Differential and Difference Equations and Computer Algebra

In honour of A.H.M. Levelt's 65th birthday

January 10, 1997

Edited by

Engelbert Hubbers
Department of Mathematics
University of Nijmegen
Nijmegen, The Netherlands

FORWORD

When I was asked by the Department of Mathematics of the University of Nijmegen to organize a one day conference in honour of Ton Levelt's retirement, my immediate answer was "Yes, of course!".

"Yes, of course!", since Ton has had an enormous influence on our department (and me). During his 35 years stay at our institute he has been a chairman for many, many years, a task in which he has put an enormous amount of energy.

On the more mathematical level he has given courses ranging over allmost all disciplines of mathematics and organized many interesting and stimulating seminars (my first contact with Ton was in 1971–1972 when he gave a course in number theory followed by a seminar in class field theory).

Internationally his pioneering work on differential equations is world wide recognized (a clear example is Prof. Bolibruch's lecture in which Levelt's theory plays a crucial role in the solution of the Riemann-Hilbert problem).

During the last twenty years his interest for computers grew rapidly, which finally turned him into an apostel for Computer Algebra, giving lectures wherever he could to explain to all of us the beauty and power of it! The influence on our institute has been enormous. As I wrote on another occasion "he created a Mathematics department in Nijmegen in which the use of Computer Algebra is almost as normal as the use of pencil and paper!".

Of course it was an easy job for me to find speakers for the conference. Everyone I invited immediately responded very positively. Unfortunately Prof. Varadarajan and Prof. M. Singer where not able to come but nevertheless they were spiritually by sending each a nice text, which I presented in their name during the conference (these texts can be found at the end of this proceedings).

Let me end by saying: THANK YOU VERY MUCH for all you did for many of us. We all wish you all the best for a happy and healthy future together with Joke, Mathematics and Computer Algebra!

Arno van den Essen
November, 1997

UNIVERSITY OF NIJMEGEN, JANUARY 10, 1997

Program

A. Bolibruch	:	Levelt's valuation method and the Riemann-Hilbert problem
M. van der Put	:	Galois theory and algorithms for difference equations
M. MacCallum	:	Solving differential equations by computer algebra
B. Buchberger	:	Towards integrating theorem proving and computer algebra
A. Nowicki	:	On the Lagutinskii-Levelt procedure for systems of polynomial differential equations
M. van Hoeij	:	Factorisation of differential operators
A. Levelt	:	Characteristic classes for singularities of linear differential and difference equations

Attendants

Table of Contents

LEVELT'S VALUATION METHOD AND THE RIEMANN-HILBERT PROBLEM

ANDREY A. BOLIBRUCH
Steklov Mathematical Institute of Russian Academy of Sciences
ul. Gubkina 8, 117966 Moscow, GSP-1
Russia
bolibr@class.mi.ras.ru

Abstract.
This article is a version of a lecture presented on January 10, 1997 in Nijmegen at symposium "Differential and difference equations and Computer algebra" in honor of the 65th birthday of A. Levelt. Here we present the concept of Levelt's valuations of a system of ODE with regular singular points and show how this concept is used in the investigation of the Riemann–Hilbert problem (both classical and many-dimensional ones).

1 Regular and Fuchsian systems on the Riemann sphere

I am very happy and proud to participate at the symposium in honor of Professor A. Levelt whose works played a very important role in my mathematical activity. The first of all I mean his remarkable work [21], where among other problems[1] he considered a problem on distinguishing of Fuchsian systems on the Riemann sphere among all systems with regular singular points. Let me remind basic notions of Fuchsian and regular singular points.

Let a system

$$\frac{dy}{dz} = B(z)y \tag{1}$$

with unknown vector function $y = (y^1, \ldots, y^p)^t$ (t means transposition) have singularities $a_1, \ldots, a_n$; that is, $B(z)$ is holomorphic in $\bar{\mathbb{C}} \setminus \{a_1, \ldots, a_n\}$ (where $\bar{\mathbb{C}}$ is the Riemann sphere).

The system is called *regular at* a_i (and a_i is *a regular singularity* for this system), if any of its solutions has at most polynomial (in $1/|z - a_i|$) growth at a_i as z tends to a_i, remaining inside some sector with the vertex at a_i (without going around this point).

This work was partially supported by Grant 96-01-00207 from the Russian Found of Basic Researches.

[1] This work is devoted to a classification of local connections which appear from differential equations.

The system is called *Fuchsian at* a_i (and a_i is *a Fuchsian singularity* of the system) if $B(z)$ has a pole there of order at most one. The system is *Fuchsian* if it is Fuchsian at all a_i.

It is well known [16] that *any Fuchsian system is regular*, but a regular system needs not to be Fuchsian. Thus the class of regular systems is broader than the Fuchsian one.

Consider system (1) in a neighborhood O_i of a singular point a_i. Let $Y(z)$ be a fundamental matrix to (1) in $O_i \setminus a_i$ and let G_i be a monodromy matrix of $Y(z)$ (i.e., G_i is a matrix of a linear transformation of $Y(z)$ under an analytic continuation along a loop, going around a_i in $O_i \setminus a_i$).

Denote by E_i the matrix $1/(2\pi i)\ln G_i$ with eigenvalues ρ_i^j normalized as follows

$$0 \leq \mathrm{Re}\rho_i^j < 1. \tag{2}$$

The matrix $Y(z)$ of regular system (1) can be decomposed in the following way

$$Y(z) = M(z)(z - a_i)^{E_i}, \tag{3}$$

where $M(z)$ is meromorphic at a_i.

This decomposition takes place for Fuchsian systems as well. Thus, one can see that *locally every Fuchsian system is meromorphically equivalent to a regular one.* May be this is the reason why the problem of distinguishing Fuchsian systems among all regular ones was not considered before Levelt.

In order to investigate this problem Levelt introduced the concept of *valuation* for a solution to system (1) at a regular singular point a_i. Let me remind it.

It follows from (3) that every solution to (1) can be presented in the form of finite "logarithmic sum"

$$y(z) = \sum_{k,l} h_{kl}(z)(z - a_i)^{\rho_i^k} \ln^{b_l}(z - a_i), \tag{4}$$

where ρ_i^k are from (2), $b_l \in \mathbb{Z}$, $b_l \geq 0$, $h_{kl}(z)$ are functions meromorphic at a_i. Denote by m_{kl} the order of zero (the order of pole with the sign minus) of the function $h_{kl}(z)$ at a_i. *The minimum* $\varphi_i(y)$ *of* m_{kl} *over all* k, l *from the logarithmic sum is called the valuation* $\varphi_i(y)$ *of* $y(z)$ *at* a_i. By definition $\varphi_i(0) = \infty$.

For instance,

$$\varphi_i\left(\left(1/(z - a_i)^2\right)(z - a_i)^{1/2}\ln(z - a_i)\right) = -2.$$

It was proved in [21] that the valuation φ_i takes a finite number of values $\infty > \psi^1 > \ldots > \psi^m$ on the space X of solutions to system (1), considered in $O_i \setminus a_i$. Moreover, it generates a filtration

$$0 \subset X^1 \subset \ldots \subset X^m = X \tag{5}$$

of X by vector subspaces $X^j = \{y \in X | \varphi_i(y) \geq \psi^j\}$ and the local monodromy operator preserves this filtration. Consider a *Levelt's basis* $y_1(z), \ldots, y_p(z)$ of the space X, that is the basis associated with filtration (5) and such that the monodromy matrix G_i has an upper-triangular form in this basis. Denote by $Y_i(z)$ a fundamental matrix to (1) whose columns coincide with the elements of this basis. Then the following statement (which is due to Levelt [21]) takes place.

Theorem 1 *The fundamental matrix $Y_i(z)$ has the following decomposition in $O_i \setminus a_i$:*

$$Y_i(z) = U_i(z)(z-a_i)^{A_i}(z-a_i)^{E_i}, \tag{6}$$

where $U_i(z)$ is holomorphic at a_i, A_i=diag$(\varphi_i^1, \dots, \varphi_i^p)$, $\varphi_i^j = \varphi_i(y_j)$, E_i is an upper-triangular matrix defined above from the monodromy matrix G_i.

The next statement which is also due to Levelt [21] completely solves the local problem of distinguishing of Fuchsian systems among all regular ones.

Theorem 2 *System (1) regular at a_i is Fuchsian at this point if and only if the matrix U_i from decomposition (6) for the system is holomorphically invertible[2] at a_i.*

Theorem 2 in particular means that *each Fuchsian system is completely determined (up to a holomorphically invertible at a_i change of the dependent variable) by its monodromy and its weighted Levelt's filtration (filtration (5) with values of valuations) at the point a_i*. It can be used for the classification of logarithmic connections in vector bundles constructed from a monodromy representation of a system (see [6], [10], Appendix D).

The numbers $\beta_i^j = \varphi_i^j + \rho_i^j$ are called *the exponents of the system at a_i*. As it follows from (6) *they coincide with the orders of asymptotics of solutions to (1) at a_i*.

To every regular singular point a_i one can attach a number

$$s_i = \sum_{j=1}^{p} \beta_i^j$$

(a sum of all exponents at a_i). Unfortunately, in general there is no connection between different Levelt's filtrations at any two different singular points. Nevertheless there is one important connection among all filtrations at all singular points on the Riemann sphere. And exactly this unique connection provides the answer to the global problem of distinguishing Fuchsian systems among regular ones. The following statement also is due to Levelt [21].

Theorem 3 *For any regular system (1) with singular points $a_1, \dots, a_n$ on the Riemann sphere the following relation holds*

$$\Sigma = \sum_{i=1}^{n} s_i \le 0, \qquad \Sigma \in \mathbb{Z}. \tag{7}$$

[2] A decomposition similar to decomposition (6) for Fuchsian systems was obtained earlier by Gantmacher in [11], but he never investigated the problem formulated above and he did not introduced a concept of valuation.

The system is Fuchsian on the whole Riemann sphere if and only if

$$\Sigma = 0. \tag{8}$$

In fact, here Levelt created a very important and useful tool for the investigation of the so-called Riemann-Hilbert problem. Let me remind very briefly the curious history of the problem.

For every system (1) with singular points $a_1, \dots, a_n$ on the Riemann sphere an analytic continuation of a fundamental matrix to the system along a loop lying in $\bar{\mathbb{C}} \setminus \{a_1, \dots, a_n\}$ with a starting point z_0 generates a linear representation

$$\chi : \pi_1(\bar{\mathbb{C}} \setminus \{a_1, \dots, a_n\}, z_0) \longrightarrow \mathrm{GL}(p, \mathbb{C}) \tag{9}$$

which is called *a monodromy representation to the system* or simply *monodromy.*

Riemann was the first to mention the problem of the reconstruction of a Fuchsian equation from its monodromy representation in a note at the end of the 1850's. In 1990 Hilbert included it in his list of "Mathematical Problems" under the 21st number. It was formulated as follows ([17]):

Prove that there always exists a linear differential equation of Fuchsian type with given singular points and a given monodromy group.

Historically the three following variants of this problem were considered: for scalar Fuchsian differential equations, for regular systems, for Fuchsian systems of differential equations.

As for scalar Fuchsian equations, it was known that time that the problem has a negative solution. This follows from the fact that a Fuchsian equation of pth order with singularities $a_1, \dots, a_n$ contains fewer parameters than the set of classes of conjugate representations (9). This goes back to Poincaré [23]), who calculated the difference between these two numbers of parameters. So in general it is impossible to construct a Fuchsian equation without an appearance of additional singularities.

Very often in mathematical literature the 21st Hilbert problem for Fuchsian systems is called the *Riemann–Hilbert problem.*

For a number of years people thought that the Riemann–Hilbert problem was completely solved by Plemelj [22] in 1908. Only recently it was realized that there was a gap in his proof (for the first time this was observed by Yu.S. Il'yashenko [2] and T. Kohn [18]). It turned out that Plemelj obtained a positive answer only to the problem concerning regular systems instead of Fuchsian ones.

According to this result of Plemelj the Riemann–Hilbert problem can be reduced to the following one

Prove that every system with regular singular points on the Riemann sphere is meromorphically equivalent to a Fuchsian system with the same singular points.

Now one can see that Levelt's Theorem 3 really could provide an algorithm for the investigation of the Riemann–Hilbert problem. Due to this theorem to prove the problem it is enough to prove that *for every regular system on the Riemann sphere there always exists a meromorphic transformation such that the transformed system has the same singular points and its sum of exponents Σ' is greater than the sum of exponents Σ of the original system.* Indeed, if the latter statement is true one can apply the corresponding meromorphic transformations until the resulting system has the sum of exponents equal zero. Then this system is Fuchsian due to Theorem 3 and we are done.

To illustrate the method let us prove the Riemann–Hilbert problem for dimension $p = 2$. The corresponding result is due to W. Dekkers [8] who used some results of the work [9] instead of Levelt's Theorem 3. The proof of Dekkers is complicated enough. But the application of the method of valuations provides a straightforward and simple proof.

Consider system (1) regular at singular points with the given monodromy. In particular let it be regular at $a_1 = 0$. Since in decomposition (6) $\det U_1(0) = 0$, without loss of generality one can assume that $U_1(z)$ has the following decomposition at zero:

$$U_1(z) = \begin{pmatrix} 1 & * \\ cz^k & dz^m \end{pmatrix} (1 + o(z)), \quad k > 0, m > 0.$$

Let $k = 1$. Consider the matrix

$$\Gamma(z) = \begin{pmatrix} 1 & -1/cz \\ 0 & 1 \end{pmatrix}.$$

Under the transformation $Y' = \Gamma Y$ our system is transformed to the system with the same singular points and such that decomposition (6) for the system at zero has the following form

$$Y_1'(z) = \Gamma(z)Y_1(z) = \Gamma(z)U_1(z)z^{A_1}z^{E_1} = \begin{pmatrix} ez^l & * \\ cz & dz^m \end{pmatrix} (1 + o(z))z^{A_1}z^{E_1} =$$

$$= \begin{pmatrix} ez^{l-1} & * \\ c & dz^m \end{pmatrix} (1 + o(z))z^{A_1'}z^{E_1},$$

where the sign $*$ denotes entries holomorphic at zero, $l > 0$,

$$A_1' = A_1 + \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.$$

The form of the matrix A_1' of valuations at zero means that the sum s_1' of exponents at zero of the new system is greater than the sum s_1 of exponents of the original one: $s_1' = s_1 + 1$. Since the transformation Γ is holomorphically invertible outside of zero, it does not change the exponents at other singular point. Thus, for the resulting system we get

$$\Sigma' = \Sigma + 1 > \Sigma$$

and we are done.

For the case $k > 1$ the corresponding proof is just slightly more complicated (one has to change the entry $-1/cz$ of the matrix Γ by an appropriate polynomial in $1/z$ of degree k).

In fact the presented proof has a gap. It works only for the case $c \neq 0$. What does the equality $c = 0$ means? It means that the fundamental matrix $Y_1(z)$ is of the form

$$Y_1(z) = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}.$$

And in turn it means that all monodromy matrices of the system are of the same form. But the latter means that the monodromy representation (9) is *reducible*. Thus, for $p = 2$ the method of valuations works well only for irreducible representations. And it shows us the difference between irreducible and reducible cases. A reducible case for $p = 2$ can be done from the following reasons: every two-dimensional representation is either commutative or one of monodromy matrices of the representation is diagonalizable. In the first case the proof is obvious, in the second one it follows also from one of Plemelj's result (see [2] or [1]).

The attempt to apply the same method to three dimensional irreducible representations turned out successful. It was proved in [5], (see also [1]) that the Riemann–Hilbert problem has the positive solution for such representations. As for reducible ones the corresponding attempt leaded to the counterexample to the Riemann–Hilbert problem. It turned out that for $p = 3$, $n = 4$ there exist reducible representations which cannot be realized as monodromy representations of any Fuchsian systems [5]. So, in this way it was proved that in general *the Riemann–Hilbert Problem has a negative solution*.

As for $p > 3$ the direct method of valuations does not work so far. Nevertheless using some additional ideas (from the theory of vector bundles) it is possible to prove that *for every irreducible representation the Riemann–Hilbert problem has a positive solution* (see [6], [19]).

I would like to mention once more that the application of the method of valuations shows us the difference between irreducible and reducible cases and it initiated us to consider the reducible case separately. Other methods do not provide reasons to do it.

2 Many-dimensional Fuchsian systems

The concept of valuations can be applied to Pfaffian systems

$$dy = \omega y \tag{10}$$

on analytic complex manifolds. Here ω is a matrix-valued differential form on a complex manifold M^m holomorphic outside of a divisor $D = \cup_{i=1}^{n} D_i$ with normal crossings. System (10) is assumed to be completely integrable with regular singular points only. The notion of regularity is defined in the same way as for systems (1) on the Riemann sphere. System (10) is called Fuchsian at D if it has at most logarithmic singularities there.

Various aspects of the theory of many-dimensional Fuchsian systems were considered by M. Yoshida and K. Takano [25], R. Gérard [12], A. Levelt [13], R.M. Hain [15], V.A. Golubeva [14], V.P. Leksin [20], by myself [3] and by other mathematicians. In many respects these investigations were inspired by problems of mathematical physics, in particular by the theory of Feynman integrals.

In [25] with the help of methods of normal forms a decomposition for Fuchsian system (10) similar to (6) was obtained. A generalization of Levelt's results on classical Fuchsian systems was presented partially in [12] and finally in [3]. Valuations were defined with the help of many-dimensional logarithmic sums similar to (4). It turned out that for every brunch D_i of divisor D it was possible to attach the number $s_i = \sum_{j=1}^{p} \beta_i^j$— the sum of exponents corresponding to D_i. Then, the following generalization of Theorem 3 was proved (see [3]).

Theorem 4 *Completely integrable Pfaffian system (10) with regular singularities along a divisor $D = \cup_{i=1}^{n} D_i$ with normal crossings on a compact Kählerian manifold M^m is Fuchsian if and only if the cycle*

$$\Sigma = \sum_{i=1}^{n} s_i D_i$$

is homologically trivial.

Note here that the classical Levelt's condition (8) also is homological. Indeed, relation (8) means that the zero-dimensional cycle $\Sigma = \sum_{i=1}^{n} s_i a_i$ is homologious to zero.

The condition of Theorem 4 can be directly used to obtain counterexamples to the generalized Riemann–Hilbert problem. This problem is formulated in the same way as the classical one. One must only change the notion of a Fuchsian system (1) by a Pfaffian Fuchsian system (10) and representation (9) by a representation

$$\chi' : \pi_1(M^m \setminus D, p_0) \longrightarrow \mathrm{GL}(p, \mathbb{C}). \tag{11}$$

Let $M^m = \mathbb{P}^m(\mathbb{C})$. Then every D_i can be determined by a homogeneous polynomial P_i of degree k_i as follows: $D_i = \{z \in \mathbb{C}^{m+1} | P_i(z) = 0\}$. Since D is a divisor with normal crossings, the group $\pi_1(\mathbb{P}^m(\mathbb{C}) \setminus D)$ is commutative with n generators $g_1, \ldots, g_n$ (corresponding to loops going around every D_i) and with only one relation:

$$\prod_{i=1}^{n} g_i^{k_i} = e. \tag{12}$$

It turns out that for this case the condition of Theorem 4 is formulated as follows

$$\sum_{i=1}^{n} s_i k_i = 0. \tag{13}$$

Now we get all we need to present a counterexample to the many-dimensional Riemann–Hilbert problem (see [4]).

Example 5 Let $m = 2, n = 2, p = 1, P_1 = z_1^2 + z_2^2 + z_3^2, P_2 = 5z_1^4 + 3z_2^4 + z_3^4$, $\chi'(g_1) = i, \chi'(g_2) = \sqrt{2}/2 + i\sqrt{2}/2$. The one-dimensional representation (11) defined by the data $D_1, D_2, \chi'(g_1), \chi'(g_2)$ cannot be realized as a monodromy representation of any Pfaffian Fuchsian system on $\mathbb{P}^2(\mathbb{C})$.

Indeed, since valuations to a system are integers, condition (13) is equivalent to the following one

$$\sum_{i=1}^{n} \rho_i k_i \equiv 0 \pmod{d},$$

where $\rho_i = \sum_{j=1}^{p} \rho_i^j$ is a sum of eigenvalues of the matrix E_i from (2), d is the most greatest divisor of the numbers $k_1, \ldots, k_n$. In our case one has

$$\rho_1 = 1/4, \rho_2 = 1/8, d = 2, \quad \text{and} \quad 2(1/4) + 4(1/8) = 1 \neq 0 \pmod 2.$$

Thus, this representation cannot be realized by any Pfaffian Fuchsian system. (Note here that necessary condition (12) is fulfilled.)

The complete answer to the Riemann–Hilbert problem for the case of a divisor D with normal crossings in $M^m = \mathbb{P}^m(\mathbb{C})$ is presented in the following simple statement (see [4]).

Proposition 6 *Let monodromy matrices $G_i = \chi'(g_i)$ of representation (11) be reduced simultaneously to an upper triangular form. Let $G_i = R_i + N_i$, where R_i are diagonal matrices and N_i are nilpotent. Then the representation can be realized by some Fuchsian system on $\mathbb{P}^m(\mathbb{C})$ with singularities along D if and only if the following relation holds*

$$\sum_{i=1}^{n} F_i k_i \equiv 0 (mod\ d),$$

where $F_i = 1/(2\pi i) ln R_i$.

3 Congratulations

Here I presented just two applications of Levelt's results on Fuchsian systems. I said nothing about his remarkable work [13] on generalized hypergeometric functions, about the connection between the exponents of a Fuchsian system and invariants of vector bundles on the Riemann sphere constructed by means of its monodromy representation (see [7]). These invariants can be calculated algorithmically from the Fuchsian system. But here we enter the region of Computer algebra and I hope that other speakers will say better about Levelt's activity in this domain.

At the end of my talk I would like to pass to Professor Levelt congratulations and best regards from Moscow mathematicians D.V. Anosov, Yu. Il'yashenko, V.A. Golubeva, V.P. Leksin.

References

1. D.V. Anosov and A.A. Bolibruch, *The Riemann–Hilbert Problem*, Aspects of Mathematics, Vieweg, Braunschweig/Wiesbaden, 1994.
2. V.I. Arnold and Yu.S. Il'yashenko, *Ordinary differential equations*, in the book: D.V. Anosov and V.I. Arnold (eds.), *Dynamical systems 1*, Encyclopaedia of the Mathematical sciences, 1, Springer, 1988.
3. A.A. Bolibruch, *Pfaffian systems of Fuchs type on a complex analytic manifold*, Math. USSR-Sbornik **31** (1977), 1031–1054.
4. A.A. Bolibruch, *An example of an insoluble Riemann-Hilbert problem on* $\mathbb{CP}^2$, in: "Geometric methods in problems of algebra and analysis", v. 2, Yaroslav. Gos. Univ., Yaroslavl' (1980), 60–64 (in Russian).
5. A.A. Bolibruch, *The Riemann-Hilbert problem*, Russian Math. Surveys, **45:2** (1990), 1–47.

6. A.A. Bolibruch, *On sufficient conditions for the positive solvability of the Riemann-Hilbert Problem*, Mathem. Notes of Ac. of Sci. of USSR , **51:2** (1992), 110–117.
7. A.A. Bolibruch, *The Riemann-Hilbert Problem and Fuchsian differential equations on the Riemann sphere*, Proceedings of the International Congress of Mathematicians, Zürich, Switzerland 1994, Birkhäuser, 1995, 1159–1168.
8. W. Dekkers, *The matrix of a connection having regular singularities on a vector bundle of rank 2 on* $\mathbb{P}^1(\mathbb{C})$, Lecture Notes in Mathem., **712**, Springer, 1979, 33–43.
9. P. Deligne, *Equations différentielles à points singuliers réguliers*, Lecture Notes in Mathem., **163**, Springer, 1970.
10. H. Esnault, E. Viehweg, *Logarithmic De Rham comlexes and vanishing theorems*, Invent. Math., **86** (1986), 161–194.
11. F.R. Gantmacher, *Theory of matrices. Volume II*, Chelsea, New York, 1959.
12. R. Gérard, *Théorie de Fuchs sur une variété analytique complexe*, J. Math. Pures et Appl., **47:4** (1968), 321–404.
13. R. Gérard et A.H.M. Levelt, *Etude d'une classe particulière de systèmes de Pfaff du type de Fuchs sur l'espace projectif complexe*, J. Math. Pures et Appl., **51** (1972), 189–217.
14. V.A. Golubeva, *Reconstruction of a Pfaff system of Fuchs type from the generators of the monodromy group*, Math. USSR-Izvestiya, **17** (1981), 227–241.
15. R.M. Hain, *On a generalization of Hilberts 21st problem*, Ann. Scient. Ec. Norm. Sup., 4 série, **19** (1986), 609–627.
16. P. Hartman, *Ordinary differential equations*, John Wiley, 1964.
17. D. Hilbert, *Mathematische Probleme*, Nachr. Ges. Wiss., Göttingen, 1900, 253–297.
18. A. Kohn Treibich, *Un resultat de Plemelj*, Progress in Mathem., **37**, Birkhäuser, 1983.
19. V.P. Kostov, *Fuchsian systems on* $\mathbb{CP}^1$ *and the Riemann-Hilbert Problem*, C.R.Acad.Sci. Paris, t. 315, Serie I (1992), 143–148.
20. V.P, Leksin, *Meromorphic Pfaffian systems on complex projective spaces*, Math. USSR-Sbornik, **57** (1987), 211–227.
21. A.H.M. Levelt, *Hypergeometric functions*, Nederl. Akad. Wetensch. Proc., Ser. A **64** (1961).
22. J. Plemelj, *Problems in the sense of Riemann and Klein, Interscience*, New York, 1964.
23. H. Poincaré, *Sur les groupes des équations linéaires*, Acta Math., **5** (1884), 201-312.
24. H. Röhrl, *Das Riemann – Hilbertsche Problem der Theorie der linearen Differentialgleichungen*, Math. Ann., **133** (1957), 1–25.
25. M. Yoshida and K. Takano, *Local theory of Fuchsian systems*, Proc. Japan Acad., **51** (1975), 219–223.

SOLVING DIFFERENTIAL AND DIFFERENCE EQUATIONS

MARIUS VAN DER PUT
Mathematisch Instituut
Rijksuniversiteit Groningen
P.O.Box 800, 9700 AV Groningen
The Netherlands
mvdput@math.rug.nl

Dedicated to Ton Levelt on the occasion of his 65th birthday

This paper is an extended version of a lecture given in honour of Ton Levelt's retirement at the University of Nijmegen. Over a long period, Ton Levelt and I have cooperated on the subject of algebraic aspects of differential equations. My interest in Kovacic's algorithm and more generally in computer algebra for differential equations has its origin in Ton's activities in this area of Mathematics. This paper is meant as a present, thanking him for his stimulating ideas.

Many types of equations will be discussed. The main theme is concerned with differential and difference equations. Ordinary Galois theory (in other words solving polynomial equations in one variable over a field) is also presented here in order to stress the anology with differential and difference equations. For the latter type of equations we aim to give an exposition of some current themes of research and results. However this paper is far form being a survey of the subject.

In general, the equations that we look at will have no (or few) solutions in the base field (or ring) K over which they are defined. We will indicate how one constructs an extension L of the base field K which contains all solutions. The group of the automorphism of L/K (which preserve some additional structure) is the Galois group associated to the equation. This group is the key for producing symbolic solutions to the equation. Algorithms for this Galois group and for symbolic solutions are the main issue of this paper.

1 A polynomial equation $f(x) = 0$ over a field

This is the ancestor of the problems that concern us here. Let K denote a field. Suppose that the polynomial $f \in K[x]$ has degree n and that f is separable, i.e. the g.c.d. of f and its derivative $\frac{df}{dx}$ is 1.
One wants to make a "minimal" extension of K in which f has n (distinct) roots.

Consider the ring extension $K \subset R$ given by

$$R =: K[X_1, \ldots, X_n, 1/d]/(f(X_1), \ldots, f(X_n))$$

where $d = \prod_{i \neq j}(X_i - X_j)$. The polynomial f has n distinct roots in R. Indeed, the images of the X_i in R are roots of f and they are distinct since d is invertible in R.

However R is not "minimal". Let $\underline{m}$ be any maximal ideal of R. Then the field $L = R/\underline{m}$ has this minimality property. One calls L *the splitting field* of f over K. It is unique up to isomorphism. The Galois group G of f over K is the group of the K-automorphisms of L/K. Let $\{x_1, \ldots, x_n\}$ denote the images of the $\{X_i\}$ in L. This is the set of the roots of f in L. The group G acts on the set $\{x_1, \ldots, x_n\}$ and in fact G can be considered as a subgroup of the group S_n of all permutations of the roots $\{x_1, \ldots, x_n\}$ of f. At this point one can ask many questions:

1. What groups $G \subset S_n$ do occur?
2. Is G computable?
3. Can one find "symbolic solutions"?

The answer to those questions depend of course on the base field K. The historical question about symbolic solutions asks if all the solutions can be expressed by means of (repeated) radicals, i.e. nth roots $\sqrt[n]{\ }$. The historical answer is: "yes" if and only if the group G is solvable.

For special fields, like $\mathbb{Q}$ or number fields or finite fields, there are theoretical algorithms which determine G. Solving polynomial equations over finite fields is rather easy. The most interesting case is $K = \mathbb{Q}$. The equation $f(x) = 0$ can be considered over all the completions of $\mathbb{Q}$, i.e. the field of real numbers $\mathbb{R}$ and for every prime p the field of p-adic numbers $\mathbb{Q}_p$. Over those fields it is easier to "solve" the equation. Solving $f(x) = 0$ over $\mathbb{Q}_p$ is closely related with solving the equation modulo p, i.e. solving $f(x) = 0 \bmod p$.
Using group theory and reductions modulo primes p of the equation one has made practical implementations of the algorithm for say $n \leq 12$.
Question 1. above for $K = \mathbb{Q}$ is the famous unsolved "inverse problem of Galois theory". It has inspired many mathematicians.

2 Differential equations in characteristic 0

An algebraic way to look at linear differential equations is the following. One works over a base field K, which is equipped with a differentiation $a \mapsto a'$. The differentiation is supposed to be nontrivial and to satisfy the rules $(a+b)' = a' + b'$ and $(ab)' = a'b + ab'$. Such a field is called a differential field. The subset of the constants $C := \{a \in K |\ a' = 0\}$ is a subfield of K as one easily sees. For the sequel it is important to suppose that C is algebraically closed. The standard (and maybe most interesting) example is:

$$K = C(z) \text{ with } C \supset \mathbb{Q} \text{ an algebraically closed field and } ' = \frac{d}{dz}.$$

A (linear homogeneous) differential equation can be given in the form

$$y^{(n)} + a_{n-1}y^{(n-1)} + \ldots + a_1 y^{(1)} + a_0 y = 0.$$

It is sometimes more efficient to work with a differential equation in matrix form. We will do this here. A differential equation in matrix form is

$$v' = Av \text{ with } A \text{ a } n \times n\text{-matrix with coefficients in } K \text{ and } v \in K^n.$$

One wants to find a "minimal" extension of K where the equation has n linearly independent solutions of the field of constants of the extension. Consider the ring $R = K[X_{i,j}, \frac{1}{d}]_{1 \le i,j \le n}$ with $d = det(X_{i,j})$. The differentiation $'$ on R extends the differentiation of K and is given by $(X'_{i,j}) = A \cdot (X_{i,j})$. In this "differential ring" the equation has n independent solutions. They are the columns of the matrix $(X_{i,j})$. The ring is not minimal in general.

Let I by an ideal of R which is maximal among the set of ideals J satisfying the condition $J' \subset J$. It turns out that I is a prime ideal. The ring $PV := R/I$ is "minimal" and is called the *Picard-Vessiot ring* of the equation. It has the property that the field of fractions L of PV, which is again a differential field, has the same field of constants as K. The Picard-Vessiot extension is unique up to isomorphism. The fundamental matrix $F = (x_{i,j})$, this is the image of the matrix $(X_{i,j})$ in PV, has as columns n independent solutions over C. The group of all differential automorphisms of PV/K, consists of the K-algebra automorphisms $\sigma : PV \to PV$ which commute with $'$. This group is by definition the Galois group G of the equation $v' = Av$ over K.
The group G acts C-linear on the n-dimensional C-vector space *Sol* of all solutions with coordinates in PV. In fact G is an *algebraic subgroup* of $Gl(Sol) = Gl(n, C)$. After having explained this theoretical construction we are left the already familiar questions.

1. What algebraic subgroups $G \subset Gl(n, C)$ do occur?
2. Is G computable?
3. Can one find "symbolic solutions"?

Of course, the answers will depend on the choice of the differential field K. The third question was posed by Liouville and solved by him in the special case $y^{(2)} = ry$ with $r \in \mathbb{C}[x]$. In modern language, "symbolic solutions" are solutions which can be expressed by using repeatedly three types of operations:
(a) Adding to the differential field M roots of a polynomial equation $f(T) = 0$ with $f \in M[T]$.
(b) Adding to the differential field M an integral $\int a dx$ of an element $a \in M$ (or in other terms a solution of $y' = a$).
(c) Adding to the differential field M an expression $e^{\int a dx}$ where $a \in M$ (or in other terms a nonzero solution of $y' = ay$).

The well known answer to question 3. is: All solutions of the equation are "symbolic solutions" if and only if the neutral component G^o of the differential

Galois group G is a solvable group.
The reader will have noticed that this does not really answer the third question, but translates it into a special case of question 2. What can one say about the latter?

For $n = 1$ the situation is rather transparent for the field $C(x)$ (with C a computable algebraically closed field such as $\overline{\mathbb{Q}}$). The equation reads $y' = ry$. Its Galois group G is an algebraic subgroup of $Gl(1, C) = C^*$ and can only be C^* or the group μ_n of the nth roots of unity.
The group G is equal to μ_n if and only if all the residues of rdx at the points of $C \cup \{\infty\}$ are rational and have n as their common denominator.
This is a complete answer. Further, by definition, any solution of $y' = ry$ is a "symbolic solution".

For $n = 2$ and the field $C(x)$, question 3. was answered by Kovacic. The algorithm which is named after him uses three ingredients:
(a) A classification of the algebraic subgroups of $Gl(2, C)$ (or more precisely of $Sl(2, C)$).
(b) For any point v of $C \cup \{\infty\}$ the solutions of the order two equation over the completed field $C(x)_v$.
(c) A gluing of "local solutions" at the points $v \in C \cup \{\infty\}$ to a possible "global solution" over $C(x)$.

We note that for a point $v \neq \infty$ this completion $C(x)_v$ is the field of formal Laurent series in $x - v$, i.e. the field $C((x - v))$. For $v = \infty$ this completion is $C((x^{-1}))$.
Kovacic's algorithm has many times been refined and implemented. Although this is not made explicit in the literature, one can use Kovacic's algorithm to determine the differential Galois group. Kovacic's algorithm does not use the full determination of the "local Galois group at the point v". This local Galois group is defined as the Galois group of the equation over the field $C(x)_v$. This group can easily be read of from the formal classification of the differential equation over $C(x)_v$.

This classification is usually attributed to Turrittin (and maybe also to G. Birkhoff). It seems almost superfluous to remind the reader that A.H.M. Levelt and his Ph.D. students R. Sommeling, M. van Hoeij have made considerable theoretical and algorithmical contributions to the classification of linear differential equations of any order over the fields $C(x)_v$. Their work culminated in algorithms for factoring (locally and globally) differential operators of any order.

Papers of M.F. Singer and F. Ulmer generalize the Kovacic algorithm (at least theoretically) to the case $n = 3$ and $K = C(x)$ (with C a computable and algebraically closed field). It seems that in principle the questions 2. and 3. are answered for $n = 3$ and $K = C(x)$.

The second question is strongly related with finding the ideal I in the construction of PV as we will indicate.

Any $B \in Gl(n,C)$ acts as an automorphism σ_B on the K-algebra

$$R = K[X_{i,j}, \frac{1}{d}]_{1\leq i,j\leq n}$$

by the formula $(\sigma_B(X_{i,j})) = (X_{i,j}) \cdot B^{-1}$. Then B belongs to $G \subset Gl(n,C)$ if and only if $\sigma_B I = I$.
Suppose that I is known and let $B \in Gl(n,C)$ by a matrix with "indeterminates" as coefficients. The Gröbner basis algorithm gives an answer to the question: What are the algebraic conditions on B such that $\sigma_B(X_{i,j}) \in I$ for all $X_{i,j}$. More precisely: explicit generators of the ideal I lead to explicit generators for the ideal which defines G.

We are not certain that the converse statement is also true. More precisely, suppose that a basis for the ideal defining the Galois group G is given. Can one find explicitely a Picard-Vessiot extension? In the case that G is connected one knows that $K \otimes O(G)$ (where $O(G)$ is the algebra of the regular functions on G) is a Picard-Vessiot extension for the equation. In the general case, there is a finite Galois extension K' of K such that $K' \otimes_K PV$ (with PV a Picard-Vessiot extension) and $K' \otimes O(G)$ are isomorphic.

Suppose that one knows that the Galois group G of the matrix differential equation $y' = Ay$ over K is *reductive*. Then there is a theoretical algorithm for finding the ideal I and the Picard-Vessiot extension. This method uses "invariant theory for G" and the possibility of finding all rational solutions (i.e. defined over K) of any differential equation derived form $y' = Ay$ by "linear algebra".
It is *believed* that there is a theoretical algorithm for determining the Picard-Vessiot extension and the Galois group G for $K = C(z)$ (and with C a computable algebraically closed field like $\bar{\mathbb{Q}}$).

Some work on implementation for $n = 3$ and special equations has been done. The algorithms make an essential use of the theory of linear algebraic groups: classification of algebraic subgroups of $Gl(2,C), Gl(3,C)$, invariant theory, representations et cetera.

3 Ordinary difference equations

A *difference field* K is a field equipped with an automorphism ϕ. The *field of constants* C is defined as $C = \{a \in K | \phi(a) = a\}$. We will assume in this section that C is an algebraically closed field of characteristic 0 and that $K \neq C$. A linear difference equation is something of the form

$$a_n\phi^n(f) + \ldots + a_1\phi(f) + a_0 f = 0, \text{ with } a_n, .., a_0 \in K \text{ and } a_n, a_0 \neq 0.$$

It is often practical to formulate the techniques and the results for a difference equation in matrix form. This is an equation of the type:

$$\phi(v) = Av \text{ where } A \in Gl(n,K) \text{ and } v \in K^n.$$

It is obvious how to translate the first equation into a matrix difference equation.
If we choose for K the field $C(z)$, then there are essentially two choices for ϕ, namely:
(i) $\phi(z) = z + 1$. In this case one speaks of *ordinary difference equations*.
(ii) $\phi(z) = qz$ with $q \in C^*$ not a root of unity. This choice defines *the q-difference equations*.

3.1 The Picard-Vessiot extension

The pattern for the construction of a Picard-Vessiot extension for the equation $\phi(v) = Av$ is the following:
Consider the ring $R = K[X_{i,j}, \frac{1}{d}]_{1\leq i,j\leq n}$ with $d = \det(X_{i,j})$. The action of ϕ on K is extended to R by the formula $(\phi X_{i,j}) = A \cdot (X_{i,j})$. This ring is in general too big and one wants to divide out by an ideal I. The action of ϕ on R is supposed to induce an action on R/I (i.e. we must have $\phi(I) \subset I$). One takes for $I \subset R$ an ideal which is maximal among the collection of all ideals J satisfying the condition $\phi J \subset J$. It turns out that I is a *radical ideal* and thus $PV := R/I$ has no nilpotent elements. The extension PV of K has the properties:
(1) ϕ extends to an automorphism of PV.
(2) There is an invertible matrix F, called a fundamental matrix, with coefficients in PV satisfying $\phi(F) = AF$.
(3) PV has only trivial ϕ-invariant ideals.
(4) PV is generated over K by the coefficients of a fundamental matrix.

An extension of K with the properties (1)-(4) above is called *a Picard-Vessiot extension* for the equation $\phi(v) = Av$ over the field K. We have seen that such an object exists. It can be shown that the Picard-Vessiot extension is unique up to isomorphism and that its set of constants is again C.
The Galois group G of the equation $\phi(v) = Av$ over K is the group of the automorphisms of PV/K which commute with ϕ. This group acts on the n-dimensional C-vector space Sol of all solutions of the equation with coordinates in PV. As before G is a linear algebraic subgroup of $Gl(Sol) = Gl(n, \mathbb{C})$.

Example 1 In this example we will demonstrate that the Picard-Vessiot extension of K can have zero divisors.
One considers the equation $f(z + 1) = \zeta f(z)$ with ζ a primitive nth root of unity (and $n > 1$). Let any ring extension $A \supset K$ be given, such that
(i) A is a domain with a ϕ-action extending ϕ on K.
(ii) C is the set of constants of A.
Suppose that $f \in A$ satisfies the equation $\phi(f) = \zeta f$. Then $\phi f^n = f^n$ and $f^n \in C$ and thus $f \in C$. Therefore $f = 0$.

The construction above leads to the Picard-Vessiot extension $PV = K[X]/I$ with $\phi X = \zeta X$ and I maximal among the ϕ-invariant ideals. It is easily seen that

$I = (X^n - 1)$ is such an ideal. The ring $PV = K[X]/(X^n - 1)$ has clearly zero divisors. The Galois group is the cyclic group of order n.

3.2 The difference field $C(z)$ with $\phi(z) = z + 1$

We recall the three basic questions:

1. Which algebraic subgroups of $Gl(n, C)$ are difference Galois groups?
2. Is the difference Galois group of an equation computable?
3. Can one find "symbolic solutions"?

The answer depends on the choice of the difference field. We will consider here the situation of an ordinary difference equation in characteristic 0, i.e. $K = C(z)$, C an algebraically closed field of characteristic 0 and $\phi(z) = z + 1$. A rather deep result holds in this case ([6]):

Theorem 2
G is the smallest algebraic subgroup of $Gl(n, C)$ such that the equation $\phi(v) = Av$ can be transformed into $\phi(w) = \phi(B^{-1})AB\, w$ with $\phi(B^{-1})AB \in G(K)$.

With regard to question 1, the current situation is:

- It is *conjectured* that an algebraic subgroup G of $Gl(n, C)$ is the Galois group of an ordinary difference equation if and only if G/G^o is cyclic.
- The previous theorem implies that any difference Galois group G has the property that G/G^o is cyclic.
- Any connected algebraic subgroup of $Gl(n, C)$ is a difference Galois group.
- For many algebraic subgroups $G \subset Gl(n, C)$ with G/G^o cyclic, it is proved that G is a difference Galois group.

The questions 2. and 3. are strongly related. We will sketch how the previous theorem solves both questions for $n = 2$. The method can be seen as a "Kovacic algorithm" for ordinary difference equations.

3.2.1 An algorithm for ordinary difference equations of order two

The field C is supposed to be a "computable" field. In practice we may suppose that $C = \bar{\mathbb{Q}}$. The difference equation of order two can be written in the form

$$\phi^2(y) + a\phi(y) + by = 0 \text{ with } a, b \in K,\ b \neq 0.$$

The first step is the classification of the possible algebraic groups $G \subset Gl(2, C)$ which can be difference Galois groups:
1. Any reducible group with G/G^o finite cyclic.
2. Any infinite imprimitive group with G/G^o finite cyclic.
3. Any group containing $Sl(2, C)$.

Associated to the equation above is the *Riccati equation* $u\phi(u) + au + b = 0$. One has:

(a) If there is no solution $u \in K$ then G is irreducible.
(b) If there is one solution u then G is of type 1, but not a diagonal group.
(c) If there are two solutions u then G is a diagonal group, not contained in C^*Id.
(d) If there are more than two solutions then $G \subset C^*Id$.

There is a quick algorithm for finding the possible u's. It consists of finding locally at $z=\infty$ the possible expansions of u and then trying to match those expansions with a rational function.
In the cases (b), (c) and (d) one has essentially to study rank one difference equations in order to calculate G. In case (a) one has to find out whether the group G is imprimitive or not. This is done with the criterion:

G is imprimitive if and only if the equation

$$\phi^2(E)E + \left(\phi^2\left(\frac{b}{a}\right) - \phi(a) + \frac{\phi(b)}{a}\right)E + \frac{\phi(b)b}{a^2} = 0 \textit{ has a solution } E \in K.$$

If E exists then the equation is equivalent to $\phi^2(y) + ry$ where $r = -a\phi(a) + \phi(b) + a\phi^2(E + \frac{b}{a})$. The equation $\phi^2(y) + ry$ is seen as an order one equation for ϕ^2 in the place of ϕ. This can easily be solved and G can be determined.
If E does not exist then G contains $Sl(2,C)$. The precise form of G can be determined by considering the second exterior product, i.e. the rank one equation $\phi(f) = -af$.

This ends the algorithm which determines the difference Galois group G. One can define “symbolic solutions” in a way similar to the case of differential equations. All solutions are symbolic if and only if G^o is a solvable group.

We remark that this algorithm is less involved than Kovacic's algorithm since we do not have to consider the finite subgroups of $Gl(2,C)$ which are not cyclic.

Example 3 $\phi^2(y) + z\phi(y) + zy = 0$. There is only one solution for the Riccati equation, namely $u = \frac{1-z}{z-2}$. Using this one can transform the equation in matrix form

$$\phi(v) = \begin{pmatrix} -1 & -\frac{z^3-6z^2+9z-3}{(z-1)^2(z-2)^2} \\ 0 & -z \end{pmatrix} v.$$

From this form one concludes that the Galois group is $G = \{\begin{pmatrix} \alpha & \beta \\ 0 & \delta \end{pmatrix} \mid \alpha^2 = 1\}$.
Moreover all the solutions are “symbolic”.

4 q-Difference equations with general q

Let C be an algebraically closed field of characteristic 0. The field $C(z)$ is equipped with the automorphism ϕ given by $\phi(z) = qz$. We suppose that q is $\neq 0$ and is *not a root of unity*. Then the field of constants is the algebraically closed field C.

The Picard-Vessiot theory, the Galois theory and the algorithms resemble those of ordinary equations. However the structure is more complicated due to the following result:

The Galois group G of an equation has the property that G/G^o is a commutative group generated by at most two elements.

A new feature of q-difference equations, when compared with ordinary difference equations, is the existence of *two* points, namely 0 and ∞, where one can study the equation locally. A particular nice set of equations are the equations $\phi(v) = Av$, which are trivial locally at 0 and ∞. We will call those equations *regular*. The precise definition is that the equations are both over $C((z))$ and $C((z^{-1}))$ equivalent to the trival equation $\phi(v) = Iv$ with I the identity matrix. In the case $C = \mathbb{C}$ one can compare the local solutions at 0 and ∞. This leads to a *connection matrix* which determines the Galois group of the regular equation. This is used to prove the following noticable result

Theorem 4 *An algebraic subgroup G of $Gl(n, C)$ is the Galois group of a regular q-difference equation if and only if G is connected.*

In [6] and [1] one can find the current results about the "inverse problem" of the Galois theory, a "Kovacic algorithm" for equations of order two and the interesting hypergeometric q-difference equation.

5 More equations

There are other types of equations. Of particular interest are:

1. *Differential equations in characteristic $p > 0$*
2. *q-Difference equations with q a root of unity.*
3. *Ordinary difference equations in charateristic $p > 0$.*

The previous methods and theory fails to work here. The main problem is the non-existence of a good Picard-Vessiot theory. The reason for this seems to be that the field of constants cannot be algebraically closed.

Let us sketch the situation in the first case, that of differential equations in characteristic $p > 0$. The derivation $'$ of the differential field K is supposed to be non trivial. If every element $a \in K$ is a pth power, then one finds the contradiction $a' = (b^p)' = pb^{p-1}b' = 0$ and $'$ is identically zero. Thus it is essential that K is not algebraically closed.

We continue with a standard situation $K = k(z)$, with k is algebraically closed and $' = \frac{d}{dz}$. The field of constants is $k(z^p)$. This is a rather big field and close to K itself. Consider the equation $v' = av$ with $a \in K^*$ chosen such that there is no solution $\neq 0$ in K (e.g. $a = z$). As before, one tries to make a Picard-Vessiot extension of the form $R = K[X, X^{-1}]/I$. On $K[X, X^{-1}]$ one extends $'$ by the formula $X' = aX$. The ideal I is chosen maximal among the ideals J with $J' \subset J$. Choose any $\lambda \in k(z)^*$. Let $I(\lambda) \subset R$ be the ideal $(X^p - \lambda^p)$. This ideal is clearly invariant under $'$, since $(X^p - \lambda^p)' = 0$. Any bigger ideal has the form $(X - \lambda)^i$ for some i with $0 < i < p$ and is not invariant under differentiation. Thus $I(\lambda)$ is maximal among the $'$-invariant ideals and $R(\lambda) := R/(X^p - \lambda^p)$ should be a Picard-Vessiot extension for the equation $y' = ay$. We note that $R(\lambda)$ has nilpotent elements. This is not a serious obstruction. The main difficulty is that the differential rings $R(\lambda_1)$ and $R(\lambda_2)$ are isomorphic if and only if $\frac{\lambda_1}{\lambda_2} \in K^p$. What we found can be formulated as: "the equation $y' = ay$ admits non-isomorphic Picard-Vessiot extensions". The conclusion must be that there is no suitable Picard-Vessiot theory which defines the Galois group of the differential equation $y' = ay$.

The machinery of Tannakian categories is the theory which produces a suitable Galois theory for the three types of equations that we have mentioned above. In fact, the Tannakian approach also works for the equations considered earlier and produces the same Galois theory. We will not go into this but try to translate the results in an elementary way for special cases.

6 Differential equations in characteristic $p > 0$

Take $K = k(z)$ with $k = \bar{k} \supset \mathbb{F}_p$ and $' = \frac{d}{dz}$. The field of constants is $K^p = k(z^p)$. An equation reads in matrix form $(\frac{d}{dz} - A)v = 0$. The operator $\frac{d}{dz} - A$ acts on K^n. Then $\psi := (\frac{d}{dz} - A)^p : K^n \to K^n$ is a K-linear! operator called the *p-curvature*. This ψ determines the equation in this special situation. From ψ one can construct a commutative p-Lie algebra over $K^p = k(z^p)$ and also a commutative algebraic Galois group of height one with this prescribed p-Lie-algebra.

Example 5 The p-curvature of the equation $y' = ay$ is the 1×1 matrix $a^{(p-1)} + a^p \in K^p$. The p-curvature of the equation $y'' = ry$ is the matrix

$$\begin{pmatrix} -1/2f' & fr - 1/2f'' \\ f & 1/2f' \end{pmatrix},$$

where f is a special solution of the equation $f^{(3)} - 4f^{(1)}r - 2fr^{(1)} = 0$ (the second symmetric power of the original equation).

One of the interesting points about differential equations in positive characteristic is the link with differential in characteristic 0. We will explain this in the special situation of a differential equation over the differential field $\mathbb{Q}(z)$ (with $' = \frac{d}{dz}$). In order to find the Galois group (or symbolic solutions) for the equation $y' = Ay$ we have seen that the local Galois groups, i.e. the Galois groups over the completions $\mathbb{Q}(z)_v$ (for points $v \in \mathbb{P}^1(\bar{\mathbb{Q}})$), are rather important. There are other completions. For every rational prime p one can consider the same equation over the field $\mathbb{Q}_p(z)$. The Galois group over this field is closely related with the study of the reduction of the equation modulo the prime p (which has a sense for all but finitely many primes). This seems to be the idea for *Grothendieck's conjecture* which can be formulated as:

All the solutions of the matrix equation $y' = Ay$ over the field $\mathbb{Q}(z)$ are algebraic over this field if and only if for all but finitely many primes p the p-curvature of the reduction modulo p is zero.

N. Katz has extended this conjecture to one which describes the Lie-algebra of the Galois group in terms of the p-curvature for almost all primes p. Moreover N. Katz has proved that Grothendieck's conjecture holds for differential equations coming form algebraic geometry and (more recently) for "rigid" differential equations.

7 q-Difference equations with $q^m = 1$

One considers the difference field $K = C(z)$ where: C an algebraically closed field of characteristic 0 and $\phi(z) = qz$ and $q^m = 1$ for some integer $m > 0$.

We note that the field of constants $C(z^m)$ is rather big and close to K itself. An equation in matrix form $\phi(v) = Av$ can be rewritten as an operator $A^{-1}\phi : K^n \to K^n$. This operator is $\mathbb{C}(z^m)$-linear. The *m-curvature* of the equation is defined as the operator $\psi_m = (A^{-1}\phi)^m : K^n \to K^n$. The main result is that the operator ψ_m is K-linear and determines the equation!
The Galois group, defined by means of a suitable Tannakian category, turns out to be the algebraic subgroup of $Gl(n, \mathbb{C}(z^m))$ generated by ψ_m.
It seems that equations of this type have some interest in theoretical physics.

8 Ordinary difference equations for $p > 0$

We summarize this theory. The difference field is $K = k(z)$ with $k = \bar{k} \supset \mathbb{F}_p$, $\phi(z) = z + 1$. The field of constants $k(z^p - z)$ is again rather big. Any matrix equation $\phi(v) = Av$ can be transformed into an operator $(A^{-1}\phi) : K^n \to K^n$. The p-curvature is defined as $\psi = (A^{-1}\phi)^p : K^n \to K^n$. The main result is that the map ψ is K-linear and determines the equation.
In particular, $\psi \in Gl(n, k(z^p - z))$ and the Galois group is the algebraic subgroup of $Gl(n, k(z^p - z))$ generated by ψ.

It is tempting to compare ordinary difference equations over $\mathbb{Q}(z)$ with their reductions modulo primes p (this reduction exists for all but finitely many primes p). Consider the ordinary difference equation

$$y(z+1) = \frac{z + 1/2}{z} y(z) \text{ over the field } \mathbb{Q}(z).$$

It has no algebraic solution $\neq 0$ over $\mathbb{Q}(z)$ and its Galois group is therefore the multiplicative group $\mathbf{G}_m$.

However for $p > 2$ the p-curvature of the reduced equation is

$$\frac{z+p-1+1/2}{z+p-1} \cdots \frac{z+1+1/2}{z+1} \cdot \frac{z+1/2}{z} \equiv 1 \text{ modulo } p.$$

In fact, there is a non zero solution for the equation over $\mathbb{F}_p(z)$. Let $k \equiv 1/2$ modulo p with $0 < k < p$. Then $y(z) := z(z+1)\ldots(z+k-1)$ is a solution.
This example shows that the naive formulation of Grothendieck's conjecture for ordinary difference equations is false! The example is not well understood and we do not know how to formulate Grothendieck's conjecture for ordinary difference equations.

References

1. P.A. Hendriks - *Algebraic Aspects of linear Differential and Difference Equations* - Thesis November 1996, Rijksuniversiteit Groningen.
2. M. van Hoeij - *Factorization of linear Differential Operators* - Thesis November 1996, Katholieke Universiteit Nijmegen.
3. J.J. Kovacic - *An algorithm for solving second order linear differential equations* - J. Symb. Comp. 2 (1986), 3-43.
4. A.H.M. Levelt - *Jordan decomposition for a class of singular differential operators* - Arkiv för Matematik 12(1) (1975), 1-27.
5. A.H.M. Levelt - *Differential Galois theory and tensor products* - Indag. Mat. 1 no 4 (1990), 439-449.
6. M. van der Put and M.F. Singer - Galois theory of difference equations - to appear in Lect. Notes in Math. Springer Verlag 1997.
7. M. van der Put - *Differential equations in characteristic p* - Compositio mathematica 97 (1995), 227-251.
8. R. Sommeling - *Characteristic Classes for Irregular Singularities* - Thesis June 1993, Katholieke Universiteit Nijmegen.
9. M.F. Singer and F. Ulmer - *Liouvillian and algebraic solutions of second and third order differential equations* - J. of Symb. Comp. 16(1) (1993), 9-13.

SOLVING DIFFERENTIAL EQUATIONS BY COMPUTER ALGEBRA

MALCOLM A.H. MACCALLUM
School of Mathematical Sciences
Queen Mary and Westfield College
London E1 4NS
UK
M.A.H.MacCallum@qmw.ac.uk

Abstract.
An overview is given of what can be done to solve ordinary differential equations by computer algebra, focussing in particular on the work of the CATHODE project, in which Levelt was a partner, and within that on the exact solution methods. The importance of Levelt's areas of interest to this work is shown.

1 Introduction

I was quite shocked to find myself at Ton's retirement. Ton seemed much too young to be retiring. I am not sure when we first met, but I think it was at the 1988 CADE meeting organized by Evelyne Tournier and others. From this and the early stages of planning our European collaboration on differential equations, I got to know him well. From the start I was impressed by his energy and enthusiasm. I was also very aware of his human warmth, which, if I may tease him, occasionally turns into fiery heat. Fortunately on those occasions his good humour, his human sympathies, and his liking for stimulating discussions quickly return. I have enormously enjoyed his company and his breadth of understanding and interests during the last few years.

I was not sure who to talk to. Ton Levelt? The rest of the audience about Ton? In the end I suppose I opted mainly for the latter, in that I said again some things Ton had heard me say before ([19, 20]). I can only hope that although he is a mathematician he will be like the physicists who are said to enjoy nothing better than having explained to them something they know perfectly well already. Whether I can live up to the qualification 'clearly explained', which is usually added, remains to be seen.

2 The CATHODE project

Ton Levelt and I were two of the partners in the ESPRIT Working Group CATHODE = Computer Algebra Tools for Handling Ordinary Differential Equations. Our motivation, to quote the original application, was

> To provide a portable computerized toolkit (CATHODE) for analytically studying ordinary differential equations (ODEs) that scientists and engineers throughout industry and academia would use on their workstations in conjunction with numerical methods and simulators currently running on supercomputers.

Among the many parts to this task are:

- making use of the best methods in the extensive literature
- combining them, which had not been done before
- adding new high-level methods
- expressing resulting algorithms in a portable way, with common primitives
- implementing the result in one or more algebra systems
- providing interfaces to numerical and graphical techniques

Note that the first 3 of these are mathematical in orientation while the other three are more IT-oriented. Nijmegen has contributed to them all (the last only rather indirectly).

It is natural to ask why one would want to do this. There are very sophisticated numerical methods for ordinary differential equations and systems. Do we need analytic methods? There are several reasons, for example

- When available, a formula covers all cases and is accurate, saving multiple numerical integrations
- one can vary parameters
- one can use the result in a subsequent stage of calculation (this is to my mind very important, and we should remember it when considering outputs from our programs)

What difficulties did we face?

- The wide range of types of equation and system
- The correspondingly enormous number of methods, mostly somewhat heuristic
- The difficulty of devising a systematic framework for these

The variety of equations and systems to be dealt with can be shown by considering the following alternatives:

- single equations or systems
- linear or nonlinear
- first or higher order

The variety of results sought from analysis may also be considerable, e.g.

- closed form solutions
- first integrals
- series solutions
- normal forms
- symmetries
- bifurcations
- numerical and graphical results

3 Levelt and the research done within CATHODE

In my talk, I could not compress more than 70 pages of reports, which were themselves already compressed, into 30 minutes. The greatest advances have come in linear equations and systems. This is one of the areas where Ton Levelt played an important part. From the beginning he saw the importance of fast methods for operations such as normal form calculations, and his ideas were very important in the development of the tools we have now. The pervasiveness of linear methods has driven the development of the common primitives for linear differential operators and related problems which was a major success (and of which Thom Mulders' Maple code made the crucial test).

Differential Galois theory, which I learnt partly from Ton's 'Indigationes Mathematicae' paper ([14]), has also played a big part. (The approach taken there is similar that of van der Put's contribution to this meeting, not, as Levelt remarked, entirely coincidentally!) This topic concerns linear equations or systems with coefficients in a differential field k, from which one can form the Picard-Vessiot extension, the differential field $K = k\langle y_1, y_2, \ldots, y_n\rangle$, where the y_i are the solutions linearly independent over k. K is an n-dimensional vector space over k. The differential Galois group consists of the differential field automorphisms of K which leave k fixed.

Use of the resulting concepts and theorems to actually solve equations, at least for equations of order 2 and 3, has developed enormously during our collaboration, and in particular has been related to factorization of linear differential operators ([28, 29]). The new work has been largely concerned with the algebraic aspects, but one of Ton's strengths is the recognition of the relation of this to local and global analytic properties. As I expected, that appeared in his own talk at the meeting and that of Mark van Hoeij.

He has also always had a strong motivation to applications, perhaps in part due to his family connections (note the references in [15]), and has been one of our more successful contactors of industry (oddly since he professes to be a real pure mathematician).

Finally, he is, among our group, one of the most knowledgeable about differential algebra and differential Gröbner bases, as well as normal Gröbner bases (cf. [4] and [16]).

In my remaining time I want, without too many details, to use the particular sub-part of CATHODE concerned with closed form solutions as a sample subject to give some sense of the interrelatedness of these areas of interest I just mentioned, though I must point out that those themes have been at least as significant in series developments of solutions of linear systems around singular points, and normal forms of non-linear systems.

4 Closed form solutions of single equations

A useful organizing principle for explaining the currently-known techniques is provided by Lie symmetry methods, as discussed in recent texts ([23, 30]), and so that is where I will begin.

A *Lie point transformation* for an ODE

$$y^{(n)} = \omega(x,\, y,\, y',\ldots,\, y^{(n-1)})$$

in variables x, y is a mapping

$$x \to \bar{x}(x,\, y), \qquad y \to \bar{y}(x,\, y).$$

It is a *Lie point symmetry* if the new variables obey the original equation,

$$H(x,\, y,\, y',\, \ldots) = 0.$$

We are usually interested only in continuous families of Lie point symmetries. Then we can impose $\mathbf{X}H = 0$ (mod $H = 0$) where the operator $\mathbf{X}$ is defined to be

$$\mathbf{X} = \xi\partial_x + \eta\partial_y + \eta'\partial_{y'} + \ldots,$$

using the abbreviated notation for partial derivatives (so $x \to x + \epsilon\xi$ etc is the infinitesimal transformation). There are formulae to get η' etc from η and ξ, a process known as prolongation.

For normal types of H, equating coefficients in this equation gives an overdetermined set of PDEs (in this case, linear ones, but when one investigates more general symmetries, they may be non-linear). The formal methods of reduction come exactly from differential algebra and differential Gröbner bases, though in practice these methods are often mixed with heuristic use of integrations.

Eventually one hopes to isolate one of the dependent variables (using a lexicographic order of terms in a Gröbner basis calculation), and then one wants, hopes and expects to end up solving a series of linear homogeneous equations (so we reach for our differential Galois theory) or single first-order equations.

These two types of outcome have a grim irony: they are themselves exactly the cases where Lie symmetry is useless (in the linear case because the Lie symmetries include addition of the complementary function, and in the first-order case because there are infinitely many Lie symmetries but no algorithm). Let us look further at the first-order case.

Suppose we have an equation $P\,dy/dx = Q$ or a system $\dot{x} = P,\ \dot{y} = Q$, with P and Q in $k[x, y]$ for some field k. If $D = P\partial_x + Q\partial_y$, these are solved if we can find a function $F(x, y)$ such that $DF = 0$ (with F non-trivially dependent on the variables). Darboux showed how to tackle this using what we now call 'Darboux polynomials', which are solutions of $Df = fg$ for some g, and this was re-investigated in [25] (which proved the essential theorem that all elementary F took a form which generalises in a simple way Liouville's theorem for integrals and set the method out as a clear procedure). With my student Y.K. Man, we found more effective ways to implement this, which in particular can be done over the integers if P and Q have rational coefficients, except for a final integration step which may introduce algebraic extensions ([22]).

As an example, consider the (disguised linear) equation

$$y\frac{\mathrm{d}y}{\mathrm{d}x} + y^2 + 4x(x+1) = 0$$

$P = y$, $Q = -(y^2+4x(x+1))$. In our method, we look for Darboux polynomials whose leading and trailing homogeneous parts are products of irreducible factors over the integers of the leading and trailing parts of $xQ - yP$ which is $-(x+1)(y^2+4x^2)$ here. One such is obviously $f = (y^2 + 4x^2)$, and one quickly finds $1/f$ is an integrating factor, leading to the solution

$$x + \frac{1}{2}\log(y^2 + 4x^2) = c$$

where c is an arbitrary constant.

These ideas, remarkably, fed back (though only partially due to CATHODE) into the study of linear systems and equations, through the work of Weil ([32]), who showed some beautiful relations between Darboux polynomials (in this more general context) and differential Galois theory. For example, for a linear system $\dot{\mathbf{y}} = \mathbf{A}\mathbf{y}$, the Darboux polynomials are given by the differential invariants and semi-invariants of the differential Galois group, and are findable as solutions of suitable symmetric products of the corresponding linear operator (now where did I put that introduction to differential Galois theory?).

This has led to a simpler and quite effective implementation, due to Ulmer and Weil, of the Kovacic algorithm for finding Liouvillian solutions (solutions "in closed form") of second-order linear equations ([31]). [It must be noted that at the time CATHODE started, the known versions of Kovacic and similar algorithms required some quite unpleasant calculations (and were not really effective), and had not been very closely related to factorization of operators. The developments during the CATHODE period, by Singer, Ulmer, Weil, Bronstein, van der Put and Hendriks, and Zharkov, altered the picture greatly. We now have more rational methods, very much related to the properties of the symmetric powers of the operator in the input equation. They rest on a deeper understanding of differential Galois group structures and properties.] I should mention that factorization of linear operators (cf. van Hoeij), normal forms of linear systems, linear algebra, and Gröbner bases all reappear in these methods.

Another generalization of the use of Darboux polynomials has been to nonlinear equations linear in their leading derivative: for instance, [1] has shown how in that case there are ways to exploit the special form of the system to reduce the task of finding first integrals to systems of more elementary equations. The examples included the Painlevé equations (whose interest arises precisely from the properties of their singularities). Yet another very active area (though not within CATHODE) has been the use of Darboux polynomials in studying the behaviour of plane dynamical systems and in particular in attempts to explore Hilbert's still-unsolved 16th problem (see e.g. [8, 17, 26, 7]).

5 Equivalence problems

Mention of dynamical systems brings us back to applications. Now it is time for a confession. I have been pretending to be a sort of pure mathematician or perhaps computer scientist. But I really work in general relativity, and I just got dragged into all this differential equations stuff by several accidents. Apart from Lie symmetries, which happened to be a second interest of my close friend and colleague Hans Stephani, the main one was an interest in a problem which can be expressed as "Where (and when) are we?".

More formally, if we have two (pseudo-)Riemannian four-dimensional metrics, which describe (coordinate patches in) space-times satisfying Einstein's equations, how do we test whether they are the same solution in different coordinates? There is a classical procedure initially given in [6], refined by [5], [3] and [13], which has now become practicable (for technical reasons it is not formally decideable, but this is not the obstacle in real-life cases, see [18]). Completing the method in such a way as to make it usable in practice, and exploiting it in examples, has formed a large part of my research since 1980, and I still work on it a good bit of my time. (For a review see [21].)

The method is essentially to use the fact that the structure group (in this case the Lorentz group) and the connection define uniquely a set of vector (or covector) fields on the frame bundle over the space-time, and that for isomorphism these sets of vector fields must map into each other identically (up to any ambiguity arising from symmetries of the space-times themselves).

Now what has this to do with differential equations? Well, the link is with the problem of transformations of differential equations which are not Lie or other symmetries, i.e. which genuinely alter the equation and may give a form simpler to solve. Indeed one can (only half jokingly) characterize the search for solution methods entirely as the search for reduction of the DEs to one of the forms $y' = 0$, $y'' = 0$ . . . which are the only ones we can really solve!

If we think of the equations in terms of a connection in the manifold of a jet bundle J, the transformations create from it a larger bundle, locally $J \times G$, whose structure group G is given by the transformations allowed (appropriately prolonged). Unlike the frame bundle in relativity, this bundle need not have uniquely-defined vector fields (I think of it as being less rigidly determined than the frame bundle is by the Riemannian structure in relativity). To overcome this, and reach a suitably unique structure, one has to introduce two extra steps: (a) "Lie-algebra compatible absorption of torsion" in which the basis vectors are changed to simplify the derivatives (linear algebra, normal forms...) and (b) if the result is still non-unique one may need to repeat the construction of a higher bundle. (For the details, which I did not have time for in the talk, see [9, 11, 24].)

To show that this method might be useful, consider the following case: one can by this means characterize all second-order non-linear equations which are equivalent to a linear one under Lie point transformations in which $\bar{x} = \bar{x}(x)$ ([12]). The equations for the transformations required can themselves be reduced to a linear problem plus a non-linear one of lower order ([2]). This suggests we can obtain a strategy for solving such problems by considering equivalence. (The techniques are also related to the way [27] recently characterized all possible Lie symmetries of second- and third-order equations and [10], at QMW, all third order ones.)

Equivalence transformations are the complement of the (Lie or other) symmetries. So far, unlike the symmetries, they have not been much used in algorithms, except for the heuristic of trying standard and well-known simple transformations. Maybe they will be more important in future work. However, one may note that like Lie symmetries, they are again useless for single first-order equations (because all such equations are equivalent to $y' = 0$) and linear equations, so the other methods mentioned earlier are again important.

6 Conclusion

This brings me full circle, back to the Lie symmetries I began with, and in particular to the point that these variegated methods I have mentioned involve, often in combination, the themes with which I associate Ton Levelt.

References

1. Albrecht, D.W., Mansfield, E.L., and Milne, A.E. (1996). Algorithms for special integrals of ordinary differential equations. *J. Phys. A* **29**, 973–991.
2. Bocharov, A.V., Sokolov, V.V., and Svinoloupov, S.I. (1993). On some equivalance problems for differential equations. Preprint, WRI/Ufa.
3. Brans, C.H. (1965). Invariant approach to the geometry of spaces in general relativity. *J. Math. Phys.* **6**, 95–102.
4. Buchberger, B. (1985). Grobner bases: an algorithmic method in polynomial ideal theory, in *Recent trends in multidimensional systems theory*, ed. N.K. Bose. (D. Reidel, Dordrecht).
5. Cartan, É. (1946). *Leçons sur la geomètrie des éspaces de Riemann* (Gauthier-Villars, Paris).
6. Christoffel, E.B. (1869). Über die transformationen der homogen differential ausdrücke zweiten grades. *J. Reine Angew. Math.* **70**, 46–70.
7. Christopher, C.J. (1994). Invariant algebraic curves and conditions for a centre. *Proc. Roy. Soc. Edin. A* **124**, 1209–1229.
8. Collins, C.B. (1993). Algebraic conditions for a centre or a focus in homogeneous systems of arbitrary degree. Preprint, University of Waterloo.
9. Gardner, R. (1989). *The method of equivalence and its applications*, CMBS 58, (SIAM Press, New York).
10. Grebot, G. (1994). On Killing tensors in vacuum space-times and the classification of third order ordinary differential equations. Ph.D. thesis, QMW, London.
11. Kamran, N. (1989). Contributions to the study of the equivalence problem of Élie Cartan and its applications to partial and ordinary differential equations. *Memoires Cl. Sci. Acad. Roy. Belg.* **45**(7).
12. Kamran, N. and Shadwick, W.F. (1986). The solution of the Cartan equivalence problem for $dy^2/d^2x = f(x, y, dy/dx)$ under the pseudo-group $\bar{x} = \phi(x)$, $\bar{y} = \psi(x, y)$, in *Field theory, quantum gravity and strings*, ed. H.J. de Vega and N. Sanchez, volume 246 of *Springer Lecture Notes in Physics.* (Springer-Verlag, Berlin and Heidelberg).
13. Karlhede, A. (1980). A review of the geometrical equivalence of metrics in general relativity. *Gen. Rel. Grav.* **12**, 693–707.
14. Levelt, A.H.M. (1990). Differential Galois theory and tensor products. *Indag. Math.* **1**, 439–450.
15. Levelt, A.H.M. (1995a). Van der waals, Korteweg, van Laar: a MAPLE excursion into the thermodynamics of binary mixtures, in *Studies for computer algebra in industry, vol. 2*, ed. A.M. Cohen, L.J. van Gastel, and S.M. Verduyn Lunel, pages 227–238. (John Wiley and Sons, Chichester).
16. Levelt, A.H.M. (1995b). Various problems solved by computer algebra, in *Studies for computer algebra in industry, vol. 2*, ed. A.M. Cohen, L.J. van Gastel, and S.M. Verduyn Lunel, pages 43–59. (John Wiley and Sons, Chichester).
17. Lloyd, N.G. and Pearson, J.M. (1993). Limit cycles and centres: an example, in *Differential equations, dynamical systems and control science*, ed. K.D. Elworthy, W.N. Everitt, and E.B. Lee, pages 143–158. (Marcel Dekker, New York).
18. MacCallum, M.A.H. (1991). Computer-aided classification of exact solutions in general relativity, in *General relativity and gravitational physics (9th Italian Conference)*, ed. R.

Cianci, R. de Ritis, M. Francaviglia, G. Marmo, C. Rubano, and P. Scudellaro, pages 318–337. (World Scientific, Singapore).

19. MacCallum, M.A.H. (1995a). Goals of Cathode, overview of problems, research and results, in *Cathode Workshop Nijmegen*, ed. A.H.M. Levelt, pages 9–14. (University of Nijmegen, Department of Mathematics).
20. MacCallum, M.A.H. (1995b). Using computer algebra to solve ordinary differential equations, in *Studies for computer algebra in industry, vol. 2*, ed. A.M. Cohen, L.J. van Gastel, and S.M. Verduyn Lunel. (John Wiley and Sons, Chichester).
21. MacCallum, M.A.H. and Skea, J.E.F. (1994). SHEEP: a computer algebra system for general relativity, in *Algebraic computing in general relativity (Proceedings of the first Brazilian school on computer algebra, vol 2)*, ed. M.J. Rebouças and W.L. Roque, pages 1–172 and index pp. 361–9. (Oxford University Press, Oxford).
22. Man, Y.K. and MacCallum, M.A.H. (1997). A rational approach to the Prelle-Singer algorithm. *J. Symb. Comp.* **24**, 31–43.
23. Olver, P.J. (1986). *Applications of Lie groups to differential equations* (Springer-Verlag, Berlin and Heidelberg).
24. Olver, P.J. (1995). *Equivalence, invariants, and symmetry* (Cambridge University Press, Cambridge).
25. Prelle, M.J. and Singer, M.F. (1983). Elementary first integrals of differential equations. *Trans. Amer. Math. Soc.* **279**, 215.
26. Schlomiuk, D. (1993). Elementary first integrals and algebraic invariant curves of differential equations. *Expositiones Math.* **11**, 433–454.
27. Schwarz, F. (1995). Symmetries of 2nd and 3rd order ODE's, in *ISSAC 95*, ed. A.H.M. Levelt, pages 16–25. (ACM Press, New York).
28. Singer, M.F. and Ulmer, F. (1993a). Galois groups of second and third order linear differential equations. *J. Symb. Comp.* **16**, 9–36.
29. Singer, M.F. and Ulmer, F. (1993b). Liouvillian and algebraic solutions of second and third order linear differential equations. *J. Symb. Comp.* **16**, 37–73.
30. Stephani, H. (1989). *Differential equations - their solution using symmetries*, ed. M.A.H. MacCallum (Cambridge University Press, New York and London).
31. Ulmer, F. and Weil, J.A. (1996). Note on Kovacic's algorithm. *J. Symb. Comp.* **22**, 179–200.
32. Weil, J.-A. (1995). Constantes et polynomes de Darboux en algèbre différentialle: applications aux systèmes différentielles linéaires. Docteur en Sciences thesis, École Polytechnique, Palaiseau.

TOWARDS INTEGRATING THEOREM PROVING AND COMPUTER ALGEBRA (ABSTRACT)

BRUNO BUCHBERGER
Research Institute for Symbolic Computation
A4232 Schloß Hagenberg
Austria
Bruno.Buchberger@risc.uni-linz.ac.at

1 The Next Goal for Symbolic Computation

Symbolic computation aims at automating mathematical problem solving in all areas of mathematics and for all phases of mathematical work:

- for the phase of *exploring* a problem and experimenting with known concepts, theorems and algorithms that may be relevant for the solution of the problem with the goal of arriving at conjectures for new theorems on the basis of which the problem can be solved,
- for the phase of *proving* conjectures,
- for the phase of *programming*, i.e. turning relevant theorems into computer-implemented algorithms.

Current symbolic computation software systems are quite impressive in terms of the range of mathematical problems for which algorithms have been invented and implemented, wich can be used in the phase of *exploring* given problems. Also, the software technology provided by these systems for *programming* new algorithms is quite satisfactory. In contrast, relatively little help is given to the user of these systems in the phase of *proving* theorems. On the other hand, existing theorem proving systems are quite strong (but still not strong enough) for support in the proving phase but quite weak in the exploring and programming phase.

We believe that one of the most natural, important, and challenging features of the next generation of symbolic computation systems should be the availability of tools for supporting the phase of *proving* theorems. In this talk we summarized, by sketching the main ideas and giving some examples, two approaches for expanding current symbolic software systems by tools for computer-supported proving:

- theorem proving by *reduction to algebraic algorithms*,
- theorem proving by imitating human general and special proof techniques (the *"Theorema"* project).

2 Theorem Proving by Reduction to Algebraic Algorithms

In the past two decades, this approach has been developed very successfully for various special classes of mathematical propositions: For each of these classes P of propositions, a translation functions T has been invented that maps P into a class of algebraic problem instances for which we have a solution algorithm. One then proves, on the meta-level, that

$$p \in P \text{ is true iff } A(T(p)) = \text{ TRUE.}$$

Examples of this approach are:

- the automated decision about the truth of certain *geometrical propositions in a formulation using coordinates* by reduction to the computation of Groebner bases, see the tuturial (Wang 1998, [11]);
- the automated decision about the truth of *propositions in the theory of real closed fields* by reduction to the computation of certain "cylindric algebraic decompositions" of Euclidean space, introduced in (Collins 1975, [7]), see also the collection of recent research articles (Caviness, Johnson 1998, [5]);
- the automated decision about the the truth of certain *geometrical propositions – and the automatic generation of such propositions – in coordinate-free formulation* by reduction to the algebraic problem of "Cayley factorization", see (Sturmfels 1993, [10]), p. 110;
- the proof of first-order equalities in equational theories by reduction to simplification in "complete theories", using the completion algorithm introduced in (Knuth-Bendix 1970, [8]), see also (Buchberger, Loos 1982, [3]);
- the proof - and the automatic generation – of combinatorial identities involving the sum and product quantifiers by reduction to the computation of Groebner bases in non-commutative algebras and/or the computation of "greatest common factorials" using the Zeilberger-Paule approach, see the original articles (Paule 1995, [9]) and (Zeilberger 1991, [13]) and the tutorial (Chyzak 1998, [6]).

3 An Alternative: The *Theorema* Project

In order to close the gap between current symbolic computation systems and theorem proving systems one could start from either of the two sides. In the *Theorema* project, we decided to start from an existing computer algebra system, namely *Mathematica*, version 3.0, see (Wolfram 1996, [12]), and to add proving facilities. The basic design of the Theorema project was introduced in (Buchberger 1996, [1]), the current state is described in (Buchberger et al. 1997, [4]).

The *Theorema* system is being built up in the following layers:

- *A symbolic computation software system* (at present, *Mathematica* 3.0) as the basic *implementation frame.*
- *A mathematical language* as a common frame for both non-algorithmic and algorithmic mathematics. Basically, we take a version of higher order logic

(with the additional concept of "sequence variables", a concept borrowed from *Mathematica*). The syntax of this language is implemented by using the syntax extension facilities of *Mathematica*. The part of the language that consists of "executable formulae" (function definitions using induction and bounded quantifiers) gets a semantic interpretation by writing appropriate functions in *Mathematica*.

- The concept of "*functor*" as the general mechanism for building up towers of mathematical domains. Using higher-order variables, the Currying mechanism, and the module concept, functors can be implemented elegantly in *Mathematica*.
- A general *predicate logic prover* of a "natural style" introduced in earlier papers by Buchberger, see for example, (Buchberger, Lichtenberger 1981, [2]) implemented in *Mathematica*.
- Various *special theorem provers corresponding, in a natural way, to the various functors* that build up mathematical domains. The design and implementation of these provers is the present main priority in the *Theorema* project. All these provers produce proofs that imitate "natural" proof styles of human mathematicians. By now, an induction prover for the natural numbers and one over the domain of lists over a given domain are already implemented, a prover for the domain of multivariate polynomials over a given domain of monomials is under way. Other special provers in this category (for the matrix functor, the power series functor, the finite sets functor, etc.) are planned. Currently, we also engage in the design of a special prover for the typical ϵ/δ proofs of analysis. All implementations are done in *Mathematica*.
- The incorporation of special *black-box theorem provers* that decide the validity of theorems by reduction to algebraic problems, see the previous section.
- A general facility that allows the *presentation of proofs in natural language and in the form of "nested cells"*, which is crucial for being able to read complicated proofs without losing the overview. This facility is based on the facilities for manipulating cells in *Mathematica* notebooks.
- Mechanisms for the *automatic generation of complicated knowledge bases* from algebraic properties of given domains and the definition of functors.

References

1. Bruno Buchberger. Symbolic Computation: Computer Algebra and Logic. In: *Proceedings of the Frontiers od Combining Systems Conference*, Munich, March 26-29, 1996, Applied Logic Series, Kluwer Academic Publishers, 1996, pp. 193-219.

2. Bruno Buchberger, F. Lichtenberger. *Mathematics for Computer Scientists: The Method of Mathematics*, German. Springer Verlag, Berlin - Heidelberg - New York, 1981.

3. Bruno Buchberger, Ruediger Loos. Algebraic Simplification. In: *Computer Algebra*, (B. Buchberger, G. Collins, R. Loos eds), Springer Wien - New York, 1982, pp. 11-43.

4. Bruno Buchberger, Tudor Jebelean, Franz Kriftner, Mircea Marin, Elena Tomuţa, Daniela Văsaru. A Survey of the Theorema Project. *Proceedings of the ISSAC 97 Conference*, (W. Kuechlin ed.), July 21-23, 1997 Maui, Hawaii, USA, ACM Publication, pp. 384-391.

5. Bob F. Caviness, Jeremy Johnson. *Quantifier Elimination and Cylindrical Algebraic Decomposition*. Text and Monographs in Symbolic Computation. Springer Verlag, Wien - New York, to appear 1998.

6. Frederic Chyzak. Groebner Bases, Symbolic Summation and Symbolic Integration. In: *Groebner Bases and Applications*, (B. Buchberger, F. Winkler eds.), Cambridge University Press, to appear 1998.

7. George E. Collins. Quantifier Elimination for Real Closed Fields by Cylindrical Algebraic Decomposition. In: *Proceedings of the Second GI Conference on Automata Theory and Formal Languages*, Lecture Notes in Computer Science, Vol. 33, Springer, Heidelberg, pp. 515-532.

8. Donald E. Knuth, P.B. Bendix. Simple Word Problems in Universal Algebras. In: *Computational Problems in Abstract Algebra*, (J. Leech ed.), Pergamon Press, Oxford, pp. 263-297.

9. Peter Paule. Greatest Factorial Factorization and Symbolic Summation, *Journal of Symbolic Computation*, Vol. 20, pp. 235-268.

10. Bernd Sturmfels. *Algorithms in Invariant Theory*. Texts and Monographs in Symbolic Computation, Springer Verlag, Wien - New York, 197 pages, 1993.

11. Dongming Wang. Groebner Bases and Geometric Theorem Proving. In: *Groebner Bases and Applications*, (B. Buchberger, F. Winkler eds.), Cambridge University Press, to appear 1998.

12. Stephen Wolfram. *The Mathematica Book*. Cambridge University Press.

13. Doron Zeilberger. *The Method of Creative Telescoping*. Journal of Symbolic Computation, Vol. 11, pp.195–204.

ON THE LAGUTINSKII - LEVELT PROCEDURE

ANDRZEJ NOWICKI
N. Copernicus University
Faculty of Mathematics and Informatics
ul. Chopina 12–18, 87–100 Toruń
Poland
anow@mat.uni.torun.pl

1 Introduction

Let $k[X] = k[x_1, \ldots, x_n]$ be the polynomial ring in n variables over a field k of characteristic zero, and let $k(X) = k(x_1, \ldots, x_n)$ be the quotient field of $k[X]$. Assume that $f = (f_1, \ldots, f_n) \in k[X]^n$, and consider a system of polynomial ordinary differential equations

$$\frac{dx_i(t)}{dt} = f_i(x_1(t), \ldots, x_n(t)), \quad i = 1, \ldots n. \tag{1.1}$$

This system has a clear meaning if k is a subfield of the field $\mathbb{C}$ of complex numbers. When k is arbitrary then there also exists a meaning. It is well known and easy to be proved that there exists a solution of (1.1) in $k[[t]]$, the ring of formal power series over k in the variable t.

The present paper is devoted to the first integrals of the above system. An element φ of $k[X] \setminus k$ (resp. of $k(X) \setminus k$) is said to be a *polynomial* (resp. *rational*) *first integral* of the system (1.1) if the following identity holds

$$\sum_{i=1}^{n} f_i \frac{\partial \varphi}{\partial x_i} = 0. \tag{1.2}$$

Throughout the paper we use the vocabulary of differential algebra (see for example [15] or [16]). Let us assume that R is a commutative ring containing the field k and d is a k-*derivation* of R, that is, $d : R \to R$ is a k-linear mapping such that $d(ab) = ad(b) + d(a)b$ for all $a, b \in R$. We denote by R^d *the ring of constants* of d, that is, the kernel of d:

$$R^d = \{a \in R;\ d(a) = 0\}.$$

The set R^d is a k-subalgebra of R. If R is a field then R^d is a subfield od R containing k. If R is without zero divisors, the derivation d can be extended in a unique way to its quotient field by setting: $d(a/b) = b^{-2}(d(a)b - ad(b))$.

We shall use the above notations for the ring $k[X]$ and its quotient field $k(X)$. Let us note that a k-derivation of $k[X]$ is completely defined by its values on the variables $x_1, \dots, x_n$. If $f = (f_1, \dots, f_n) \in k[X]^n$ then there exists a unique k-derivation d of $k[X]$ such that $d(x_i) = f_i$ for all $i = 1, \dots, n$. This derivation is defined by

$$d(\varphi) = \sum_{i=1}^{n} f_i \frac{\partial \varphi}{\partial x_i}, \tag{1.3}$$

for any $\varphi \in k[X]$. Thus, the set of all polynomial first integrals of (1.1) coincides with the set $k[X]^d \setminus k$, where

$$k[X]^d = \{\varphi \in k[X];\ d(\varphi) = 0\}$$

and d is the k-derivation defined by (1.3). Moreover, the set of all rational first integrals of (1.1) coincides with the set $k(X)^d \setminus k$, where

$$k(X)^d = \{\varphi \in k(X);\ d(\varphi) = 0\}$$

and d is the unique extension of the k-derivation (1.3) to $k(X)$.

The rings of constants $k[X]^d$ and $k(X)^d$ are intensively studied from a long time; see for example [9], [10], [24], [26], [27], where many references on this subject can be found.

Derivations of polynomial rings play an important role in commutative algebra and algebraic geometry. Several known problems may be formulated using derivations of $k[X]$ and their rings of constants; in particular: the fourteenth problem of Hilbert, the Jacobian conjecture, the Cancellation problem. Many interesting results concerning polynomial derivations can be found in the papers of Arno van den Essen (University of Nijmegen) ([6], [7], [8], [9]). Note also that Harm Derksen (University of Nijmegen), in [3], showed that the famous Nagata's counterexample [23] to the fourteenth problem of Hilbert can be put in the form $k[X]^d$ for some k-derivation d with $n = 32$. Thus, he proved that there exists k-derivation d of $k[x_1, \dots, x_{32}]$ such that the ring $k[X]^d$ is not finitely generated over k. Today we know ([28], [4]), that there exists also such a derivation for $n \geq 7$.

If d is a given k-derivation of $k[X]$ then it is difficult to describe its ring of constants; to decide whether this ring is finitely generated or to find its generating set. But it is also difficult to decide if the ring of constants is trivial, that is, $k[X]^d = k$ or $k(X)^d = k$. Let us recall that this is equivalent to the problem of the nonexistence of polynomial, respectively rational, first integral for the associated system (1.1) of polynomial ordinary differential equations.

There exists an algebraic method of proving the nonexistence of nontrivial constants for some polynomial derivations. Maciejewski and Strelcyn, in [19] (see also [20]), called this method as *the Lagutinskii - Levelt procedure.*

In this paper we describe some applications and the basic steps of the Lagutinskii - Levelt procedure.

2 A theorem of Jouanolou

In Chapter 4 of his book [14], J. -P. Jouanolou gives the following result.

Theorem 1. *Let $s \geq 2$ be a natural number and let d be the k-derivation of $k[x, y, z]$ defined by*

$$d(x) = z^s, \quad d(y) = x^s, \quad d(z) = y^s. \tag{2.1}$$

Then, for every polynomial P in $k[x, y, z]$, the following equation

$$d(F) = PF \tag{2.2}$$

does not admit a nontrivial solution F in $k[x, y, z]$. In particular, the field of constants $k(x, y, z)^d$ reduces to k, or equivalently, the system of differential equations

$$\frac{dx}{dt} = z^s, \quad \frac{dy}{dt} = x^s, \quad \frac{dz}{dt} = y^s \tag{2.3}$$

does not admit any nontrivial rational first integral.

The theorem would fail for $s = 1$; the subfield of constants does not reduce to k as $x^3 + y^3 + z^3 - 3xyz$ for instance is a constant of d. Moreover, in this case, equation (2.2) has very simple solutions with $P \neq 0$; for example, $P = F = x + y + z$.

Assume now that $P = 0$ and consider the equation

$$d(F) = 0, \tag{2.4}$$

that is, try to find some nonconstant polynomial, that will be a first integral of system (2.3). At the present time, we do not know any direct proof of the fact that no such first integral does exist, even for the most simple case $s = 2$.

At a first glance, it seems feasible to look for a homogeneous polynomial solution F of a given degree p of equation (2.4) by the method of "indeterminate coefficients". A homogeneous polynomial F of degree p in $k[x, y, z]$ can indeed be written

$$F(x, y, z) = \sum_{i+j+k=p} a_{ijk} x^i y^j z^k, \tag{2.5}$$

so that the right-hand side of (2.5) can be substituted to F in equation (2.4). All that leads to a linear system $\mathcal{L}(p)$ for the unknowns a_{ijk}. In principle, for a given p, it is possible to write down the system $\mathcal{L}(p)$ and to solve it; but, finding a general rule to get $\mathcal{L}(p)$ for an arbitrary p is much more difficult. In particular, we have to make use of computer algebra to write down $\mathcal{L}(10)$ and no general rule for $\mathcal{L}(p)$ appears. In what concerns nonsolvability of equation (2.2), the direct proof for second degree polynomials F is already astonishingly long and complicated.

In Jouanolou's book, two different proofs of his theorem are given. The first one, described on pages 160–192, is due to Jouanolou and the second one, sketched on pages 193–195, is due to A. M. H. Levelt, the referee of the book.

Trying to understand the proof of Levelt, we have gradually realized that the starting point of it relies on some very clever and general ideas, which can be applied to many other derivations. The proof of Levelt (published in [14]) is unfortunately written in an extremely concise way. The same proof, with a detailed discussion of all its steps, one can find in the paper of Moulin - Ollagnier, Strelcyn and the author [22].

The proof under consideration divides in two parts, the "local analysis", which is fairly general and the "global analysis" which relies on elementary algebraic geometry and is very specific to Jouanolou's example (see [22]).

This is a remarkable fact that in many nontrivial examples, the local analysis is sufficient to yield the nonexistence of nontrivial constants of derivations. In this paper we consider only the local analysis.
In fact, the basic ideas of the method were already introduced by M. N. Lagutinskii in his pioneering, but unfortunately completely unknown, works [17] and [18]. See [5], where one can find more details on Lagutinskii and his papers on integrability which are direct continuation of the Darboux paper [2].

3 Darboux polynomials

Let us introduce (as in [21], [22]) a new notion that dates back to Darboux's memoir [2]. Let d be a k-derivation of $k[X]$. We say that a polynomial $f \in k[X]$ is a *Darboux polynomial of* d if $f \neq 0$ and $d(f) = hf$, for some $h \in k[X]$. In this case the polynomial h (which is unique) is said to be *a polynomial eigenvalue of* f.

Darboux polynomials with nonzero eigenvalues (for $k = \mathbb{R}$ or $\mathbb{C}$) are well known in the theory of polynomial differential equations. They coincide with the so-called *partial first integrals* (see, for example, [21] and [29]) of the system of polynomial differential equations determined by d.

Every element belonging to the ring of constants with respect to d is of course a Darboux polynomial. In the vocabulary of differential algebra, Darboux polynomials coincide with generators of principal differential ideals, that is, $f \in k[X]$ is a Darboux polynomial iff $f \neq 0$ and the ideal (f) is differential (i.e., $d(f) \in (f)$).

Note now some simple, but useful, propositions.

Proposition 2. *If $f \in k[X]$ is a Darboux polynomial of d, then all factors of f are also Darboux polynomials of d.*

Thus, looking for Darboux polynomials of a given k-derivation d reduces to looking for irreducible ones.

Proposition 3. *Let d be a k-derivation of $k(X)$ such that $d(k[X]) \subseteq k[X]$ (where k is a field). Let f and g be nonzero coprime polynomials in $k[X]$. Then $f/g \in k(X)^d$ iff f and g are Darboux polynomials with the same eigenvalue.*

We say that a k-derivation d of $k[X]$ is *homogeneous*, if the polynomials $d(x_1, \dots, d(x_n)$ are homogeneous of the same degree.

Proposition 4. *Let d be a homogeneous k-derivation of $k[X]$. If $f \in k[X]$ is a Darboux polynomial of d, then the eigenvalue h of f is homogeneous and all* *the homogeneous components of f are also Darboux polynomials with the common eigenvalue equal to h.*

Note that Darboux polynomials of a homogeneous derivation are not necessarily homogeneous. Indeed, let $n = 2$, $d(x_1) = x_1$, $d(x_2) = 2x_2$, and let $f = x_1^2 + x_2$. Then d is homogeneous, f is a Darboux polynomial of d (because $d(f) = 2f$), and f is not homogeneous.

If $n = 2$ then homogeneous k-derivation of $k[X]$ have the following special property

Proposition 5 ([22]). *Every homogeneous k-derivation of $k[x_1, x_2]$ has a Darboux poly-nomial.*

If $n > 2$ then the above property does not hold, in general (see for example Theorem 1).

4 Basic steps of the Lagutinskii - Levelt procedure

Let $V_1, \ldots, V_n$ be n homogeneous polynomials of the same degree s in $k[X]$ and consider the derivation d_V defined by

$$d_V(x_i) = V_i, \quad 1 \leq i \leq n. \tag{4.1}$$

We will be interested in the following general equation

$$d_V(F) = \sum_{i=1}^{n} V_i \frac{\partial F}{\partial x_i} = PF \tag{4.2}$$

in which F is an unknown polynomial of some degree $m \geq 1$, while the "eigenvalue" P is some unknown element of $k[X]$.

We may assume (by Section 3) that F is a homogeneous irreducible nontrivial polynomial of some degree m and P is a homogeneous polynomial of degree $s - 1$. Using Euler's formula

$$\sum_{i=1}^{n} x_i \frac{\partial F}{\partial x_i} = mF, \tag{4.3}$$

we get from (4.2) an equation in which the partial derivative of F with respect to the last variable x_n no longer appears:

$$\sum_{i=1}^{n-1} (x_n V_i - x_i V_n) \frac{\partial F}{\partial x_i} = (x_n P - mV_n)F. \tag{4.4}$$

A point $Z \in \mathbb{P}^{n-1}(k)$ will be called a *Darboux point* of derivation d_V if vector $V(z) = (V_1(z), \ldots, V_n(z))$ is proportional to the vector $z = (z_1, \ldots, z_n)$, for every system z of homogeneous coordinates of Z.

Let then Z be a Darboux point of the derivation d_V; without lost of generality, we can suppose that the last coordinate z_n of $z = (z_1, \ldots, z_n)$ is equal to 1. By the definition of a Darboux point, all the differences $V_i(z_1,\dots,1) - z_iV_n(z_1,\dots,1)$ vanish so that $[P(z_1,\dots,1) - mV_n(z_1,\dots,1)]F(z_1,\dots,1) = 0$. Let us stress the fact that we cannot a priori exclude the possibility that $F(z_1,\dots,1) \neq 0$.

Choose now the local affine coordinates $y_1,\dots,y_{n-1}$ defined by $x_1 = z_1 + y_1,\dots,x_{n-1} = z_{n-1} + y_{n-1}$. This change of coordinates sends the studied Darboux point Z to the origin of our new coordinate system. Let $f \in k[y_1,\dots,y_{n-1}]$ be the polynomial defined by

$$f(y_1,\dots,y_{n-1}) = F(z_1 + y_1,\dots,z_{n-1} + y_{n-1},1). \tag{4.5}$$

In this local system of coordinates, equation (4.4) becomes

$$\sum_{i=1}^{n-1}(v_i - (z_i + y_i)v_n)\frac{\partial f}{\partial y_i} = (p - mv_n)f. \tag{4.6}$$

The study of this equation will be called the *local analysis* of our derivation d_V. Looking simultaneously at many or all such equations in various Darboux points and at their relationships will be called a *global analysis* of the derivation.

Note now the following lemma which is easy to be proved.

Lemma 6. *Let $f_1,\dots,f_r,p,g$ be polynomials in $k[x_1,\dots,x_r]$ such that*
(*a*) $f_1(0) = \dots = f_r(0) = 0$,
(*b*) $g \neq 0$,
(*c*) $f_1\frac{\partial g}{\partial x_1} + \dots + f_r\frac{\partial g}{\partial x_r} = pg$.
Let $\tilde{f}_1,\dots,\tilde{f}_r$ be the linear homogeneous components of $f_1,\dots,f_r$, respectively, and let h be the nonzero homogeneous component of the lowest degree of g. Then

$$\tilde{f}_1\tfrac{\partial h}{\partial x_1} + \dots + \tilde{f}_r\tfrac{\partial h}{\partial x_r} = p(0)h.$$

We are interested in equation (4.6), that we need study around the point $(0,\dots,0)$ of k^{n-1}. The involved polynomials are in general nonhomogeneous polynomials in $n-1$ variables and can be decomposed into their homogeneous components: $\phi = \sum \phi_{(i)}$, where each polynomial $\phi_{(i)}$ is homogeneous of degree i; in particular, $\phi_{(0)}$ is the constant term of polynomial ϕ. Let $\mu_Z(F)$ be the lowest integer such that $f_{(i)} \neq 0$, i. e., the multiplicity of F at point Z. Using now Lemma 6 we get

$$\sum_{i=1}^{n-1}(v_i - (z_i + y_i)v_n)_{(1)}\frac{\partial h}{\partial y_i} = (p - mv_n)_{(0)}h, \tag{4.7}$$

where h is the nontrivial homogeneous component $f_{(\mu_Z(F))}$ of lowest degree of f.

In equation (4.7), partial derivatives of h are multiplied by linear homogeneous polynomials and h by a constant.

Then, homogeneous polynomial h is a nontrivial eigenvector of a *linear derivation* (linear differential operator) $d_L : k[t_1,\dots,t_\nu] \longrightarrow k[t_1,\dots,t_\nu]$ defined by

$$d_L(h) = \sum_{i=1}^{\nu} l_i\frac{\partial h}{\partial t_i} = \chi h, \tag{4.8}$$

where coefficients l_i are linear forms in variables $t_1, \dots, t_\nu$; $l_i(t_1, \dots, t_\nu) = \sum_{j=1}^{\nu} l_{ij} t_j$ and $L = (l_{ij})_{1 \le i,j \le \nu}$ is the $\nu \times \nu$ corresponding matrix.

Of course, in our case, $t_i = y_i, 1 \le i \le n-1$, χ is the constant term $(p - mv_n)_{(0)}$ while the l_i are the linear components $(v_i - (z_i + y_i)v_n)_{(1)}$.

Lemma 7 ([22]). *Let h be a nontrivial homogeneous polynomial eigenvector of the derivation d_L defined in the equation* (4.8)*, where χ is the corresponding eigenvalue. Denote by $\rho_1, \dots, \rho_\nu$ the ν eigenvalues of L (belonging to an algebraic closure of k).*

Then, there exist ν non-negative integers $i_1, \dots, i_\nu$ such that

$$\left.\begin{array}{lcl} \sum_{j=1}^{\nu} \rho_j i_j & = & \chi \\ \sum_{j=1}^{\nu} i_j & = & \deg(h) \end{array}\right\} \tag{4.9}$$

The above eigenvalues $\rho_1, \dots, \rho_\nu$ is said to be the *Lagutinskii - Levelt exponents* (see [19], [20]).

In the next sections we present several applications of the Lagutinskii - Levelt procedure.

5 The Halphen system

Consider the following three-dimensional system of differential equations:

$$\left\{\begin{array}{lcl} \frac{dx_1}{d_t} & = & x_2x_3 - x_1(x_2 + x_3), \\ \frac{dx_2}{d_t} & = & x_3x_1 - x_2(x_3 + x_1), \\ \frac{dx_3}{d_t} & = & x_1x_2 - x_3(x_1 + x_2). \end{array}\right. \tag{5.1}$$

This system is called the *Halphen system* ([12], [19]) or the *Darboux - Brioschi - Halphen system* ([1]).

As an illustration of the Lagutinskii - Levelt procedure we prove the following proposition.

Proposition 8 ([19]). *The system* (5.1) *does not admit any polynomial first integral.*

Proof. Let d be the k-derivation of $k[x_1, x_2, x_3]$ defined by the system (5.1), that is,

$$\left\{\begin{array}{lcl} d(x_1) & = & x_2x_3 - x_1(x_2 + x_3), \\ d(x_2) & = & x_3x_1 - x_2(x_3 + x_1), \\ d(x_3) & = & x_1x_2 - x_3(x_1 + x_2). \end{array}\right.$$

We must prove that $k[x_1, x_2, x_3]^d = k$. Suppose that there exists a polynomial $F \in k[x_1, x_2, x_3] \setminus k$ such that $d(F) = 0$. Let $m = \deg F \ge 1$. Since the derivation d is homogeneous, we may assume that the polynomial F is homogeneous.

Consider the point $z=(1,1,1)$. Observe that z is a Darboux point of d. Now the equation (4.6) has a form $w_1\frac{\partial f}{\partial y_1}+w_2\frac{\partial f}{\partial y_2}=qf$, where

$$\begin{array}{rcl} w_1 & = & -y_1(1+2y_2+y_1y_2), \\ w_2 & = & -y_2(1+2y_2+y_1y_2), \\ q & = & -m(y_1y_2-1). \end{array}$$

Thus the Lagutinskii - Levelt exponents are: $\rho_1=\rho_2=-1$, and $\chi=m$. By Lemma 7, there exist two nonnegative integers j_1 and j_2 such that

$$-(j_1+j_2)=j_1\rho_1+j_2\rho_2=m\geq 1;$$

but it is a contradiction. □

Maciejewski and Strelcyn, in [19], prove that the system (5.1) does not have also any rational first integral. In the proof of this fact they use the Lagutinskii - Levelt procedure.

Consider now the following two n-dimensional generalization of (5.1).

$$\frac{dx_j}{dt}=\sum_{i=1}^{n}(-1)^i x_{j+i-1}x_{j+i},\quad j=1,\ldots,n, \tag{5.2}$$

where $x_{n+i}=x_i$ for $i=1,\ldots,n$.

$$\frac{dx_j}{dt}=\left(\frac{2}{x_j}-\sum_{i=1}^{n}\frac{1}{x_i}\right)x_1x_2\cdots x_n,\quad j=1,\ldots,n. \tag{5.3}$$

If $n=3$ then the above systems coincide with (5.1).

As a consequence of the Lagutinskii - Levelt procedure we obtain:

Theorem 9 ([20]). *For odd $n\geq 3$ the system* (5.2) *does not admit any rational first integral.*

Theorem 10 ([20]). *For $n\geq 3$ the system* (5.3) *does not admit any polynomial first integral.*

6 An example

Let d be the k-derivation of $k[X]=k[x_1,\ldots,x_n]$ defined for $n\geq 2$ by:

$$d(x_i)=(x_i+x_{i+1})^s,\quad i=1,\ldots,n, \tag{6.1}$$

where $s\geq 1$ and $x_{n+1}=x_1$.

If $n=2$, then $[X]^d\neq k$; the polynomial x_1-x_2 belongs to $k[X]^d$. However, by the Lagutinskii - Levelt procedure, we have:

Theorem 11 ([22]). *Let d be the derivation defined by* (6.1)*. Then $k[X]^d=k$, for all $s\geq 1$ and $n\geq 3$.*

7 Linear derivations

Let d be a k-derivation of $k[X] = k[x_1, \ldots, x_n]$ such that

$$d(x_i) = \sum_{j=1}^{n} a_{ij} x_j, \quad i = 1, \ldots, n, \tag{7.1}$$

where each a_{ij} belongs to k. Let $\lambda_1, \ldots, \lambda_n$ be the n eigenvalues (belonging to an algebraic closure $\overline{k}$ of k) of the matrix $[a_{ij}]$.

Using the Lagutinskii - Levelt procedure we may prove the following two theorems.

Theorem 12 ([25], [26]). *If d is a k-derivation of $k[X]$ of the form* (7.1)*, the following conditions are equivalent:*

(1) $k[X]^d = k$*;*

(2) *The eigenvalues $\lambda_1, \ldots, \lambda_n$ are $\mathbb{N}$-independent.*

Theorem 13 ([25], [26]). *If d is a k-derivation of $k[X]$ of the form* (7.1)*. The following conditions are equivalent:*

(1) $k(X)^d = k$*;*

(2) *The Jordan matrix of the matrix $[a_{ij}]$ has one of the following two forms:*

$$(a) \qquad \begin{bmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{bmatrix},$$

where the eigenvalues $\lambda_1, \ldots, \lambda_n$ are $\mathbb{Z}$-independent; or

$$(b) \qquad \begin{bmatrix} \lambda_1 & & & & & & 0 \\ & \ddots & & & & & \\ & & \lambda_{i-1} & & & & \\ & & & \begin{bmatrix} \lambda_i & 1 \\ 0 & \lambda_{i+1} \end{bmatrix} & & & \\ & & & & \lambda_{i+2} & & \\ & & & & & \ddots & \\ 0 & & & & & & \lambda_n \end{bmatrix}$$

for some $i \in \{1, \ldots, n-1\}$ where $\lambda_i = \lambda_{i+1}$ and the eigenvalues $\lambda_1, \ldots, \lambda_i, \lambda_{i+2}, \ldots, \lambda_n$ are $\mathbb{Z}$-independent.

8 Factorisable derivations

Let $n \geq 2$ and let $W_1, \ldots, W_n \in k[X] = k[x_1, \ldots, x_n]$ be homogeneous $\mathbb{Z}$-independent polynomials of the same degree $s \geq 1$. The k-derivation

$$d(x_i) = x_i W_i, \quad i = 1, \ldots, n, \tag{8.1}$$

as well as the corresponding system of ordinary differential equations is called *factorisable*.

The factorisable systems of ordinary differential equations was intensively studied from a long time; see for example [13] and [11], where many references on this subject can be found.

One of the main features of a factorisable derivation is the fact that the polynomials $x_1, \dots, x_n$ are always Darboux polynomials of it. Consequently any polynomial of the form

$$C \prod_{i=1}^{n} x_i^{\alpha_i}, \tag{8.2}$$

where $C \neq 0$ and $\alpha_1, \dots, \alpha_n$ are nonnegative integers, is also a Darboux polynomial of it.

As a consequence of the Lagutinskii - Levelt procedure we obtain the following two theorems.

Theorem 14 ([22]). *Let d be a factorisable derivation defined by* (8.1). *Suppose that all its homogeneous Darboux polynomials are of the form* (8.2). *Then:*

(1) *All its Darboux polynomials are also of this form;*

(2) $k(X)^d = k$.

If W is a homogeneous polynomial of degree s, then $W^{(k)}$ denotes the coefficient of the monomial x_k^s which appears in W.

Theorem 15 ([22]). *Let d be a factorisable derivation defined by* (8.1).

(1) *If for some k, $1 \leq k \leq n$, the elements $W_1^{(k)}, \dots, W_n^{(k)}$ are $\mathbb{N}$-independent, then $k[X]^d = k$.*

(2) *If for some $k \in \{1, \dots, n\}$, the elements $W_1^{(k)}, \dots, W_n^{(k)}$ are $\mathbb{Z}$-independent, then $k(X)^d = k$.*

Consider now the k-derivation d of $k[X]$ defined (for $n \geq 2$) by:

$$d(x_i) = x_i x_{i+1}, \quad i = 1, \dots n, \tag{8.3}$$

where the index $n+1$ is identified with the index 1, i. e., $x_{n+1} = x_1$.

It is a factorisable derivation for which Theorem 15 cannot be applied. Nevertheless the Lagutinskii - Levelt procedure, together with specific arguments, leads to the proof that $k[X]^d = k$ and even $k(X)^d = k$ (see [22]).

Acknowledgments. I like to thank A. M. H. Levelt, A. van den Essen and the organizers for the possibility of participating in such a nice conference.

I also like to thank J.-M. Strelcyn, A. Maciejewski and J. Moulin-Ollagnier for many inspiring discussions concerning the Lagutinskii - Levelt procedure.

References

1. M. J. Ablowitz, S. Chakravarty, B. M. Herbst, *Integrability, computation and applications*, Acta Appl. Math., **39**(1995), 5 - 37.
2. G. Darboux, *Mémoire sur les équations différentielles algébriques du premier ordre et du premier degré* Bull. Sc. Math. 2ème série **t. 2** (1878), 60–96, 123–144, 151–200.
3. H. G. J. Derksen, *The kernel of a derivation*, J. Pure Appl. Algebra **84**(1993), 13 – 16.
4. J.K. Deveney, D.R. Finston, *G_a actions on $\mathbb{C}^3$ and $\mathbb{C}^7$*, Communications in Algebra **22**(1994), 6295 - 6302.
5. V. A. Dobrovolskii, N. V. Lokot, J. -M. Strelcyn, *Mikhail Nikolaevich Lagutinskii*, Preprint 1995.
6. A. van den Essen, *Locally finite and locally nilpotent derivations with applications to polynomial flows and polynomial morphisms*, Proc. Amer. Math. Soc., **116**(1992), 861 – 871.
7. A. van den Essen, *An algorithm to compute the invariant ring of a G_a-action on an affine variety*, J. Symbolic Computation, **16**(1993), 551 – 555.
8. A. van den Essen, *Locally finite and locally nilpotent derivations with applications to polynomial flows and polynomial morphisms*, Proc. Amer. Math. Soc., **116**(1992), 861 - 871.
9. A. van den Essen, *Locally nilpotent derivations and their applications III*, J. Pure Appl. Algebra, **98**(1995), 15 - 23.
10. A. van den Essen, *Seven lectures on polynomial automorphisms*, Proceedings of the Curacao Conference, Kluwer Academic Publishers, 1995, 3 - 39.
11. B. Grammaticos, J. Moulin Ollagnier, A. Ramani, J. -M. Strelcyn, S. Wojciechowski, *Integrals of quadratic ordinary differential equations in $\mathbb{R}^3$: the Lotka – Volterra system*, Physica – A, **163** (1990), 683–722.
12. G.-H. Halphen, *Sur un systéme d'equations différentielles*, C. R. Acad. Sci., **92**(1881), 1101 - 1103, 1404 - 1407.
13. J. Hofbauer, K. Sigmund, *The Theory of Evolution and Dynamical Systems. Mathematical Aspects of Selection*, London Mathem. Society Student Text **7**, Cambridge University Press, Cambridge, 1988.
14. J. -P. Jouanolou, *Equations de Pfaff algébriques*, Lect. Notes in Math. **708**, Springer-Verlag, Berlin, 1979.
15. I. Kaplansky, *An Introduction to Differential Algebra*, Hermann, Paris, 1976.
16. E. R. Kolchin, *Differential Algebra and Algebraic Groups*, Academic Press, New York, London, 1973.
17. M. N. Lagutinskii, *Partial Algebraic Integrals* (in Russian), Kharkov, 1908.
18. M. N. Lagutinskii, *Applications of the polar operations to integration of ordinary differential equations in the finite form* (in Russian), Soobshch. Kharkov. Mat. Obshch, **12**(1911), 111-243.
19. A. Maciejewski, J.-M. Strelcyn, *On the non-integrability of the Halphen system*, Preprint 1994.
20. A. Maciejewski, J.-M. Strelcyn, *Non-integrability of the generalized Halphen system*, Preprint 1995.
21. J. Moulin Ollagnier, *Liouvillian first integrals of homogeneous polynomial 3-dimensional vector fields*, Colloq. Math., **70**(1996), 195-216.
22. J. Moulin Ollagnier, A. Nowicki, J. -M. Strelcyn, *On the non-existence of constants of derivations: The proof of a theorem of Jouanolou and its development,* Bull. Sci. Math., **119**(1995), 195 - 233.
23. M. Nagata, *On the fourteenth problem of Hilbert*, Proc. Intern. Congress Math., 1958, 459 – 462, Cambridge Univ. Press, New York, 1966.
24. A. Nowicki, *Rings and fields of constants for derivations in characteristic zero*, J. Pure Appl. Algebra, **96**(1994), 47 - 55.
25. A. Nowicki, *On the non-existence of rational first integrals for systems of linear differential equations*, Linear Algebra and Its Applications, **235**(1996), 107 - 120.
26. A. Nowicki, *Polynomial derivations and their rings of constants*, UMK, Toruń, 1994.
27. A. Nowicki, M. Nagata, *Rings of constants for k–derivations in $k[x_1, \ldots, x_n]$*, J. Math. Kyoto Univ., **28**(1988), 111 – 118.
28. P. Roberts, *An infinitely generated symbolic blow-up in a power series ring and a new counterexample to Hilbert's fourteenth problem,* J. Algebra **132**(1990), 461 – 473.
29. H. Żołądek, *On algebraic solutions of algebraic Pfaff equations*, preprint 1993.

FACTORIZATION OF DIFFERENTIAL OPERATORS WITH RATIONAL FUNCTIONS COEFFICIENTS

MARK VAN HOEIJ
Department of Mathematics
University of Nijmegen
Toernooiveld, 6525 ED Nijmegen
The Netherlands
hoeij@sci.kun.nl

Abstract.
This paper is an extended version of a talk at the symposium "Differential and difference equations and Computer algebra" in honor of the 65'th birthday of professor A.H.M. Levelt.

1 Introduction

A differential equation

$$y^{(n)} + a_{n-1}y^{(n-1)} + \cdots + a_1 y' + a_0 y = 0$$

corresponds to a differential operator

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

acting on y. 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 $k(x)[\partial]$. Multiplication in this ring corresponds to composition of differential operators. A factorization $f = LR$ where $L, R \in \overline{k}(x)[\partial]$ is useful for computing solutions of f because solutions of the right-hand factor R are solutions of f as well.

The topic in this paper is a new method for factorization in the ring $\overline{k}(x)[\partial]$. In previous methods (c.f. [3, 4, 11, 19, 20]) one of the steps in the algorithm is to combine local data at all singularities in order to find a first order factor. Combining all this local data can lead to exponentially large algebraic extensions of the field of constants k. To avoid this computational difficulty, we will give a method that tries to construct a factor (not necessarily of order 1) of a differential operator using not all local data simultaneously, but computing with only 1 singularity at a time. This leads to an efficient algorithm that can compute first order and higher order factors of differential operators in many cases. For the case of factors of order 1 the algorithm can easily be completed, so all first order factors and can be computed, but not all higher order factors. To complete the algorithm for the case of higher order factors we can use a method, obtained from the literature (c.f. [3, 5, 21]), that will be the exterior power method.

One ingredient of the algorithm is the following: When r is a *local* factor of an operator f, i.e. r has coefficients in $k((x))$ instead of $k(x)$, then, given some bounds on the degrees that occur in the rational functions coefficients, we can construct an operator $R \in k(x)[\partial]$ of minimal order such that r is a right-hand factor of R. Then R is a right-hand factor of f.

The problem is that there can be infinitely many local factors r, and that usually for most irreducible local factors r the operator R constructed from r equals f even when f is reducible. For this reason we need to introduce some terminology, the exponential parts, which helps us choose (one or several) local factors r, such that either f is irreducible or at least one of these local factors r will result in a non-trivial factor R of f. The exponential parts can be defined and computed using an algorithm for local factorization, or (as we will do below) using formal solutions. Or (in particular for matrix differential operators) one can also use Sommeling's approach [18] based on Levelt's [12] work on singularities of matrix differential equations.

2 Exponential parts of local differential operators

Let V be the universal extension (called R in lemma 2.1.1 in [7]) of $k((x))$. This is a differential ring extension of $\overline{k((x))}$ consisting of all solutions of all $f \in k((x))[\delta]$.

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

$$f : V \to V.$$

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

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

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

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

The V_e are $\overline{k}$-vector spaces and also $k((x))[\delta]$-modules. So $f(V_e) \subset V_e$ for all $f \in k((x))[\delta] \setminus \{0\}$. Then $f(V_e) = V_e$ because f is surjective on V. The kernel of f on V_e is denoted by $V_e(f) = V(f) \bigcap V_e$. Denote

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

These μ_e are useful for factorization because they are independent of the order of the multiplication, i.e. if $f, g \in k((x))[\delta] \setminus \{0\}$ then

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

This follows from the fact that the dimension of the kernel of the composition of two surjective linear maps equals the sum of the dimensions of the kernels.

We will define E, $\sim$ and V_e in such a way that the subspaces V_e of V are as small as possible (more precisely: V_e is an indecomposable $\overline{k} \cdot k((x))[\delta]$-module) because then the integers $\mu_e(f)$ give as much as possible information about f. Denote the set

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

and the map

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

as $\mathrm{Exp}(e) = \exp(\int \frac{e}{x} dx)$. To define $\mathrm{Exp}(e)$ without ambiguity one can use the way that the universal extension was constructed. Then $\mathrm{Exp}(e_1 + e_2) = \mathrm{Exp}(e_1)\mathrm{Exp}(e_2)$ so Exp behaves like an exponential function. For rational numbers q we have $\mathrm{Exp}(q) = x^q \in \overline{k((x))}$. Denote

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

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

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

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

3 The main idea of the algorithm

Let $f \in k(x)[\partial]$ and suppose a non-trivial factorization $f = LR$ exists with $L, R \in \overline{k}(x)[\partial]$. We want to determine a right-hand factor of f. This could be done if we knew a non-zero subspace $W \subset V(R)$, cf. section 4. However, a priori we only know that $V(R) \subset V(f)$ but this does not give any non-zero element of $V(R)$.

For any exponential part e of f at a point $p \in P^1(\overline{k})$ we have (after applying a transformation we may assume that $p = 0$) $V_e(R) \subset V_e(f)$ and $\mu_e(L) + \mu_e(R) = \mu_e(f)$. Suppose that we are in a situation where $\mu_e(L) = 0$. Then the dimensions of $V_e(R)$ and $V_e(f)$ are the same and hence we have found a subspace $V_e(f) = V_e(R)$ of $V(R)$. Then we can factor f (cf. section 4). Note that we do not necessarily find the factorization LR, it is possible that instead of R a right-hand factor of R is found.

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

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

So we can factor any reducible operator which has:

1. A first order left-hand factor and a singularity with more than 1 exponential part.
2. Or more generally: an operator with a left-hand factor of order d and a singularity at which there are more than d different exponential parts.
3. By using the adjoint we can also factor operators which have a right-hand factor of order d and a point p with more than d different exponential parts.
4. An operator which has a singularity with an exponential part e of multiplicity 1. Then we can distinguish two cases $\mu_e(L) = 0$ or $\mu_e(R) = 0$. The latter case is reduced to the former case using the adjoint. We call the minimum of the multiplicities taken over all exponential parts of all singularities the *minimum multiplicity*. By checking both cases $\mu_e(L) = 0$ or $\mu_e(R) = 0$ any operator f with minimum multiplicity 1 is either irreducible or it is factored by our method.

If a first order left or right-hand factor exists, then our approach can compute a factorization whenever there is a singularity with at least two different exponential parts. This reduces the problem of finding all first order factors to the same problem for lower order operators. The only case that remains is when each singularity has only 1 exponential part. However, this special case is a trivial case for Beke's method because we need to check only one possibility in Beke's method, and in fact this reduces to problem to computing rational solutions after having applied a transformation $\partial \mapsto \partial + r$ for some rational function r that we can compute from f. Combining this with the algorithm above, we obtain an algorithm that can compute all first order factors. It can also compute higher order factors in many cases. The remaining cases can be treated by the exterior power method that can be found in the literature. In this method the problem of computing factors of order d is reduced to computing factors of order 1 of the d-th exterior power of f.

4 Computing a right-hand factor R

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

The assumption from section 3 was that an $e \in E$ is known for which $\mu_e(f) > 0$ and $\mu_e(L) = 0$. From this we concluded that $V_e(f) \subset V(R)$. Using this information and the algorithm for local factorization it is possible to compute an $r \in \overline{k}((x))[\delta]$

such that $V(r) \subset V(R)$, i.e. r is a right-hand factor of the operator R that we look for.

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

There are two ways of choosing the number d. The first is to try all values $d = 1, 2, \ldots, n-1$. Suppose that for a certain d we find an R that has r as a right-hand factor and for numbers smaller than d such R could not be found. Then d is minimal and hence R is a right-hand factor of f. The second approach to take $d = n-1$. If we find $R = a_d\partial^d + \cdots + a_0\partial^0$ that has r as a right-hand factor we can compute $\text{GCRD}(R, f)$. This way we also find a right-hand factor of f.

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

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

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

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

in $k[[x]]^m$. This is a system of linear equations with coefficients in $k[[x]]$ which should be solved over $k[x]$. One way of solving this is to convert it to a system of linear equations over k using the bound N. A much faster way is the Beckermann-Labahn algorithm which was found first by Labahn and Beckermann, and later independently by Derksen [6, 2]. Their method is as follows

Sketch of the Beckermann-Labahn algorithm

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

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

Define the degree of a vector of polynomials as the maximum of the degrees of these polynomials. From the basis for M_i we can find a non-zero $A_i \in M_i$ with minimal degree. Suppose there exists a non-zero $R = a_d\partial^d + \cdots + a_0\partial^0 \in k[x, \partial]$

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

Algorithm Construct R

For $i = 0, 1, 2, \ldots$ do

- Compute M_i and $A_i \in M_i$ of minimal degree.
- If $\deg(A_i) > N$ then RETURN "R does not exist".
- If $\deg(A_i) = \deg(A_{i-3})$ then
  Comment: the degree did not increase 3 steps in a row so it is likely that a right-hand factor is found.
  If $A_i = (a_0, \ldots, a_d)$ then write $R = a_d\partial^d + \cdots + a_0\partial^0$. Divide by a_d to make R monic. Test if R and f have a non-trivial right-hand factor in common. If so, return this right-hand factor, otherwise continue with the next i.

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

References

1. Beckermann B., Labahn G., *A uniform approach for Hermite Padé and simultaneous Padé Approximants and their Matrix-type generalizations*, Numerical Algorithms, **3**, p. 45-54, (1992).
2. Beckermann B., Labahn G., *A uniform approach for the fast computation of Matrix-type Padé approximants*, SIAM J. Matrix Analysis and Applications, p. 804-823, (1994).
3. Beke E., *Die Irreduzibilität der homogenen linearen Differentialgleichungen*, Math. Ann. **45**, p. 278-294, (1894).
4. Bronstein M., *Linear Ordinary Differential Equations: breaking through the order two barrier.* Proceedings ISSAC 92, ACM Press, p. 42-48, (1992).
5. Bronstein M., *An improved algorithm for factoring linear ordinary differential operators.* Proceedings ISSAC 94, Oxford, U.K., ACM Press, p. 336-340, (1994).
6. Derksen H., *An algorithm to compute generalized Padé-Hermite forms* Manuscript. Available by ftp at `daisy.math.unibas.ch` in `/pub/hderksen/pade.dvi` (1994).
7. Hendriks P.A., van der Put M., *Galois action on solutions of a differential equation*, J. Symb. Comp. (1995).
8. van Hoeij M., *Formal Solutions and Factorization of Differential Operators with Power Series Coefficients*, University of Nijmegen Report nr. 9528, to appear in J. Symb. Comp.
9. van Hoeij M., *Factorization of Differential Operators with Rational Functions Coefficients*, University of Nijmegen Report nr. 9552, to appear in J. Symb. Comp.
10. van Hoeij M., Weil J.A., *An algorithm for computing invariants of differential Galois groups*, to appear in J. Pure and Applied Algebra.
11. Kovacic J., *An algorithm for solving second order linear homogeneous differential equations*, J. Symb. Comp **2** p. 3-43 (1986)

12. Levelt, A.H.M., *Jordan decomposition for a class of singular differential operators*, Arkiv für matematik, 13 (1), p. 1-27, (1975).
13. Levelt A.H.M., *Differential Galois theory and tensor products*, Indagationes Mathematicae, 1 (4), p. 439-450, (1990).
14. Loewy A., *Über vollständig reduzible lineare homogene Differentialgleichungen*, Math. Ann., **62**, 89-117, (1906).
15. Malgrange, B., *Sur la réduction formelle des équations différentielles à singularités irrégulières*, Manuscript, (1979).
16. Ore O., *Formale Theorie der linearen Differentialgleichungen (Zweiter Teil)*, J. für d. Reine u. angew. Math., **168**, p. 233-252, (1932).
17. Ore O., *Theory of non-commutative polynomial rings*, Ann. of Math. **34** p. 480-508, (1933).
18. Sommeling R., *Characteristic classes for irregular singularities*, Ph.D. thesis, University of Nijmegen. (1993).
19. Schwarz F., *A factorization Algorithm for Linear Ordinary Differential Equations.* Proceedings of ISSAC 89, ACM Press, p. 17-25, (1989).
20. Singer M.F., *Liouvillian solutions of n-th order homogeneous linear differential equations.* Amer.J.Mat. **103**, p. 661-682, (1981).
21. Tsarev S.P., *On the problem of factorization of linear ordinary differential operators*, Programming & computer software, v. 20, **1**, p. 27-29, (1994).

CHARACTERISTIC CLASSES FOR SINGULARITIES OF LINEAR DIFFERENTIAL EQUATIONS

A.H.M. LEVELT
Department of Mathematics
University of Nijmegen
Toernooiveld, 6525 ED Nijmegen
The Netherlands
ahml@sci.kun.nl

1 Introduction

Here is an example of the type of equations we have in mind:

$$x^2y'' + (3x-1)y' + y = 0 \tag{1}$$

which has the 'solution'

$$y = \sum_{n=0}^{\infty} n!\, x^n.$$

Putting $y_1 = y$, $y_2 = y'$ in (1) we get

$$\frac{d}{dx}\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ \frac{1}{x^2} & \frac{3x-1}{x^2} \end{pmatrix}\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = 0. \tag{2}$$

The solution space of this system of homogeneous first linear differential equations can be viewed as the null space of the differential operator

$$D : \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \mapsto \frac{d}{dx}\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} + \begin{pmatrix} 0 & 1 \\ \frac{1}{x^2} & \frac{3x-1}{x^2} \end{pmatrix}\begin{pmatrix} y_1 \\ y_2 \end{pmatrix}.$$

2 Definitions and notations

- k is a field of characteristic 0.
- $\mathcal{O} = k[[x]]$ is the ring of formal power series in x with coefficients in k.
- $K = k((x))$ is the field of fractions of $\mathcal{O}$, the field of formal Laurant series in x with finite pole order.
- θ is the formal derivation $x\, d/dx$ on K

$$\theta(\sum_{i=m}^{i} a_i x^i) = \sum_{i=m}^{i} i a_i x^i.$$

- V is a finite dimensional K vector space.
- $D : V \to V$ is a differential operator, i.e.
  (i) D is k-linear.
  (ii) $D(a\,v) = \theta(a)v + a\,D(v)$ for all $a \in K, v \in V$.
- $K \subset L$ is a finite field extension. If k is algebraically closed, then $L = k((t)), t = x^{1/p}$ for some $p \in \mathbb{N}^*$. In that case $\bar{K} = \cup_{p=1}^{\infty} k((x^{1/p}))$ is the algebraic closure of K. In the sequel finite extension fields of K are taken within $\bar{K}$.
- $\theta : L \to L$ is the (unique) extension of the derivation θ on K. (Note that $\theta(t) = t/p$.)
- $V_L = L \otimes_K V$, extension of scalars.
- $D_L : V_L \to V_L$ the differential operator defined by

$$D_L(a \otimes v) = \theta(a) \otimes v + a \otimes D(v) \text{ for all } a \in L, v \in V.$$

If no confusion arises we'll write sometimes D instead of D_L.

A choice of a basis in V leads to a matrix representation of the differential operator and makes the connection with what was called 'differential operator' in the introduction.

Let $e = (e_1, \ldots, e_n)$ be a K-basis in V. Define the $n \times n$ matrix A with entries $A_{j,i}$ by

$$D(e_i) = \sum_{j=1}^{n} A_{j,i} e_j \text{ for all } i \in \{1, \ldots, n\}.$$

A is called *the matrix of D with respect to the basis e*. Now let $f = (f_1, \ldots, f_n)$ be another basis of V and B the matrix of D with respect to f. Define the (invertible) matrix T by

$$f_i = \sum_{j=1}^{n} T_{j,i} e_j \text{ for all } i \in \{1, \ldots, n\}.$$

Then one has

$$B = T^{-1}AT + T^{-1}\theta(T).$$

$\mathcal{D} = K < \theta >$ denotes the ring of (abstract) differential operators $P = \sum_i a_i \theta^i$ where the coefficients a_i belong to K. The (non-commutative) multiplication is the the composition of differential operators.

A couple (V, D) of a vector space plus differential operator can be viewed as a left $\mathcal{D}$-module by $P(v) = \sum_i a_i D^i(v)$ for all $v \in V$.

3 A theorem and a problem

Differential operators $D : V \to V$ in the above sense closely resemble linear applications in finite dimensional vector spaces. Here follows an example.

Theorem 1 *(Levelt, 1974) There exists a semi-simple differential operator $S : V \to V$ and a nilpotent linear transformation $N : V \to N$ such that:*

(i) $D = S + N$.
(ii) S *and* N *commute.*

The couple S, N *is uniquely determined by the above conditions.*

Corollary 2 *There exist a finite field extension* $K \subset L = k'((t))$, $k \subset k'$ *finite and* $t = x^{1/p}$ *and an* L*-basis* e *of* V_L *such that*

$$Mat(D_L, e) = \begin{pmatrix} \lambda_1 & * & \cdots & \cdots & 0 \\ 0 & \ddots & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ \vdots & & \ddots & \ddots & * \\ 0 & \cdots & \cdots & 0 & \lambda_n \end{pmatrix}, \tag{3}$$

where $\lambda_i \in k'[1/t]$ *and* $* = 0$ *or* $* = 1$.

In particular, after a convenient scalar extension $K \subset L$ the operator D_L has a non-zero eigenvector.

Problem How to define the characteristic polynomial of D?

$\prod_{i=1}^n (T - \lambda_i)$ doesn't work, because the λ_i are not uniquely determined by D, but only up to the addition of $m/p, m \in \mathbb{Z}$. Normalizations of the type $0 \leq Re(\lambda_i) < 1$ lead to bad properties, e.g. $\prod_{i=1}^n (T - \lambda_i)$ will not belong to $K[T]$ in general.

Here the question arises what one expects from a 'characteristic polynomial'. One could think of the following requirements:

- It should classify semi-simple differential operators.
- It should have good functorial properties (e.g. convenient formulas for direct sums and tensor products).
- Rationality: it should be an algebraic object defined over K.

The problem was solved by R. Sommeling in his Ph.D. thesis (*Characteristic classes for irregular singularities*, University of Nijmegen, 1993). In the sequel a somewhat simplified version will be presented. For most proofs the reader is referred to Sommeling's thesis. In order to avoid technical digressions we shall assume from now on that k is algebraically closed.

4 Eigenvectors, normalization, simple modules

As was said before for given (V, D) there exist a finite extension $K \subset L = k((t)), t = x^{1/d}, a \in L, v \in V_L \setminus \{0\}$ such that $D(v) = a\,v$.

Now for $c \in L, c \neq 0$ define $w = c\,v$. Then $D(w) = b\,w$, where $b = a + \theta(c)/c$. Here we have a problem: there are too many eigenvalues. One can partly restrict the choice by normalization. For this note that

$$\frac{\theta(c)}{c} = z_0 + z_1 t + z_2 t^2 + \cdots \text{ where } z_i \in k, z_0 \in \frac{1}{d}\mathbb{Z}. \tag{4}$$

Conversely, for given $z_1, z_2, \ldots \in k, z_0 \in (1/d)\mathbb{Z}$ there exists $c \in L$ satisfying (4). So we see that D has an eigenvalue

$$b = \frac{\beta_{-m}}{t^m} + \cdots + \frac{\beta_{-1}}{t} + \beta_0, \text{ where } \beta_i \in k, m \in \mathbb{N}.$$

We need a more precise result.

Proposition 3 *There exists $a \in \bar{K}$ and $v \in V_{K(a)}, v \neq 0$ satisfying*

(i) $D_{K(a)}(v) = a\,v$.

(ii)

$$a = \frac{\alpha_{-m}}{t^m} + \cdots + \frac{\alpha_{-1}}{t} + \alpha_0, \text{ where } \alpha_i \in k, t = x^{1/d}, K(a) = k((t)).$$

a is called *normalized eigenvalue.*

Definition 4 $a, b \in \bar{K}$ are called *equivalent*, notation $a \sim b$, if there exists $c \in \bar{K}^*$ such that $b = a + \theta(c)/c$. $a \in \bar{K}$ is called *special* if for all conjugates b of a over K the relation $b \sim a$ implies $b = a$.

One easily checks that normalized eigenvalues are special and that to each eigenvalue a there exists a normalized eigenvalue b equivalent to a.

We shall now construct a $\mathcal{D}$-module to any special $a \in \bar{K}$. Let d be the degree of A over K and $t = x^{1/d}$. Then $K(a) = k((t))$ and there exist $a_0, a_1, \ldots, a_{d-1} \in K$ such that

$$a = a_0 + \frac{a_1}{t} + \cdots + \frac{a_{d-1}}{t^{d-1}}.$$

Define $V(a)$ as the K-vector space K^d and $D : V(a) \to V(a)$ by $D = \theta + A - J_d$ where

$$A = \begin{pmatrix} a_0 & \frac{a_{d-1}}{x} & \cdots & \cdots & \frac{a_1}{x} \\ a_1 & \ddots & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & \frac{a_{d-1}}{x} \\ a_{d-1} & \cdots & \cdots & a_1 & a_0 \end{pmatrix}, \quad J_d = \begin{pmatrix} 0 & & & & \\ & \frac{1}{d} & & & \\ & & \ddots & & \\ & & & \ddots & \\ & & & & \frac{d-1}{d} \end{pmatrix}.$$

Then $(V(a), D)$ is called the *canonical module associated to a.*

Properties:

- $(V(a), D)$ is a simple $\mathcal{D}$-module.
- Any simple $\mathcal{D}$-module is isomorphic to a $(V(a), D)$.
- If $b \in \bar{K}$ is another special element, then $V(a) \tilde{\to} V(b) \iff a \sim b$.
- $D(v) = a\,v$ for some non-zero $v \in V(a)_{K(a)}$
- $(\rho(v))_{\rho \in Gal(K(a)/K)}$ is a $K(a)$-basis of $V(a)_{K(a)}$.
- Minimal polynomial of a/K equals the characteristic polynomial of A.

5 Characteristic classes

Here follows another list of notations and definitions.

- $\mathcal{M}$ is the set of monic polynomials in $K[T]$. $\mathcal{M}$ is closed under multiplication; it is an abelian monoid.
- $\mathcal{I}$ is the subset of $\mathcal{M}$ of the irreducible polynomials.
- $p \sim q$ for $p, q \in \mathcal{I}$ means:

  (i) p and q have the same splitting field L.

  (ii) There exists $c \in L^*$ such that $q(T) = p(T + \theta(c)/c)$.
- Since $\sim$ is compatible with the multiplication in $\mathcal{M}$ the multipication induces a monoid structure in $\mathcal{M}/\sim$.
- $c(V, D)$ for a (V, D) is defined as follows. Choose a special such that $(V, D) \xrightarrow{\sim} V(a)$. Then $c(V, D) \in \mathcal{M}/\sim$ is the equivalence class of p_a, the minimal polynomial of a over K.
- $f \sim g$ for $f, g \in \mathcal{M}$ is defined as follows. Factorize f, g into elements of $\mathcal{I}$. Then there exists a bijection between the two sets of irreducible factors such that corresponding factors are equivalent.
- $c(V, D)$ for (V, D) general can now be defined with the help of a composition series $V = V_0 \supset V_1 \supset \cdots \supset V_r = 0$, $D(V_i) \subset V_i$. The quotients V_{i-1}/V_i are simple $\mathcal{D}$-modules. Let $f_i \in \mathcal{I}$ represent V_{i-1}/V_i. Then $f_1 \cdots f_r$ represents $c(V, D)$. The well-known properties of composition series guarantee that this is a valid definition of the characteristic class of (V, D).

The following exactness property immediately follows from the above definitions. If

$$0 \to V' \to V \to V'' \to 0 \tag{5}$$

is an exact sequence of $\mathcal{D}$-modules (we have omitted D), then

$$c(V) = c(V')\, c(V'').$$

In order to define the characteristic map we first define the subgroup Q of $K(T)^*$ by $Q = \{f/g \mid f, g \in \mathcal{M}\}$. $\sim$ can be extended (uniquely) to Q. We will denote by $\mathcal{C}$ the abelian group $Q/\sim$. On the other hand, let $K_0(\mathcal{D})$ the Grothendieck group (free abelian group of isomorphism classes of $\mathcal{D}$-modules modulo the subgroup generated by $[V] - [V'] - [V'']$ for all exact sequences (5)). Then by standard arguments the map $(V, D) \to \mathcal{M}/\sim$ induces the characteristic map

$$c : K_0(\mathcal{D}) \to \mathcal{C} \tag{6}$$

The characteristic map is an injective homomorphism of abelian groups. From now on we shall write the group operation in $\mathcal{C}$ as an addition.

6 Multiplicative structure

The tensor product (Z, D) of $\mathcal{D}$-modules $(V_1, D_1), (V_2, D_2)$ is defined by

(i) $Z = V_1 \otimes V_2$ as a K-vector space.

(ii) $D(v_1 \otimes v_2) = D_1(v_1) \otimes v_2 + v_1 \otimes D(v_2)$ for all $v_1 \in V_1, v_2 \in V_2$.

This tensor product induces a (commutatitive) multiplication into $K_0(\mathcal{D})$ which turns the Grotendieck group into a commutative ring. The characteristic map c transports this ring structure to $Im(c)$. We want a direct description of the product structure in $Im(c)$. Hence

Problem Compute $c(Z, D)$ from $c(V_1, D_1)$ and $c(V_2, D_2)$.

Obviously it suffices to do this for $V_1 = V(a), V_2 = V(b)$, where a, b are normalized eigenvalues.

Solution Define

$$R(T) = resultant_S(p_a(S), p_b(T - S)) \in K[T]. \tag{7}$$

Let

$$R(T) = \prod_{j=1}^{n} f_j^{\mu_j} \tag{8}$$

be the prime factorization of $R(T)$ in $K[T]$. Define

$$l = \operatorname{lcm}(\deg(f_1), \ldots, \deg(f_n)), \tag{9}$$

$$h_i = \frac{l}{\deg(f_i)}. \tag{10}$$

Then $c(Z, D)$ is represented by

$$\prod_{i=1}^{n} \prod_{m=0}^{h_i - 1} f_i \left(T + \frac{m}{l}\right)^{\mu_i / h_i}. \tag{11}$$

Sketch of a proof. For the normalized eigenvalues a, b we have the following diagram

$$\begin{array}{ccccccc} K(a) & \subset & K(a,b) & = & L & = & k((t)) \\ \cup & & \cup & & & & \\ K & \subset & K(b), & & & & \end{array} \tag{12}$$

where $t = x^{1/l}$. Define $d_a = \deg(a/K)$, $d_b = \deg(b/K)$, $d = \gcd(d_a, d_b)$, $l = \operatorname{lcm}(d_a, d_b)$. Then $[L : K] = l$ and $d_a\, d_b = d\, l$. Let ρ be a generator of the Galois group G of L over K. There exist eigenvectors v, w

$$v \in V(a)_{K(a)}, v \neq 0, D(v) = a\, v,$$

$$w \in V(b)_{K(b)}, w \neq 0, D(w) = b\, w.$$

Note that

$$(v, \rho(v), \ldots, \rho^{d_a - 1}(v)) \text{ is a basis of } V(a)_{K(a)}$$

and

$$(w, \rho(w), \ldots, \rho^{d_b-1}(w)) \text{ is a basis of } V(b)_{K(b)}.$$

Define

$$z_{i,j} = \rho^i(v) \otimes \rho^j(w) \text{ for } 0 \leq i < d_a,\ 0 \leq j < d_b.$$

Then $z_{i,j} \in Z_L$, $(z_{i,j})_{i,j}$ is an L-basis of Z_L and

$$D(z_{i,j}) = (\rho^i(a) + \rho^j(b))z_{i,j}.$$

Note that $\rho^i(a) + \rho^j(b)$ is special (even a normalized eigenvalue). In the table

$$\begin{array}{llll} z_{0,0} & \rho(z_{0,0}) & \cdots\ \cdots & \rho^{l-1}(z_{0,0}) \\ z_{1,0} & \rho(z_{1,0}) & \cdots\ \cdots & \rho^{l-1}(z_{1,0}) \\ \vdots & \vdots & & \vdots \\ z_{d-1,0} & \rho(z_{d-1,0}) & \cdots\ \cdots & \rho^{l-1}(z_{d-1,0}) \end{array}$$

we have again all elements of the basis $(z_{i,j})_{i,j}$. To each row of the table we are going to apply the following theorem.

Theorem 5 (Structure Theorem) *Let (V, D) be a $\mathcal{D}$-module, $K \subset L$ a finite extension with Galois group G, $a \in L$ special and $v \in V \setminus \{0\}$ such that $D(v) = a\,v$. Assume that $(\sigma(v))_{\sigma \in G}$ is linearly independent over L. Then there exists a $\mathcal{D}$-submodule W_i of V having the following properties:*

(i) $W_L = \sum_{\sigma \in G} L\sigma(v)$ *as $\mathcal{D}_L$-modules.*
(ii) $W \stackrel{\sim}{\to} (V(0/l) \oplus \cdots \oplus V((h-1)/l)) \otimes_K V(a)$, *an isomorphism of $\mathcal{D}$-modules, where $h = [L : K(a)]$.*

Application of the Structure Theorem.
For $i \in \{0, \ldots, d-1\}$ look at the eigenvector $z_{i,0}$ of $D : Z_L \to Z_L$. We have $D(z_{i,0}) = (\rho^i(a) + b)z_{i,0}$ and $\rho^i(a) + b$ is special. Moreover, $(\rho^j(z_{i,0}))_{0 \leq j < l}$ is linearly independent over L. Hence, in virtue of the Structure Theorem, there exists a $\mathcal{D}$-module W_i of V such that:

$$\begin{aligned} (W_i)_L &= \sum_{j=0}^{l-1} L\rho^j(z_{i,0}), \\ W_i &\stackrel{\sim}{\to} \left(V\left(\frac{0}{l}\right) \oplus \cdots \oplus V\left(\frac{h_i - 1}{l}\right)\right) \otimes_K V(\rho^i(a) + b), \end{aligned}$$

where

$$h_i = [L : K(\rho^i(a) + b)] = l/\deg(\rho^i(a) + b).$$

Define $W = W_0 + \cdots + W_{d-1}$. Then

$$\begin{aligned} W_L &= \sum_{i=0}^{d-1}\sum_{j=0}^{l-1} L\rho^j(z_{i,0}) = Z_L, \\ W &\stackrel{\sim}{\to} \bigoplus_{i=0}^{d-1}\bigoplus_{m=0}^{h_i-1} V\left(\frac{m}{l}\right) \otimes_K V(\rho^i(a) + b). \end{aligned} \tag{13}$$

Because of (13) we have $W = Z = V(a) \otimes_K V(b)$.

Let p_i be the minimal polynomial of $\rho^i(a) + b$ over K. Then it is easy to see that $p_i(T + m/l)$ represents the characteristic class of $V(m/l) \otimes V(\rho^i(a) + b)$. Hence the characteristic class of Z is represented by

$$\prod_{i=0}^{d-1} \prod_{m=0}^{h_i-1} p_i\left(T + \frac{m}{l}\right). \tag{14}$$

Note that $p_i = p_j$ is possible for $i \neq j$. The zeros of p_i are

$$\rho^i(a) + b, \rho(\rho^i(a) + b), \ldots, \rho^{d_i-1}(\rho^i(a) + b),$$

where $d_i = \deg(\rho^i(a) + b) = [K(\rho^i(a) + b) : K]$. Since $[L : K(\rho^i(a) + b)] = h_i$ and $[L : K] = l$ we have $l = d_i h_i$. It follows that

$$\rho^i(a) + b, \rho(\rho^i(a) + b), \ldots, \rho^{l-1}(\rho^i(a) + b)$$

is the sequence of zeros of $p_i^{h_i}$. Hence

$$\prod_{i=0}^{d-1} \prod_{j=0}^{l-1} (T - \rho^j(\rho^i(a) + b)) = \prod_{i=0}^{d-1} p_i^{h_i}.$$

The left-side equals

$$\prod_{i=0}^{d_a-1} \prod_{j=0}^{d_b-1} (T - (\rho^i(a) + \rho^j(b))) = resultant_S(p_a(S), p_b(T - S))$$

and now (11) immediately follows.

Due to M. van Hoeij's local factoization algorithm (cf. *Factorization of Linear Differential Operators*, Ph.D. thesis, University of Nijmegen, 1996) characteristic classes of differential operators can now be computed. Formula (11) leads to an algorithm for the characteristic class of a tensor product (i.e. the product in the characteristic ring).

Appendix

A TOAST TO TON

MICHAEL SINGER
Mathematics Department
North Carolina State University
Raleigh, NC 27695-8205
USA
singer@math.ncsu.edu

Here's to Ton! Has it been so long?
    Must he really now be retired?
I guess it's true and now's the time
    To wish him well from those he's inspired.

His first result that I did learn
    Is elegant, concise and far surpasses the norm.
Who can dispute the power and beauty
    Of Levelt's Differential Jordan Normal Form?

And then I found he had done much more.
    A very nice thesis – go, take a look –
That rested dormant, waiting to be used
    To answer Hilbert's question by Bolibruch.

And if you are interested in forms that are Pfaffian
    But don't want proofs that appeal to none but a pagan.
You can find an anonymous gem in Jouanalou's book
    Due to our man right here in Nijmegen!

There is more – from classes characteristic to computations symbolic,
    Many results about which he could boast.
But now join me and wish him – good health, much fun, good luck to come
    And raise your glasses to Ton – A Toast!

DEAR TON

WIM SCHIKHOF
Department of Mathematics
University of Nijmegen
Toernooiveld, 6525 ED Nijmegen
The Netherlands
`schikhof@sci.kun.nl`

We have been colleagues at the same institute for many years, and there may be several things worth mentioning at an occasion like this, but let me just pick one particular experience.

I can be announced as your first PhD student.

To indicate the importance of your mathematical influence on me, we have to go back quite some years: it was in the sixties, when you entered the Mathematical Department as a young professor. At that time I was a junior staff member, trying to find a suitable subject and advisor for a PhD. The summer course you presented made such an impression on me that I decided to try and ask whether you would be interested in p-adic harmonic analysis, a subject I'd got involved in currently through suggestions of Professor Springer.

You answered two things:

1. I don't know anything about that subject, and
2. Why not? Let's give it a try.

Almost at once you organized weekly meetings in the evening at your house in which we worked together. That is to say, and stated more correctly: you were working and I was watching and listening.

Well, Ton, maybe you don't even remember these sessions (I recall we had only seven or eight, probably because you decided that after that I was able to work on my own), but I do, and I like to let you know that they had a big influence on my further research activities. Why?

Because here, for the first time, I witnessed the process of mathematical research, how to get ideas and when it is time to drop some, the importance of having good examples, of attitude, endurance, preparedness to do ugly computations, etc.

True, in the years that followed you always have been willing to listen to me, giving advice, encouraging me, and I thank you for that too, but I think that during those first sessions I learned how to become a grownup mathematician, and I am remembering this period as being the most important lesson you taught me, and this opportunity seems to be appropriate to finally say a special thank you for it.

I regret that I cannot be present at this celebration. So, I have to wish you by means of this reading: very fine years to come and that they may be filled with activities that have your enthousiasm.

Wim Schikhof

PERSONAL LETTER

V. S. VARADARAJAN
University of California
Los Angeles, CA 90095-1555
USA
vsv@math.ucla.edu

I have been fortunate to know Professor Levelt for the past several years and have always admired his deep insights in many beautiful parts of mathematics. I am thinking of his work on generalized hypergeometric functions which was the foundation for the work of Beukers and Heckman; his pioneering work on the reduction theory of meromorphic connections which was a source of great inspiration for my own work with Donald Babbitt on problems of reduction and moduli for meromorphic connections; and his ideas on tensor categories and differential Galois theory. I must also mention his beautiful work with Van den Essen on Pfaffian connections in several variables which brought to light several issues of nilpotents over general rings that also arose in my work with Babbitt. I could go on and on and I am sure there are many more that I have not known or understood.

I am sure even after retirement he will interest himself in mathematical questions. I wish him many happy years of retirement, and hope that one day soon I can visit him.

Raja