A new zero-test for formal power series

Joris van der Hoeven
Département de Mathématiques (bât. 425)
Université Paris-Sud
91405 Orsay Cedex
France
joris@texmacs.org

ABSTRACT

In this paper, we present a new zero-test for expressions which are constructed from formal power solutions to algebraic differential equations using the ring operations and differentiation. We also provide a survey of all existing methods that we know of and a detailed comparison of these methods with our approach.

1. INTRODUCTION

Zero-testing is an important issue on the analysis side of symbolic computation. Standard mathematical notation provides a way of representing many transcendental functions. However, trivial cases apart, this notation gives rise to the following problems:

- Expressions may not be defined: consider $1/0$, $\log(0)$ or $\log(e^{x+y} - e^x e^y)$.
- Expressions may be ambiguous: what values should we take for $\log(-1)$ or $\sqrt{z^2}$?
- Expressions may be redundant: $\sin^2 x + \cos^2 x$ and 1 are different expressions, but they represent the same function.

Often, one is interested in expressions which represent functions in a ring. In that case, the third problem reduces to deciding when a given expression represents the zero function.

As to the first two problems, one has to decide where and how we want our functions to be defined. In this paper, we will be concerned with expressions that represent formal power series (in fact, this approach covers most elementary calculus on special functions, using analytic continuation if necessary). The expressions will then be formed from the constants and the indeterminates using the ring operations and power series solutions to algebraic differential equations. The correctness and non-ambiguity of expressions may be ensured by structural induction. This may involve zero-testing for the series represented by subexpressions.

Several classical approaches for zero-testing exist [9, 6, 10, 11, 7, 12] and we provide a quick survey of them in section 2. Our new zero-test, which is described in section 5, is based on a similar approach as [10, 11, 12]. We believe the algorithm to be interesting for five main reasons:

- We treat differential equations of arbitrary order.
- Our method accommodates divergent power series solutions.
- It reformulates previous work from [10, 11, 12] in the more standard setting of differential algebra.
- We believe it to be more efficient. With some more work, it might be possible to give complexity bounds for the algorithm (or a modified version of it) along the same lines as [12]. Such bounds are also interesting in relation to "witness conjectures" [17, 13, 16, 8].
- On the longer run, the algorithm might generalize to the multivariate setting of partial differential equations with initial conditions on a subspace of dimension > 0.

Throughout the paper, we will assume that the reader is familiar with differential algebra and the notations used in this field; see section 3 and [2] for a nice introduction. The proof of our algorithm also uses a result from the preprint [15], which is too complicated to be presented here, although we do provide a sketch of the proof in section 4.

We plan to provide some examples and more explanations in a forthcoming journal paper. We are also writing a lecture note about the subject of section 4. No implementations are available yet.

2. A SURVEY OF EXISTING APPROACHES

A *differentially algebraic power series* is a power series f which satisfies a non-trivial algebraic differential equation $P(f) = 0$. Consider a power series expression constructed from z and the constants in some field $\mathcal{C}$ like $\mathbb{Q}$, using $+, -, \cdot$ and left composition of infinitesimal power series by differentially algebraic power series $\varphi_1, \ldots, \varphi_p$. Then it is a classical problem to test whether such an expression represents zero. There are many approaches for this problem.

2.1 Structural approaches.

If the differentially algebraic power series are particularly simple, then it is sometimes possible to characterize all possible relations between the power series under consideration. This is clearly the case if we restrict the differentially algebraic power series to be algebraic.

A more interesting example is obtained when we also allow left composition with $\log(1+z)$ and $\exp z$. In this case, the Ax theorem [1] and the Risch structure theorem [9] may be used to design a fast zero-test.

The structural approach may yield very efficient algorithms when it works. However, it requires the characterization of all possible relations in a given context, where we merely asked for a test whether a particular one holds. Consequently, the approach usually only applies in very specific situations.

2.2 Bounding the valuation.

An obvious way to test whether an expression represents the zero power series is to obtain a bound for its valuation in terms of its size if the expression does *not* represent zero. Khovanskii has given reasonably good uniform bounds (of the form $O(2^{s^2})$, where s denotes the input size) for the number of zeros for systems of real Pfaffian functions [6]. These bounds may be adapted to the power series context.

This approach is interesting because it only requires fast power series expansions [3, 14] for implementing a zero-test. However, such a zero-test might be slow for expressions which can be quickly rewritten to zero (like $x-x$, where x is a complicated expression). Also, if we want the approach to be efficient, good bounds (such as the ones predicted by witness conjectures [17, 13, 16, 8]) would be necessary. At the moment, we only have Khovanskii-type bounds in the case of Pfaffian functions. A new strategy for obtaining bounds, which might generalize to higher order equations by adapting the algorithm in this paper, has been proposed in [12]. However, the obtained bounds are still doubly exponential.

2.3 The logical approach.

From a theoretical point, it is also interesting to ask whether zero-tests always exist. This question has been answered very precisely and in a very general context by Denef and Lipschitz [4, 5]. In the present setting of power series expressions, their approach uses the well-known fact that the set of differentially algebraic power series is closed under the ring operations and composition. However, the equations one obtains for sums, products, etc. may be very complicated, so that that approaches which essentially use this fact are deemed to be very inefficient.

2.4 Groebner bases and saturation.

Another simple approach was proposed by Shackell in [11] (see the first algorithm). The idea is to keep all algebraic relations which hold between a finite number of power series in a Groebner basis G. If we want to test a new relation, then we include it in G and look whether we obtain a contradiction. If not, then we keep on adding the derivatives of all relations in G into G. Under certain hypotheses, this process always ends up in a contradiction or a proof that the added relations all hold. However, the approach does not seem to provide any reasonable complexity bounds.

2.5 Varying the initial conditions.

Yet another interesting approach [7] to the zero-test problem is to change our point of view. The differentially algebraic power series φ_i at the top of this section are usually specified by a finite number of algebraic differential equations and initial conditions. Now instead of asking whether a given expression represents zero, we may ask for which initial conditions for $\varphi_1, \ldots, \varphi_p$ the expression represents zero.

It turns out that the set of such initial conditions is a closed algebraic set V. The "difficult" cases in the zero-test correspond to the situation in which the original initial conditions are in the closure of an open subset W of V where the answer is "easier". It would be interesting to investigate whether this approach of varying the initial conditions may yield a better power series analogue for Khovanskii's results. A present disadvantage of the method is that it only applies in the convergent case and that it is not yet clear how to obtain complexity bounds.

2.6 The generalized solution approach.

The approach in this paper is similar to the algorithm in [10]. A better understanding (and a complexity analysis) of this algorithm were obtained in [12]. In order to explain the underlying idea behind the present algorithm, let us assume for simplicity that $p=1$ and that $f=\varphi_1$ satisfies the algebraic differential equation $Q(f)=0$.

Now suppose that we want to test whether $P(f)=0$ for a second algebraic differential polynomial P. Then we first use differential algebra to determine a third equation $R(f)=0$ which is equivalent to $P(f)=0$ and $Q(f)=0$ under certain non-degeneracy conditions. Now we consider f as an indeterminate and try to solve $R(f)=0$ in a suitable differential overfield $\mathbb{L}$ of $\mathcal{C}[[z]]$. This field $\mathbb{L}$ consists of so called logarithmic transseries and has the nice property that $Q(f)=0$ still has a unique solution in $\mathbb{L}$ for the initial conditions of f. Hence, $Q(f)=0$ if and only if $R(f)=0$ admits a solution $\tilde{f}$ in $\mathbb{L}$, in which case we *necessarily* have $\tilde{f}=f$.

The approach has the advantages that it accommodates divergent differentially algebraic power series $\varphi_1, \ldots, \varphi_p$ and that the degeneracy of the initial conditions is not amplified during the resolution process. We also have a good hope to obtain complexity bounds along the same lines as in [12] and some hope to generalize the approach to the multivariate setting. We finally expect the approach to be one of the most efficient ones in practice, although no implementations are available yet.

3. THE EFFECTIVE SETUP

Let $\mathcal{C}$ be an *effective field of constants* of characteristic 0. This means that all elements of $\mathcal{C}$ can be represented effectively and that there are algorithms for performing the field operations and testing equality (or, equivalently, for zero-testing).

Let $\mathcal{R}$ be an *effective differential ring* (i.e. the differentiation is effective too). We assume that the elements of $\mathcal{R}$ are formal power series in $\mathcal{C}[[z]]$, that $\mathcal{R} \supseteq C[z]$, and that the differentiation δ on $\mathcal{R}$ corresponds to the differentiation $\delta = z\partial/\partial z$ on $\mathcal{C}[[z]]$. Moreover, we will assume that $\mathcal{R}$ is an *effective power series domain*, i.e. there exists an algorithm which takes $f \in \mathcal{R}$ and $k \in \mathbb{N}$ on input and which computes the coefficient $f_k \in \mathcal{C}$ of z^k in f. Notice that this implies the existence of an algorithm to compute the valuation of $f \in \mathcal{R}$.

Now consider a non zero differential polynomial

$$Q \in \mathcal{R}[F, \ldots, F^{(r)}] \subseteq \mathcal{R}\{F\}$$

of order r (recall that $F^{(r)} = \delta^r F$) and a power series solution $f \in \mathcal{C}[[z]]$ to $Q(f) = 0$. We will assume that f is not a multiple solution, i.e. $\frac{\partial Q}{\partial F^{(i)}}(f) \neq 0$ for some $i \in \{0, \ldots, r\}$ (if f is a multiple solution, then we may always replace Q by a non-zero $\frac{\partial Q}{\partial F^{(i)}}$ and continue doing this until f is no longer a multiple solution). Choose i such that the valuation of $\frac{\partial Q}{\partial F^{(i)}}(f)$ is minimal, say k. Then modulo a transformation of the form

$$f \to f_0 + \cdots + f_k z^k + \tilde{f} z^{k+1}$$

and division of the equation by a suitable power of z, we may also assume that

$$Q = LF + zM, \tag{1}$$

where $L \in \mathcal{C}[\delta]$ and $M \in \mathcal{R}\{F\}$. Let $\Lambda \in \mathcal{C}[k]$ be the polynomial we get from L when reinterpreting δ as an indeterminate k. Then (1) yields a recurrence relation for all but a finite number of coefficients of f:

$$f_k = -\frac{1}{\Lambda(k)}(M(f))_{k-1}. \tag{2}$$

Indeed, the only k for which this relation does not hold are roots of Λ. There are at most r such k and they correspond to the initial conditions for f. Let s be the largest root of Λ in $\mathbb{N}$ (or -1 if such a root does not exist). Then we notice in particular that f is the unique solution to $Q(f) = 0$ whose first $s+1$ coefficients are $f_0, \ldots, f_s$.

In what follows, we will show that the differential ring $\mathcal{R}\{f\}$ is again an effective power series domain. Now elements in $\mathcal{R}\{f\}$ can naturally be represented as the images of differential polynomials in $\mathcal{R}\{F\}$ under the substitution $F \to f$. It therefore suffices to design an algorithm to test whether $P(f) = 0$ for a given differential polynomial $P \in \mathcal{R}\{F\}$. Our algorithm is based on Ritt reduction and the resolution of algebraic equation in more general rings of formal power series. We will use standard notations from differential algebra:

- I_P denotes the *initial* and S_P denotes the *separant* of a differential polynomial P.

- The *rank* of $P \in \mathcal{R}\{F\}$ is given by $\operatorname{rank} P = (r, d) \in \mathbb{N}^2$, where r is the order of P and $d = \deg_{F^{(r)}} P$ the degree of P in $F^{(r)}$. Notice that the set $\mathbb{N}^2$ of possible ranks is well-ordered w.r.t. the lexicographical ordering. We will write V_P for $(F^{(r)})^d$.

- Given $A, B \in \mathcal{R}\{F\}$, we denote by $A \operatorname{rem} B$ the *Ritt reduction* of A with respect to B. We thus have a relation
$$I_B^\alpha H_B^\beta A = XB + (A \operatorname{rem} B),$$
where $\alpha, \beta \in \mathbb{N}$, $X \in \mathcal{R}\{F\}$ and $\operatorname{rank}(A \operatorname{rem} B) < \operatorname{rank} B$.

REMARK 1. At a first glance, our setting may seem less general than the one in the beginning of section 2. However, since we will prove that $\mathcal{R}\{f\}$ is again an effective power series domain, we may repeat the construction after replacing $\mathcal{R}$ by $\mathcal{R}\{f\}$, and add as many other functions $f_2, \ldots, f_p$ as we like. In fact, it suffices to add one f_i for each new subexpression of the form $\varphi_j \circ g$.

4. LOGARITHMIC TRANSSERIES SOLUTIONS TO ALGEBRAIC DIFFERENTIAL EQUATIONS

It is well known that any non-trivial algebraic equation with coefficients in $\mathcal{C}[[z]]$ has a solution in the field $\mathcal{C}^{\text{alg}}[[z^{\mathbb{Q}}]]$ of Puiseux series over the algebraic closure $\mathcal{C}^{\text{alg}}$ of $\mathcal{C}$. We will sketch the proof of an analogous result in the case of algebraic differential equations. For a full proof (of a more general result) we refer to [15].

4.1 Logarithmic transseries

In order to solve equations of the form $\delta f = 1$, it is clear that solutions to such equations might involve logarithms. In fact, they may even involve iterated logarithms.

Let $\mathfrak{L}$ be the totally ordered group of *logarithmic monomials* with powers in $\mathbb{Q}$. More precisely, the elements of $\mathfrak{L}$ are monomials

$$\mathfrak{m} = z^{-\alpha_0} (\log z)^{\alpha_1} \cdots (\log_l z)^{\alpha_l}, \tag{3}$$

where $\alpha_0, \ldots, \alpha_l \in \mathbb{Q}$ and $\log_l$ stands for the l-th iterated logarithm. Given such a monomial, we write $\mathfrak{m} \succ 1$ if and only if $\alpha_i > 0$, where i denotes the least i with $\alpha_i \neq 0$ in (3). This defines a total ordering $\succ$ on $\mathfrak{L}$. The asymptotic relation $\mathfrak{m} \prec \mathfrak{n}$ corresponds to writing $\mathfrak{m} = o(\mathfrak{n})$ as $z \to 0$ in analysis.

A subset $\mathfrak{S} \subseteq \mathfrak{L}$ is said to be *grid-based*, if there exist monomials $\mathfrak{m}_1 \prec 1, \ldots, \mathfrak{m}_m \prec 1$ and $\mathfrak{n}$ in $\mathfrak{L}$, such that $\mathfrak{S} \subseteq \mathfrak{m}_1^{\mathbb{N}} \cdots \mathfrak{m}_m^{\mathbb{N}} \mathfrak{n}$. A *grid-based logarithmic transseries* is a mapping $\mathfrak{L} \to \mathcal{C}$ with grid-based support. We will usually write such series using the infinite sum notation $f = \sum_{\mathfrak{m} \in \mathfrak{L}} f_{\mathfrak{m}} \mathfrak{m}$ and we denote the set of all logarithmic transseries by $\mathbb{L} = \mathcal{C}[[\mathfrak{L}]]$. Since the support of each non-zero $f \in \mathbb{L}$ is grid-based (whence well-ordered), this support admits a $\succcurlyeq$-maximal element $\mathfrak{d}_f$ which is called the *dominant monomial* of f.

It can be shown [13] that $C[[\mathfrak{L}]]$ is a field for the operations

$$\begin{aligned} f + g &= \sum_{\mathfrak{m} \in \mathfrak{L}} (f_{\mathfrak{m}} + g_{\mathfrak{m}}) \mathfrak{m}; \\ fg &= \sum_{\mathfrak{m} \in \mathfrak{L}} \left(\sum_{\mathfrak{m} = \mathfrak{v}\mathfrak{w}} f_{\mathfrak{v}} g_{\mathfrak{w}} \right) \mathfrak{m}. \end{aligned}$$

In the second formula, the grid-based support property ensures that $\sum_{\mathfrak{m} = \mathfrak{v}\mathfrak{w}} f_{\mathfrak{v}} g_{\mathfrak{w}}$ is a finite sum. There also exists a natural derivation δ on $\mathcal{C}[[\mathfrak{L}]]$, which sends each monomial $\mathfrak{m} \in \mathfrak{L}$ of the form (3) to

$$\delta \mathfrak{m} = \left(-\alpha_0 + \frac{\alpha_1}{\log z} + \cdots + \frac{\alpha_l}{\log z \cdots \log_l z} \right) \mathfrak{m}. \qquad (4)$$

This derivation extends to the whole of $\mathbb{L}$ by (infinitary) "strong linearity" [13].

Before proving that solutions to algebraic differential equations with coefficients in $\mathbb{L}$ always exist, we first observe that we have the following uniqueness result:

LEMMA 1. *Let $Q \in \mathcal{R}\{F\}$ be a differential polynomial of the form (1), let $f \in \mathcal{C}[[z]]$ be a solution to $Q(f) = 0$ and let s be defined as in section 3. Then the equation $Q(\tilde{f}) = 0$ with side condition $\tilde{f} - f \prec z^s$ admits f as its unique solution in $\mathbb{L}$.*

PROOF. Each series f in $\mathbb{L}$ may be expanded as a Puiseux series in z

$$f = \sum_{k \in \mathbb{Q}} f_k z^k, \qquad (5)$$

where the coefficients f_k are series in $\mathcal{C}[[\mathfrak{F}]]$ and

$$\mathfrak{F} = (\log z)^{\mathbb{Q}} (\log \log z)^{\mathbb{Q}} \cdots .$$

Notice that we may interpret $\mathfrak{L}$ as the lexicographical product of $z^{\mathbb{Q}}$ and $\mathfrak{F}$. For the expansion (5), the recurrence relation (2) still determines the coefficients of f in a unique way for all $k > s$. □

4.2 Asymptotic differential equations

A classical way to solve algebraic equations over power series is to use the Newton polygon method. We have generalized this method to algebraic differential equations. In fact, it is more convenient to solve *asymptotic differential equations* of the form

$$P(f) = 0 \quad (f \prec \mathfrak{m}), \qquad (6)$$

where $P \in \mathbb{L}\{F\}$ and $\mathfrak{m} \in \mathfrak{L}$. In the sequel, we will assume that $\mathcal{C}$ is algebraically closed.

In order to solve (6), we start by determining all possible dominant monomials $\mathfrak{n} \prec \mathfrak{m}$ of non-zero solutions and their corresponding coefficients. Actually, it is convenient to characterize such *potential dominant monomials* first. It suffices to characterize when 1 is a potential dominant monomial: we will then say that $\mathfrak{n}$ is a potential dominant monomial, if 1 is a potential dominant monomial for the equation

$$P_{\times \mathfrak{n}}(f) = 0 \quad (f \prec \mathfrak{m}/\mathfrak{n}).$$

Here $P_{\times \mathfrak{n}}$ denotes the unique differential polynomial in $\mathbb{L}\{F\}$ with $P_{\times \mathfrak{n}}(f) = P(f\mathfrak{n})$ for all f.

Write $P = \sum_{\boldsymbol{i}} P_{\boldsymbol{i}} F^{(\boldsymbol{i})}$ using multi-indices $\boldsymbol{i}$ and let $\mathfrak{d}_P = \max_{\preccurlyeq} \mathfrak{d}_{P_{\boldsymbol{i}}}$. Then the *dominant part* of P is defined to be the scalar differential polynomial

$$\Delta_P = \sum_{\boldsymbol{i}} P_{\boldsymbol{i}, \mathfrak{d}_P} F^{(\boldsymbol{i})}$$

in $\mathcal{C}\{F\}$, where $P_{\boldsymbol{i}, \mathfrak{d}_P} = (P_{\boldsymbol{i}})_{\mathfrak{d}_P}$. We also define the dominant part $\Delta_{P;z} \in \mathcal{C}[[\mathfrak{F}]]\{F\}$ of P w.r.t. z by

$$\Delta_{P;z} = \sum_{\boldsymbol{i}} P_{\boldsymbol{i}, \nu} F^{(\boldsymbol{i})},$$

where ν is the valuation of P in z and $P_{\boldsymbol{i},\nu}$ denotes the coefficient of z^ν in $P_{\boldsymbol{i}}$.

Assume first that $\Delta_P \in \mathcal{C}[F](\delta F)^{\mathbb{N}}$ and $\Delta_P = \Delta_{P;z}$. Then we define the *differential Newton polynomial* of P by $N_P = \Delta_P$ and we have

$$P(c + \varepsilon) - N_P(c) \prec_z \mathfrak{d}_P$$

for all $c \in \mathcal{C}$ and $\varepsilon \prec_z 1$. Here $\mathfrak{v} \prec_z \mathfrak{w}$, if

$$\mathfrak{w}/\mathfrak{v} = z^{-\alpha_0} \cdots (\log_l z)^{\alpha_l}$$

with $\alpha_0 > 0$. We say that 1 is a potential dominant monomial of a solution to $P(f) = 0$ if and only if N_P admits such a non-zero constant root $c \in \mathcal{C}^*$ (and c is a potential dominant term). Furthermore, N_P admits a non-zero root if and only if $N_P \notin \mathcal{C}$, because $N_P \in \mathcal{C}[F](\delta F)^{\mathbb{N}}$ and $\mathcal{C}$ is algebraically closed.

If $\Delta_P \neq \Delta_{P;z}$ or $\Delta_P \notin \mathcal{C}[F](\delta F)^{\mathbb{N}}$, then we use the technique of "upward shifting". Given $A \in \mathcal{C}[[\mathfrak{F}]]\{F\}$, we define $A \uparrow$ to be the unique differential polynomial in $\mathbb{L}\{F\}$ such that

$$A \uparrow (f \circ e^{1/z}) = A(f) \circ (e^{1/z})$$

for all f. For instance, $(\delta F - 1) \uparrow = -z\delta F - 1$, and we notice that the logarithmic solution $\log z$ of $\delta f = 1$ transforms to the non-logarithmic solution z^{-1} of $-z\delta f = 1$ under upward shifting $f \mapsto f \uparrow = f \circ e^{1/z}$. Now we proved in [15] that after a finite number of replacements $P \to \Delta_{P;z} \uparrow$ we obtain a differential polynomial $\tilde{P}$ with $\Delta_{\tilde{P}} = \Delta_{\tilde{P};z}$ and $\Delta_{\tilde{P}} \in \mathcal{C}[F](\delta F)^{\mathbb{N}}$. We say that 1 is a potential dominant monomial w.r.t. (6) if and only if $1 \prec \mathfrak{m}$ and $N_P := N_{\tilde{P}}$ admits a non-zero root in $\mathcal{C}^*$.

It is clear that if f is a solution to (6), then $\mathfrak{d}_f$ must be a potential dominant monomial of a solution. We say that a potential dominant monomial $\mathfrak{n} \prec \mathfrak{m}$ is *classical*, if $N_{P_{\times \mathfrak{n}}}$ is not homogeneous (i.e. $N_{P_{\times \mathfrak{n}}} \notin \mathcal{C}(\delta F)^{\mathbb{N}}$). These classical potential dominant monomials are finite in number and they can be determined from something which resembles the Newton polygon in the algebraic case [13, 15], by using a succession of multiplicative conjugations $P \to P_{\times z^\alpha}$ and upward shiftings $P \to \Delta_{P;z} \uparrow$ of the dominant parts w.r.t. z.

Once we have found a potential dominant term $\varphi = \tau$ of a solution to (6), we may consider the *refinement*

$$f = \varphi + \tilde{f} \quad (\tilde{f} \prec \tilde{\mathfrak{m}}). \qquad (7)$$

In other words, a refinement is a change of variables together with the imposition of a new asymptotic constraint. It transforms (6) into a new asymptotic differential equation

$$P_{+\varphi}(\tilde{f}) = 0 \quad (\tilde{f} \prec \tilde{\mathfrak{m}}). \qquad (8)$$

Using the possibly transfinite process of determining potential dominant terms and making refinements, one finds all solutions to (6). However, a more careful study is required to ensure that one remains in the context of grid-based transseries and that (for instance) no transseries like

$$\log z + \log_2 z + \log_3 z + \cdots \qquad (9)$$

may occur as solutions of (6).

In order to do this, it is convenient to associate an invariant to the equation (6): the highest possible degree of the *differential* Newton polynomial $N_{P_{\times \mathfrak{n}}}$ that we can achieve for a monomial $\mathfrak{n} \prec \mathfrak{m}$ is called the *Newton degree* of (6) and we denote it by $\deg_{\prec \mathfrak{m}} P$. In the algebraic case, the Newton degree measures the number of solutions to the asymptotic equation (6), when counting with multiplicities. In the differential case, it only gives a lower bound (see theorem 1 below). Also, an equation of Newton degree 0 does not admit any solutions.

Now we have shown in [13, 15] that the Newton degree decreases during refinements and that quasi-linear equations (i.e. equations of Newton degree 1) always admit solutions. Finally, in the case when $\deg_{\prec \tilde{\mathfrak{m}}} P_{+\varphi} = \deg_{\prec \mathfrak{m}} P \geqslant 2$, it is possible to replace φ by a solution to a quasi-linear equation of the form

$$\frac{\partial^{\alpha_0 + \cdots + \alpha_r} P}{(\partial F)^{\alpha_0} \cdots (\partial F^{(r)})^{\alpha_r}}(\varphi) = 0 \quad (\varphi \prec \mathfrak{m}), \qquad (10)$$

and force the Newton degree to strictly decrease after a finite number of steps. In other words, the transfinite resolution process has been replaced by an essentially finite algorithm, which avoids solutions of the form (9). In particular, these methods yield the following theorem:

THEOREM 1. *Consider an asymptotic algebraic differential equation* (6) *of Newton degree $d > 0$ over $\mathbb{L}$. Then* (6) *admits at least d solutions in $\mathbb{L}$ when counting with multiplicities.*

5. THE ALGORITHM

In this sequel, we assume that Q, f and s are as in section 3. We will give an algorithm to test whether $P(f) = 0$ for given $P \in \mathcal{R}\{F\}$. We will write $P \equiv 0$ if and only if $P(f) = 0$.

5.1 Statement of the algorithm

Algorithm $P \equiv 0$
INPUT: a differential polynomial $P \in \mathcal{R}\{F\}$
OUTPUT: **true** if and only if $P \equiv 0$

Step 1. [Initialize]
 $H := 1$
 $R := P$
 reducing := **true**

Step 2. [Reduction]
 while reducing
  if $R \in \mathcal{R}$ **then return** $R = 0$
  else if $I_R \equiv 0$ **then** $R := R - I_R V_R$
  else if $S_R \equiv 0$ **then**
   $H := I_R H, R := R \operatorname{rem} S_R$
  else if $Q \operatorname{rem} R \neq 0$ **then**
   $H := I_R S_R H, R := Q \operatorname{rem} R$
  else $H := I_R S_R H$, reducing := **false**

Step 3. [Final test]
 let k be minimal with $\deg_{\prec z^k} H_{+f_0+\cdots+f_k z^k} = 0$
 $k := \max\{k, s\}$
 return $\deg_{\prec z^k} R_{+f_0+\cdots+f_k z^k} \neq 0$

REMARK 2. In the particular case when an asymptotic differential equation (6) has power series coefficients in $\mathcal{C}[[z]]$ and $\mathfrak{m} = z^k$, its Newton degree $\deg_{\prec z^k} P$ is the minimal degree of a term $P_{\times z^k, \boldsymbol{i}} f^{(\boldsymbol{i})}$ in $P_{\times z^k}$ with $\mathfrak{d}_{P_{\times z^k, \boldsymbol{i}}} = \mathfrak{d}_{P_{\times z^k}}$.

In particular, the minimal k in step 3 can be found by expanding the power series coefficients $H_i(f)$ of H in z using any fast expansion algorithm for solutions to differential equations [3, 14].

5.2 Correctness and termination proof

THEOREM 2. *The above algorithm for testing whether $P \equiv 0$ terminates and is correct.*

PROOF. In the loop in step 2, we notice that the rank of R strictly decreases at each iteration. Also, the rank of I_R (or S_R) in each recursive call of the zero-test is strictly smaller than the rank of R (and whence the rank of P). These two observations, and the fact that the set of possible ranks is well-ordered, imply the termination of the algorithm; the existence of a minimal k with $\deg_{\prec z^k} H_{+f_0+\cdots+f_k z^k} = 0$ will be proved below.

As to the correctness of the algorithm, we claim that at the start and the end inside the loop in step 2, we maintain the properties that $H \not\equiv 0$ and the existence of a relation of the form

$$H^\alpha P = AR + B \qquad (11)$$

for $\alpha \in \mathbb{N}$ and differential polynomials A and B with $B \equiv 0$. Indeed, we have $H = A = 1$ and $B = 0$ at the first entry. If $I_R \equiv 0$ and $\tilde{R} = R - I_R V_R$, then we have $H^\alpha P = AR + B = A\tilde{R} + (B + AI_R V_R)$, with $B + AI_R V_R \equiv 0$. If $S_R \equiv 0$, $\tilde{H} = I_R H$ and $\tilde{R} = R \operatorname{rem} S_R$, then $I_{S_R}^\beta R = X S_R + \tilde{R}$ for some $\beta \in \mathbb{N}$ and differential polynomial X. Also, $I_{S_R} = dI_R$, where $d \geqslant 2$ is the degree of R in the highest $f^{(r)}$ occurring in R. Consequently, denoting $\tilde{\alpha} = \max(\alpha, \beta)$, we have

$$\begin{aligned} \tilde{H}^{\tilde{\alpha}} P &= I_R^{\tilde{\alpha}} H^{\tilde{\alpha}} P \\ &= I_R^{\tilde{\alpha}} H^{\tilde{\alpha}-\alpha} R + I_R^{\tilde{\alpha}} H^{\tilde{\alpha}-\alpha} B \\ &= d^{-\tilde{\alpha}} I_R^{\tilde{\alpha}-\beta} H^{\tilde{\alpha}-\alpha} \tilde{R} + \\ &\quad (d^{-\tilde{\alpha}} I_R^{\tilde{\alpha}-\beta} H^{\tilde{\alpha}-\alpha} X S_R + I_R^{\tilde{\alpha}} H^{\tilde{\alpha}-\alpha} B). \end{aligned}$$

The case when $Q \operatorname{rem} R \neq 0$ is treated in a similar way. This proves our claim; notice that (11) implies $P \equiv 0 \Leftrightarrow R \equiv 0$. By definition, we also have $R = 0 \Leftrightarrow R \equiv 0$ if $R \in \mathcal{R}$ at the first test in the loop.

Let us now assume that the algorithm reaches step 3. Since $H \not\equiv 0$, we may write $H(f) = c_l z^l + O(z^{l+1})$ with $c_l \neq 0$ for some $l \in \mathbb{N}$. For this l, we have $\deg_{\prec z^l} H_{+f_0+\cdots+f_l z^l} = 0$, which implies that there exists a minimal number k, such that both $\deg_{\prec z^k} H_{+f_0+\cdots+f_k z^k} = 0$ and $k \geqslant s$. If $\deg_{\prec z^k} R_{+f_0+\cdots+f_k z^k} = 0$, then we have $R(f) \sim R(f_0 + \cdots + f_k z^k) \neq 0$, whence $R \not\equiv 0$ and $P \not\equiv 0$. Conversely, assume that $\deg_{\prec z^k} R_{+f_0+\cdots+f_k z^k} \neq 0$. Then theorem 1 implies the existence of a series $\tilde{f} \in C[[\mathfrak{L}]]$ with $R(\tilde{f}) = 0$ and $\tilde{f} - f \prec z^k$. Since $Q \operatorname{rem} R = 0$ and $I_R S_R | H$, we have a relation of the form

$$H^\beta Q = XR, \tag{12}$$

where $\beta \in \mathbb{N}$ and X is a differential polynomial. Now $\deg_{\prec z^l} H_{+f_0+\cdots+f_l z^l} = 0$ implies $H(\tilde{f}) \neq 0$, so that $Q(\tilde{f}) = 0$. But, by lemma 1, there exists a unique solution in $C[[\mathfrak{L}]]$ to the equation $Q(\tilde{f}) = 0$ with the side condition $\tilde{f} - f \prec z^s$. Hence $\tilde{f} = f$, $R(f) = 0$ and $P \equiv 0$. □

6. REFERENCES

[1] Ax, J. On Schanuel's conjecture. *Ann. of Math. 93* (1971), 252–268.

[2] Boulier, F. *Étude et implantation de quelques algorithmes en algèbre différentielle*. PhD thesis, University of Lille I, 1994.

[3] Brent, R., and Kung, H. Fast algorithms for manipulating formal power series. *Journal of the ACM 25* (1978), 581–595.

[4] Denef, J., and Lipshitz, L. Power series solutions of algebraic differential equations. *Math. Ann. 267* (1984), 213–238.

[5] Denef, J., and Lipshitz, L. Decision problems for differential equations. *The Journ. of Symb. Logic 54*, 3 (1989), 941–950.

[6] Khovanskii, A. G. *Fewnomials*. American Mathematical Society, Providence, RI, 1991.

[7] Péladan-Germa, A. Testing identities of series defined by algebraic partial differential equations. In *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes* (1995), G. Cohen, M. Giusti, and T. Mora, Eds., Springer-Verlag, pp. 393–407. Proceedings of the 11th International Symposium, AAECC-11, Paris, France, July 1995.

[8] Richardson, D. The uniformity conjecture. In *Lecture Notes in Computer Science* (2001), vol. 2064, Springer Verlag, pp. 253–272.

[9] Risch, R. Algebraic properties of elementary functions in analysis. *Amer. Journ. of Math. 4*, 101 (1975), 743–759.

[10] Shackell, J. A differential-equations approach to functional equivalence. In *ISSAC '89 Proceedings* (Portland, Oregon, 1989), G. Gonnet, Ed., A.C.M. Press, pp. 7–10.

[11] Shackell, J. Zero-equivalence in function fields defined by algebraic differential equations. *Trans. Amer. Math. Soc. 336/1* (1993), 151–172.

[12] Shackell, J., and van der Hoeven, J. Complexity bounds for zero-test algorithms. Tech. Rep. 2001-63, Prépublications d'Orsay, 2001.

[13] van der Hoeven, J. *Automatic asymptotics*. PhD thesis, École polytechnique, France, 1997.

[14] van der Hoeven, J. Relax, but don't be too lazy. Tech. Rep. 78, Prépublications d'Orsay, 1999. Submitted to JSC.

[15] van der Hoeven, J. Complex transseries solutions to algebraic differential equations. Tech. Rep. 2001-34, Univ. d'Orsay, 2001.

[16] van der Hoeven, J. Fast evaluation of holonomic functions near and in singularities. *JSC 31* (2001), 717–743.

[17] van der Hoeven, J. Zero-testing, witness conjectures and differential diophantine approximation. Tech. Rep. 2001-62, Prépublications d'Orsay, 2001.

Note

All papers from the author can be consulted at

`http://www.math.u-psud.fr/~vdhoeven`

This paper has been written using GNU TeXmacs; see

`http://www.texmacs.org`