrm{degl}(a_i) + 1$ if $v(a_i) = 0$. Using these relations and induction with respect to the order of R it follows that the algorithm in section 8.1 in [8] produces a solution y with valuation e and $\mathrm{degl}(y) = j$ for every exponent e of R and every integer j with $0 \leq j < \nu_e(R)$.

□

Lemma 5 *Let $f \in k((x))[\delta]$ be of order n and $e \in E$. Let v' be 0 if $e = 0$ and $v(e)$ otherwise (so $v' \in \mathbb{Q}$ and $v' \leq 0$). Let $d = v_0(S_e(f))$. Then d is an integer divided by the ramification index of e. The coefficient of δ^i in f has valuation $\geq d + (n-i)v'$.*

The proof of the lemma is easy, we skip it. The *ramification index* of e is defined as the smallest positive integer n such that $e \in \overline{k}((x^{1/n}))$.

Proposition 1 Bound for $v_0(S_e(r))$: *Let $Rr + lL = c$ where R, r, l, L, c in $k((x))[\delta]$ with $R \neq 0$, $L \neq 0$, $r \neq 0$,* $\mathrm{order}(c) < \mathrm{order}(L)$ *and* $\mathrm{order}(r) < \mathrm{order}(L)$.

Take an $e \in E$ with $\nu_e(L) > \nu_e(r)$. Take a solution $y \in V_*$ of L with $v(y) = e$ and $\mathrm{degl}(y) = \nu_e(L) - 1$. *Let $M = \infty$ if $c(y) = 0$ and $M = v(c(y)) - e \in \mathbb{Q}$ if $c(y) \neq 0$. Then*

$$c(y) \neq 0 \quad \text{and} \quad v_0(S_e(r)) = M - v_0(S_e(R))$$

or $v_0(S_e(r)) + e$ is in the canonical list of R.

Note: It is not a priori known which e we can take, i.e. which e satisfies equation (9). Also note that $\nu_e(L) > \nu_e(r)$ implies that $\nu_e(L) > 0$ in other words: e is in the canonical list of L.

In the two applications in section 3 we have $c = 0$ or $c = 1$. If $c = 0$ then $M = \infty$ so then the first case in the proposition can not occur. If $c = 1$ then $M = 0$. So in both applications the proposition can be used without computing a solution y with the desired property.

Proof:

$$Rr(y) = (Rr + lL)(y) = c(y).$$

Denote $z = \mathrm{Exp}(-e)y$ and $w = S_e(r)(z)$. Then $v(z) = 0$ and $\mathrm{degl}(z) = \mathrm{degl}(y) = \nu_e(L) - 1 \geq \nu_e(r) = \nu_0(S_e(r))$. Now $S_e(R)S_e(r) + S_e(l)S_e(L) = S_e(c)$ and z is a solution of $S_e(L)$ so

$$S_e(R)(w) = S_e(R)(S_e(r)(z)) = S_e(c)(z) \tag{7}$$

Now $S_e(c)(z) = \mathrm{Exp}(-e)c(y)$ so

$$v(S_e(R)(w)) = v(c(y)) - e = M.$$

By lemma 3 and $\mathrm{degl}(z) \geq \nu_0(S_e(r))$ it follows that

$$v(w) = v(S_e(r)(z)) = v_0(S_e(r)) + v(z) = v_0(S_e(r)). \tag{8}$$

According to lemma 3 and equation 7 there are two possibilities (if $M = \infty$ then the first case can not occur)

$$v(S_e(R)(w)) = v_0(S_e(R)) + v(w)$$

or $\nu_{v(w)}(S_e(R)) > \mathrm{degl}(w)$ which implies that $v(w)$ is an element of the canonical list of $S_e(R)$. The latter case implies that $v(w)+e$ is in the canonical list of R. So $v_0(S_e(r)) = v(w) = v(S_e(R)(w)) - v_0(S_e(R)) = M - v_0(S_e(R))$ or $v_0(S_e(r)) + e = v(w) + e$ is in the canonical list of R.

□

Note that both two cases imply a lower bound for $v_0(S_e(r))$. Since we do not know which of these two cases holds (unless $M = \infty$ then the first case can not occur) we have to take the minimum of these two bounds to obtain a lower bound for $v_0(S_e(r))$. In the case where $v_0(S_e(r)) + e$ is in the canonical list of R we obtain a lower bound for $v_0(S_e(r))$ by taking the minimal $m \in \frac{1}{\mathrm{ram}(e)}\mathbb{Z}$ for which $m + e$ is in the canonical list of R. Here $\mathrm{ram}(e)$ is the ramification index of e. Then by lemma 5 we obtain a lower bound for the valuation of the coefficients of r.

The order of an operator equals the sum of the ν_e taken over all $e \in E$. Since $\mathrm{order}(L) > \mathrm{order}(r)$ we must have

$$\nu_e(L) > \nu_e(r) \tag{9}$$

for at least one $e \in E$. Note, however, that we do not know for which e equation 9 holds. So to obtain a lower bound for the valuations of the coefficients of r we must take the minimum of these lower bounds for all canonical exponential parts e of L.

Example, continued from section 3.2: Now we will use the bound to compute the rational solutions r of the mixed equation in the example of section 3.2. We can write

$$r = \frac{n_3}{D_3}\partial^3 + \ldots + \frac{n_0}{D_0}\partial^0.$$

The only singularities of f are $x = 0$ and $x = \infty$. The point $x = 0$ is an irregular singularity so we must compute the canonical list:

$$\alpha - \frac{1}{x}, 2 - \alpha - \frac{1}{x}, \alpha + \frac{1}{x}, 2 - \alpha + \frac{1}{x}.$$

Here α is a root of the polynomial $1 - 4Z + 2Z^2$ (note that it is not necessary to compute all canonical exponential parts, it suffices to compute them up to conjugation). Now the smallest possible difference between canonical exponential parts which is an integer divided by the ramification index is 0. So we have $v_0(S_e(r)) \geq 0$ for some e in the canonical list. Then by lemma 5 it follows that the coefficient of δ^i in r (here r localized at the point $x = 0$, in δ notation instead of ∂ notation, cf. section 3.4 in [9]) has valuation $\geq i - 3$. Now we should convert this bound for the δ notation to a bound in ∂ notation. The result is that $r_i = n_i/D_i$ has valuation $\geq i - 3 + i$ at the point $x = 0$. So we can take $D_i = x^{3-2i}$ (D_i is not a polynomial if $i \geq 2$, however. In these cases the notion of the degree of D_i is problematic. But then we can simply interpret degree(D_i) as -1 times the valuation of D_i at the point infinity).

Now we want a lower bound for the valuation of r_i at infinity (i.e. an upper bound for degree(n_i) $-$ degree(D_i)). The operator f is regular singular at infinity and the Newton polynomial is $T^4 - 5T^2 + 2T = T(T-2)(T^2 + 2T - 1)$. Then by lemma 1 it follows that $v_0(l_\infty(r)) \geq -2$. Here $l_\infty(r)$ is r localized at infinity, cf. section 3.4 in [9]. We have to convert this to a bound for the valuation of r_i at infinity. The result is that the valuation of r_i at infinity is $\geq -2 - 2i$. This means degree(n_i) $-$ degree(D_i) $\leq 2 + 2i$. Hence degree(n_i) $\leq 2 + 2i +$ degree(D_i) $= 5$. So we can write r with $4 \cdot (5 + 1)$ undetermined coefficients. Twenty-four indeterminates is not very much so approach 1 in section 4, solving linear equations, will be efficient enough to be able to handle this example. These linear equations are obtained from RRem$(fr, f) = 0$.

References

[1] A. Abramov, M. Bronstein, M. Petkovšek *On polynomial solutions of linear operator equations*. Proceedings ISSAC 95, ACM Press, 290-296.

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

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

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

[5] M. Bronstein *Linear Ordinary Differential Equations: breaking through the order two barrier*. Proceedings ISSAC 92, ACM Press, 42-48.

[6] H. Derksen *An algorithm to compute generalized Padé-Hermite forms* Manuscript. Available by ftp at `daisy.math.unibas.ch` in `/pub/hderksen/pade.dvi`

[7] P. Hendriks, M. v.d. Put *Galois action on solutions of a differential equation*, Preprint, to appear in J. Symb. Comput.

[8] M. van Hoeij, *Formal Solutions and Factorization of Differential Operators with Power Series Coefficients*, University of Nijmegen Report nr. 9528, submitted to J. Symb. Comput, available at
`http://www-math.sci.kun.nl/math/compalg/diffop/`

[9] M. van Hoeij, *Factorization of Differential Operators with Rational Functions Coefficients*, University of Nijmegen Report nr. 9552, submitted to J. Symb. Comput, available at
`http://www-math.sci.kun.nl/math/compalg/diffop/`

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

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

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

[13] F. Schwarz *A factorization Algorithm for Linear Ordinary Differential Equations.* Proceedings of ISSAC 89, ACM Press, 17-25.

[14] M.F. Singer, *Testing Reducibility of Linear Differential Operators: A Group Theoretic Perspective*, To appear in J. of Appl. Alg. in Eng. Comm. and Comp.

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

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