Math. Ann. 267, 213–238 (1984)

Mathematische Annalen

Power Series Solutions of Algebraic Differential Equations*

J. Denef and L. Lipshitz

Department of Mathematics, University of Leuven, Celestijnenlaan 200 B, B-3030 Heverlee, Belgium
Department of Mathematics, Purdue University, West Lafayette, In 47907, USA

1. Introduction

In this paper we investigate how far M. Artin's Approximation Theorems [2, 3] can be extended to the case of differential equations. We also obtain related decidability and undecidability results. Artin [3] proved

Theorem 1.1. *Let K be any field, and let $K[[x_1, \ldots, x_n]]$ be the ring of formal power series over K in the variables $x_1, \ldots, x_n$. Let $\sum$ be a system of polynomial equations over $K[x_1, \ldots, x_n]$ in the unknowns $y=(y_1, \ldots, y_m)$.*

(i) (Approximation Theorem.) *If $\sum$ has a solution $\bar{y} \in K[[x_1, \ldots, x_n]]$ then it also has a solution $y \in K[[x_1, \ldots, x_n]]$ which is algebraic over $K[x_1, \ldots, x_n]$ and which agrees with the original solution $\bar{y}$ to any specified order.*

(ii) (Strong Approximation.) *If for every $i \in \mathbb{N}$, $\sum$ has a solution in $K[[x_1, \ldots, x_n]]$ modulo the ideal $(x_1, \ldots, x_n)^i$, then $\sum$ has a solution in $K[[x_1, \ldots, x_n]]$.*

(iii) (Existence of an approximation function.) *For every $\alpha \in \mathbb{N}$ there exists $\beta(\alpha) \in \mathbb{N}$ with the following property. If $\sum$ has a solution $\bar{y}$ in $K[[x_1, \ldots, x_n]]$ $\operatorname{mod}(x_1, \ldots, x_n)^{\beta(\alpha)}$, then $\sum$ has a solution y in $K[[x_1, \ldots, x_n]]$ with $y \equiv \bar{y} \operatorname{mod}(x_1, \ldots, x_n)^{\alpha}$.*

In the special case $n=1$, this theorem was first obtained by Greenberg [11] (see also Birch and McCann [7]). For more about strong approximation theorems see [6] and [10].

In Sect. 2 we consider algebraic ordinary differential equations (ADE's) (i.e. differential equations which are polynomial equations in $x, y_1, \ldots, y_m$ and the derivatives $y_i^{(j)}$ of the y's) and we obtain analogues of Theorem 1.1 (for $n=1$): If K has characteristic zero, then Theorem 1.1(i) (for $n=1$) remains valid for systems of ADE's, if we replace "algebraic" by "differentially algebraic" (see Theorem 2.1). A

* The first author thanks the Institute for Advanced Study for its hospitality and support. The second author thanks the N.S.F. for its support

power series (in one variable) is called differentially algebraic if it satisfies some nontrivial ADE in one unknown. Much is known about differentially algebraic power series, e.g. Maillet [16] and Popken [20] (see also Mahler [15]) gave bounds on the rate of growth of the coefficients a_n of such a power series, viz $|a_n| \leqq c_1(n!)^{c_2}$. (See also the recent results of Sibuya and Sperber [27]).

If K is an algebraically closed field, a real closed field, or a field which is henselian with respect to a discrete valuation (e.g. the field of p-adic numbers $\mathbb{Q}_p$), and if K has characteristic zero, then the Strong Approximation Theorem 1.1(ii) (for $n=1$) remains valid for systems of ADE's (see Theorem 2.10). In 2.10 we prove this Strong Approximation Theorem by a method (ultraproducts) which is not effective, but in Sect. 3 we give an effective proof, which is however longer and much more tedious. In 2.12 we show that the Strong Approximation Theorem for ADE's is not true when $K=\mathbb{R}(t)$. (We expect it is not true for $K=\mathbb{Q}$, but have not been able to prove this). Theorem 1.1(iii) (for $n=1$) is false for ADE's, but a weaker version (Theorem 2.14) remains true for ADE's, if $K=\mathbb{R}$, $\mathbb{C}$ or $\mathbb{Q}_p$.

In Sect. 3 we use the results of Sect. 2 to give an algorithm (Theorem 3.1) for deciding when a system $\sum$ of ADE's over $\mathbb{Q}[x]$ has a solution in $\mathbb{C}[[x]]$, or $\mathbb{R}[[x]]$, or $\mathbb{Q}_p[[x]]$. For this, we show how to compute a $\beta \in \mathbb{N}$ such that $\sum$ has a solution if and only if it has a solution mod x^β. Note that the existence of a solution of $\sum$ in $\mathbb{R}[[x]]$ is equivalent with the existence of a solution which is a C^∞ function in a neighborhood of 0. (This follows easily from Theorem 10.1 of Malgrange [17].) Hence there is an algorithm for deciding when a system of ADE's has a C^∞ solution near $x=0$. However (Proposition 3.3), there do not exist algorithms for deciding when a system of ADE's has a nonzero solution, or a convergent solution in $\mathbb{C}[[x]]$ (or $\mathbb{R}[[x]]$).

In Sect. 4 we present some results about algebraic partial differential equations which show, inter alia, that most of the above results do not extend to this case. From the above mentioned Theorem 2.1 it follows that if a system of ADE's has a unique power series solution $y=(y_1, \ldots, y_m)$ then the y_i are differentially algebraic. However, in the case of partial differential equations we obtain the following result (Theorem 4.2): For every computable function $f: \mathbb{N} \to \mathbb{Q}$ the power series $y_1 = \sum_n f(n) x_1^n$ occurs as part of the unique solution $(y_1, \ldots, y_m) \in \mathbb{C}[[x_1, \ldots, x_r]]$ of some system of algebraic partial differential equations. (The converse is also true - see Theorem 4.1.) We also show (Theorem 4.11) that there does not exist an algorithm to decide if a linear partial differential equation (in one dependent variable) has a solution in $\mathbb{C}[[x_1, \ldots, x_r]]$. We also show (Theorem 4.12) that there is a system of linear partial differential equations which has infinitely many power series solutions over $\mathbb{Q}$ but no computable solutions. (For other results on differential equations with no computable solutions see [1, 21, 22].) For algebraic partial differential equations the Strong Approximation Theorem 1.1(ii) holds over $\mathbb{C}$ but not over $\mathbb{R}$ or $\bar{\mathbb{Q}}$ (the algebraic closure of $\mathbb{Q}$) - see 4.10 and 4.7 below.

In this paper we only consider power series over a field of characteristic zero. If K is a perfect field of characteristic $p \neq 0$ then the solvability in $K[[x]]$ of a system of ADE's can be reduced to the solvability of a system of polynomial equations, by writing the unknowns y as $y = z_1^p + x z_2^p + \ldots + x^{p-1} z_p^p$, where the z_i are new unknowns.

2. Approximation Theorems for Differential Equations

In this section K is a field of characteristic zero, $K(x)$ is the field of rational functions over K, and $K[[x]]$ is the ring of formal power series over K, in one variable x. Thus $K[[x]]$ is a differential ring with derivation trivial on K, and $x'=1$. Let F be a differential field, R a differential subring of F, and $\bar{y}$ an element of F. We say that $\bar{y}$ is *differentially algebraic* over R if there exists a non-zero differential polynomial over R in one variable y, which vanishes on $\bar{y}$ (see Kaplansky [13].) (If $R=\mathbb{Q}[x]$, then $\bar{y}$ is called differentially algebraic.) We will prove

Theorem 2.1 (Approximation Theorem). *Let R be a differential subring of $K[[x]]$, and let $\sum$ be a set of differential polynomials in $y_1, \ldots, y_m$ over R. Suppose $\bar{y}_1, \ldots, \bar{y}_m \in K[[x]]$ is a solution of $\sum=0$. Let $\alpha \in \mathbb{N}$. Then there exist $\bar{\bar{y}}_1, \ldots, \bar{\bar{y}}_m \in K[[x]]$ which are differentially algebraic over R, such that*

$$(\bar{\bar{y}}_1, \ldots, \bar{\bar{y}}) \text{ is a solution of } \textstyle\sum=0$$
$$\bar{y}_1 \equiv \bar{\bar{y}}_1, \ldots, \bar{y}_m \equiv \bar{\bar{y}}_m \bmod x^\alpha .$$

Remark. From Ritt [23] and Seidenberg [26] it follows that if a system of algebraic differential equations has a solution in some differential field extension then it has a differentially algebraic solution (but not necessarily a power series solution).

The key lemma in proving the algebraic analogue of Theorem 2.1 (i.e. Greenberg's theorem [11]) is the Hensel-Rychlik lemma: If $p(x,y) \in K[[x]]\,[y]$ and $\bar{y} \in K[[x]]$ satisfies $p(x,\bar{y})=0 \bmod x^{2k+1}$ and $\frac{\partial p}{\partial y}(x,\bar{y}) \not\equiv 0 \bmod x^{k+1}$, then there exists $\bar{\bar{y}} \in K[[x]]$ such that $p(x,\bar{\bar{y}})=0$ and $\bar{\bar{y}} \equiv \bar{y} \bmod x^{k+1}$. Lemma 2.3 below gives a generalization of the Hensel-Rychlik lemma to the differential case. The proof of Lemma 2.3 is based on a result of Hurwitz [12], that if $\bar{y}=\sum a_i x^i$ is a solution to $P(x,y,y',\ldots,y^{(n)})=0$ with $\frac{\partial P}{\partial y^{(n)}}(x,\bar{y},\bar{y}',\ldots,\bar{y}^{(n)}) \neq 0$ then the a_i, for i large enough, are determined by a recursion formula. Hurwitz used this recursion formula to prove that

$$\sum_n \frac{x^n}{(n^n)!}$$

is not differentially algebraic. The key lemma in Hurwitz [12] is the following

Lemma 2.2. *Let $P(x,y,y',\ldots,y^{(n)})$ be a differential polynomial over $K[[x]]$ in the differential indeterminate y, of order n. Let $k \in \mathbb{N}$ be fixed. Then*

$$\begin{aligned} P^{(2k+2)} = {} & y^{(n+2k+2)} f_n + y^{(n+2k+1)} f_{n+1} + y^{(n+2k)} f_{n+2} \\ & + \ldots + y^{(n+k+2)} f_{n+k} + f_{n+k+1}, \end{aligned} \tag{1}$$

where the f_j are differential polynomials in y of order at most j, for $j=n$, $n+1, \ldots, n+k+1$, and

$$f_n = \frac{\partial P}{\partial y^{(n)}} . \tag{2}$$

(Notice that $f_{n+1}, f_{n+2}, \ldots$ depend upon k.)

Let $q \in \mathbb{N}$, *then*

$$P^{(2k+2+q)} = y^{(n+2k+2+q)} f_n + y^{(n+2k+1+q)} [f_{n+1} + q f_n'] + \ldots + y^{(n+2k+2+q-k)} \left[f_{n+k} + q f_{n+k-1}' + \ldots + \binom{q}{k} f_n^{(k)} \right] + h_{n+k+q+1}, \tag{3}$$

where $h_{n+k+q+1}$ *is a differential polynomial in* y *of order at most* $n+k+q+1$.

Proof. We have

$$P' = y^{(n+1)} f_n + g_n,$$

where g_n is a differential polynomial in y of order at most n. Formula (1) is easily proved by induction on k. Formula (3) is obtained by differentiating (1) q times, and using Leibniz's rule. Q.E.D.

Lemma 2.3. *Let* $P(x, y, y', \ldots, y^{(n)})$ *be a differential polynomial over* $K[[x]]$ *in the differential indeterminate* y, *of order* n. *Let* $\bar{y} \in K[[x]]$, *and suppose*

$$\frac{\partial P}{\partial y^{(n)}} (x, \bar{y}, \bar{y}', \ldots, \bar{y}^{(n)}) = c_0 x^k + c_1 x^{k+1} \times \ldots, \tag{1}$$

with $c_0 \neq 0$.

There exists a least $r \in \mathbb{N}$, $0 \leqq r \leqq k$, *such that, with the notation of Lemma 2.2,*

$$\left[f_{n+r} + q f_{n+r-1}' + \ldots + \binom{q}{r} f_n^{(r)} \right] (0, \bar{y}(0), \bar{y}'(0), \ldots) \tag{2}$$

is a nonzero polynomial in q.

Let $\gamma \in \mathbb{N}$ *be bigger than any root* $q \in \mathbb{N}$ *of polynomial* (2). *Suppose*

$$P(x, \bar{y}, \bar{y}', \ldots, \bar{y}^{(n)}) \equiv 0 \bmod x^{2k+2+\gamma+r}, \tag{3}$$

then there exists $\bar{\bar{y}} \in K[[x]]$, *such that*

$$\bar{\bar{y}} \equiv \bar{y} \bmod x^{n+2k+2+\gamma}, \tag{4}$$

and

$$P(x, \bar{\bar{y}}, \bar{\bar{y}}', \ldots, \bar{\bar{y}}^{(n)}) = 0. \tag{5}$$

Proof. From (1) and formula (2) in Lemma 2.2, it follows that

$$f_n^{(k)}(0, \bar{y}(0), \bar{y}'(0), \ldots) = c_0 \neq 0.$$

Thus polynomial (2) is non-zero for $r = k$, from this follows the existence of r. We will write $\bar{y}_0^{(j)}$ for $\bar{y}^{(j)}(0)$ and $\bar{\bar{y}}_0^{(j)}$ for $\bar{\bar{y}}^{(j)}(0)$. From (2) and formula (3) in Lemma 2.2, it follows for all $\bar{\bar{y}} \in K[[x]]$, with $\bar{\bar{y}}_0^{(j)} = \bar{y}_0^{(j)}$ for $j \leqq n+r$, that

$$P^{(2k+2+q)}(0, \bar{\bar{y}}_0, \bar{\bar{y}}_0', \ldots) = \bar{\bar{y}}_0^{(n+2k+2+q-r)} A(0, \bar{\bar{y}}_0, \bar{\bar{y}}_0', \ldots, q) + H_{n+2k+1+q-r}(0, \bar{\bar{y}}_0, \bar{\bar{y}}_0', \ldots), \tag{6}$$

where

$$A(x, y, y', \ldots, q) = f_{n+r} + q f'_{n+r-1} + \cdots + \binom{q}{r} f_n^{(r)}, \tag{7}$$

and $H_{n+2k+1+q-r}$ is a differential polynomial in y of order at most $n+2k+1+q-r$. We determine $\bar{\bar{y}} \in K[[x]]$ by

$$\begin{aligned} \bar{\bar{y}}_0 &= \bar{y}_0 \\ \bar{\bar{y}}'_0 &= \bar{y}'_0 \\ &\vdots \\ \bar{\bar{y}}_0^{(n+2k+1+\gamma)} &= \bar{y}_0^{(n+2k+1+\gamma)} \end{aligned} \tag{8}$$

and,

$$\bar{\bar{y}}_0^{(n+2k+2+q-r)} = \frac{-H_{n+2k+1+q-r}(0, \bar{\bar{y}}_0, \bar{\bar{y}}'_0, \ldots)}{A(0, \bar{\bar{y}}_0, \bar{\bar{y}}'_0, \ldots, q)}, \tag{9}$$

for $q \geqq \gamma + r$.

Notice that (8) implies (4), and that (9) and (6) imply

$$P^{(2k+2+q)}(0, \bar{\bar{y}}_0, \bar{\bar{y}}'_0, \ldots) = 0, \quad \text{for} \quad q \geqq \gamma + r. \tag{10}$$

From (3) and (4) it follows that

$$P(x, \bar{\bar{y}}, \bar{\bar{y}}', \ldots, \bar{\bar{y}}^{(n)}) \equiv 0 \bmod x^{2k+2+\gamma},$$

hence

$$P^{(j)}(0, \bar{\bar{y}}_0, \bar{\bar{y}}'_0, \ldots) = 0, \quad \text{for} \quad j = 0, 1, 2, \ldots, 2k+1+\gamma. \tag{11}$$

From (6) and (8) it follows for $q = \gamma, \gamma+1, \ldots, \gamma+r-1$ that

$$\begin{aligned} &P^{(2k+2+q)}(0, \bar{\bar{y}}_0, \bar{\bar{y}}'_0, \ldots) \\ &= \bar{\bar{y}}_0^{(n+2k+2+q-r)} A(0, \bar{\bar{y}}_0, \bar{\bar{y}}'_0, \ldots, q) + H_{n+2k+1+q-r}(0, \bar{\bar{y}}_0, \bar{\bar{y}}'_0, \ldots) \\ &= \bar{y}_0^{(n+2k+2+q-r)} A(0, \bar{y}_0, \bar{y}'_0, \ldots, q) + H_{n+2k+1+q-r}(0, \bar{y}_0, \bar{y}'_0, \ldots) \\ &\quad (\text{because } n+2k+2+q-r \leqq n+2k+1+\gamma) \\ &= P^{(2k+2+q)}(0, \bar{y}_0, \bar{y}'_0, \ldots). \end{aligned}$$

Thus from (3) it now follows that

$$P^{(2k+2+q)}(0, \bar{\bar{y}}_0, \bar{\bar{y}}'_0, \ldots) = 0, \quad \text{for} \quad q = \gamma, \gamma+1, \ldots, \gamma+r-1. \tag{12}$$

Thus from (11), (12) and (10), (5) follows.

Lemma 2.4. *Let* $n \in \mathbb{N}$, *and*

$$P(Y_0, Y_1, \ldots, Y_n) \in K[[x]]\,[Y_0, \ldots, Y_n].$$

Let $\bar{y} \in K[[x]]$ *be a solution of the differential equation*

$$P(\bar{y}, \bar{y}', \ldots, \bar{y}^{(n)}) = 0. \tag{1}$$

Suppose

$$\frac{\partial P}{\partial Y_n}(\bar{y}, \bar{y}', \ldots, \bar{y}^{(n)}) \neq 0 . \tag{2}$$

Let $\alpha \in \mathbb{N}$. Then there exists $\beta \in \mathbb{N}$, such that for all

$$\tilde{P}(Y_0, Y_1, \ldots, Y_n) \in K[[x]][Y_0, \ldots, Y_n],$$

with

$$P \equiv \tilde{P} \bmod x^{\beta},$$

there exists $\bar{\bar{y}} \in K[[x]]$ such that

$$\tilde{P}(\bar{\bar{y}}, \bar{\bar{y}}', \ldots, \bar{\bar{y}}^{(n)}) = 0,$$
$$\bar{\bar{y}} \equiv \bar{y} \bmod x^{\alpha}.$$

Proof. From (2) it follows that there exists $k \in \mathbb{N}$ such that

$$\frac{\partial P}{\partial Y_n}(x, \bar{y}, \bar{y}', \ldots, \bar{y}^{(n)}) = cx^k + c_1 x^{k+1} + \ldots,$$

with $c \neq 0$.

If $\beta \geqq k+1$, then

$$\frac{\partial \tilde{P}}{\partial Y_n}(x, \bar{y}, \bar{y}', \ldots, \bar{y}^{(n)}) = cx^k + \ldots .$$

Let $\tilde{f}_n, \tilde{f}_{n+1}, \ldots, \tilde{f}_{n+k+1}$ be obtained from $\tilde{P}$, in the same way that $f_n, \ldots, f_{n+k+1}$ are obtained from P in Lemma 2.2.

If $\beta \geqq 3k+3$, then

$$\tilde{f}^{(\lambda)}_{n+\mu}(0, \bar{y}(0), \bar{y}'(0), \ldots) = f^{(\lambda)}_{n+\mu}(0, \bar{y}(0), \bar{y}'(0), \ldots), \tag{3}$$

for $\mu = 0, 1, \ldots, k$, and $\lambda = 0, 1, \ldots, k$.

Let r and $\gamma \geqq \alpha$ be as in Lemma 2.3. From (3) it follows that this r and γ also satisfy the data of Lemma 2.3 if we replace P by $\tilde{P}$.

If $\beta \geqq 2k+2+\gamma+r$, then (1) implies

$$\tilde{P}(x, \bar{y}, \bar{y}', \ldots, \bar{y}^{(n)}) \equiv 0 \bmod x^{2k+2+\gamma+r}.$$

Now apply Lemma 2.3 with P replaced by $\tilde{P}$. Q.E.D.

The following lemma follows immediately from Ritt [23, p. 6], but we give a self contained proof. (A different elimination result is given in Rubel [25].) First we need some notation. Let $\sum$ be a set of differential polynomials in $y_1, \ldots, y_m$ over a differential field L of characteristic 0. Let $\bar{y}_1, \ldots, \bar{y}_m$ be a solution of $\sum = 0$. (By a solution we mean any solution in any differential field extension of L.) Let S be the differential ring generated by $\bar{y}_1, \ldots, \bar{y}_{m-1}$ over L, and suppose $\bar{y}_m$ is differentially algebraic over S. Let

$$P(y_m, y_m', \ldots, y_m^{(n)})$$

be a non-zero differential polynomial over S in y_m of *lowest rank* vanishing on $\bar{y}_m$

(i.e. lowest possible order n, and lowest degree in $y_m^{(n)}$). Let n be the order of P, and d the degree of P in $y_m^{(n)}$. Let

$$F(y_1, y_1', \ldots, y_m, \ldots, y_m^{(n)})$$

be a differential polynomial over L in $y_1, \ldots, y_m$ of order n in y_m and of degree d in $y_m^{(n)}$ such that

$$F(\bar{y}_1, \bar{y}_1', \ldots, \bar{y}_{m-1}, \bar{y}_{m-1}', \ldots, y_m, y_m', \ldots, y_m^{(n)}) = P(y_m, \ldots, y_m^{(n)}).$$

Write

$$\begin{aligned} F(y_1, y_1', \ldots, y_m^{(n)}) = A_0(y_1, \ldots, y_m^{(n-1)})\,(y_m^{(n)})^d \\ + A_1(y_1, \ldots, y_m^{(n-1)})(y_m^{(n)})^{d-1} + \ldots \end{aligned} \tag{1}$$

with $A_0, A_1, \ldots$ differential polynomials of order less than n in y_m. Then from the minimality of P we have

$$\frac{\partial F}{\partial y_m^{(n)}}(\bar{y}_1, \ldots, \bar{y}_m^{(n)}) \neq 0 \quad \text{and} \quad A_0(\bar{y}_1, \ldots, \bar{y}_m^{(n-1)}) \neq 0. \tag{2}$$

Let $\sum'$ be the set of all differential polynomials in $y_1, \ldots, y_{m-1}$ over L vanishing on $\bar{y}_1, \ldots, \bar{y}_{m-1}$. Let $\bar{\bar{y}}_1, \ldots, \bar{\bar{y}}_m$ be any solution of

$$\textstyle\sum' = 0, \tag{3}$$

$$F = 0, \tag{4}$$

$$\frac{\partial F}{\partial y_m^{(n)}} \neq 0, \tag{5}$$

$$A^0 \neq 0. \tag{6}$$

Lemma 2.5. *With the above notation $\bar{\bar{y}}_1, \ldots, \bar{\bar{y}}_m$ is also a solution of $\sum$.*

Proof. [We write $\bar{y}$ for $(\bar{y}_1, \bar{y}_1', \ldots, \bar{y}_2, \bar{y}_2', \ldots, \bar{y}_m, \bar{y}_m', \ldots)$, and similarly for $\bar{\bar{y}}$.] Let

$$G(y_1, y_1', \ldots, y_m, \ldots, y_m^{(l)})$$

be a differential polynomial over L in $y_1, \ldots, y_m$, of order l in y_m. Suppose that $G \in \sum$.

The following arguments apply to every $(\bar{\bar{y}}_1, \ldots, \bar{\bar{y}}_m)$ satisfying (3), (4), (5), and (6). Differentiating (4) we obtain

$$\bar{\bar{y}}_m^{(n+1)} \frac{\partial F}{\partial y_m^{(n)}}(\bar{\bar{y}}) = H(\bar{\bar{y}}_1, \ldots, \bar{\bar{y}}_m, \ldots, \bar{\bar{y}}_m^{(n)}), \tag{7}$$

where H is a differential polynomial in $y_1, \ldots, y_m$ over L of order at most n in y_m. [And the same H works for all $\bar{\bar{y}}$ satisfying (3)–(6)].

By substituting (7) several times in G, we obtain

$$\left(\frac{\partial F}{\partial y_m^{(n)}}(\bar{\bar{y}})\right)^{\lambda} G(\bar{\bar{y}}_m, \ldots, \bar{\bar{y}}_m^{(l)}) = M(\bar{\bar{y}}_1, \bar{\bar{y}}_1', \ldots, \bar{\bar{y}}_m, \ldots, \bar{\bar{y}}_m^{(n)}) \tag{8}$$

for some $\lambda \in \mathbb{N}$ and some differential polynomial M over L in $y_1, \ldots, y_m$ of order *at most* n in y_m. [And the same M works for all $\bar{\bar{y}}$ satisfying (3)–(6).]

From (1) and (4) it follows that

$$A_0(\bar{\bar{y}}_1, \ldots, \bar{\bar{y}}_m^{(n-1)})(\bar{\bar{y}}_m^{(n)})^d = -A_1(\bar{\bar{y}}_1, \ldots, \bar{\bar{y}}_m^{(n-1)})(\bar{\bar{y}}_m^{(n)})^{d-1} - \ldots. \tag{9}$$

By substituting (9) several times into M we get

$$(A_0(\bar{\bar{y}}_1, \ldots, \bar{\bar{y}}_m^{(n-1)}))^\gamma M(\bar{\bar{y}}_1, \ldots, \bar{\bar{y}}_m^{(n)}) = W(\bar{\bar{y}}_1, \ldots, \bar{\bar{y}}_m^{(n)}), \tag{10}$$

for some $\gamma \in \mathbb{N}$ and some differential polynomial W over L in $y_1, \ldots, y_m$ of order in y_m at most n and of degree in $y_m^{(n)}$ *less* than d. (And the same W works for all $\bar{\bar{y}}$ satisfying (3)–(6)). From (8) and (10) it now follows that

$$\left(\frac{\partial F}{\partial y_m^{(n)}}(\bar{\bar{y}})\right)^\lambda (A_0(\bar{\bar{y}}))^\gamma G(\bar{\bar{y}}) = W(\bar{\bar{y}}). \tag{11}$$

Now $\bar{y}$ satisfies (3)–(6), hence

$$\left(\frac{\partial F}{\partial y_m^{(n)}}(\bar{y})\right)^\lambda (A_0(\bar{y}))^\gamma G(\bar{y}) = W(\bar{y}). \tag{11'}$$

Since $G \in \sum$ and $\sum(\bar{y}) = 0$, we obtain $G(\bar{y}) = 0$, and by (11')

$$W(\bar{y}) = 0. \tag{12}$$

Since $W(\bar{y}_1, \ldots, \bar{y}_{m-1}^{(l)}, y_m, \ldots, y_m^{(n)})$ is a differential polynomial in y_m over S, vanishing on $\bar{y}_m$, of smaller rank than P, we obtain (by the minimality of P) that

$$W(\bar{y}_1, \ldots, \bar{y}_{m-1}^{(l)}, y_m, \ldots, y_m^{(n)})$$

is identically zero as a polynomial in $y_m, y_m', \ldots, y_m^{(n)}$. Thus we can write

$$W(y_1, \ldots, y_m^{(n)}) = \sum_{ij} V_{ij}(y_1, \ldots, y_{m-1}^{(l)})(y_m^{(i)})^j$$

with $V_{ij} \in \sum'$.

Thus, (3) implies now that

$$W(\bar{\bar{y}}) = 0.$$

Hence, from (5), (6), and (11) it follows that

$$G(\bar{\bar{y}}) = 0.$$

Lemma 2.6. *Let $K \subset L$ be differential fields. Suppose $z_1, \ldots, z_m \in L$ are differentially algebraic over K. Let F be the differential field generated by $z_1, \ldots, z_m$ over K. If $z_{m+1} \in L$ is differentially algebraic over F, then z_{m+1} is also differentially algebraic over K.*

Proof. It is easy to verify that $z \in L$ is differentially algebraic over K if and only if

$$\operatorname{Tr}\deg_K K(z, z', z'', z''', \ldots) < \infty.$$

Thus we obtain

$$\operatorname{Tr}\deg_K F < \infty, \ \operatorname{Tr}\deg_F F(z_{m+1}, z_{m+1}', \ldots) < \infty.$$

Hence

$$\operatorname{Tr}\deg_K K(z_{m+1}, z_{m+1}', \ldots) < \infty.$$

Proof of Theorem 2.1. We prove Theorem 2.1 by induction on m. The case $m=0$ is trivial. We may suppose that $\sum$ contains a non-zero polynomial, otherwise the theorem is trivial. Then, by renumbering the $y_1, \ldots, y_m$, we may suppose that $\bar{y}_m$ is differentially algebraic over S (S defined as in Lemma 2.5). We now use the result and the notation of Lemma 2.5, with L the fraction field of R. Without loss of generality we may suppose that $\alpha \in \mathbb{N}$ is big enough so that we have for all $\bar{\bar{y}}=(\bar{\bar{y}}_1, \ldots, \bar{\bar{y}}_m) \in K[[x]]$ that

$$\bar{\bar{y}} \equiv \bar{y} \bmod x^\alpha \text{ implies } \frac{\partial F}{\partial y_m^{(n)}}(\bar{\bar{y}}) \neq 0 \quad \text{and} \quad A_0(\bar{\bar{y}}) \neq 0).$$

Let β be as in Lemma 2.4 (for $\bar{y}$ replaced by $\bar{y}_m$). Choose $\beta' \geqq \alpha$ big enough such that we have for all $\bar{\bar{y}}_n, \ldots, \bar{\bar{y}}_{m-1} \in K[[x]]$

$$\bar{\bar{y}}_1 \equiv \bar{y}_1, \ldots, \bar{\bar{y}}_{m-1} \equiv \bar{y}_{m-1} \bmod x^{\beta'}$$

implies

$$P(Y_0, Y_1, \ldots, Y_n) \equiv F(\bar{\bar{y}}_1, \ldots, \bar{\bar{y}}_{n-1}, \ldots, Y_0, Y_1, \ldots, Y_n) \bmod x^\beta, \text{ in } K[[x]][Y_0, \ldots, Y_n].$$

By the induction hypothesis there exist $\bar{\bar{y}}_1, \ldots, \bar{\bar{y}}_{m-1} \in K[[x]]$, which are differentially algebraic over R, and such that

$$\bar{\bar{y}}_1, \ldots, \bar{\bar{y}}_{m-1} \text{ is a solution of } \textstyle\sum'$$
$$\bar{\bar{y}}_1 \equiv \bar{y}_1, \ldots, \bar{\bar{y}}_{m-1} \equiv \bar{y}_{m-1} \bmod x^{\beta'}.$$

From Lemma 2.4, it now follows that there exist $\bar{\bar{y}}_m \in K[[x]]$ such that

$$F(\bar{\bar{y}}_1, \ldots, \bar{\bar{y}}_{m-1}, \ldots, \bar{\bar{y}}_m, \bar{\bar{y}}_m', \ldots, \bar{\bar{y}}_m^{(n)})=0$$
$$\bar{y}_m \equiv \bar{\bar{y}}_m \bmod x^\alpha.$$

From the result of Lemma 2.5 it follows now that $\bar{\bar{y}}_1, \ldots, \bar{\bar{y}}_m$ is a solution of $\sum$. From Lemma 2.6 it follows that $\bar{\bar{y}}_m$ is differentially algebraic over R.

Theorem 2.7. *Let $K \subset L$ be fields of characteristic zero satisfying one of the three following conditions.*

(1) *K and L are algebraically closed fields*

(2) *K and L are real closed fields*

(3) *K is Henselian with respect to a discrete valuation, (i.e. K is the fraction field of a Henselian discrete valuation ring) and every finite system of polynomial equations over K, which has a solution in L, also has a solution in K.*

Let $\sum$ be a set of differential polynomials in $y_1, \ldots, y_m$ over $K[[x]]$. If $\sum=0$, has a solution $\bar{y}_1, \ldots, \bar{y}_m \in L[[x]]$, then $\sum=0$ also has a solution $\bar{\bar{y}}_1, \ldots, \bar{\bar{y}}_m \in K[[x]]$.

Remark. Case (3) applies when L is the field of p-adic numbers, $\mathbb{Q}_p$, and K is the algebraic closure of $\mathbb{Q}$ in $\mathbb{Q}_p$ [11].

Proof. From Theorem 2.1 it follows that we may suppose that $\bar{y}_1, \ldots, \bar{y}_m$ are differentially algebraic over $K[[x]]$. Let $P(x, y, y', \ldots, y^{(n)})$ be a differential polynomial over $K[[x]]$ of lowest rank vanishing on $\bar{y}_1$. Hence $\frac{\partial P}{\partial y^{(n)}}(x, \bar{y}_1, \bar{y}_1', \ldots) \neq 0$. Let

$$\bar{y}_1 = \sum_{i=0}^{\infty} \frac{a_i}{i!} x^i, \quad \text{with} \quad a_i \in L.$$

From formula (6) in Lemma 2.3 it follows that

$$a_i = \frac{H_{i-1}(a_0, a_1, a_2, \ldots, a_{i-1})}{R(i)}, \tag{4}$$

for all i bigger than some $\eta \in \mathbb{N}$, where $R(i)$ is a polynomial in i with coefficients in L, and the H_{i-1} are polynomials in $a_0, a_1, \ldots, a_{i-1}$ with coefficients in K. (We have $R(i) \neq 0$, for $i > \eta$).

Thus we obtain that there exists a subfield L_1 of L which is finitely generated over K, such that

$$\bar{y}_1, \ldots, \bar{y}_m \in L_1[[x]].$$

However, we have even more: from the special form of the denominator of (4) it follows that there exist a finite number of elements $c_1, \ldots, c_r \in L$ such that the coefficients of $\bar{y}_1, \ldots, \bar{y}_m$ lie in

$$K\left[c_1, \ldots, c_r, \frac{1}{w_1}, \frac{1}{w_2}, \ldots, \frac{1}{w_j}, \ldots\right],$$

where the w_j are polynomials over $\mathbb{Q}$ of *bounded* degree in the $c_1, \ldots, c_r$.

Our system of differential equations $\sum = 0$, reduces in the obvious way to a system of equations and inequations in the $c_1, \ldots, c_r$. Thus the theorem follows at once from the following lemma.

Lemma 2.8. *Let K and L be as in Theorem 2.7, satisfying condition* (1), (2) *or* (3). *Let $F_i(x_1, \ldots, x_r) \in K[x_1, \ldots, x_r]$, for $i \in \mathbb{N}$, and let $W_j(x_1, \ldots, x_r) \in \mathbb{Q}[x_1, \ldots, x_r]$, for $j \in \mathbb{N}$. Suppose there exists $D \in \mathbb{N}$, such that* $\deg W_j(x_1, \ldots, x_r) \leqq D$ *for all $j \in \mathbb{N}$.*

Let $c_1, \ldots, c_r \in L$, be such that $F_i(c_1, \ldots, c_r) = 0$, $W_j(c_1, \ldots, c_r) \neq 0$, for all $i, j \in \mathbb{N}$. Then there exist $b_1, \ldots, b_r \in K$ such that $F_i(b_1, \ldots, b_r) = 0$, $W_j(b_1, \ldots, b_r) \neq 0$ for all $i, j \in \mathbb{N}$.

Proof. Since $K[x_1, \ldots, x_r]$ is a Noetherian ring, we may suppose that the set of the F_i is finite. When the set of the W_j is also finite, then the Lemma is true, because every finite system of polynomial equations over K which has a solution in L also has a solution in K (see e.g. Lang [14, Theorem 5, p. 278]), and because every inequality $a \neq 0$ is equivalent with $\exists b$: $ab = 1$. By taking more polynomials F_i, we may suppose that the F_i generate the prime ideal I of all polynomials over K vanishing on $c_1, \ldots, c_r$. Since the singular locus of a variety, has codimension at least one, we have that $(c_1, \ldots, c_r)$ is a nonsingular point of the K-variety V defined by I. Thus we may suppose that

$$\det\left(\frac{\partial F_i}{\partial x_k}\right)_{\substack{i=1,\ldots,h \\ k=d+1,\ldots,r}} (c_1, \ldots, c_r) \neq 0,$$

where d is the Krull dimension of V and $h = r - d$. Thus there exist $a_1, \ldots, a_r \in K$, such that $F_i(a_1, \ldots, a_r) = 0$ for all i, and $\det\left(\frac{\partial F_i}{\partial x_k}\right)(a_1, \ldots, a_r) \neq 0$. Hence $(a_1, \ldots, a_r)$ is a nonsingular K-rational point on V. The lemma now follows from the following Lemma 2.9, which we will also need in Sect. 3.

Lemma 2.9. *Let K be as in Theorem 2.7 and let K_0 be a finitely generated subfield of K. Let I be a prime ideal of $K_0[x_1, \dots, x_r]$, and let $W_j(x_1, \dots, x_r), j \in \mathbb{N}$ be a collection of polynomials over K_0, of bounded degree. Let*

$$V = \{(x_1, \dots, x_r) \in \bar{K} : I \text{ vanishes on } (x_1, \dots, x_r)\},$$

where $\bar{K}$ is the algebraic closure of K. Suppose that for every j there exists $(x_1, \dots, x_r) \in V$ such that $W_j(x_1, \dots, x_r) \neq 0$. Suppose that there exists a nonsingular point $(a_1, \dots, a_r)$ on V which is rational over K. Then there exists a K-rational point $(b_1, \dots, b_r)$ on V such that $W_j(b_1, \dots, b_r) \neq 0$ for all $j \in \mathbb{N}$.

Proof. To simplify the argument we will suppose in case (1) that $K \subseteq \mathbb{C}$ and in case (2) that $K \subseteq \mathbb{R}$. This hypothesis can be eliminated by using the elementary equivalence of all algebraically closed fields of characteristic 0, and all real closed fields. We may suppose that

$$\det\left(\frac{\partial F_i}{\partial x_k}\right)_{\substack{i=1,\dots,h \\ k=d+1,\dots,r}} (a_1, \dots, a_r) \neq 0, \tag{1}$$

where $F_i \in I$, for $i = 1, \dots, h$ and where d is the Krull dimension of V and $h = r - d$.

We claim that there exists $\varepsilon \in \mathbb{R}$, $\varepsilon > 0$, such that for all $b_1, \dots, b_d \in K$, with $|a_k - b_k| < \varepsilon$ for $k = 1, \dots, d$, there exist $b_{d+1}, \dots, b_r \in K$ with $F_i(b_1, \dots, b_r) = 0$, for $i = 1, \dots, h$. [The absolute value $|\,|$ is the usual one in case (1) or (2) and the one associated to the valuation in case (3)]. Indeed, in case (1) or (2), the implicit function theorem implies that there exists $b_{d+1}, \dots, b_r \in \mathbb{C}$, respectively $\in \mathbb{R}$, with the required property. But this implies that we can find $b_{d+1}, \dots, b_r \in K$ with the required property. In case (3) we use the Hensel-Rychlik Lemma [10, Sect. 3] instead of the implicit function theorem. This finishes the proof of the claim. It is well known (see e.g. [19, p. 342]) that (1) implies $F_1, \dots, F_h$ generate the ideal I localised at $(x_1 - a_1, \dots, x_r - a_r)$. Hence, we conclude that if $(b_1, \dots, b_d) \in K$ is close enough to $(a_1, \dots, a_d)$, then there exist $b_{d+1}, \dots, b_r \in K$ such that $(b_1, \dots, b_r) \in V$. We have that

$$S_j \overset{\text{def}}{=} \{(x_1, \dots, x_d) \in \bar{K}^d : \exists x_{d+1}, \dots, x_r \in \bar{K}$$
$$(x_1, \dots, x_r) \in V \quad \text{and} \quad W_j(x_1, \dots, x_r) = 0\}$$

is a constructible set (in the sense of algebraic geometry). By looking at the explicit elimination procedure, and by the fact that the W_j have bounded degree, we see that there exists $D_0 \in \mathbb{N}$, such that all the S_j can be defined by polynomials of degree at most D_0, and with coefficients in K_0. Moreover, no S_j contains a non-empty Zariski-open subset of $\bar{K}^d$, because (since $W_j \notin I$) the Krull-dimension of the intersection of V with the zero set of W_j is at most $d - 1$.

Thus if $(b_1, \dots, b_r) \in V$, and if $W_j(b_1, \dots, b_r) = 0$, for some j, then there is a nontrivial polynomial over K_0, in d variables, of degree at most D_0, which vanishes on $(b_1, \dots, b_d)$. Since K satisfies (1), (2) or (3), it is easy to see that for every finitely generated subfield K_1 of K, there exists an element of K which is arbitrarily close to zero and which has degree larger than D_0 over K_1.

Let K_1 be the field generated by $a_1, \ldots, a_d$ over K_0. Then there exist $b_1, \ldots, b_d \in K$ which are arbitrary close to $a_1, \ldots, a_d$, and such that every field extension in the tower

$$K_1 \subset K_1(b_1) \subset K_1(b_1, b_2) \subset \ldots \subset K_1(b_1, \ldots, b_d) \tag{2}$$

has degree larger than D_0.

There exist $b_{d+1}, \ldots, b_r \in K$ such that $(b_1, \ldots, b_r) \in V$. If $W_j(b_1, \ldots, b_r) = 0$, for some j, then there is a nontrivial polynomial over K_1 of degree at most D_0 which vanishes on $(b_1, \ldots, b_d)$. But this would contradict (2).

Theorem 2.10 (Strong Approximation). *Let K be an algebraically closed or a real closed field, or a field which is Henselian with respect to a discrete valuation (e.g. $K = \mathbb{Q}_p$). Suppose that K has characteristic zero.*

Let

$$P_l(y_1, y_1', y_1'', \ldots, y_m, y_m', y_m'', \ldots),\ l = 1, 2, 3, \ldots$$

be differential polynomials in $y_1, \ldots, y_m$ over $K[[x]]$. Suppose that for every $n \in \mathbb{N}$ there exist $\bar{y}_1, \ldots, \bar{y}_m \in K[[x]]$ such that

$$P_l(\bar{y}_1, \bar{y}_1', \ldots, \bar{y}_m, \ldots) \equiv 0 \bmod x^n,$$

then there exist $\bar{\bar{y}}_1, \ldots, \bar{\bar{y}}_m \in K[[x]]$ such that

$$P_l(\bar{\bar{y}}_1, \bar{\bar{y}}_1', \ldots, \bar{\bar{y}}_m, \ldots) = 0,\ l = 1, 2, \ldots.$$

Proof. We use the ultraproduct construction, see [6, Sect. 1]. A (longer) proof without using the ultraproduct construction is implicit in the proof of Theorem 3.1. Let K^* be the ultraproduct $\left(\prod_{i \in \mathbb{N}} K\right)/D$ with respect to a nonprincipal ultrafilter D on $\mathbb{N}$. As in [6], there exist $\bar{y}_1, \ldots, \bar{y}_m \in K^*[[x]]$ such that

$$P_l(\bar{y}_1, \bar{y}_1', \ldots, \bar{y}_m, \bar{y}_m', \ldots) = 0,\ l = 1, 2, \ldots.$$

We now apply Theorem 2.7.

Remark 2.11. Theorem 2.10 for the case $K = \mathbb{C}$ is trivial, because $\mathbb{C}^* \cong \mathbb{C}$ over any countably generated subfield [6]. Thus when $K = \mathbb{C}$, Theorem 2.10 remains true for partial differential equations. However, when $K = \mathbb{R}$, Theorem 2.10 is not true for partial differential equations (see [5] or 4.10, below).

Remark 2.12. Theorem 2.10 is not true for all fields K. Indeed let $K = \mathbb{R}(t)$. In [9] it is shown that there exists a polynomial $P \in K[u, z_1, \ldots, z_r]$ such that for all $\alpha \in K$ we have

$$\alpha \in \mathbb{N} \leftrightarrow \exists z_1, \ldots, z_r \in K : P(\alpha, z_1, \ldots, z_r) = 0. \tag{1}$$

Consider the system of differential equations

$$xy' - (\alpha + x)y - 1 = 0,\ \alpha' = 0, \tag{2}$$

in the differential unknowns y and α.

The solutions of (2) in $K[[x]]$ are

$$y = \sum_{n=0}^{\infty} \frac{x^n}{(-\alpha)(1-\alpha)\ldots(n-\alpha)},\ \alpha \in K - \mathbb{N}.$$

Moreover, if $\alpha \in \mathbb{N}$ then (2) has no solution in $K[[x]]$, but it has a solution mod x^{α}. Thus the system

$$P(\alpha, z_1, \ldots, z_r) = 0,$$
$$\alpha' = 0, z_1' = 0, \ldots, z_r' = 0,$$
$$xy' - (\alpha + x)y - 1 = 0$$

in the differential indeterminates $y, \alpha, z_1, \ldots, z_r$ has no solution in $K[[x]]$, although it has for every n, a solution mod x^n. Q.E.D.

Recently Sibuya and Sperber [27] have shown that if $y = \sum a_n x^n$, with $a_n \in \bar{\mathbb{Q}}$ (the algebraic closure of $\mathbb{Q}$) is differentially algebraic then y has a positive v-adic radius of convergence for every non-archimedean valuation v of $\bar{\mathbb{Q}}$. Putting this together with our results we get

Theorem 2.13. *Let $\sum$ be a set of differential polynomials in $y_1, \ldots, y_m$ over $\mathbb{Q}(x)$. If $\sum = 0$ has a solution in $\mathbb{Q}_p[[x]]$, then it also has a solution in $\mathbb{Q}_p[[x]]$ which has a nonzero radius of convergence (with respect to the p-adic metric).*

Proof. Let K be the algebraic closure of $\mathbb{Q}$ in $\mathbb{Q}_p$. From Theorem 2.7 (and the remark following 2.7) it follows that $\sum = 0$ also has a solution in $K[[x]]$. From Theorem 2.1 it follows that $\sum = 0$ has a solution in $K[[x]]$ which is differentially algebraic over $K(x)$, and this solution is convergent by the result of [27].

Theorem 2.14 (Existence of an Approximation Function). *Let K be $\mathbb{C}$, $\mathbb{R}$ or $\mathbb{Q}_p$ and let $\sum$ be a set of differential polynomials in $y = (y_1, \ldots, y_m)$ over $K[[x]]$. For every $\alpha \in \mathbb{N}$ there exists $\beta(\alpha) \in \mathbb{N}$ with the following property: Let $\varepsilon \in \mathbb{R}$, $\varepsilon > 0$. If $\bar{y} = \sum_n \bar{a}_n x^n$ is a solution of $\sum \equiv 0 \bmod x^{\beta(\alpha)}$ then there exists a solution $y = \sum_n a_n x^n$ of $\sum = 0$ such that*

$$|a_n - \bar{a}_n| < \varepsilon \quad \textit{for} \quad n = 0, 1, \ldots, \alpha. \tag{1}$$

Proof. Suppose that the theorem is not true. Then there exists $\alpha \in \mathbb{N}$ with the following property: For every $\beta \in \mathbb{N}$ there exists $\varepsilon_\beta \in \mathbb{R}$, $\varepsilon_\beta > 0$ and a solution $\bar{y}_\beta = \sum_n \bar{a}_{n\beta} x^n$ of $\sum \equiv 0 \bmod x^\beta$ such that there is no solution $y = \sum_n a_n x^n$ of $\sum = 0$ with $|a_n - \bar{a}_{n\beta}| < \varepsilon_\beta$ for $n = 0, 1, \ldots, \alpha$. Let K^* be the ultraproduct $\left(\prod_{i \in \mathbb{N}} K\right)\Big/D$ with respect to a nonprincipal ultrafilter D on $\mathbb{N}$ (see [6, Sect. 1]). The sequence $(\bar{y}_\beta)_{\beta \in \mathbb{N}}$ determines a solution $\bar{y} = \sum_n \bar{a}_n x^n \in K^*[[x]]$ of $\sum = 0$, with $\bar{a}_n$ the equivalence class in K^* of the sequence $(\bar{a}_{n\beta})_{\beta \in \mathbb{N}}$. From Theorem 2.7, with $L = K^*$, it follows that there exists a solution $y = \sum_n a_n x^n \in K[[x]]$ of $\sum = 0$. However even more is true: We claim that there exists a $\beta \in \mathbb{N}$ such that for every $\varepsilon \in \mathbb{R}$, $\varepsilon > 0$ there exists a solution $y = \sum_n a_n x^n \in K[[x]]$ of $\sum = 0$ such that $|a_n - \bar{a}_{n\beta}| < \varepsilon$ for $n = 0, 1, \ldots, \alpha$. Notice that this contradicts our hypothesis. The proof of the claim is identical with the proof of Theorem 2.7 – we need only adapt Lemma 2.8 as follows: If in Lemma 2.8, $L = K^*$ and $c_1 = (c_{1\beta})_{\beta \in \mathbb{N}}, \ldots, c_r = (c_{r\beta})_{\beta \in \mathbb{N}}$ then there exists $\beta \in \mathbb{N}$ such that $b_1, \ldots, b_r$ can be taken arbitrarily close to $c_{1\beta}, \ldots, c_{r\beta}$. Indeed, in the proof of Lemma 2.8 we can take $a_1 = c_{1\beta}, \ldots, a_r = c_{r\beta}$ for a suitable $\beta \in \mathbb{N}$, and in Lemma 2.9 we can take $b_1, \ldots, b_r$ arbitrarily close to $a_1, \ldots, a_r$.

Remark 2.15. In Theorem 2.14 we cannot replace (1) by $a_n=\bar{a}_n$ for $n=0,1,\ldots,\alpha$. A counterexample follows from (2) in Remark 2.12.

3. Some Decision Problems

Theorem 3.1. *Let K be $\mathbb{C}$, $\mathbb{R}$ or $\mathbb{Q}_p$. There exists an algorithm for deciding whether a finite system of algebraic ordinary differential equations over $\mathbb{Q}[x]$ has a solution in $K[[x]]$. (An algebraic ordinary differential equation* (ADE) *over $\mathbb{Q}[x]$ is an equation $P=0$, where P is a differential polynomial in several variables over $\mathbb{Q}[x]$.)*

Proof. We give an algorithm such that given such a system $\sum$, we can compute a $\beta \in \mathbb{N}$ such that $\sum$ has a solution in $K[[x]]$ if and only if it has a solution $\bmod x^\beta$. We can consider this as a constructive proof of the Strong Approximation Theorem 2.10.

We first give an algorithm for systems $\sum$ of the following form (1)+(2)+(3)

$$\begin{cases} P_h(y_1,y_2,\ldots,y_h,y_1',\ldots,y_h^{(n_h)})=0 \\ P_{h+1}(y_1,y_2,\ldots,y_{h+1},y_1',\ldots,y_{h+1}^{(n_{h+1})})=0 \\ \quad\cdots \\ P_m(y_1,y_2,\ldots,y_m,y_1',\ldots,y_m^{(n_m)})=0 \end{cases} \tag{1}$$

and

$$\begin{cases} \operatorname{ord} H_1(y_1,\ldots,y_m,y_1',\ldots)\leqq k_1 \\ \quad\cdots \\ \operatorname{ord} H_s(y_1,\ldots,y_m,y_1',\ldots)\leqq k_s \end{cases} \tag{2}$$

and

$$\begin{cases} \text{a finite number of polynomial equations and inequations} \\ \text{over } \mathbb{Q} \text{ in the Taylor coefficients of } y_1,\ldots,y_m. \end{cases} \tag{3}$$

Here, the P_i are differential polynomials over $\mathbb{Q}[x]$ in $y_1,\ldots,y_i$ of order n_i in y_i (thus they form a *triangular* system), the H_i are differential polynomials over $\mathbb{Q}[x]$ *including* among others all the $\dfrac{\partial P_i}{\partial y_i^{(n_i)}}$, and the $k_1,\ldots,k_s$ are natural numbers. By ord we mean the discrete valuation on $K[[x]]$. By a solution of $\sum \bmod x^\beta$ we mean a solution in $K[[x]]$ of (2)+(3) which satisfies (1) $\bmod x^\beta$.

We will apply Lemma 2.3 to every P_i, with the y of Lemma 2.3 replaced by y_i. By running over a finite number of cases (i.e. by replacing $\sum$ by a disjunction of bigger $\sum$'s), we may suppose that for any P_i the numbers k and r in Lemma 2.3 are the same for every solution in $K[[x]]$ of (2)+(3). Let $\mathbf{t}$ be the vector whose components are the Taylor coefficients of $\bar{y}_1,\ldots,\bar{y}_m \in K[[x]]$. Let $I_i(q,\mathbf{t}) \in \mathbb{Q}[q,\mathbf{t}]$ be the polynomial (2) of Lemma 2.3, for $P=P_i$.

(i) From Lemma 2.3 it follows that for every $\gamma \in \mathbb{N}$ we can compute $\beta \in \mathbb{N}$ such that if $\bar{y}_1,\ldots,\bar{y}_m \in K[[x]]$ satisfy (1) $\bmod x^\beta$ and (2)+(3) and $\gamma > \max\{q \in \mathbb{N} : I_i(q,\mathbf{t})=0$ for some $i\}$ then (1)+(2)+(3) has a solution in $K[[x]]$. Start with $\gamma=0$.

(ii) Compute β for this value of γ as in (i). By running over a finite number of cases, we may suppose that $\sum \bmod x^\beta$ is equivalent to a finite system of polynomial equations $\sum_1$ and inequations $\sum_2$ over $\mathbb{Q}$ in the Taylor coefficients $\mathbf{t}$. (Only a finite number of components of $\mathbf{t}$ are involved.) We calculate the prime ideals of $\mathbb{Q}[\mathbf{t}]$ belonging to the ideal generated by the equations of $\sum_1$. By running over a finite number of cases we may suppose that $\sum_1$ is irreducible over $\mathbb{Q}$. Let $\bar{K}$ be the algebraic closure of K, and let

$$V=\{\mathbf{t}\in\bar{K}:\mathbf{t} \text{ satisfies } \textstyle\sum_1\}.$$

If V has no K-rational point, then $\sum$ has no solution $\operatorname{mod} x^\beta$, and β satisfies the requirement of the theorem.

Suppose that V has a K-rational point. We may suppose that there exists a nonsingular point on V which is rational over K. Indeed, otherwise we add the equations of the singular locus to $\sum_1$, and decompose the new system into irreducible components over $\mathbb{Q}$, and keep repeating this process, which has to eventually stop because the Krull dimension of V decreases at each stage. We may suppose that there is a K-rational point on V which satisfies all the inequations of $\sum_2$, because otherwise $\sum \operatorname{mod} x^\beta$ has no solution and this β works. Compute (by elimination theory over an algebraically closed field)

$$E\overset{\text{def}}{=}\{q\in\mathbb{N}:\exists i\forall\mathbf{t}\in V(I_i(q,\mathbf{t})=0)\}.$$

Notice that the number of elements of E is not larger than

$$\textstyle\sum_i (\text{degree of } I_i \text{ in } q). \tag{4}$$

If $\gamma\leqq\operatorname{Max}E$, then choose a new value for γ which is bigger than $\operatorname{Max}E$, and start all over again at step (ii). Thus we calculate a new β and get a new set E, which contains the previous E. Since the cardinality of E is bounded by (4) the process has to stop eventually, and we may suppose that

$$\gamma>\operatorname{Max}E. \tag{5}$$

We now claim that the β which is calculated from this γ by (i), satisfies the requirement of the Theorem. Indeed we will prove that, in this case, $\sum$ has a solution in $K[[x]]$. We know that V is irreducible over $\mathbb{Q}$, and that V has a K-rational nonsingular point. Moreover from (5) it follows that no inequality in the list $\sum_2$, $I_i(q,\mathbf{t})\neq 0$ for $q=\gamma,\ \gamma+1,\ \gamma+2,\dots$ is violated for every $\mathbf{t}\in V$. From Lemma 2.9 it now follows that there exists $\mathbf{t}\in K$ such that $\sum_1$ and $\sum_2$ are satisfied and such that

$$I_i(q,\mathbf{t})\neq 0,\quad \text{for}\quad q=\gamma,\gamma+1,\dots.$$

Thus (i) implies that $\sum$ has a solution in $K[[x]]$. This proves the Theorem for systems of the form (1)+(2)+(3). We shall now deal with the general case. (The remaining part of the proof can be considerably shortened by using the notion of characteristic set in Ritt [23, pp. 3–7]). We shall prove that given a system of ADE's $\sum$, in indeterminates $y_1,\dots,y_m$, and a system Π of conditions of the form $\operatorname{ord}H_i\leqq k_i$, $i=1,\dots,s$ where the H_i are differential polynomials in $y_1,\dots,y_m$ one can compute a $\beta\in\mathbb{N}$ such that the system $\sum$, Π has a solution if and only if it has a solution $\operatorname{mod} x^\beta$. We shall prove this by induction on the rank of $\sum$ defined below.

First we introduce some notation. Let $\sum^i$ be the set of polynomials in $\sum$ which involve only the indeterminates $y_1,\dots,y_i$ and which do not involve only $y_1,\dots,y_{i-1}$. We define the rank of a differential polynomial P in $\sum^i$ as $\operatorname{rk}(P)=(m,n)$

where m is the order of P in Y_i and n is the degree of P in $y_i^{(m)}$. We order the ranks lexicographically. This is a well ordering. (We shall use 0 to denote the rank $(0,0)$.) We define the rank of $\sum^i=\{P_1,\ldots,P_k\}$ with $\mathrm{rk}(P_j)\geqq\mathrm{rk}(P_{j+1})$ for $j=1,\ldots,k-1$ to be the sequence $(\mathrm{rk}(P_1),\mathrm{rk}(P_2),\ldots,\mathrm{rk}(P_k),0,0,\ldots)$ and we order these sequences lexicographically. Finally we define the rank of $\sum$, $\prod$ to be $\mathrm{rk}(\sum)=(\mathrm{rk}(\sum^m), \mathrm{rk}(\sum^{m-1}),\ldots,\mathrm{rk}(\sum^1))$. (We take the rank of an empty system to be $(0,0,\ldots)$). We order these sequences of length m lexicographically. It is not hard to see that the set of ranks is well ordered – we leave this to the reader. Now let $\sum$, Π be given and assume that we can compute β for all systems of lower rank. Let j be the largest value of i for which the following conditions do *not* hold: $\sum^i$ consists of at most one polynomial P_i (of rank (m,n) say) and $\mathrm{ord}\dfrac{\partial P_i}{\partial y_i^{(m)}}\leqq k$ occurs in Π for some $k\in\mathbb{N}$. If there is no such i, after a relabelling of the indeterminates we are in the special case treated above. Let P_j be a polynomial of lowest rank (m,n) in $\sum^j$ and consider 2 cases

(i) $\mathrm{ord}\,P'_j\leqq k$ does not occur in Π $\left(\text{where } P'_j=\dfrac{\partial P_j}{\partial y_j^{(m)}}\right)$

(ii) $\mathrm{ord}\,P'_j\leqq k$ does occur in Π and there is at least one other polynomial Q in $\sum^j$.

Case (i). Obtain $\sum_1$ from $\sum$ by replacing $P_j=0$ by $P_j-\dfrac{1}{n}y_j^{(m)}P'_j=0$ and adjoining $P'_j=0$. Here $\mathrm{rk}(P_j)=(m,n)$. Notice that $\mathrm{rk}(\sum_1)<\mathrm{rk}(\sum)$ and so we can compute β_1 for $\sum_1$, Π. Let $\Pi_2=\Pi\cup\{\mathrm{ord}\,P'_j<\beta_1\}$. Notice from the definition of β_1 that $\sum$, Π has a solution iff either $\sum_1$, Π or $\sum$, Π_2 has a solution. And for any $\gamma\geqq\beta_1$, if $\sum$, Π has a solution $\mathrm{mod}\,x^\gamma$, then either $\sum_1$, Π or $\sum$, Π_2 has a solution $\mathrm{mod}\,x^\gamma$. Hence if we could compute β_2 for $\sum$, Π_2 we could take $\beta=\max(\beta_1,\beta_2)$ and so it is sufficient to treat case (ii).

Case (ii). Let $P_j=\sum_{i=0}^{n} a_i y_j^{(m)^i}$ and $P'_j=\sum_{i=1}^{n} i a_i y_j^{(m)^{i-1}}$. Again we consider 2 cases: (a) ord $(a_n)\leqq k$ occurs in Π for some $k\in\mathbb{N}$ or (b) it does not.

Case (ii) (a). Let $\mathrm{rk}(Q)=(m',n')$. Then $m'>m$ or $m'=m$ and $n'\geqq n$. Let $Q=\sum_{i=0}^{n'} b_i y_j^{(m')^i}$. Recall that if $m'>m$ then $\dfrac{d^{m'-m}}{dx^{m'-m}}P_j=P'_j y_j^{(m')}+S$ where S has order $<m'$ in y_j. In this case let $T=(P'_j y_j^{(m')}+S)y^{(m')^{n'-1}}b_{n'}$. If $m'=m$ let $T=b_{n'}P_j y_j^{(m)^{n'-n}}$. Now obtain $\sum_3$ by replacing $Q=0$ in $\sum$ by $P'_jQ-T=0$ if $m'>m$, or by $a_nQ-T=0$ if $m'=m$. Notice that $\sum$, Π has a solution iff $\sum_3$, Π does, and for each γ if $\sum$, Π has a solution $\mathrm{mod}\,x^\gamma$, then $\sum_3$, Π has a solution $\mathrm{mod}\,x^{\gamma-m'+m}$. Also $\mathrm{rk}(\sum_3)<\mathrm{rk}(\sum)$, and so we are done by induction.

Case (ii) (b). Thus $\mathrm{ord}(a_n)\leqq k$ does not occur in Π. Let $\sum_4$ be $\sum$ with $P_j=0$ replaced by $P_j-a_n y_j^{(m)^n}=0$ and with $a_n=0$ adjoined. Notice that $\sum_4$ has lower rank and so we can compute β_4 for $\sum_4$, Π. Let $\Pi_5=\Pi\cup\{\mathrm{ord}(a_n)<\beta_4\}$. Then as above $\sum$, Π has a solution iff either $\sum_4$, Π or $\sum$, Π_5 does. And for any $\gamma\geqq\beta_4$, if $\sum$, Π has a solution $\mathrm{mod}\,x^\gamma$ so does either $\sum_4$, Π or $\sum$, Π_5. This completes the proof of Theorem 3.1.

Remark 3.2. (i) We have used the facts that we can decide whether a finite system of polynomial equations has a solution in $\mathbb{C}$, $\mathbb{R}$ or $\mathbb{Q}_p$. The first two are well known. The third follows from [4].

(ii) Theorem 3.1 remains true for differential equations over $K_0[x]$ if $K_0 \subset K$ is a computable field (i.e. a field in which $+$ and $\cdot$ are computable), for which there is an algorithm to test whether a polynomial in one variable over K_0 is irreducible (this implies that we can compute the prime ideals belonging to our ideal), and for which $\mathbb{N}$ is a computable subset of K_0.

(iii) If we replace K in Theorem 3.1 by any Henselian discrete valuation field of characteristic zero then it remains true that we can compute β.

(iv) If one were just interested in the existence of an algorithm to decide if systems of ADE's have power series solutions one could proceed as follows. Use Lemma 2.3 and some elimination theory to put a recursive structure on the ring of differentially algebraic power series over $k[x]$, where k is the algebraic closure of $\mathbb{Q}$ in K. We know from Theorems 2.1 and 2.7 that if a system $\sum = 0$ has a solution in $K[[x]]$ then it has a differentially algebraic solution in $k[[x]]$. On the other hand if $\sum = 0$ has no solution in $K[[x]]$, then, by Theorem 2.10, $\sum = 0 \bmod x^n$ has no solution for some n. Hence to check if $\sum = 0$ has a solution or not, one could search for a differentially algebraic solution in $k[[x]]$ (using the above mentioned recursive structure) and at the same time check whether $\sum = 0$ has a solution $\bmod x^n$ for $n = 1, 2, \ldots$.

(v) *Identity problems.* Let K_0 be a field satisfying the conditions of Remark 3.2(ii) above (e.g. $\mathbb{Q}$ or $\bar{\mathbb{Q}}$) and let $f_1, \ldots, f_n \in K_0[[x]]$ be differentially algebraic. We consider terms $T(z_1, \ldots, z_r)$ built up from elements of K_0, variables $z_1, z_2, \ldots$, $+$, $-$, $\cdot$ and $f_1, \ldots, f_n$ where compositions $f(g)$ are only allowed when $g \in (z_1, z_2, \ldots) K_0[[z_1, z_2, \ldots]]$, (identifying a term with its Taylor series. Notice that the Taylor series of any such term is computable.) There is an algorithm for deciding if $T \equiv 0$ (as an element of $K_0[[z_1, z_2, \ldots]]$.)

This can be proved as follows. First reduce to the one variable case by replacing z_i by $t_i x$ where the t_i are algebraically independent over K_0 (so K_0 is replaced by $K = K_0(t_1, t_2, \ldots)$). With each term $T = \bar{y} \in K[[x]]$ associate a system of ADE's $\sum_T(y_1, \ldots, y_{n_T})$ which has a unique solution $\bar{y}_1, \ldots, \bar{y}_{n_T} \in K[[x]]$ and $\bar{y}_{n_T} = \bar{y}$. To test if $T \equiv 0$ apply the above algorithm to the system $\sum_T \cup \{y_{n_T} = 0\}$. We shall publish a more detailed account of this application elsewhere.

Corollary to Theorem 3.1. *There exists an algorithm for deciding whether a system of* ADE's *over* $\mathbb{Q}[x]$ *has a* C^∞ *solution near* $x = 0$.

Proof. This follows easily from Theorems 3.1 and 10.1 of [17].

Part (i) of the following theorem appears in Singer [28]. We include it for completeness.

Proposition 3.3. (i) *There is no algorithm to decide whether a finite system of* ADE's *over* $\mathbb{Q}[x]$ *has a solution in* $\mathbb{C}[[x]]$ *with* $y_1 \neq 0$.

(ii) *There is no algorithm to decide whether a finite system of* ADE's *over* $\mathbb{Q}[x]$ *has a convergent solution in* $\mathbb{C}[[x]]$ *(or* $\mathbb{R}[[x]]$*. The corresponding problem for* $\mathbb{Q}_p[[x]]$ *is decidable – cf. Theorems 2.13 and 3.1).*

Proof. (i) Consider the system

$$xy' = \alpha y, \ \alpha' = 0, \ y \neq 0$$

in the differential indeterminates y and α. Notice that the solutions of this system are $y = ax^{\alpha}$, $a \neq 0$ and hence this system has a solution $y \in \mathbb{C}[[x]]$ if and only if $\alpha \in \mathbb{N}$. Hence the question of the solubility of any diophantine equation in $\mathbb{N}$ can be reduced to a question of the solubility of a system of ADE's, together with some inequalities $y_i \neq 0$, in $\mathbb{C}[[x]]$.

(ii) Consider the system

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

in the differential indeterminates y and α. In $\mathbb{C}[[x]]$ it has the solutions $\alpha \in \mathbb{C}$, $y = \sum_{n=0}^{\infty} (1-\alpha)(2-\alpha)\ldots(n-\alpha)x^n$ which converges iff $\alpha \in \mathbb{N}$, in which case y is a polynomial. Hence again any diophantine problem can be reduced to the question of whether a system of ADE's has a convergent solution.

Remarks 3.4. (1) Theorem 3.3(i) shows that there is no algorithm for deciding whether systems of ADE's have solutions in $\mathbb{C}((x))$.

(2) If in the proof of Theorem 3.3(ii) we use an ADE whose solutions are $y = \sum \frac{(1-\alpha)(2-\alpha)\ldots(n-\alpha)}{n!} x^n$ we can conclude that the problem of determining whether systems of ADE's have entire solutions, given that they have convergent solutions, is also undecidable.

(3) The model theory of differentially closed fields has been extensively studied, see for example Robinson [24], Blum [8], Wood [29], and Singer [28]. It is for example well known that the theory of differentially closed fields of characteristic 0 is decidable.

4. Computable Power Series and Partial Differential Equations

The fact that a power series $\sum_n a_n x^n$, $a_n \in \mathbb{Q}$ satisfies a nontrivial ADE implies strict conditions on the growth of the a_n's and denominators of the a_n's [15, 16, 20]. It seems natural to ask whether any analogous results hold for power series in several variables satisfying systems of partial differential equations. Since every power series f in x_2 satisfies $\frac{\partial f}{\partial x_1} = 0$, and since whenever a power series, g, in one variable satisfies an ADE there is a system of ADE's which has g as part of its unique power series solution, one is led to ask what power series (in several variables) can occur in the unique solutions in $\mathbb{C}[[x_1, \ldots, x_n]]$ of systems of algebraic partial differential equations (see below). This question is answered in Theorems 4.1 and 4.2 below. Analogous results do not hold for $\mathbb{R}$ in place of $\mathbb{C}$ (Cor. 4.8). In this section we also establish some undecidability results for linear PDE's (Theorem 4.11) and some definability results for systems of linear PDE's (Theorem 4.13).

Let $x=(x_1,\ldots,x_n)$, $y=(y_1,\ldots,y_m)$ be several variables. A system of algebraic partial differential equations (SPDE) is a system of equations of the form

$$F_l\left(x,y,\ldots\frac{\partial^{i_1+i_2+\cdots}y_j}{\partial x_1^{i_1}\partial x_2^{i_2}\ldots},\ldots\right)=0,\quad l=1,\ldots,r,$$

where the F_l are polynomials over $\mathbb{Q}$.

Theorem 4.1. *If a* SPDE *has a unique solution* y *in* $\mathbb{C}[[x]]$, *then* $y\in\mathbb{Q}[[x]]$ *and the* y_j *are computable power series [i.e. the map* $i\to i^{\text{th}}$ *coefficient of* y_j *(*i *a multi index) is computable as a map between the recursive structures* $\mathbb{N}$ *and* $\mathbb{Q}$*].*

Proof. Let S be a SPDE and let $a\in\mathbb{C}$. We know from Remark 2.11 that if for all $n\in\mathbb{N}$ S has a solution mod$(x)^n$ with the i^{th} coefficient of y_j equal to a then S has a solution with the i^{th} coefficient of y_j equal to a. Now let $y\in\mathbb{C}[[x]]$ be the unique solution of the SPDE S. If $y_j\notin\mathbb{Q}[[x]]$, then there is an automorphism of $\mathbb{C}$ which moves y_j, contradicting the uniqueness. Fix multi-index i and $j\in\mathbb{N}$. We shall show how to compute a_{ij}, the i^{th} coefficient of y_j. Let

$$S_n=\{a\in\mathbb{C}:\exists y\in\mathbb{C}[[x]] \text{ such that } y \text{ is a solution of } S\,\mathrm{mod}(x)^n \text{ and } a \text{ is the } i^{\text{th}} \text{ coefficient of } y_j\}.$$

By elimination theory over $\mathbb{C}$ it follows that each S_n is finite or cofinite. From the above we know that $\bigcap_{n\in\mathbb{N}} S_n=\{a_{ij}\}$. Now, since $\mathbb{C}$ is uncountable, the intersection of countably many cofinite sets is infinite. Thus there exists an $n_0\in\mathbb{N}$ with S_{n_0} a singleton. By elimination theory over $\mathbb{C}$ we can decide for a given n whether S_n is a singleton. Thus we can compute n_0 and we can find an element of S_{n_0}. This element is equal to a_{ij}.

Remark. We call a power series computable if its coefficients belong to $\mathbb{Q}$ and form a computable sequence of rationals. (This is different from a computable sequence of computable reals [21].)

Theorem 4.2. *If* $y_1=\sum_{i\in\mathbb{N}}a_ix_1^i\in\mathbb{Q}[[x_1]]$ *is a computable power series, then there exist* $y_2,\ldots,y_m\in\mathbb{Q}[[x_1,\ldots,x_n]]$ *(*n, m *large enough) such that* $y=(y_1,\ldots,y_m)$ *is the unique solution in* $\mathbb{C}[[x]]$ *of some* SPDE.

Definition. Let $R(f_1,\ldots,f_l)$ be a relation between $f_1,\ldots,f_l\in k[[x]]$. We say that R is *strongly existentially definable (s.e. definable)* over k if there exists $x'=(x'_1,\ldots,x'_{n'})$ and a SPDE $S(y_1,\ldots,y_l,\,y_{l+1},\ldots,y_m)$ such that in $k[[x,x']]$

$$\begin{aligned}R(f_1,\ldots,f_l)&\Leftrightarrow\exists y_{l+1}\ldots y_m\in k[[x,x']]:S(f_1,\ldots,f_l,y_{l+1},\ldots,y_m)\\&\Leftrightarrow\exists!\,y_{l+1}\ldots y_m\in k[[x,x']]:S(f_1,\ldots,f_l,y_{l+1},\ldots,y_m)\,.\end{aligned}$$

Lemma 4.3 (Definability of Composition). *Let* $p(x)\in\mathbb{Q}[x]$ *be fixed, with no constant term. The relation between* $f,g\in k[[x,z_1]]$ *given by*

$$g=f(x,p(x))$$

is s.e. definable.

Proof. Indeed $g=f(x,p(x)) \Leftrightarrow \left(\frac{\partial g}{\partial z_1}=0 \text{ and } g\equiv f \bmod (p(x)-z_1)\right)$. If $g=f(x,p(x))$ then $g=f(x,z_1+(p(x)-z_1))\equiv f(x,z_1) \bmod p(x)-z_1$, and if the righthand side is satisfied, just put $z_1=p(x)$.

Lemma 4.4. *The relation between $f(z,x)$, $g(z,x)$, $h(z,x)\in k[[z,x]]$ given by*

$$\text{if} \quad f(z,x)=\sum_i f_i(z)x^i$$

$$g(z,x)=\sum_i g_i(z)x^i$$

then

$$h(z,x)=\sum_i f_i(z)g_i(z)x^i \qquad (i \text{ multi-index})$$

is s.e. definable.

Proof. Let $\bar{x}=(\bar{x}_1,\ldots,\bar{x}_n)$ be new variables. We use the following notation:

$$x\bar{x}=x_1\bar{x}_1, x_2\bar{x}_2, \ldots, x_n\bar{x}_n$$

$$(x\bar{x})^i=(x_1\bar{x}_1)^{i_1}(x_2\bar{x}_2)^{i_2}\ldots(x_n\bar{x}_n)^{i_n}, \quad \text{for} \quad i=(i_1,\ldots,i_n) \quad \text{a multi-index}.$$

We have

$$f(z,x)g(z,\bar{x})=\sum_{i,j} f_i(z)g_j(z)x^i\bar{x}^j \qquad i,j \text{ multi indices}$$

$$=\sum_i f_i(z)g_i(z)(x\bar{x})^i+\sum_{u=\{u_1,\ldots,u_k\}\subset(x,\bar{x})} u_1u_2\ldots u_k\sum_{i,l} q_{il}(z)u^l(x\bar{x})^i$$

$$l \text{ multi index}$$

where we sum over all $u=\{u_1,\ldots,u_k\}\subset(x_1,x_2,\ldots,x_n,\bar{x}_1,\ldots,\bar{x}_n)$, $(k\leqq n)$, satisfying

(I) $u\neq\emptyset$ and not both $x_j,\bar{x}_j$ belong to u $(j=1,\ldots,n)$. This representation is unique for the following reason: the multi degrees of the terms in the series belonging to one u are all different from these belonging to another u. Indeed, if $u\neq u'$, then e.g. $x_e\in u$ and $x_e\notin u'$. Suppose now that $x_1^{i_1}\ldots x_e^{i_e}\ldots x_n^{i_n}\bar{x}_1^{j_1}\ldots\bar{x}_e^{j_e}\ldots\bar{x}_n^{j_n}$ has nonzero coefficient in both the series belonging to u and to u'. Since $x_e\in u$ we have $i_e>j_e$, and since $x_e\notin u'$ we have also $i_e\leqq j_e$, but this is a contradiction.

Let $w_1,\ldots,w_n$ be new variables. Thus there exist *unique* $q_u(z,u,w)\in k[[z,u,w]]$ (u ranging over all $u\subset(x,\bar{x})$ satisfying (I)) such that

$$f(z,x)g(z,\bar{x})=h(z,x\bar{x})+\sum_{u\subset(x,\bar{x})} u_1u_2\ldots u_kq_u(z,u,x\bar{x}).$$

The condition $q_u(z,u,w)\in k[[z,u,w]]$ can be expressed by putting some partial derivatives equal to zero. The proof follows now from Lemma 4.3.

Definition. Let $f\in k[[x]]$. We say that f is s.e. definable (over k) if the set $\{f\}$ is s.e. definable.

Lemma 4.5. *Let $p(x)\in\mathbb{Q}[x]$ be a fixed polynomial. Then the power series $\sum_i p(i)x^i$ (i multi index) is s.e. definable (over any k).*

Proof. It is sufficient to prove Lemma 3 for $p(x)=x_1^{j_1}x_2^{j_2}\ldots x_n^{j_n}$ a monomial. We have

$$x_1(1-x_1)^{-2}=\sum_{i_1} i_1x_1^{i_1}, \qquad (1-x_1)^{-1}=\sum_{i_1} x_1^{i_1}.$$

Thus from Lemma 4.4 it follows that

$$\sum_{i_1} i_1^{j_1} x_1^{i_1}, \ldots, \sum_{i_n} i_n^{j_n} x_n^{i_n}$$

are s.e. definable. Moreover

$$\sum_{i_1,\ldots,i_n} i_1^{j_1}\ldots i_n^{j_n} x_1^{i_1}\ldots x_n^{i_n} = \Big(\sum_{i_1} i_1^{j_1} x_1^{j_1}\Big)\Big(\sum_{i_2} i_2^{j_2} x_2^{j_2}\Big)\cdots\Big(\sum_{i_n} i_n^{j_n} x_n^{j_n}\Big)$$

Lemma 4.6. *If* $\sum_i a_i x^i \in k[[x]]$ *is s.e. definable, and if*

$$\begin{aligned} b_i &= 1 \quad \text{if} \quad a_i = 0 \\ b_i &= 0 \quad \text{if} \quad a_i \neq 0, \qquad (i \text{ multi index}) \end{aligned} \tag{1}$$

then $\sum_i b_i x^i$ *is s.e. definable (over k).*

Proof. We have

$$\forall i[b_i \text{ satisfies (1)] if and only if}$$

$$\forall i[(b_i = 0 \quad \text{or} \quad b_i = 1)] \text{ and} \tag{2}$$

$$\forall i \exists c_i, d_i \in k[(1-b_i) = a_i c_i \quad \text{and} \quad a_i = (1-b_i)d_i]. \tag{3}$$

Condition (2) can be s.e. defined by

$$\sum b_i^2 x^i = \sum b_i x^i,$$

which is definable by Lemma 4.4.

Condition (3) can be s.e. defined by

$$\exists(\sum c_i x^i)\exists(\sum d_i x^i)[\sum x^i - \sum b_i x^i = \sum a_i c_i x^i \quad \text{and} \quad \sum a_i x^i = \sum d_i x^i - \sum b_i d_i x^i]$$

which can be s.e. defined by Lemma 4.4.

The only remaining problem is that c_i and d_i are not unique when $a_i = 0$ and $b_i = 1$. The uniqueness is restored if we add

$$\forall i[(b_i c_i = b_i \quad \text{and} \quad b_i d_i = b_i)] \tag{4}$$

Theorem 4.2′. *Let* $\alpha : A \subset \mathbb{N}^n \to \mathbb{N}$ *be a partial recursive function*[1]. *Then, the set*

$$S = \Big\{\sum_i a_i x^i \in k[[x]] : a_i = \alpha(i) \quad \text{if} \quad i \in A\Big\} \qquad (i \text{ a multi index})$$

is s.e. definable over k.

Proof. From Matijasevič's theorem, [18], it follows that there exists a polynomial $p(x,t,u) \in \mathbb{Z}[x,t,u]$ $(x = (x_1, \ldots, x_n)$, t one variable, and u several variables) such that

$$(i \in A \quad \text{and} \quad j = \alpha(i)) \Leftrightarrow \exists l \in \mathbb{N} : p(i,j,l) = 0$$
$$(l \text{ a multi-index}, j \text{ one index})$$

---

1 A partial recursive function is a computable function from a recursive enumerable subset A of $\mathbb{N}^n$ to $\mathbb{N}$. A recursively enumerable subset is a subset whose members can be enumerated by an algorithm

From Lemma 4.5 it follows that

$$\sum_{i,j,l} p(i,j,l)u^l t^j x^i$$

is s.e. definable.

From Lemma 4.6 it follows that the power series

$$g \stackrel{\text{def}}{=} \sum_{\substack{i,j,l \\ p(i,j,l)=0}} u^l t^j x^i$$

is s.e. definable. Since α is a function on A, we have

$$g = \sum_i (g_i(u)t^{\alpha(i)})x^i ,$$

with $g_i(u) \in \mathbb{N}[[u]]$, and

$$g_i(u) \neq 0 \Leftrightarrow i \in A .$$

We have now, $\sum_i a_i x^i \in S$ if and only if

$$t\frac{\partial g}{\partial t} = \sum_i a_i(g_i(u)t^{\alpha(i)})x^i .$$

But the right side of the last equation is s.e. definable by Lemma 4.4.

Proof of Theorem 4.2. Trivially from Theorem 4.2′.

Corollary 4.7. *There exists a* SPDE *having a solution in* $\mathbb{C}[[x]]$, *but no solution in* $\bar{\mathbb{Q}}[[x]]$. *($\bar{\mathbb{Q}}$ is the algebraic closure of $\mathbb{Q}$.)*

Proof. Let $i \to P_i(x_2, x_3)$ be a computable enumeration of all homogeneous non-zero polynomials over $\mathbb{Z}$. For $a \in \mathbb{C}$ we have

$$\begin{aligned} a \notin \bar{\mathbb{Q}} &\Leftrightarrow \forall i P_i(x_2, ax_2) \neq 0 \\ &\Leftrightarrow \exists (\textstyle\sum b_i x_1^i \in \mathbb{C}[[x_1]]): \\ &\textstyle\sum_i b_i P_i(x_2, ax_2)x_1^i = \sum_i x_2^{\deg P_i} x_1^i . \end{aligned} \tag{1}$$

From Theorem 4.2′ it follows that $\sum_i P_i(x_2, x_3)x_1^i$ and $\sum_i x_2^{\deg P_i} x_1^i$ are s.e. definable. From the proof of Lemma 4.3 we obtain that $\sum_i P_i(x_2, ax_2)x_1^i$ is s.e. definable. From Lemma 4.4 it now follows that the right side of (1) is s.e. definable.

Corollary 4.8. *There exists a* SPDE *which has a unique solution y in* $\mathbb{R}[[x]]$, *and such that $y_1 \in \mathbb{Q}[[x]]$ and y_1 is not computable.*

Proof. Let $A \subset \mathbb{N}$ be a recursively enumerable non-recursive set, enumerated by a Turing machine M.

For $i, j \in \mathbb{N}$, let

$$\begin{aligned} \alpha(i,j) &= 1 \quad \text{if } j \text{ has already appeared at time } i \text{ in the output of } M \\ &= 0 \quad \text{otherwise.} \end{aligned}$$

Thus $\alpha(i,j)$ is a computable function, and

$$a_{ij} \overset{\text{def}}{=} \sum_{k=1}^{i} \alpha(k,j)\,10^{-k}$$

is a computable sequence of rational numbers.

However the sequence of rational numbers

$$b_j \overset{\text{def}}{=} \sum_{k=1}^{\infty} \alpha(k,j)\,10^{-k}$$

is *not* computable, because

$$b_j = 0 \quad \text{if} \quad j \notin A$$
$$(b_j \neq 0 \quad \text{and} \quad b_j \in \mathbb{Q}) \quad \text{if} \quad j \in A .$$

(Notice that $0{,}11111\ldots = 1/9$.)

We have

$$b_j - \frac{1}{10^i} \leqq a_{ij} \leqq b_j ,$$

and these relations completely determine the b_j.

Moreover, from Theorem 4.2 it follows that $\sum_{ij} a_{ij} x_1^i x_2^j$ is s.e. definable. Considering the power series

$$\left(\sum_j b_j x_2^j\right)\left(\sum_i x_1^i\right) = \sum_{ij} b_j x_1^i x_2^j , \quad \text{and} \quad \sum_{ij} \frac{1}{10^i} x_1^i x_2^j ,$$

and using Lemma 4.9 below, we obtain that $\sum_j b_j x_2^j$ is a s.e. definable power series over $\mathbb{R}$.

Lemma 4.9. *The set*

$$S = \left\{\sum_i c_i x^i \in \mathbb{R}[[x]] : c_i \geqq 0, \forall i\right\}, \qquad (i \text{ multi-index})$$

is s.e. definable over $\mathbb{R}$.

Proof. We have

$$\begin{aligned} c_i \geqq 0, \forall i &\Leftrightarrow \exists c_{ij} \in \mathbb{R} : (c_i = c_{i,0}^2 \quad \text{and} \quad c_{i,j} = c_{i,j+1}^2) \ \ j \textit{ one } \text{index} \\ &\Leftrightarrow \exists \sum_{i,j} c_{i,j} x^i t_1^j \in \mathbb{R}[[x, t_1]] : \\ &\sum_i c_i x^i + t_1 \sum_{i,j} c_{i,j} x^i t_1^j = \sum_{i,j} c_{i,j}^2 x^i t_1^j . \end{aligned} \tag{1}$$

The right hand side of (1) is s.e. definable by Lemma 4.4.

Remark. The sequence b_j in the proof of Corollary 4.9 is still a computable sequence of computable reals. However, by applying Lemma 4.6 we obtain a s.e. definable sequence of rationals (over $\mathbb{R}$) which is not a computable sequence of computable reals.

Corollary 4.10. *There is a* SPDE *which has a solution in* $\mathbb{R}[[x_1, \ldots, x_n]] \bmod (x_1, \ldots, x_n)^\alpha$ *for all* $\alpha \in \mathbb{N}$, *but has no solution in* $\mathbb{R}[[x_1, \ldots, x_n]]$.

Proof. The condition on $c \in \mathbb{R}$ and $y = \sum a_i x^i$ that $\sum (c-i)x^i = \sum a_i^2 x^i$ is s.e. definable by a SPDE. This SPDE satisfies the Corollary.

Remark. A result equivalent to Cor. 4.10 appears in [5].

We shall now establish some results for linear PDE's and systems of linear PDE's. Let $P(m_1, \ldots, m_r) \in \mathbb{Z}[m_1, \ldots, m_r]$ and let

$$y = \sum_{m_1, \ldots, m_r} c_{m_1, \ldots, m_r} x_1^{m_1} x_2^{m_2} \ldots x_r^{m_r}, \quad c_{m_1, \ldots, m_r} \in \mathbb{C}.$$

Then

$$P\left(x_1 \frac{\partial}{\partial x_1}, \ldots, x_r \frac{\partial}{\partial x_r}\right) y = \sum_{m_1, \ldots, m_r} c_{m_1, \ldots, m_r} P(m_1, \ldots, m_r) x_1^{m_1} \ldots x_r^{m_r}.$$

Hence $P(m_1, \ldots, m_r) = 0$ has *no* nonnegative integer solutions if and only if the linear PDE

$$P\left(x_1 \frac{\partial}{\partial x_1}, \ldots, x_r \frac{\partial}{\partial x_r}\right) y = \sum_{m_1, \ldots, m_r} x_1^{m_1} \ldots x_r^{m_r} = \left(\frac{1}{1-x_1}\right)\left(\frac{1}{1-x_2}\right) \ldots \left(\frac{1}{1-x_r}\right)$$

has a power series solution (which if it exists is convergent) in $\mathbb{C}[[x_1, \ldots, x_r]]$. Thus from the undecidability of Hilbert's Tenth Problem [18] we have

Theorem 4.11. *There does not exist an algorithm to decide whether a linear* PDE *has a power series solution in* $\mathbb{C}[[x_1, \ldots, x_r]]$ *(for r large enough, say* $\geqq 9$*).*

Next consider the equation

$$P\left(x_1 \frac{\partial}{\partial x_1}, \ldots, x_r \frac{\partial}{\partial x_r}\right) y = \left(\frac{1}{1-x_1}\right) \ldots \left(\frac{1}{1-x_{r-1}}\right)\left(\sum_{n=0}^{\infty} \lambda_n x_r^n\right)$$
$$= \sum_{m_1, \ldots, m_r} \lambda_{m_r} x_1^{m_1} \ldots x_r^{m_r}. \tag{1}$$

We see that (1) has a power series solution y if and only if

$$n \in V \stackrel{\text{def}}{=} \{m_r \in \mathbb{N} : \exists m_1, \ldots, m_{r-1} \quad P(m_1, \ldots, m_r) = 0\} \Rightarrow \lambda_n = 0. \tag{2}$$

Notice that V can be any recursively enumerable set [18].

Theorem 4.12. *There exists a system of linear* PDE's, *having a power series solution over* $\mathbb{Q}$, *but no computable power series solution.*

Proof. Let $V_1, V_2 \subseteqq \mathbb{N}$ be two recursively enumerable, recursively inseparable sets. Let P_i, $i = 1, 2$ be polynomials such that

$$V_i = \{m_r \in \mathbb{N} : \exists m_1, \ldots, m_{r-1} \quad (P_i(m_1, \ldots, m_r) = 0)\}.$$

Consider the following system $\sum$ (in the unknowns y_1, y_2, u)

$$P_1\left(x_1 \frac{\partial}{\partial x_1}, \ldots, x_r \frac{\partial}{\partial x_r}\right) y_1 = \left(\frac{1}{1-x_1}\right) \ldots \left(\frac{1}{1-x_{r-1}}\right) u$$

$$P_2\left(x_1\frac{\partial}{\partial x_1},\dots,x_r\frac{\partial}{\partial x_r}\right)y_2=\left(\frac{1}{1-x_1}\right)\dots\left(\frac{1}{1-x_{r-1}}\right)\left(u-\frac{1}{1-x_r}\right)$$

$$\frac{\partial u}{\partial x_1}=0,\frac{\partial u}{\partial x_2}=0,\dots,\frac{\partial u}{\partial x_{r-1}}=0.$$

If $\sum$ has a power series solution y_1, y_2, u then $u=\sum_{n=0}^{\infty}\lambda_n x_r^n$ with $n\in V_1 \Rightarrow \lambda_n=0$ and $n\in V_2 \Rightarrow \lambda_n=1$. Conversely for every such u there exist power series y_1 and y_2 satisfying $\sum$. (Hence $\sum$ has uncountably many solutions over $\mathbb{Q}$.) $\sum$ can have no computable power series solution $u=\sum\lambda_n x_r^n$ because then $\{n\in\mathbb{N}:\lambda_n=0\}$ would be a recursive separation of V_1 and V_2.

Now let $V\subseteq\mathbb{N}$ be a recursive set. Applying the above construction to $V_1=\mathbb{N}-V$, $V_2=V$, we see that there is a system $\sum$ of linear PDE's in the unknowns y_1, y_2, u such that if $\bar{y}_1$, $\bar{y}_2$, $\bar{u}$ is a power series solution of $\sum$ then $\bar{u}=\sum\chi_V(n)x_r^n$, where χ_V is the characteristic function of V. Conversely if $\bar{u}=\sum\chi_V(n)x_r^n$ then there exist $\bar{y}_1$ and $\bar{y}_2$ such that $\bar{y}_1$, $\bar{y}_2$, $\bar{u}$ satisfy $\sum$. Repeating the above argument for two variables x_1, x_2 instead of x_r, we see that for every computable function $f:\mathbb{N}\to\mathbb{N}$ there is a system $\sum$ of linear PDE's in the unknowns y_1, y_2, u such that $\sum$ has a power series solution y_1, y_2 if and only if $u=\sum_n x_1^n x_2^{f(n)}$.

Theorem 4.13. *Let $f:\mathbb{N}\to\mathbb{N}$ be a computable function. Then there exists a system $\sum$ of linear partial differential equations over $\mathbb{Q}[x_1,\dots,x_r]$ in the unknowns $u, y_1, y_2,\dots$ such that $\sum$ has a power series solution $y_1, y_2,\dots$ if and only if $u=\sum_n f(n)x_1^n$.*

Proof. If there is such a system for $u=\sum c_{m_1,\dots,m_r}x_1^{m_1}\dots x_r^{m_r}$ we shall say that u is definable by LPDE's. We have already observed that $\sum_n x_1^n x_2^{f(n)}$ is definable by LPDE. By applying $x_2\frac{\partial}{\partial x_2}$, we see that $\sum_n f(n)x_1^n x_2^{f(n)}$ is definable by LPDE's. Let $u=\sum_n a_n x_1^n$ $\left(\text{i.e. } \frac{\partial u}{\partial x_2}=0,\dots,\frac{\partial u}{\partial x_r}=0\right)$. Then $\left(\frac{1}{1-x_2}\right)u=\sum_{m,n}a_n x_1^n x_2^m$. Consider

$$\left(\frac{1}{1-x_2}\right)u-\sum f(n)x_1^n x_2^{f(n)}. \tag{3}$$

If for all n, the coefficient of $x_1^n x_2^{f(n)}$ in (3) is zero then $u=\sum_n f(n)x_1^n$, and conversely. Now this last condition can be imposed by an equation similar to (1) above.

Question. Does Proposition 4.13 remain valid if we ask that $\sum$ have a *unique* solution $y_1, y_2, \dots$?

Acknowledgements. We would like to thank B. Dwork and M. Singer for stimulating conversations on the subject of algebraic differential equations, M. Gromov for stimulating conversations which suggested the investigation in Sect. 4, and S. Kochen for encouraging us to work out the explicit algorithm given in Sect. 3.

References

1. Aberth, O.: The failure in computable analysis of a classical existence theorem for differential equations. Proc. AMS **30**, 151–156 (1971)
2. Artin, M.: On the solutions of analytic equations. Invent. Math. **5**, 277–291 (1968)
3. Artin, M.: Algebraic approximation of structures over complete local rings. Publ. Math. I.H.E.S. **36**, 23–58 (1969)
4. Ax, J., Kochen, S.: Diophantine problems over local fields III. Ann. Math. **83**, 437–456 (1966)
5. Becker, J., Denef, J., Lipshitz, L.: Further remarks on the elementary theory of formal power series rings. In: Model theory of algebra and arithmetic. Proceedings Karpacz, Poland (1979). Lecture Notes in Mathematics, Vol. 834. Berlin, Heidelberg, New York: Springer 1979
6. Becker, J., Denef, J., Lipshitz, L., van den Dries, L.: Ultraproducts and approximation in local rings I. Invent. Math. **51**, 189–203 (1979)
7. Birch, B.J., McCann, K.: A criterion for the p-adic solubility of Diophantine equations. Quart. J. Math. Oxford **18**, 54–63 (1967)
8. Blum, L.: Ph. D. Thesis, M.I.T. (1968)
9. Denef, J.: The diophantine problem for polynomial rings and fields of rational functions. Trans. A.M.S. **242**, 391–399 (1978)
10. Denef, J., Lipshitz, L.: Ultraproducts and approximation in local rings II. Math. Ann. **253**, 1–28 (1980)
11. Greenberg, M.: Rational points in henselian discrete valuation rings. Publ. Math. I.H.E.S. **31**, 59–64 (1966)
12. Hurwitz, A.: Sur le développement des fonctions satisfaisant à une équation différentielle algébrique. Ann. Ecole Norm. Sup. **6**, 327–332 (1889)
13. Kaplansky, I.: An introduction to differential algebra. Actualités Scientifiques et Industrielles No. 1251. Paris: Hermann 1957
14. Lang, S.: Algebra. New York: Addison Wesley 1965
15. Mahler, K.: Lectures on transcendental numbers. Lecture notes in Mathematics, Vol. 546. Berlin, Heidelberg, New York: Springer 1976
16. Maillet, E.: Sur les series divergentes et les équations différentielles. Ann. Sci. Ecole Norm. Sup. Ser. 3, **20**, 487–518 (1903)
17. Malgrange, B.: Sur les points singuliers des équations différentielles. L'Enseignement Math. **20**, 147–176 (1974)
18. Matijasevič, Yu.: Enumerable sets are diophantine. Dokl. Akad. Nauk SSSR **191**, 279–282 (1970) = Sov. Math. Dokl. **11**, 354–357 (1970)
19. Mumford, D.: Introduction to algebraic geometry. Mimeographed notes
20. Popken, J.: Über arithmetische Eigenschaften analytisches Functionen. Amsterdam: North-Holland 1935
21. Pour-el, M., Richards, I.: A computable ordinary differential equation which possesses no computable solution. Ann. Math. Logic **17**, 61–90 (1979)
22. Pour-el, M., Richards, I.: The wave equation with computable initial data such that its unique solution is not computable. Adv. Math. **39**, 215–239 (1981)
23. Ritt, J.F.: Differential algebra. AMS colloquium publications XXXIII (1950)
24. Robinson, A.: On the concept of a differentially closed field. Bull. Res. Counc. Israel **8F**, 113–128 (1959)
25. Rubel, L.: An elimination theorem for systems of algebraic differential equations. Houston J. of Math. **8**, 289–295 (1982)
26. Seidenberg, A.: An elimination theory for differential algebra, Cal. U. Publ. Math. (New Ser.) **3**, 31–66 (1956)
27. Sibuya, Y., Sperber, S.: Arithmetic properties of power series solutions of algebraic differential equations. Ann. Math. **113**, 111–157 (1981)
28. Singer, M.: The model theory of ordered differential fields. J. Symb. Logic **43**, 82–91 (1978)
29. Wood, C.: The model theory of differential fields revisited. Israel J. of Math. **25**, 331–352 (1976)

Received September 28, 1983