ELSEVIER Journal of Pure and Applied Algebra 117 & 118 (1997) 353–379

JOURNAL OF
PURE AND
APPLIED ALGEBRA

An algorithm for computing invariants of differential Galois groups[1]

Mark van Hoeij[a,*], Jacques-Arthur Weil[b]

[a] Department of Mathematics, University of Nijmegen, 6525 ED Nijmegen, Netherlands

[b] Département Mathématiques, Faculté des Sciences, 123 Av. Albert Thomas, F-87060 Limoges, France

Abstract

This paper presents an algorithm to compute invariants of the differential Galois group of linear differential equations $L(y)=0$: if $V(L)$ is the vector space of solutions of $L(y)=0$, we show how given some integer m, one can compute the elements of the symmetric power $Sym^m(V(L))$ that are left fixed by the Galois group. The bottleneck of previous methods is the construction of a differential operator called the 'symmetric power of L'. Our strategy is to split the work into first a fast heuristic that produces a space that contains all invariants, and second a criterion to select all candidates that are really invariants.

The heuristic is built by generalizing the notion of exponents. The checking criterion is obtained by converting candidate invariants to candidate dual first integrals; this conversion is done efficiently by using a symmetric power of a formal solution matrix and showing how one can reduce significantly the number of entries of this matrix that need to be evaluated. © 1997 Published by Elsevier Science B.V.

1991 Math. Subj. Class.: 68Q40, 34A05, 13A50

1. Introduction

Let C be a field of characteristic 0 and $\overline{C}$ be its algebraic closure. Denote $k=\overline{C}(x)$ with the derivation $\partial=(\mathrm{d}/\mathrm{d}x)$. Let

$$L(y)=\sum_{i=0}^{n} a_i y^{(i)}=0, \quad a_n \neq 0, \; a_i \in C[x]$$

[*] Corresponding author. E-mail: hoeij@sci.kun.nl.

[1] The work in this paper was prepared in the Dutch NWO project AIDA.

PII S0022-4049(97)00018-2

denote a homogeneous linear differential equation of nth order. For such differential equations, there is a differential Galois theory analogous to that for polynomial equations. Let $y_1, \ldots, y_n$ be a basis of the vector space $V(L)$ of solutions. By adjoining the solutions $y_1, \ldots, y_n$ and all their derivatives to k, we get a differential field extension $K \supset k$ (called a Picard–Vessiot extension); the differential Galois group G of L (over k) is then defined as the group of k-automorphisms of the differential field K (i.e., k-automorphisms of K that commute with the derivation). The group G acts faithfully on the vector space $V(L)$, and so G can be viewed as a subgroup of $GL(V(L))$. It 'measures' the differential relations satisfied by the solutions of $L(y) = 0$ over k. One way to obtain information on G (and thus on the solutions) is to compute invariants:

Definition 1. An element v of some symmetric power $Sym^m(V(L))$ that is fixed by the differential Galois group G is called an invariant of G.

A standard method for computing invariants consists of building an operator $L^{\circledS m}$ (for a definition see Section 2.3) whose solution space is a G-homomorphic image of $Sym^m(V(L))$ and then search for rational solutions of this operator. Via differential Galois theory, one can (usually) reconstruct invariants from these rational solutions (see [23] for more details).

However, the computation of $L^{\circledS m}$ can be complicated for computers. For this and for other reasons (cf. Section 2.3) we will use the companion system of L, which we note $Y' = AY$. It is then easy to construct a system $Y' = S^m(A)Y$ whose solution space is *G-isomorphic* with $Sym^m(V(L))$. Our algorithm consists of finding rational solutions of the latter system under two guidelines: we do not perform a costly conversion into an equation and for efficiency we use as much as possible the structure of the system (i.e., the fact that it is a symmetric power of a companion matrix system).

In Section 2, we develop and motivate this approach and its links with the previous methods. Let F denote a rational (i.e., entries in $k = \overline{C}(x)$) solution of $Y' = S^m(A)Y$. Such an F will be called a *dual first integral*. In Section 3, we define generalized exponents of a local differential operator and show how to use these to compute bounds for the numerators of denominators of the entries of F. Let $Sym^m(\hat{U})$ denote the mth symmetric power matrix (definitions follow later) of $\hat{U}$, where $\hat{U}$ is a fundamental solution matrix of $Y' = AY$. Note that $Sym^m(\hat{U})$ can be computed from a basis $\hat{y}_1, \ldots, \hat{y}_n$ of formal solutions of L. Using the bounds from Section 3, we show in Section 4 how the evaluation of a finite number of terms of the series in $Sym^m(\hat{U})$ (plus linear algebra) yields all rational solutions of $Y' = S^m(A)Y$. Our strategy is first to design a fast heuristic to construct a space that contains all invariants (plus maybe some additional rubbish), then to convert these (candidate) invariants to (candidate) dual first integrals using the matrix $Sym^m(\hat{U})$. Then we check which candidate invariants are really invariants by checking which candidate dual first integrals are indeed dual first integrals. To do this conversion efficiently, we show how to reduce significantly the number of rows and columns of $Sym^m(\hat{U})$ that need to be evaluated.

The algorithm is implemented in MAPLE; an experimental code is available from the authors.

2. Invariants of differential Galois groups

In this section, we recall some basic facts and notation about the various ways to present the invariants of differential Galois groups. For more detailed introductions to differential Galois theory, unfamiliar readers could consult [3, 5, 13, 15, 17].

2.1. *Two presentations of the invariants*

If y is a generic solution of $L(y)=0$, we can form the vector

$$Y=(y,y',y'',\dots,y^{(n-1)})^{\mathrm{t}}.$$

This vector satisfies a first-order linear system $Y'=AY$, where A is the *companion matrix* of L. Let $y_1,\dots,y_n$ denote a basis, fixed once and for all, of the solution space $V(L)$ of $L(y)=0$. Then the vectors $Y_i=(y_i,y_i',y_i'',\dots,y_i^{(n-1)})^{\mathrm{t}}$ form a fundamental system of solutions of $Y'=AY$. This solution space is G-isomorphic with $V(L)$. The $n\times n$ matrix U whose columns are the Y_i is called a *fundamental solution matrix* for $Y'=AY$.

2.1.1. *Polynomial invariants*

It is well known [12] that $Sym(V(L))$ can be identified with the polynomial ring $\overline{C}[X_1,\dots,X_n]$, where $X_1,\dots,X_n$ are variables on which G acts the same as on $y_1,\dots,y_n$. Under this identification, we will say that a homogeneous polynomial P that is fixed by the Galois group is a *polynomial invariant*. In the sequel, the coefficients (in $\overline{C}$) of such a P will be referred to as the *vector of coefficients of the invariant*, or the *vector invariant*.

Let $f=P(y_1,\dots,y_n)\in K$. As P is an invariant, f is fixed by G. The differential Galois correspondence then implies that $f\in k$. We will call this f the *value* of P.

For an invariant in $Sym^m(V(L))$, the expression of P depends on the choice of the basis of $V(L)$. But the value f of the invariant is independent of this choice. For some applications, one just needs this value (for example, to compute algebraic solutions [21] or to solve second order equations [25]), and there, 'to compute an invariant' means 'to compute its value'. For other applications (to compute Liouvillian solutions [23]), one needs the expression of the polynomial invariant, together with its value.

2.1.2. *The symmetric power system*

Let y denote again a generic solution of $L(y)=0$, and let $\mu_{[m_1,\dots,m_n]} := y^{m_1}\cdot(y')^{m_2}\cdots(y^{(n-1)})^{m_n}$ (with $\sum m_i=m$) denote a differential monomial of degree m in y.

Then

$$\mu'_{[m_1,\dots,m_n]} = m_1\mu_{[m_1-1,m_2+1,\dots,m_n]} + \cdots + m_{n-1}\mu_{[m_1,\dots,m_{n-1}-1,\,m_n+1]}$$
$$+m_n\left(-\sum_{j=1}^{n}\frac{a_{j-1}}{a_n}\mu_{[\dots,m_j+1,\dots,m_n-1]}\right)$$

(with the convention that $\mu_{[\dots,-1,\dots]}=\mu_{[\dots,m+1,\dots]}=0$) so this derivative is a k-linear combination of monomials of degree m in the $y^{(i)}$. As there are $N=\binom{n+m-1}{n-1}$ such monomials, the vector

$$Y=(y^m,\dots,y^{(n-2)}(y^{(n-1)})^{m-1},(y^{(n-1)})^m)$$

of all such monomials satisfies an $N \times N$ system $Y'=S^m(A)Y$. Note that the matrix $S^m(A)$ is very sparse and that it is immediately given by the relations above. So it can be computed quickly, even for large n and m.

2.1.3. The symmetric power matrix

Let K be a field. The action of $g\in Gl_n(K)$ on K^n induces an action, denoted by $Sym^m(g)$, on the vector space $Sym^m(K^n)$. In other words, we have a group homomorphism $Sym^m : Gl_n(K)\rightarrow Gl(Sym^m(K^n))$. After having chosen a ordering on the monomials in $X_1,\dots,X_n$ of degree m, we can identify the vector space $Sym^m(K^n)$ with K^N (here N is the number of such monomials; $N=\binom{n+m-1}{n-1}$)). This way a group homomorphism

$$Sym^m : Gl_n(K)\rightarrow Gl_N(K). \qquad (1)$$

has been defined.

Remark 2. The above definition of $Sym^m(g)$ (which from now on will be considered as an element $Gl_N(K)$ instead of $Gl(Sym^m(K^n))$) depends on the ordering that was chosen for the monomials of degree m. It is irrelevant which ordering we choose, however, to have a consistent definition we must always use the same ordering. We will use the lexicographic ordering with $X_1<\cdots<X_n$.

The matrix $Sym^m(g)$ is called mth *symmetric power matrix* of the matrix g. We use the same symbol Sym^m for symmetric powers of vector spaces as well. We use the symbol S^m for the symmetric power of a differential system (cf. Section 2.1.2); Sym^m is not the same matrix construction as S^m and this is why we must use a different notation.

Remark 3. If g is the matrix (g_{ij}) then $Sym^m(g)$ can be computed as follows: Put $v_i = \sum_j c_j g_{ij}$ and Y is the vector[2] of monomials in the v_i. Then $Sym^m(g)_{r,s}$ is found from the rth entry of Y by taking the coefficient of the sth monomial in the c_j, multiplied by a multinomial coefficient. However, for convenience we will ignore this multinomial coefficient. This alters the definition of $Sym^m(g)$ by multiplying it with a diagonal non-singular matrix with integer entries.

2.2. Dual first integrals

Proposition 4. *Let A be the companion matrix of a differential operator L, let G be the differential Galois group and let W be the solution space of $Y' = S^m(A)Y$. There exists a G-isomorphism*

$$\lambda : Sym^m(V(L)) \to W.$$

Let U be a fundamental solution matrix of $Y' = AY$. Then the columns of $Sym^m(U)$ form a basis of W.

Proof. Let K be the Picard–Vessiot extension generated by the entries of U. From Remark 3 one can verify that $Sym^m(U)$ satisfies the equation $Y' = S^m(A)Y$. As Sym^m is a group homomorphism, $Sym^m(U)$ is an invertible matrix and hence the second statement follows.

The entries of $Sym^m(U)$ are in K, so $W \subset K^N$ and hence the Galois group G acts on W. Let $g \in G$. Because K is the base field in the construction of the homomorphism Sym^m in the previous section, automorphisms of K commute with Sym^m, i.e., $g(Sym^m(U)) = Sym^m(g(U))$.

The automorphism g acts on U as multiplication on the right with a matrix $\tilde{g} \in Gl_n(\overline{C})$. Let W_2 be the solution space of $Y' = AY$. The columns of U form a basis of W_2. On this choice of basis, the action of g on W_2 is given by the matrix $\tilde{g}$. The action of g on $V(L)$ is also the matrix $\tilde{g}$, where $U_{1,1}, \dots, U_{1,n}$ is chosen as a basis for $V(L)$. Then by definition of the matrix $Sym^m(\tilde{g})$, the action of g on $Sym^m(V(L))$ is given by the matrix $Sym^m(\tilde{g})$.

$$g(Sym^m(U)) = Sym^m(g(U)) = Sym^m(U \cdot \tilde{g}) = Sym^m(U) \cdot Sym^m(\tilde{g}).$$

So g acts on W as the matrix $Sym^m(\tilde{g})$, where the columns of $Sym^m(U)$ are chosen as basis for W. So the matrix of the action of g is the same for W as for $Sym^m(V(L))$, hence W is G-isomorphic with $Sym^m(V(L))$. □

We can describe λ more explicitly as follows. After choosing a basis $y_1, \dots, y_n$ of $V(L)$, or equivalently, after choosing a fundamental solution matrix U of $Y' = AY$, an

[2] Defining a vector of monomials implies choosing an ordering on the monomials, we take the same ordering as in Remark 2.

element of $Sym^m(V(L))$ can be represented as a homogeneous polynomial P in the variables $X_1,\dots,X_n$ of degree m. Let $\mathscr{C} \in \overline{C}^N$ be the vector of coefficients of P. Then

$$\lambda(P) = Sym^m(U)\cdot\mathscr{C} \in W. \tag{2}$$

Note that in fact both $Sym^m(V(L))$ and W are defined independently of a choice of basis $y_1,\dots,y_n$, and that $\lambda : Sym^m(V(L)) \to W$ is also independent of this choice.

Via λ, an invariant in $Sym^m(V(L))$ can be presented as an element $F \in W$ whose entries are left fixed by the Galois group; this is equivalent with saying that $F \in W \cap k^N$. An invariant given in this presentation (i.e., given as a rational solution F of $Y' = S^m(A)Y$) will be called a *dual first integral.*[3]

Lemma 5. *Let P be a polynomial invariant and let $\mathscr{C}$ be the vector of its coefficients. Then, $Sym^m(U)\cdot\mathscr{C}$ is a dual first integral.*

Conversely, let F be a dual first integral and let the vector $\mathscr{C}$ be such that $F = Sym^m(U)\cdot\mathscr{C}$. Then, $\mathscr{C}$ is the vector of coefficients of a polynomial invariant P. Moreover, the first entry of F is the value of P.

Proof. The first two statements follow from Eq. (2) and the fact that λ is a G-isomorphism. For the third statement note that the first row in $Sym^m(U)$ is the vector of all monomials in $y_1,\dots,y_n$. Hence, the first entry of F equals $P(y_1,\dots,y_n)$, i.e., P with y_i substituted for X_i. □

A different way to explain the relation between invariants and dual first integrals is given by the following proposition.

Proposition 6. *Let K be the Picard–Vessiot extension and G the differential Galois group of L. Define the $\overline{C}$-algebra homomorphism*

$$\phi : Sym(V(L)) \to K[X_1,\dots,X_n]$$

by (it suffices to define ϕ for homogeneous elements of degree 1)

$$\phi(y) = \sum_{i=1}^{n} X_i y^{(i-1)} \quad \textit{for } y \in V(L).$$

Then ϕ is an embedding (as $\overline{C}$-algebra and as G-module) of $Sym(V(L))$ in $K[X_1,\dots,X_n]$.

Proof. ϕ gives an embedding (as $\overline{C}$-vector space and as G-module) of $V(L)$ in $K\cdot X_1 + \cdots + K\cdot X_n$. Furthermore, if $y_1,\dots,y_n$ is a $\overline{C}$-basis of $V(L)$ then their images form a K-basis of $K\cdot X_1 + \cdots + K\cdot X_n$ because the Wronskian of $y_1,\dots,y_n$ has non-zero determinant. Hence, ϕ is an embedding of $Sym_{\overline{C}}(V(L))$ in $Sym_K(K\cdot X_1 + \cdots + K\cdot X_n) = K[X_1,\dots,X_n]$. □

[3] This name comes from the fact that solutions of the dual of $Y' = S^m(A)Y$ are first integrals for $Y' = AY$.

If we identify the K-vector space of homogeneous polynomials of degree m with K^N then the maps ϕ and λ from $Sym^m(V(L))$ to K^N coincide up to some diagonal matrix with integer entries (see also Remark 3).

2.3. Computational aspects

The operator whose solution space is spanned by all monomials of degree m in the y_i is noted $L^{\circledS m}$ and is called the mth *symmetric power of L*. Its solution space is a G-homomorphic image of $Sym^m(V(L))$ [20]; $V(L^{\circledS m}) = p(W)$ where $p : K^N \to K$ is the projection on the first component. The order of $L^{\circledS m}$ is $\leq N = \binom{n+m-1}{n-1}$ (the number of monomials of degree m in n variables); it is $<N$ if and only if there is a non-zero $P \in \overline{C}[X_1, \ldots, X_n]$, homogeneous of degree m, having value 0, i.e., $P(y_1, \ldots, y_n) = 0$. In this case it can happen that the value of a homogeneous polynomial P of degree m is in k even though P is not an invariant. If $order(L^{\circledS m}) = N$ then P is invariant if and only if its value is in k. So, the standard method for computing invariants is the following: replace L (if necessary) by an operator with an isomorphic solution space, in such a way that $L^{\circledS m}$ has the correct dimension N. Then the set of values of the invariants of degree m is the space of rational solutions of $L^{\circledS m}$, cf. [21, 23]. The usual method (given in [20]) to construct $L^{\circledS m}$ amounts to converting the system $Y' = S^m(A)Y$ to an equation by using the (putative) cyclic vector $(1, 0, \ldots, 0)$.

This method has three drawbacks. First, the cost of the computation of $L^{\circledS m}$ grows very fast with m and n (because we must perform elimination on systems whose size grows exponentially). So, in practice, the computation becomes rapidly impossible.

Secondly, if $L^{\circledS m}$ does not have the right order, then one has to perform a transformation on L and re-do the whole computation (though some information can be saved, see [26]).

And thirdly, for some applications, one indeed needs the invariant in the form of a dual first integral (e.g., [7]).

The first motivation of this paper was not to find a faster method, but a method that would work when computation of $L^{\circledS m}$ fails, and that would avoid the above drawbacks. The approach in this paper consists of solving directly the system $Y' = S^m(A)Y$, without converting it to an equation. For any point $x_0 \in \mathbb{P}^1(\overline{C})$, the system has a local formal fundamental solution matrix $Sym^m(\hat{U})$ where $\hat{U}$ is a local solution matrix of $Y' = AY$. The system $Y' = S^m(A)Y$ has a rational solution F (a dual first integral) if and only if there exists $\mathscr{C} \in \overline{C}^N$ such that $Sym^m(\hat{U})\mathscr{C} = F \in k^N$. We will use this in Section 4 to compute F. Thanks to Lemma 5, this will give us the invariants in all presentations at the same time.

3. Bounds on exponents using generalized exponents

This section addresses the question of finding the denominator and a bound on the numerator of each entry of a dual first integral F.

When computing rational solutions of a differential operator L, one first computes a lower bound for the integer exponents of L at each point $x_0 \in \mathbb{P}^1(\overline{C})$. We would like to compute rational solutions of symmetric powers (and other constructions) of differential operators. In the regular singular case, [22] give the bound for the integer exponents of symmetric powers $L^{\circledS m}$ in terms of the exponents of L. In the irregular singular case, however, we cannot obtain a bound for the integer exponents of $L^{\circledS m}$ from the exponents of L. The reason is that in this case there are "too few exponents": in the irregular singular case, there are, counted with multiplicity, less than *order*(L) exponents. To handle this difficulty we will use a generalization of exponents. An alternative way to get a bound (a different bound than ours) is found in Lemma 3.3 in [18] using a different generalization of exponents found in [4].

For convenience of notation we will now assume that the point of interest is the point $x=0$. Then L in $C(x)[\partial]$ is viewed as an element of the ring $C((x))[\delta]=C((x))[\partial]$, where

$$\delta = x\partial.$$

3.1. A few preliminaries on local differential operators

In this section we list a few known facts about local differential operators that will be used in later sections.

Definition 7. Let $L=\sum a_{i,j}x^i\delta^j \in C((x))[\delta]$ be non-zero and let T be a variable. Let v be the smallest integer such that $a_{v,j}\neq 0$ for some j. Then the Newton polynomial $N_0(L)$ for slope 0 of an operator L is defined as $\sum a_{v,j}T^j \in C[T]$.

If L can be written as a product $L=L_1\cdot L_2$ then $N_0(L_2)$ is a factor of $N_0(L)$. The Newton polynomial is used in algorithms for computing factorizations and/or formal solutions of differential operators. One defines a Newton polygon and for each slope in the Newton polygon a Newton polynomial can be defined. Definition 7 gives the Newton polynomial only for slope 0 in the Newton polygon. Definitions and properties of Newton polygons and polynomials can be found in [2, 10, 14, 24].

Definition 8. The *exponents* of L are those elements $e \in \overline{C}$ for which there is a solution of L of the form

$$x^e s \quad \text{where } s \in \overline{C((x))}[\log(x)] \quad \text{with } v(s)=0.$$

Here the valuation $v(s)$ is defined as the smallest rational number such that the coefficient of $x^{v(s)}$ in s is non-zero.

Note: If $s \in \overline{C((x))}[\log(x)]$ then $s \in \overline{C}((x^{1/r}))[\log(x)]$ for some integer r. The smallest r with this property is called the *ramification index* of s. The valuation $v(s)$ for $s \neq 0$ is the largest number in $\mathbb{Q}$ such that $sx^{-v(s)} \in \overline{C}[[x^{1/r}]][\log(x)]$. The valuation of 0 is ∞.

The following is a well-known property of exponents. It is generalized in Proposition 13.

Lemma 9. *An element $e \in \overline{C}$ is an exponent of L if and only if e is a root of $N_0(L)$.*

Note: In the literature exponents are often also called *indices*, and the Newton polynomial $N_0(L)$ is then called the *indicial polynomial* or *indicial equation.*

We denote the *linear universal extension* of $C((x))$ by V. This is a ring that contains $\overline{C((x))}$ and a basis of solutions of all homogeneous linear differential equations over $C((x))$. Furthermore, V is minimal with this property. A construction is given in [9], Lemma 2.1.1. From the way that V is constructed in [9] it follows that one can define a map

$$\mathrm{Exp}: \overline{C((x))} \rightarrow V$$

with the following properties: $\mathrm{Exp}(e)$ is a non-zero solution of $\delta - e$, $\mathrm{Exp}(q) = x^q$ for $q \in \mathbb{Q}$ and

$$\mathrm{Exp}(e_1 + e_2) = \mathrm{Exp}(e_1)\mathrm{Exp}(e_2)$$

for $e_1, e_2 \in \overline{C((x))}$, i.e., Exp behaves like an exponential function. One can think of $\mathrm{Exp}(e)$ as

$$\mathrm{Exp}(e) \text{ “ = ” } \exp\left(\int \frac{e}{x}\mathrm{d}x\right) \text{ “ = ” } x^e.$$

We have

$$\mathrm{Exp}(e) \in C((x)) \Leftrightarrow e \in \mathbb{Z} + x \cdot C[[x]]$$

and

$$\mathrm{Exp(e)} \in \overline{C((x))} \Leftrightarrow e \in \overline{C((x))} \cap \left(\bigcup_r \left(\frac{1}{r}\mathbb{Z} + x^{1/r} \cdot \overline{C}[[x^{1/r}]] \right) \right).$$

Definition 10. Define the substitution map

$$S_e : \overline{C((x))}[\delta] \rightarrow \overline{C((x))}[\delta]$$

for $e \in \overline{C((x))}$ as the $\overline{C((x))}$-homomorphism that maps δ to $\delta + e$.

The substitution map has the following well-known property: $\mathrm{Exp}(e)y$ is a solution of L if and only if y is a solution of $S_e(L)$.

3.2. Definition of generalized exponents

Using the substitution map, one can rewrite the standard property of exponents (Lemma 9) as follows:

Lemma 11. *Let $L \in \overline{C((x))}[\delta]\backslash\{0\}$. An element $e \in \overline{C}$ is an exponent of L if and only if 0 is a root of the Newton polynomial $N_0(S_e(L))$.*

With this lemma in mind, we can generalize the exponents by replacing the set $\overline{C}$ by a larger set of exponents E. Define

$$E = \bigcup_r \overline{C}[x^{-1/r}].$$

In the following definition we need to generalize Definition 7 to non-zero elements of $\overline{C((x))}[\delta]$. Take $q \in \mathbb{Q}$ minimal such that the coefficient of x^q in L is non-zero. Then $N_0(L)$ is this coefficient (which is in $\overline{C}[\delta]$) with δ replaced by the variable T.

Definition 12. Let $L \in \overline{C((x))}[\delta]\backslash\{0\}$. For an element $e \in E$ the number $v_e(L)$ is defined as the multiplicity of the root 0 in $N_0(S_e(L))$.

$e \in E$ is called a *generalized exponent*[4] of L if $v_e(L) > 0$. The number $v_e(L)$ is called the multiplicity of the generalized exponent e in the operator L.

Alternative approaches are found in the literature (e.g., [6, 16]). The exponents are those generalized exponents that are in $\overline{C}$.

The generalized exponent should not be confused with the definition of exponential part in Section 3.2 in [11]. A generalized exponent is an element of the set E, whereas an exponential part is an element of the set $E/\sim$. Here the equivalence $\sim$ is defined by

$$e_1 \sim e_2 \Leftrightarrow e_1 - e_2 \in \frac{1}{ram(e_1)}\mathbb{Z},$$

where $ram(e_1)$ is the ramification index of e_1. From the definition in Section 3.2 in [11], it follows that the multiplicity $\mu_{e_1}(L)$ of an exponential part e_1 equals the sum of the multiplicities $v_{e_2}(L)$ of the generalized exponents e_2 taken over all $e_2 \in E$ for which $e_2 \sim e_1$. So by Theorem 1 in [10], it follows that

$$\sum_{e \in E} v_e(L) = order(L). \tag{3}$$

Many mathematical and algorithmic difficulties with irregular singular operators are caused by the fact that for such operators there are (counted with multiplicity) “too few” exponents. Because of Eq. (3) these difficulties no longer exist when using generalized exponents; for our purposes the irregular singular case is not different from the regular singular case.

Computing the generalized exponents can be done using one of the several factorization algorithms. It is a subproblem of computing formal solutions, so the generalized

[4] A generalized exponent was called *canonical exponential part* in [11]. We changed this name to point out the use of this notion, which is to generalize methods that use exponents (for example, [22]) to the irregular singular case.

exponents can be computed using a part of the algorithm for computing formal solutions, cf. [2, 24]. We use "algorithm semi-regular parts" in [10]. This algorithm is a modified version of Malgrange's factorization algorithm [14]. It uses a different type of ramifications (obtained from [2]) to minimize the algebraic extensions.

The relation between generalized exponents and formal solutions is the following (this is Theorem 1 in [11]):

Proposition 13. *Let $L \in C((x))[\partial]\backslash\{0\}$. An element $e \in E$ is a generalized exponent of L if and only if L has a solution of the form*

$$\mathrm{Exp}(e)s \quad \textit{where} \quad s \in \overline{C((x))}[\log(x)] \quad \textit{and} \quad v(s) = 0.$$

Note that, instead of using a Newton polynomial, the generalized exponents can be defined from the formal solutions using this proposition. A different generalization of exponents by using formal solutions is found in [4].

3.3. Minimal exponents

As already mentioned, our reason for introducing generalized exponents was to obtain information about the exponents of $L^{\circledS m}$ without computing the operator $L^{\circledS m}$. Now a natural question arises: Given the generalized exponents of L at the point $x = 0$, can one determine all (generalized) exponents of $L^{\circledS m}$? The answer is negative, as showed by the following example.

Example 14. Consider the operators $L_1 = \partial^3 + x$ and $L_2 = \partial^3 + x + 1$. These operators are regular at $x = 0$. Hence both L_1 and L_2 have power series solutions with valuations 0, 1 and 2 at $x = 0$; the exponents at $x = 0$ are $0, 1, 2$ for both operators. Making products of these solutions, one finds solutions of $L_1^{\circledS 2}$ and $L_2^{\circledS 2}$ with valuations 0, 1, 2, 3, 4. Hence $L_1^{\circledS 2}$ and $L_2^{\circledS 2}$ will have at least the exponents 0, 1, 2, 3, 4 at $x = 0$. However, not all exponents of $L_1^{\circledS 2}$ and $L_2^{\circledS 2}$ have been determined by this. $L_2^{\circledS 2}$ is regular at $x = 0$, so it has exponents 0, 1, 2, 3, 4, 5. But $L_1^{\circledS 2}$ has exponents 0, 1, 2, 3, 4, 6 at $x = 0$ ($x = 0$ is an apparent singularity, i.e., all solutions are analytic). The conclusion of this example is that the exponents 0, 1, 2 determine the smallest exponents of the second symmetric power, but not necessarily all exponents.

Let M be a differential operator whose solution space is spanned by differential monomials in the solutions of L. If L is regular at a point $x = \alpha$ (where $\alpha \in \overline{C}$), then M need not be regular at $x = \alpha$. However, products, sums and derivatives of analytic functions are analytic, hence all local solutions of M at $x = \alpha$ are analytic. It follows that all generalized exponents of M at $x = \alpha$ are integers, bounded from below by 0. So in this section we only need to compute lower bounds for the exponents of M at the singularities of L and the point infinity. These remarks and the example suggest that, instead of trying to find all generalized exponents of symmetric powers of L, we should settle for a different goal, namely to compute the *minimal generalized exponents.*

Definition 15. Let r be a positive integer. Define the following partial ordering $\leq_r$ on E:

$$e_1 \leq_r e_2 \Leftrightarrow e_1 - e_2 \in \frac{1}{r}\mathbb{Z} \quad \text{and} \quad e_1 - e_2 \leq 0.$$

For a set $S \subset E$ define $min_r(S)$ as the set of minimal elements of S with respect to the ordering $\leq_r$.

For an element $L \in C((x))[\delta]\backslash\{0\}$ define $min_r(L)$ as $min_r(S)$ where S is the set of generalized exponents of L.

If L has an integer exponent $e \in \mathbb{Z}$ then $min_r(L) \cap \frac{1}{r}\mathbb{Z}$ contains at least one element which is $\leq e$. So if we can compute min_r for symmetric powers of L then we find lower bounds for the integer exponents of these symmetric powers. This is done by Proposition 17 below, using the following definition.

Definition 16. The *symmetric product*[5] of L_1 and L_2, denoted by $L_1 \circledS L_2$, is the monic differential operator of minimal order for which

$$y_1 y_2 \in V(L_1 \circledS L_2) \quad \text{for all } y_1 \in V(L_1), y_2 \in V(L_2).$$

The notation $L^{(i)}$ denotes the monic differential operator defined by

$$V(L^{(i)}) = \{\partial^i y \mid y \in V(L)\}.$$

Proposition 17. *Let L_1 and L_2 be non-zero elements of $C((x))[\delta]$. Let r be the least common multiple of all ramification indices of the generalized exponents of L_1 and L_2. Define for sets $S_1, S_2 \subset E$ the sum $S_1 + S_2$ as $\{s_1 + s_2 \mid s_1 \in S_1, s_2 \in S_2\} \subset E$. Then*

$$min_r(L_1 \circledS L_2) = min_r(min_r(L_1) + min_r(L_2)).$$

Corollary 18. *Let m be a positive integer and r be the ramification index of L. Denote for $S \subset E$ the set $m \cdot S$ as $S + S + \cdots + S$ (m times). Then*

$$min_r(L^{\circledS m}) = min_r(m \cdot min_r(L)).$$

In particular, if $L^{\circledS m}$ has an integer exponent e then $min_r(m \cdot min_r(L)) \cap \frac{1}{r}\mathbb{Z}$ contains one element which is a lower bound for e. This lower bound can be computed from r, m and $min_r(L)$.

Remark 19. The fact that such a lower bound exists is not new (Lemma 3.3 in [18]). However, the bound in our proposition is sharper. It gives precisely the smallest exponent of $L^{\circledS m}$ in $\frac{1}{r}\mathbb{Z}$. So in case all ramification indices are 1 (i.e., $r = 1$) our bound for the smallest integer exponent is sharp (see also Example 29).

[5] Strictly speaking, this name is mathematically hazy. We use it to emphasize the resemblance with the symmetric power construction $L^{\circledS m}$.

We postpone the proof of the proposition till after the proof of Theorem 21. To prove this theorem we first need to introduce some notation.

Denote[6] $V_e = \mathrm{Exp}(e) \cdot (\overline{C} \cdot C((x))[e])[\log(x)]$ as in [10,11]. Note that $\overline{C} \cdot C((x))[e] = \overline{C} \cdot C((x^{1/ram(e)}))$ where $ram(e)$ is the ramification index of e. We have $V_{e_1} = V_{e_2}$ if and only if $e_1 \sim e_2$ and (cf. Theorem 3 in [10])

$$V = \bigoplus_{e \in E/\sim} V_e. \tag{4}$$

Now define

$$E_r = \overline{C}[x^{-1/r}] \subset E \quad \text{and} \quad V_{*,r} = \bigoplus_{e \in E_r/\sim} V_e.$$

For $e \in E_r$ define

$$V_{e,r} = \mathrm{Exp}(e) \cdot (\overline{C} \cdot C((x^{1/r})))[\log(x)].$$

If $e_1 - e_2 \in \frac{1}{r}\mathbb{Z}$ then $V_{e_1,r} = V_{e_2,r}$ so $V_{e,r}$ can be defined for $e \in E_r/(\frac{1}{r}\mathbb{Z})$. $V_{e,r}$ is the direct sum of the V_{e_1} taken over all $e_1 \in E_r/\sim$ for which e is e_1 modulo $\frac{1}{r}\mathbb{Z}$. Hence by the direct sum in Eq. (4) it follows that

$$V_{*,r} = \bigoplus V_{e,r}, \tag{5}$$

where the sum is taken over all $e \in E_r/(\frac{1}{r}\mathbb{Z})$.

Definition 20. The *ramification index* $ram(L)$ of $L \in C((x))[\partial]$ is defined as the least common multiple of the ramification indices of all generalized exponents of L.

From Theorem 3 in [10], it follows that $V(L) \subset V_{*,r}$ if and only if $ram(L)$ divides r. $V_{*,r}$ is a differential ring extension of $\overline{C((x))}$ consisting of all solutions of all $L \in C((x))[\delta]$ for which $ram(L)$ divides r. Hence if the ramification indices of two operators L_1 and L_2 divide the integer r then the same holds for the operators $L_1 \circledS L_2$, $L_1^{(1)}$ (Definition 16) and for the least common left multiple of L_1 and L_2.

Theorem 21. *Let $L \in C((x))[\delta] \setminus \{0\}$ be of order d and let r be a positive integer. Suppose that the ramification indices of the generalized exponents divide the integer r.*

(i) *There exists a basis $y_1, \ldots, y_n$ of $V(L)$ which satisfies the following condition:*

$$y_i = \mathrm{Exp}(e_i) s_i \quad \textit{for some } s_i \in (\overline{C} \cdot C((x^{1/r})))[\log(x)],\ v(s_i) = 0 \tag{6}$$

where $e_1, \ldots, e_n \in E$.

(ii) *Suppose $y_1, \ldots, y_n$ is a basis of the solution space $V(L)$ which satisfies condition (6). Then*

$$min_r(L) = min_r(\{e_1, \ldots, e_n\}).$$

[6] Here $\overline{C} \cdot C((x))$ denotes the smallest subfield of the algebraic closure of $C((x))$ that contains both $\overline{C}$ and $C((x))$.

Proof. Let $e \in min_r(L)$. Since $\{e_1,\dots,e_n\}$ is a subset of the set of all generalized exponents of L (there are at most $order(L)=d$ different generalized exponents) it follows that the number of elements in $min_r(\{e_1,\dots,e_n\})$ cannot be larger than the number of elements in $min_r(L)$. So we only need to prove that $e \in min_r(\{e_1,\dots,e_n\})$. Without loss of generality, we may assume that $e_i - e \in \frac{1}{r}\mathbb{Z}$ for $i \leq t$ and $e_i - e \notin \frac{1}{r}\mathbb{Z}$ for $i > t$. We need to show that $t \neq 0$ and that there is one $i \leq t$ with $e_i - e \leq 0$. Then the theorem is proven as follows: We may assume that $e_i - e \in \frac{1}{r}\mathbb{Z}$ is minimal, so $e_i \in min_r(\{e_1,\dots,e_n\})$. Because of the minimality of e we cannot have $e_i - e < 0$ hence $e = e_i$.

The algorithm in Section 8.4 in [10] produces a basis $\tilde{y}_1,\dots,\tilde{y}_n$ of formal solutions (see also the proof of Theorem 1 in [11]) where each basis element can be written in the form $\tilde{y}_i = \mathrm{Exp}(\tilde{e}_i)\tilde{s}_i$ with $\tilde{s}_i \in C((x))[\tilde{e}_i, \log(x)]$ and $v(\tilde{s}_i)=0$ and where every generalized exponent $\tilde{e}_i$ of L occurs. Since $(C((x))[\tilde{e}_i])[\log(x)] \subset (\overline{C}\cdot C((x^{1/r})))[\log(x)]$ this basis satisfies condition (6). Furthermore, the generalized exponent e of L occurs in this basis so one of the elements of this basis is of the form $y = \mathrm{Exp}(e)s$ (with $s \in C((x))[e, \log(x)]$ and $v(s)=0$). Then $y \in V_{e,r}$ and $y \in V(L)$.

Because of condition (6), each y_i is an element of $V_{e_i,r}$. Since the y_i form a basis of $V(L)$, it follows that y is a $\overline{C}$ linear combination of $y_1,\dots,y_n$. Because of the direct sum in Eq. (5), it follows that y is a linear combination of $y_1,\dots,y_t$, since e_i for $i > t$ is not equal to e modulo $\frac{1}{r}\mathbb{Z}$ and so y_i is in a different component than $V_{e,r}$ for $i > t$. Dividing by $\mathrm{Exp}(e)$, we obtain that $s \in V_{0,r} = (\overline{C}\cdot C((x^{1/r})))[\log(x)]$ is a linear combination of the $\mathrm{Exp}(e_i - e)s_i \in V_{0,r}$ for $i \leq t$. Hence the valuation of at least one of the $\mathrm{Exp}(e_i - e)s_i$ is $\leq v(s) = 0$. The valuation of the s_i is 0 and the valuation of $\mathrm{Exp}(e_i - e) \in C((x^{1/r}))$ is $e_i - e$. So for at least one $i \leq t$ we have $e_i - e \leq 0$ and so the theorem follows. □

Remark 22. Without the condition $s_i \in (\overline{C}\cdot C((x^{1/r})))[\log(x)]$ the statement need not hold. Take for example $L = \delta^2 - \frac{1}{2}\delta$ and $r=1$. Then $min_r(L) = \{0, \frac{1}{2}\}$. Now take $e_1 = e_2 = 0$, $s_1 = 1$ and $s_2 = 1+x^{1/2}$. Then s_2 does not satisfy condition (6) and $min_r(L) \neq min_r(\{e_1, e_2\}) = \{0\}$.

Remark 23. The existence result (i) is also found in [6] (with a different terminology, though).

Proof of Proposition 17. Let $y_i = \mathrm{Exp}(e_i)s_i$, $i = 1,\dots,order(L_1)$ be a basis of $V(L_1)$ and $\tilde{y}_j = \mathrm{Exp}(\tilde{e}_j)\tilde{s}_j$, $j=1,\dots,order(L_2)$ be a basis of $V(L_2)$ which both satisfy condition (6). Then the products $y_i\tilde{y}_j$ span $V(L_1 \circledS L_2)$. Let S be a set of pairs (i,j) such that $\{y_i\tilde{y}_j \mid (i,j) \in S\}$ is a basis for $V(L_1 \circledS L_2)$. Now $y_i\tilde{y}_j = \mathrm{Exp}(e_i + \tilde{e}_j)s_i\tilde{s}_j$ and $s_i\tilde{s}_j \in (\overline{C}\cdot C((x^{1/r})))[\log(x)]$ with $v(s_i\tilde{s}_j)=0$. Hence by Theorem 21 it follows that $min_r(L_1 \circledS L_2) = min_r(\{e_i + \tilde{e}_j \mid (i,j) \in S\})$.

Now $\{e_i + \tilde{e}_j \mid (i,j) \in S\}$ is a subset of the set T of all $e_i + \tilde{e}_j$. So for each $e \in min_r(\{e_i + \tilde{e}_j \mid (i,j) \in S\})$ there must be precisely one $\tilde{e} \in min_r(T)$ such that $\tilde{e} \leq_r e$. Furthermore T is a subset of the set of all generalized exponents of $L_1 \circledS L_2$. Hence for each

$\tilde{e} \in min_r(T)$ there must be precisely one $e \in min_r(L_1 ⓢ L_2) = min_r(\{e_i + \tilde{e}_j \mid (i,j) \in S\})$ such that $e \leq_r \tilde{e}$. Then it follows that $min_r(T)$ equals $min_r(L_1 ⓢ L_2)$. □

Lemma 24. *Let $L \in C((x))[\delta]$ be non-zero and let r be the ramification index of L. If $0 \notin min_r(L)$ then*

$$min_r(L^{(1)}) = \{e + v(e) - 1 \mid e \in min_r(L)\}.$$

If $0 \in min_r(L)$ then

$$min_r(L^{(1)}) = \{m\} \cup \{e + v(e) - 1 \mid e \in min_r(L) \backslash \{0\}\}$$

where $m \in \mathbb{Z}$, $m \geq -1$, or

$$min_r(L^{(1)}) = \{e + v(e) - 1 \mid e \in min_r(L) \backslash \{0\}\}.$$

Note that $order(L^{(1)}) = dim(\partial(V(L))) = dim(V(L)) - dim(V(L) \cap V(\partial))$. So $order(L^{(1)}) = order(L) - 1$ if $1 \in V(L)$ and $order(L^{(1)}) = order(L)$ otherwise.

Proof. If $y = \mathrm{Exp}(e)s$ where $s \in (\overline{C} \cdot C((x^{1/r})))[\log(x)]$ with $v(s) = 0$ and $e \neq 0$ then the derivative y' is of the form $\mathrm{Exp}(e + v(e) - 1)t$ for some $t \in (\overline{C} \cdot C((x^{1/r})))[\log(x)]$ with $v(t) = 0$. Now the first statement follows by applying Theorem 21.

For the second statement we note that $v_0(L) > 0$ means that there is a formal solution $y \in (\overline{C} \cdot C((x^{1/r})))[\log(x)]$ of L with $v(y) = 0$. The valuation of the derivative y' is ∞ or is an integer ≥ -1. Now distinguish the two cases: $v(y') \in min_r(L^{(1)})$ (then: $v(y')$ is an integer $m \geq -1$) or $v(y') \notin min_r(L^{(1)})$ (then the other case holds). □

Note that in the case $0 \in min_r(L)$ one can get a slightly stronger statement about $min_r(L^{(1)})$ by noting that $-1 \in min_r(L^{(1)})$ if and only if $v_0(L) > 1$. We will not use this small improvement of the lemma.

Define $v' : E \to \mathbb{Q}$ as follows: $v'(e) = v(e)$ for all $e \in E \setminus \{0\}$ and $v'(0) = 0$. It follows from the lemma that for each $e \in min_r(L^{(1)})$ there is an $\tilde{e} \in min_r(L)$ such that $e - (\tilde{e} + v'(\tilde{e}) - 1)$ is a non-negative integer. Repeating this, we see that for each $e \in min_r(L^{(i)})$ there is an $\tilde{e} \in min_r(L)$ such that $e - (\tilde{e} + i \cdot v'(\tilde{e}) - i)$ is a non-negative integer.

Theorem 25. *Let L be a non-zero differential operator in $C((x))[\delta]$ and r be its ramification index. Let $m_0, \ldots, m_{n-1}$ be non-negative integers and M the symmetric product of the operators $(L^{(i)})^{ⓢ m_i}$. Define $B_i = \{e + i \cdot v'(e) - i\} \mid e \in min_r(L)\}$ and $B = m_0 \cdot B_0 + \cdots + m_{n-1} \cdot B_{n-1}$. Suppose M has a non-zero solution y in $(\overline{C} \cdot C((x^{1/r})))[\log(x)]$. Then $B \cap \frac{1}{r}\mathbb{Z}$ contains an element $\leq v(y)$.*

The theorem gives a lower bound for the valuation of solutions of M in $(\overline{C} \cdot C((x^{1/r})))[\log(x)]$. The bound can be computed from $m_0, \ldots, m_{n-1}$, r and $min_r(L)$.

To compute the bound we need to compute the set of sums $m_0 \cdot B_0 + \cdots + m_{n-1} \cdot B_{n-1}$ and to take the smallest element which is in $\frac{1}{r}\mathbb{Z}$. This means computing in a splitting field: it is not sufficient to take only one generalized exponent in each conjugacy class of generalized exponents. One can try to avoid splitting fields for computing this bound by various tricks (for example, floating point computations) but we will not go into this.

In the following procedure, the notation l_α denotes the $\overline{C}$-automorphism of $\overline{C}(x)[\partial]$ given by $l_\alpha(x)=x+\alpha$ and $l_\alpha(\partial)=\partial$; this transformation moves the point $x=\alpha$ to $x=0$. Similarly, l_∞ is a $\overline{C}$-automorphism of $\overline{C}(x)[\partial]$ given by $l_\infty(x)=1/x$ and $l_\infty(\partial)=-x^2\partial$; this moves the point infinity to $x=0$.

Algorithm 1 (Procedure global-bounds).

Input: An operator $L\in C(x)[\partial]$, and non-negative integers $m_0,\ldots,m_{n-1}$.

Output: A rational function $Q\in C(x)$ and an integer N such that every rational solution $y\in\overline{C}(x)$ of $M=(L^{(0)})^{\circledS m_0}\circledS\cdots\circledS(L^{(n-1)})^{\circledS\, m_{n-1}}$ can be written as the product of Q and a polynomial in x of degree $\leq N$.

```
(i) $Q:=1$.
(ii) After multiplication on the left by an element of $C[x]$, we may assume that $L=a_n\partial^n+\cdots+a_0\partial^0$ with $a_i\in C[x]$ and $\gcd(a_0,\ldots,a_n)=1$.
(iii) For each irreducible factor $p$ of $a_n$ in $C[x]$ (not $\overline{C}$) do
    (a) Let $\alpha\in\overline{C}$ be a root of $p$.
    (b) Compute the generalized exponents of $l_\alpha(L)$ at the point $x=0$.
    (c) Let $r$ be the ramification index of $l_\alpha(L)$ at $x=0$; compute the $min_r$ of the set of generalized exponents.
    (d) Compute the set $B$ from Theorem 25.
    (e) If $B\cap\frac{1}{r}\mathbb{Z}$ is empty then stop the algorithm and RETURN the following output: $Q=0$ and $N=0$.
    (f) Let $b_\alpha\in\mathbb{Z}$ be the smallest element of $B\cap\frac{1}{r}\mathbb{Z}$, rounded above to an integer.
    (g) Replace $Q$ by $Q\cdot p^{b_\alpha}$.
(iv) Perform steps 3b, 3c, 3d, 3e, 3f with $\alpha=\infty$.
(v) Add $2\cdot(0\cdot m_0+1\cdot m_1+\cdots+(n-1)\cdot m_{n-1})$ to $b_\infty$.
(vi) Let $N$ be $-b_\infty$ plus the valuation of $Q$ at infinity (this valuation is the degree of the denominator of $Q$ minus the degree of the numerator of $Q$).
(vii) Return: $Q$ and $N$.
```

Remark 26. Note that, even if $Q=N=0$, there may be an invariant (whose value is zero): see the Hurwitz example in the next section for an illustration.

The fact that the algorithm works follows from the following observations:

- Because algebraic conjugation over C is an automorphism of the differential field $\overline{C}(x)$, it follows that if $\alpha_1,\alpha_2\in\overline{C}$ are conjugated over C then the two bounds $b_{\alpha_1},b_{\alpha_2}\in\mathbb{Z}$ will be the same. Hence, we need to take only one α in every conjugacy class of the singularities of L. In other words: we need to compute the bound for only one root of each factor of a_n in $C[x]$. Furthermore, the function $Q\in\overline{C}(x)$ will be an element of $C(x)$.

- Note that for all $\alpha \in \mathbb{P}^1(\overline{C})$ the map l_α on $\overline{C}(x)[\partial]$ commutes with taking symmetric products and LCLMs (least common left multiples) because the map l_α on $\overline{C}(x)$ commutes with multiplication and addition. However, l_α does not commute with derivation if $\alpha = \infty$. So l_α only commutes with the construction $L \mapsto L^{(1)}$ on $\overline{C}(x)[\partial]$ if $\alpha \in \overline{C}$. The solution space of $l_\infty(L^{(1)})$ equals x^2 times the solution space of $l_\infty(L)^{(1)}$, so the valuations are 2 higher than in Lemma 24. For the point $x = \infty$ there is a lemma similar to Lemma 24 with the following differences: $e + v'(e) - 1$ is replaced by $e + v'(e) + 1$ and $m \geq -1$ is replaced by $m \geq 1$. We need a different Theorem 25 specifically for the point $x = \infty$, i.e., for operators $L \in C((\frac{1}{x}))[\partial]$ instead of $L \in C((x))[\partial]$. The only difference will be that $e + i \cdot v'(e) - i$ needs to be replaced by $e + i \cdot v'(e) + i$. The algorithm computes the bound given by Theorem 25 and then adds $2 \cdot (0 \cdot m_0 + 1 \cdot m_1 + \cdots + (n-1) \cdot m_{n-1})$ to correct for this difference.

Example 27 (PSL_3). The following example was adapted from Katz by Elie Compoint [7]. The component of the identity of its Galois group is $PSL_3(C)$ in its eight-dimensional representation. Let $\delta = x(\mathrm{d}/\mathrm{d}x)$ and

$$L = \delta\left(\delta - \tfrac{1}{2}\right)\left(\delta - \tfrac{1}{4}\right)\left(\delta + \tfrac{1}{4}\right)\left(\delta - \tfrac{1}{8}\right)\left(\delta - \tfrac{5}{8}\right)\left(\delta + \tfrac{1}{8}\right)\left(\delta + \tfrac{5}{8}\right) - x\left(\delta + \tfrac{1}{3}\right)\left(\delta - \tfrac{1}{3}\right).$$

We want to compute the invariants of degree 2 and 3.

The generalized exponents of $l_\infty(L)$ are $-\frac{1}{3}, \frac{1}{3}$ and all conjugates of $x^{-1/6} + \frac{2}{3}$. The ramification index is $r = 6$. Now $-\frac{1}{3} \leq_r \frac{1}{3}$ and all other generalized exponents are different modulo $\frac{1}{r}\mathbb{Z}$. Hence $min_r(l_\infty(L))$ contains 7 elements; all generalized exponents except $\frac{1}{3}$. Now the smallest element in $(\frac{1}{r}\mathbb{Z}) \cap (2 \cdot min_r(l_\infty(L)))$ is $-\frac{2}{3}$. Rounded above to an integer this is 0. The smallest element in $(\frac{1}{r}\mathbb{Z}) \cap (3 \cdot min_r(l_\infty(L)))$ is -1.

The generalized exponents (which are in fact exponents) of L at $x = 0$ are $-\frac{5}{8}, -\frac{1}{4}, -\frac{1}{8}, 0, \frac{1}{8}, \frac{1}{4}, \frac{1}{2}$ and $\frac{5}{8}$. So the ramification index is $r = 1$. Since all exponents are different modulo $\frac{1}{r}\mathbb{Z}$ the set $min_r(L)$ equals the set of exponents. Now the smallest element in $(\frac{1}{r}\mathbb{Z}) \cap (2 \cdot min_r(L))$ is 0 and the smallest element in $(\frac{1}{r}\mathbb{Z}) \cap (3 \cdot min_r(L))$ is -1.

So the procedure *global-bounds* gives the following output for the second symmetric power of $L: Q = 1$ and $N = 0$. This means that the values of all invariants of degree 2 are constants. For the third symmetric power the output is $Q = 1/x$ and $N = 2$, which means that the values of the invariants of degree 3 must be of the form $\frac{1}{x} \cdot (c_0 x^0 + c_1 x^1 + c_2 x^2)$ for some constants c_0, c_1, c_2 which will be computed in the next section.

4. The algorithm for computing invariants

We now have all ingredients for an algorithm. There exists an invariant of degree m if and only if there is a rational solution F to $Y' = S^m(A)Y$. The previous section gives the denominators and bounds for the degrees of the numerators of the entries of F. Thus, the problem can be reduced to linear algebra.

To obtain the numerators in F, we consider a local fundamental solution matrix $\hat{U}$ at some (possibly singular) point $x_0 \in \mathbb{P}^1(\overline{C})$. We can assume $x_0 = 0$ in our algorithm after having applied the map l_{x_0}. Now $F = Sym^m(\hat{U}) \cdot \mathscr{C}$ for some constant vector $\mathscr{C}$. We start with undetermined constants in $\mathscr{C}$, compute sufficiently many terms of the power series in $Sym^m(\hat{U})$ and then express the numerators in F in terms of the constants in $\mathscr{C}$, see below. As the evaluation of the series is usually the most costly part of the algorithm, our main goal below will be to reduce the number of columns and rows of $Sym^m(\hat{U})$ that need to be evaluated during the process.

4.1. Computing candidate invariants

First, we perform the above idea only on the first row of $Sym^m(\hat{U})$. The reason for choosing this particular row is that the bounds in Theorem 25 (compare the generalized exponents of L and $L^{(1)}$) are smaller than the bounds for other rows (unless there are less than 3 singularities).

Suppose $\hat{y}_i$, $1 \le i \le n = order(L)$, is a basis of formal solutions satisfying condition (6). Then a monomial in these $\hat{y}_i$ (i.e., a product $\prod(\hat{y}_i)^{m_i}$) is again of the form (6), where the generalized exponent equals $\sum m_i e_i$. The following lemma reduces the number of columns of $Sym^m(\hat{U})$ that need to be evaluated.

Lemma 28. *Let $\hat{y}_i$ be a basis of local formal solutions satisfying condition* (6) *and let r be the ramification index. An entry of a vector $\mathscr{C}$ of coefficients of an invariant can only be non-zero if the generalized exponent of the corresponding monomial is in $\frac{1}{r}\mathbb{Z}$.*

Proof. Let $N = \binom{n+m-1}{n-1}$ and let $\hat{U}$ be a formal fundamental matrix of $Y' = AY$ such that the first row is $\hat{y}_1, \ldots, \hat{y}_n$, i.e. the entries of $\hat{U}$ are the $0, \ldots, (n-1)$th derivatives of $\hat{y}_1, \ldots, \hat{y}_n$. Let P be a polynomial invariant and $\mathscr{C}$ be the vector of its coefficients. Then $Sym^m(\hat{U}) \cdot \mathscr{C} \in \overline{C}(x)^N \subset (V_{0,r})^N$. Note that each column of $Sym^m(\hat{U})$ is an element of $(V_{e,r})^N$ where e is the generalized exponent of the first element (which is a monomial in the $\hat{y}_i$) of this column. From the fact that the columns of $Sym^m(\hat{U})$ are linearly independent and the direct sum (5), it follows from $Sym^m(\hat{U})\mathscr{C} \in (V_{0,r})^N$ that $\mathscr{C}$ can only have a non-zero entry for those columns which are in $(V_{0,r})^N$, i.e., for those monomials whose generalized exponent is in $\frac{1}{r}\mathbb{Z}$. □

Note that the above lemma is sharp, i.e., we must consider the generalized exponents in $\frac{1}{r}\mathbb{Z}$. Taking only generalized exponents in $\mathbb{Z}$ is not sufficient as is shown by the following example.

Example 29. Let $L \in \mathbb{Q}((x))[\partial]$ be the monic operator of order 4 which has the following local solutions at $x = 0$

$$y_1 = \mathrm{Exp}\left(\frac{1}{x^{1/2}} + \frac{1}{10}\right) \cdot (1 + x^{1/2})$$

y_2 is the conjugate (replace $x^{1/2}$ by $-x^{1/2}$) of y_1

$$y_3 = \operatorname{Exp}\left(\frac{1}{x^{1/2}} + \frac{4}{10}\right)$$

and y_4 is the conjugate of y_3. The ramification index of L is 2. L has an invariant of degree 2, even though none of the monomials $y_i y_j$ has a generalized exponent in $\mathbb{Z}$. The monomials $y_1 y_4$ and $y_2 y_3$ have generalized exponent $\frac{1}{2}$. And, in fact, $y_1 y_4 - y_2 y_3 = 2x$ is the value of an invariant of degree 2.

Algorithm 2 (Heuristic for computing invariants).
Input: an operator L, an integer m, a point x_0, and a number v.
Output: a vector space of candidate invariants of degree m and their corresponding candidate values, given as a parameterized candidate vector invariant and candidate value.

(i) If $x_0 \neq 0$ then apply recursion on $l_{x_0}(L)$ as follows: replace L and x_0 by $l_{x_0}(L)$ and 0, apply this algorithm and then apply the inverse of l_{x_0} on the candidate values of the invariants.

(ii) Use the procedure global-bounds to find the bounds Q_1, N_1 for rational solutions of the mth symmetric power of L.

(iii) Compute a basis of formal solution $\hat{y}_i$ at $x=0$ having property (6) in Theorem 21. Let r be the ramification index.

Let $\mathscr{Y}$ denote the vector of all monomials of degree m in the $\hat{y}_i$. Each of these monomials has a generalized exponent in $\overline{C}[x^{-1/r}]$.

(iv) Take a vector $\mathscr{C}$ of unknown constants and set to zero every entry corresponding to a monomial with a generalized exponent that is not an element of $\frac{1}{r}\mathbb{Z}$.

(v) Compute $p_1 := \frac{1}{Q_1}\mathscr{Y} \cdot \mathscr{C} \bmod x^{N_1+v+1}$.

(vi) Build a linear system on $\mathscr{C}$ by equating to zero every term with degree higher than N_1 and all terms involving a log or a non-integer power of x.

(vii) Return: the solution of this system (this is a vector space consisting of candidate vector invariants) and the corresponding (vector space of) rational functions $f_1 := p_1 Q_1$.

Proposition 30. *Denote by $W_{L,m,v}$ the vector space of candidate vector invariants produced by the above heuristic. Denote $W_{L,m,\infty} = \bigcap_v W_{L,m,v}$. Then:*

(i) *For all $v \in N$, any vector of coefficients of an invariant of degree m is in $W_{L,m,v}$.*

(ii) *There exists $v_0 \in N$ such that $W_{L,m,\infty} = W_{L,m,v_0}$.*

Proof. Recall from Section 3 that the value of any invariant of degree m is the product of Q_1 by a polynomial of degree at most N_1. According to Lemma 28, we have only computed necessary (but in general not sufficient) linear conditions. Hence (i) follows. Increasing v adds more conditions on $\mathscr{C}$ so $W_{L,m,i+1} \subset W_{L,m,i}$. As $W_{L,m,\infty}$ is finite dimensional, this implies (ii). □

This algorithm is called a heuristic because there is no easy way of deciding whether its output is the vector space of invariants or a larger vector space. The number ν is can be chosen arbitrarily; the strategies of choice will be discussed in the next section.

Remark 31. We have $order(L^{\circledS\, m}) < N = \binom{n+m-1}{n-1}$ if and only if the solutions of L satisfy a homogeneous polynomial relation of degree m. In this case, the value of a non-zero invariant can be zero, and furthermore it can also happen that $W_{L,m,\infty}$ contains elements that are not invariants (see the F_{36} Example 37). Note that since we do not compute $L^{\circledS m}$ we have no easy way of checking if this case $order(L^{\circledS m}) < N$ occurs, so this would be a serious problem if we only had the heuristic to compute invariants. We do not have this problem if we use the algorithm *Invariants* below; then the case $order(L^{\circledS m}) < N$ does not cause difficulties anymore.

Example 32 (*PSL_3* (*continued*)). Let L be the eighth-order operator in the PSL_3 example in Section 3. We had found the bounds for rational solutions of $L^{\circledS 2}$ and $L^{\circledS 3}$. Applying the heuristic with $x_0 = 0$ and $\nu = 10$ the following (candidate) invariants are obtained:

$$\begin{aligned} P_2 = {} & \frac{352}{32805}c_0X_1X_7 - \frac{3249799168}{215233605}c_0X_4^2 - \frac{36064}{6561}c_0X_3X_5 \\ & + \frac{20240}{6561}c_0X_6X_2 + \frac{12397}{3645}c_0X_8^2 \end{aligned}$$

and $P_2(\hat{y}) = c_0$,

$$\begin{aligned} P_3 = {} & -\frac{15167488}{405}c_1X_8X_6X_2 + \frac{35500589056}{12301875}c_1X_1^2X_6 + \frac{659456}{10125}c_1X_1X_8X_7 \\ & - \frac{36929536}{54675}c_1X_7X_4X_5 - \frac{743206912}{22275}c_1X_8X_3X_5 + \frac{106172416}{3267}c_1X_2X_3^2 \\ & - \frac{3479057727488}{81192375}c_1X_1X_3X_4 + \frac{46450432}{3375}c_1X_8^3 + \frac{12176702046208}{66430125}c_1X_8X_4^2 \\ & + \frac{424689664}{18225}c_1X_6X_5^2 + c_1X_7^2X_2 \end{aligned}$$

and

$$P_3(\hat{y}) = c_1\frac{1}{x}(1 + \frac{9144576}{3025}x + \frac{17832200896512}{3826625}x^2),$$

where c_0, c_1 denote arbitrary constants. Note that $L^{\circledS 2}$ and $L^{\circledS 3}$ have order 36 and 120, respectively. Computing $L^{\circledS 3}$ is practically infeasible, whereas the above computation only takes a few minutes.

4.2. Strategies for the heuristic

In the heuristic the point x_0 and the number ν can be chosen. The advantage of choosing a singular point x_0 is that the number of monomials that need to be considered

(Lemma 28) in the heuristic is often smaller, and so we need to evaluate fewer columns of $Sym^m(\hat{U})$. This still holds (and is important for the efficiency) for the algorithm *Invariants* below.

Example 33 (PSL_3 (*continued again*)). In the PSL_3 example of Section 3, if we would take a regular point x_0 then the heuristic would need to evaluate 36 monomials for the invariants of degree 2, and 120 monomials for degree 3. However, when taking the singularity $x_0 = 0$, only 5 monomials of degree 2 have an integer exponent (the algorithm only considers monomials with an exponent in $\frac{1}{r}\mathbb{Z}$, and $r = 1$ in this example). And only 15 monomials of degree 3 have an integer exponent. So when using the singular point $x_0 = 0$ the computation for both the heuristic and the algorithm is much quicker than, say, with the regular point $x_0 = 1$.

Taking a point in which a ramification occurs can be disadvantageous, because computing modulo x^N in $C[[x^{1/r}]]$ involves more coefficients in C than computing modulo x^N in $C[[x]]$. So, the point $x_0 = 0$ (ramification index is 1) in the PSL_3 example is more favorable than the point $x_0 = \infty$ (ramification index is 6). A point where the generalized exponents require algebraic extensions can have both advantages and disadvantages. The disadvantage is obvious: computing the formal solutions and evaluating monomials will be more costly. The advantage is that many monomials need not be considered, for example:

Example 34. Suppose that $order(L) = 3$ and that at the point $x_0 = 0$ we have 3 generalized exponents e_1, e_2, e_3 which are algebraic over $C((x))$ of degree 3. From $c_1e_1 + c_2e_2 + c_3e_3 \in \frac{1}{r}\mathbb{Z}$ and $c_1, c_2, c_3 \in \mathbb{Z}$ it follows that $c_1 = c_2 = c_3$ and hence only 1 monomial needs to be considered. So, for order 3, what would appear to be the worst case (the e_i are algebraic of degree 3), is in fact a relatively easy case.

By reasoning as in Section 1.c of [18], an application of Cramer's formulas shows that we can take the following value for the number v_0 in Proposition 30: $N(1+(N-1)d+Nd_1)$ (where $N = \binom{n+m-1}{n-1}$, d is the maximum degree of the a_i, and d_1 bounds the degrees of the numerator and denominator of Q_1). Thus, the above heuristic could be turned into an algorithm (but then the kernel problem $order(L^{\circledS m}) < N$ of Remark 31 would need to be addressed as well). However, this value for v_0 is usually much larger than necessary. So it is more efficient first to use the heuristic with a small value of v, and then to apply the full algorithm *Invariants* from Section 4.3.

If one already has some information about the group then sometimes the heuristic algorithm is sufficient to compute the invariants. Because if we know how many linearly independent invariants of degree m exist, we can simply use the heuristic by just increasing the value of v. If at a certain point the space of candidate vector invariants has the correct dimension then it is certain (even in the problem case $order(L^{\circledS m}) < N$) that all invariants have been determined because the invariants form a subspace of the candidate invariants. In practice, the required number v is usually much smaller than the theoretical bound v_0 above.

Example 35 (*Hurwitz*). The following operator has Galois group G_{168} (cf. [22]). Let $\partial = \mathrm{d}/\mathrm{d}x$ and

$$L = \partial^3 + \frac{7x-4}{x(x-1)}\partial^2 + \frac{2592x^2 - 2963x + 560}{252x^2(x-1)^2}\partial + \frac{-40805 + 57024x}{24696x^2(x-1)^2}.$$

The Galois group has invariants of degree 4, 6, 14, 21. The heuristic with $m = 4$, $x_0 = \infty$, $v = 10$ yields (in 0.75 s) a one-dimensional space generated by $P = 1728X_1X_2^3 + X_1^3X_3 - 1728X_2X_3^3$ together with the value 0. The fact that the space of invariants of degree 4 has dimension exactly 1 proves that P is indeed an invariant. Similarly, the heuristic yields the other invariants quickly (see also [27]): for the invariant of degree 21, we need to compute 37 monomials at infinity (using a regular point it would have been 253 monomials).

4.3. Finding and proving which candidates are invariants

Let the monomial μ be a product of $y^{(i)}$ to the power m_i, $i = 0, \ldots, n-1$. If y is a solution of L then μ is a solution of the symmetric product of the operators $(L^{(i)})^{ⓢ m_i}$. By "applying procedure global-bounds on μ", we mean applying the procedure global-bounds on these numbers $m_0, \ldots, m_{n-1}$.

Algorithm 3 (Algorithm invariants).
Input: L, m, x_0 (optional: v)
Output: the space of invariants in vector and dual forms

(i) Like in the heuristic, if $x_0 \neq 0$ then apply the transformation l_{x_0}, use recursion, and transform back.

(ii) Now we may assume $x_0 = 0$. Compute a basis of formal solutions of L at the point $x = 0$ having property (6) in Theorem 21. Construct $\hat{U}$, the fundamental solution matrix of $Y' = AY$ from this.

(iii) Obtain $F_1 = f$ and $\mathscr{C}$ from the heuristic. Note that f and $\mathscr{C}$ contain parameters.

(iv) for i from 2 to N do:

- Let μ_i be the ith monomial of degree m in $y, y', \ldots, y^{(n-1)}$. Obtain Q_i and N_i from procedure global-bounds applied to L and μ_i.
- Let $p_i := (1/Q_i)Sym^m(\hat{U})_i\mathscr{C} \bmod x^{N_i+1}$ and $F_i := p_i \cdot Q_i$. $Sym^m(\hat{U})_i$ denotes the ith row of $Sym^m(\hat{U})$.
- equate all terms involving logarithms or fractional powers of x to 0 (this gives a set of linear equations in the parameters. If the equations are non-trivial we use them to reduce the number of parameters).

(v) Now F is a vector of rational functions and $\mathscr{C}$ is a vector of constants. F and $\mathscr{C}$ contain parameters. The relation $F' - S^m(A)F = 0$ yields a system of linear equations in the parameters. Solve this system.

(vi) *Output*: a basis of solutions $\mathscr{C}$ of this system and the corresponding dual first integrals $F \in k^N$.

Theorem 36. *The output of this algorithm is exactly the space of invariants of degree m and the corresponding dual first integrals.*

Proof. That any vector of coefficients of an invariant is an element of the vector space produced by the algorithm follows from the fact that this was true for our heuristic, and from the fact that we only added necessary linear conditions in this algorithm. Hence also every dual first integral F is an element of the vector space produced by the algorithm. Conversely, as the F produced by the algorithm are rational vectors satisfying $F' = S^m(A)F$, they are dual first integrals. So, by Lemma 5, the corresponding $\mathscr{C}$ are indeed vectors of coefficients of invariants. □

4.4. Improvements and variants

Lemma 28 provided a speedup in the algorithm; it reduces the number of rows of $Sym^m(\hat{U})$ that need to be evaluated. It turns out that the number of columns that need to be evaluated can be reduced as well, using the following observation: $F' = S^m(A)F$ is not a random system of differential equations; there are recurrence relations so that, once some entries of F are known, the other entries can be deduced straightforwardly. Hence these latter entries, and the corresponding rows in $Sym^m(\hat{U})$, need not be considered in step iv in Algorithm 3. This provides a significant improvement of our algorithm, see below.

The recurrence relations are found as follows: Let y be a solution of $L(y) = 0$ and let $\mu_{[m_1,\dots,m_n]} = y^{m_1} \cdots (y^{(n-1)})^{m_n}$ with $m_1 + \cdots + m_n = m$ denote a differential monomial of degree m. Then:

$$\mu'_{[m_1,\dots,m_n]} = m_1 \mu_{[m_1-1,m_2+1,\dots,m_n]} + \cdots + m_{n-1}\mu_{[m_1,\dots,m_{n-1}-1,m_n+1]} + m_n\left(-\sum_{j=1}^{n} \frac{a_{j-1}}{a_n}\mu_{[\dots,m_j+1,\dots,m_n-1]}\right)$$

(with the convention that $\mu_{[\dots,-1,\dots]} = \mu_{[\dots,m+1,\dots]} = 0$). So, by replacing m_{n-1} by $m_{n-1}+1$ in the above, we have

$$\mu_{[m_1,\dots,m_{n-1},m_n+1]} = \frac{1}{m_{n-1}+1}(\mu_{[m_1,\dots,m_{n-1}+1,m_n]} - m_1\mu_{[m_1-1,m_2+1,\dots,m_{n-1}+1,m_n]} - \cdots + m_n \sum_{j=1}^{n} \frac{a_{j-1}}{a_n}\mu_{[\dots,m_j+1,\dots,m_{n-1}+1,m_n-1]}). \qquad (*)$$

These relations must be understood as relations among the components of a solution F of $F' = S^m(A)F$. So, if we know all entries of F corresponding to monomials $\mu_{[\dots,i]}$ (and $\mu_{[\dots,i-1]}$ if $i > 0$), then the relations $(*)$ provide the entries corresponding to the

$\mu[\dots,i+1]$. Thus, in the algorithm, we only need to evaluate the rows corresponding to the $\mu[\dots,0]$. A detailed study of the recursion shows that in the same way the rows corresponding to some of the $\mu_{[\dots,0]}$ can be skipped as well. This way, instead of evaluating $N=\binom{n+m-1}{n-1}$, we only need to evaluate[7] $\binom{n+m-3}{n-2}$ rows of $Sym^m(\hat{U})$ in step iii of Algorithm 3. Also note that, unless the number of singularities is <3, the rows corresponding to $\mu_{[\dots,i]}$ have larger bounds as i increases (Theorem 25 or the example below). So, the above relations allow us to skip the evaluation of most of the rows, but what is even more important for the efficiency is that we can skip the rows that have the worst bounds.

Step v of the algorithm can also be improved along the same lines. In the above process, we used the derivatives of the rows corresponding to the $\mu_{[m_1,\dots,m_{n-1},m_n]}$ with $m_{n-1}\neq 0$ to construct the entries of F. Thus, the corresponding relations are automatically satisfied in step v of Algorithm 3. Hence in step v we only need to consider the rows corresponding to monomials $\mu_{[\dots,m_{n-2},0,m_n]}$. This eliminates a lot of redundant equations.

Example 37 (F_{36}). Let

$$L=\partial^3+\frac{5(9x^2+14x+9)\partial}{48(x+1)^2x^2}-\frac{5(81x^3+185x^2+229x+81)}{432(x+1)^3x^3}.$$

This example, taken from [8], has Galois group F_{36} (in their notation). We search for invariants of degree $m=6$.

The number of monomials to be evaluated is 8 at $x=0$ and $x=\infty$, it is 16 at $x=-1$ and 28 at a regular point, so we work at $x=0$. The heuristic at $x=0$ with $v=10$ yields a 4-dimensional space of candidate invariants of degree 6 in 0.5 s. The complete algorithm (with the use of the above recurrence relations) then gives (as expected) a 2-dimensional space of invariants of degree 6 generated by

$$\frac{45}{4}X_1^6+135X_3X_2y_{1,1}^4+15X_2^4X_1^2+\frac{675}{2}y_{1,3}^2X_2^2X_1^2 \\ -\frac{3645}{16}X_3^4X_1^2-90X_3^3X_2^3-\frac{3645}{2}X_3^5X_2=-\frac{32805}{16}(x+1)^2x^5$$

and

$$-\frac{9}{2}X_1^6+\frac{135}{2}X_3X_2y_{1,1}^4-135X_3^2X_2^2X_1^2+\frac{3645}{4}X_3^4X_1^2 \\ +6X_3X_2^5-45X_3^3X_2^3\frac{729}{8}X_3^5X_2=\frac{6561}{8}(x+1)^2x^5.$$

The corresponding dual first integrals are

$$F_1=\Bigg[-\frac{32805}{16}(x+1)^2x^5,-\frac{10935}{32}x^4(x+1)(7x+5),$$

[7] This is for $n\geq 4$. For $n=2$ we need one row, and for $n=3$, we need $m+1$ rows.

$$
\begin{aligned}
&-\frac{1215}{128}x^3(-23+49x^2+74x), -\frac{243}{128}x^3(743+1463x^2+2086x), \ldots,\\
&\frac{5}{339738624(x+1)^9x^6}(258162545x^3+8763967375x^8\\
&+3454336210x^6+4799496375x^9+1442053125x^{10}+184528125x^{11}\\
&+8908159010x^7+430643385x^2-2112440530x^5-2098573250x^4\\
&-44227701x-23914845), \frac{5}{2717908992(x+1)^{10}x^7}(2491291800x^3\\
&+553584375x^{12}+30189672025x^8-9719448300x^6+30901623000x^9\\
&+16603359750x^{10}+4702779000x^{11}+9196060400x^7-804729978x^2\\
&\left.-7242904720x^5+2863772665x^4-156676680x+71744535)\right]
\end{aligned}
$$

and

$$
\begin{aligned}
F_2 = &\left[\frac{6561}{8}(x+1)^2x^5, \frac{2187}{16}x^4(x+1)(7x+5),\right.\\
&\frac{243}{128}x^3(-55+89x^2+130x), \frac{243}{128}x^3(299+587x^2+838x),\\
&\frac{243x^2(205x^3+445x^2+83x-93)}{256(x+1)}, \ldots,\\
&\frac{1}{1358954496(x+1)^9x^6}(-1661573743x^3+3565866895x^8\\
&+1902296722x^6+3956079015x^9+1442053125x^{10}+184528125x^{11}\\
&-1020492670x^7-1846340487x^2+12149631662x^5+9005910718x^4\\
&+236373147x-23914845), \frac{1}{10871635968(x+1)^{10}x^7}(-12566581020x^3\\
&+553584375x^{12}+41118775225x^8+41735111940x^6+33723573540x^9\\
&+17335654830x^{10}+4791352500x^{11}+42844772456x^7+3414074670x^2\\
&\left.+13326450920x^5-21103738535x^4-68103180x+71744535)\right].
\end{aligned}
$$

To use the recurrence relations $(*)$, we have to compute the rows corresponding to monomials $y^i(y')^{6-i}$, so that makes 7 rows (instead of 28). The bounds are more favorable for these 7 rows than for the other rows, and indeed the corresponding 7 entries of F_1 and F_2 are smaller expressions than most of the other entries. We printed the first 4 entries and the 2 last entries above. One sees that the last entries are significantly larger expressions. Precisely these large (hence: costly to compute) entries can be skipped in step iv of Algorithm 3, as these are the entries that are given by the recursion. This is the main reason why these relations are crucial for the efficiency.

The computation time is 36.7 s and uses 1.5 Mb of memory. We performed the same computation without using the recursion improvements, it took 263.5s and used 2.5Mb. We then tried the first step of the standard method (computation of $L^{\circledS 6}$): this took 4587 s and more than 10 Mb of memory.

5. Conclusion

We do not claim that our method is always better than the method via symmetric powers of operators. However, we have practical evidence that this method can handle much larger examples (and generally faster) than the previous one at our disposal.

To compute all invariants of a given equation, we now face the following open problem: given L, can one bound the degrees of the generators of the invariant ring (when G is reductive)? As shown in [7], a solution to this problem would yield an algorithm for computing reductive unimodular Galois groups.

The method extends readily to systems: we then need formal solutions of systems (e.g., via cyclic vectors); but we lose the recurrence relations that enhance the algorithm, so the best there seems (surprisingly) to convert the system to an equation, apply the above algorithms, and then perform the correct change of variables to obtain the invariants of the original system.

We believe that the philosophy heuristic-checking is very suitable for computation. Information on the invariants can be obtained quickly by the heuristic and by modular arithmetic. If desired, this information can then be checked by Algorithm 3. Furthermore, Algorithm 3 provides additional useful information, namely the dual first integrals corresponding to the invariants.

Applications of this algorithm are the computation of first integrals [26], the computation of differential relations satisfied by the solutions [7], the computation of algebraic and Liouvillian solutions [21, 23, 25] and, more generally, to compute information on the Galois group. Extensions of the above techniques to other constructions on $V(L)$ (and several applications) will be described in a subsequent paper.

Acknowledgements

The research of the second author was supported by the Dutch NWO-MRI (project AIDA). The authors thank the universities of Groningen and Nijmegen as well as the École Polytechnique for their support and hospitality during the preparation of this paper. Some computations were done on the machines of the CNRS-GDR MEDICIS at the École Polytechnique.

We would like to thank Elie Compoint, Marius van der Put, Felix Ulmer, and Michael Singer for useful remarks concerning this paper. We also thank Elie for swamping us with complicated examples that helped us with the implementation.

References

[1] S.A. Abramov, M. Bronstein and M. Petkošek, On polynomial solutions of linear operators, Proc. ISSAC'95 (ACM Press, New York, 1995).

[2] A. Barkatou, Rational Newton Algorithm for computing formal solutions of linear differential equations, Proc. ISSAC'88 (ACM Press, New York, 1988).

[3] D. Bertrand, Théorie de Galois différentielle, Cours de DEA, Notes rédigées par R. Lardon, Université de Paris VI, 1986.

[4] D. Bertrand and F. Beukers, Équations différentielles linéaires et majorations de multiplicités, Ann. Scient. Éc. Norm. Sup. 4ème série 18 (1985) 181–192.

[5] F. Beukers, Differential Galois theory, in: Waldschmidt, Moussa, Luck and Itzykson, eds., From Number Theory to Physics (Springer, Berlin, 1992).

[6] E. Coddington and N. Levinson, Theory of Ordinary Differential Equations (MacGraw-Hill, New York, 1955).

[7] E. Compoint, Équations différentielles et relations algébriques, preprint, 1995, Université de Paris 6.

[8] W. Geiselmann and F. Ulmer, Constructing a third order differential equation, preprint, Proc. 4th Rhine Workshop on Computer Algebra (1996).

[9] P. Hendriks and M. van der Put, Galois action on solutions of a differential equation, J. Symbolic. Comput. (1995).

[10] M. van Hoeij, Formal solutions and factorization of differential operators with power series coefficients, University of Nijmegen, Report No. 9528.

[11] M. van Hoeij, Factorization of differential operators with rational coefficients, University of Nijmegen, Report No. 9552.

[12] S. Lang, Algebra (Addison-Wesley, Reading, MA, 3rd ed., 1992).

[13] A.H.M. Levelt, Differential Galois theory and tensor products, Indag. Math. (1989) + erratas.

[14] B. Malgrange, Sur la réduction formelle des équations différentielles à singularités irrégulières, manuscript, 1979.

[15] J. Martinet and J.P. Ramis, Généralités sur la théorie de Galois différentielle, in: E. Tournier, ed., Computer Algebra and Differential Equations (Academic Press, New York, 1990).

[16] M. van der Put, Singular complex differential equations: an introduction Nieuw Achief voor Wiskunde, 4de serie 13 (3) (1995) 451–470.

[17] M.F. Singer, An outline of differential Galois theory, in: E. Tournier, ed., Computer Algebra and Differential Equations (Academic Press, New York, 1990).

[18] M.F. Singer, Moduli of linear differential equations on the Rieman sphere, Pac. J. Math. 160 (1993).

[19] M.F. Singer, Testing reducibility of linear differential operators: a group theoretic perspective, J. Appl. Alg. Eng. Comm. Comp. 7 (1996) 77–104.

[20] M.F. Singer and F. Ulmer, Galois groups for second and third order linear differential equations, J. Symbolic. Comput. 16 (1993) 1–36.

[21] M.F. Singer and F. Ulmer, Liouvillian and algebraic solutions of second and third order linear differential equations, J. Symbolic. Comput. 16 (1993) 37–73.

[22] M.F. Singer and F. Ulmer, Necessary conditions for liouvillian solutions of (third order) linear differential equations, J. Appl. Alg. Eng. Comm. Comput. 6 (1995) 1–22.

[23] M.F. Singer and F. Ulmer, Linear differential equations and products of linear forms, preprint, presented at the MEGA'96 conference, Eindhoven, 6–8 June 1996.

[24] E. Tournier, Solutions formelles d'équations différentielles, Thèse d'Etat, Faculté des Sciences de Grenoble, 1987.

[25] F. Ulmer and J.A. Weil, Note on Kovacic's algorithm prepublication IRMAR 94-13, Rennes Juillet 94, J. Symbolic. Comput., to appear.

[26] J.A. Weil, First integrals and Darboux polynomials of homogeneous linear differential systems, in: M. Giusti and T. Mora, eds., Proc. AAECC 11, Lecture Notes in Comp. Sci., Vol. 948 (Springer, Berlin, 1995).

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