JOURNAL OF COMPLEXITY 2, 271–294 (1986)

On Expansion of Algebraic Functions in Power and Puiseux Series, I*

D. V. CHUDNOVSKY AND G. V. CHUDNOVSKY

Department of Mathematics, Columbia University, New York, New York 10027

Received May 5, 1986

We present algorithms that (a) reduce an algebraic equation, defining an algebraic function, to a Fuchsian differential equation that this function satisfies; and (b) compute coefficients in the expansions of solutions of linear differential equations in the neighborhood of regular singularities via explicit linear recurrences. This allows us to compute the Nth coefficient (or N coefficients) of an algebraic function of degree d in $O(dN)$ operations with $O(d)$ storage (or $O(dN)$ storage).

INTRODUCTION

Formal power series manipulations are one of the most attractive features of computer algebra systems. For a mathematician, physicist, or engineer the possibility of fast computation of the coefficients in the expansions of functions of interest built from relatively simple objects such as algebraic and/or differential equations is crucial in a vast variety of problems. Considerable attention was devoted for some time to the development of various algorithms for fast power series computations. See particularly a very good review in Knuth (1981, Chap 4.7), and original papers by Brent and Kung (1978), Brent and Traub (1980), and Kung and Traub (1978).

The construction of fast algorithms for the computation of expansions of algebraic functions is a major building block in the comprehensive formal power series packages for computer algebra systems. Knowledge of expansions of algebraic functions is important in many areas of mathematics. Some

* This work was supported in part by the NSF under Grant DMS-8409626 and the U.S. Air Force under Grant AFOSR-81-0100.

0885-064X/86 $3.00

examples of applications are presented in Kung and Traub (1978) (e.g., generating functions of combinatorial analysis and some functions of mathematical physics). Other applications include the p-adic tests of integrability in elementary functions of Abelian integrals, as presented in Chudnovsky and Chudnovsky (1984b, 1985b), where studying the denominators of the integrand of an Abelian integral is sufficient to determine the elementarity of the integral. For these and many other applications (see below) one needs fast algorithms that compute coefficients of power and Puiseux expansions of algebraic functions over various fields of constants (say, finite fields or algebraically closed fields of characteristic zero). It is noted in Kung and Traub (1978) that the classical method of computation of algebraic functions by comparison of coefficients requires $O(N^n)$ operations to compute N terms of the expansion of an algebraic function of degree n. Thus it was a considerable improvement, when Kung and Traub (1978) presented an algorithm that computes N terms in the expansion of an algebraic function of degree n in $O(nM(N))$ operations, where $M(N)$ is the number of operations sufficient to multiply two Nth-degree polynomials. Here $M(N) = O(N^2)$, but $M(N) = O(N \log N)$ if the Fast Fourier Transformation is used. Kung and Traub (1978) asked whether or not a general algebraic function can be computed in less than $O(M(N))$ operations. This question was suggested to the present authors by J. Traub. We show in this paper that there exists an algorithm that requires $O(d \cdot N)$ operations and $O(dN)$ storage to compute N coefficients in the expansion of an algebraic function $y(x)$ given by an equation $P(x, y(x)) \equiv 0$ of total degree d. Moreover, to compute only the Nth coefficient of the expansion of $y(x)$ requires at most $O(d)$ storage space.

This paper is devoted to a detailed, ready-to-implement exposition of the algorithms. In fact, with a view toward further applications we present additional algorithms for computation of power series expansions of regular solutions of linear differential equations. These algorithms are an important part of an algebraic function algorithm. However, the linear differential equation algorithm will play an important role in further fast algorithms of expansion computations, particularly in the algorithm of computation of power series solutions to algebraic (nonlinear) differential equations. In these algorithms, which we hope to present for implementation later, linearization methods (similar to Siegel's (1966) methods reduce a nonlinear differential equation to a particular linear one by means of formal power series substitutions.

The algorithm, and the paper, consists of two parts. Part I comprises Sections 1–3; Part II, Sections 4–7 (Chudnovsky and Chudnovsky, 1987). First, we replace an algebraic equation $P(x, y(x)) \equiv 0$ defining a function $y(x)$ by a linear differential equation with rational (polynomial) function coefficients, satisfied by $y(x)$. This is done in Section 1, where several important questions are discussed, such as the construction of a linear differential equation satisfied by $y(x)$ of a minimal order, the proof of Fuchsianity

of the corresponding linear differential equation, and the reconstruction of an algebraic function and its linear differential equation from the initial part of its Puiseux expansions. In Section 2 we touch upon the theory of Fuchsian linear differential equations in several variables. These generalizations (involving the computation of generators of ideals in polynomial rings) are necessary for computation of expansions of algebraic functions in several variables. In Section 3 we present a summary of the theory of Fuchsian linear differential equations, including the relationship between the monodromy theory of Fuchsian linear differential equations and their indicial equations ($e^{2\pi i\alpha}$ is an eigenvalue of the local monodromy matrix at $x = x_0$ for a root α of the indicial equation at $x = x_0$). In the exposition we follow G. V. Chudnovsky (1980a). The reader who wants to pursue the subject further, in particular to consider polylogarithmic expansions of solutions of Fuchsian linear differential equations and methods of computations of their monodromy matrices as well as their applications in physics and number theory, can consult D. V. Chudnovsky (1980) and G. V. Chudnovsky (1980b).

One of the most efficient methods of determining power series (regular) expansions of solutions of linear differential equations is to substitute an undetermined power series $y(x) = (x - x_0)^\alpha \sum_{N=0}^{\infty} y_N \cdot (x - x_0)^N$ in the differential equation, and determine the coefficients y_n successively. This naive, but essentially correct, method has serious drawbacks, for, even in the regular case, the logarithmic term in the expansion of $y(x)$ can occur when there are roots of the indicial equation at $x = x_0$ that differ by integers. The Frobenius method, which we present in Section 4, gives the determination of a complete set of solutions of a linear differential equation in the regular case. The Frobenius method provides an on-line algorithm for the determination of regular expansions of solutions of linear differential equations, whose coefficients have regular power series expansions (are analytic functions). In Section 5 we describe a famous criterion (Forsyth, 1959) for the absence of logarithmic terms in the expansion of solutions of linear differential equations at $x = x_0$. In Section 6 the Frobenius method is modified for the case of linear differential equations with rational (polynomial) coefficients. In this case the successive coefficients y_N in the expansion $(x - x_0)^\alpha \sum_{N=0}^{\infty} y_N (x - x_0)^N$ and in similar expansions in the presence of logarithmic terms, of a regular solution $y(x)$, are determined from a finite-term linear recurrence whose coefficients are explicit polynomials in n. The length of this recurrence is called in the classical literature "the rank" of the linear differential equations, and is always bounded by the (maximal) degree of the polynomial coefficients of the Fuchsian equation. This recurrence, together with initial conditions (these are necessary only when logarithmic terms are present and are given in Section 6 as well), determines the Nth coefficient y_N in terms of $y_{N-1}, \ldots, y_{N-r}$, where r is "the rank" of the linear differential equation. Finally, to construct an expansion of an arbitrary algebraic function one has to represent it as a linear combination of a fundamental system of regular solutions. The corre-

sponding coefficients can be determined by comparison of the few first terms in the expansion of an algebraic function with the expansion of basic solutions of the fundamental system; see Section 7 for a discussion of expansions of algebraic functions and the general method of Newton polygons.

It seems that the number of operations $O(N)$ required to compute N terms in the expansion of an algebraic function is the best possible and cannot be improved. However, to be precise about this statement, we have to specify over what ring one looks for the coefficients in the expansion of an algebraic function. If one deals, say, in rational integer arithmetic, then the typical algebraic function with rational coefficients in its expansion has numerators and denominators of the Nth coefficient growing as a geometric progression in N. Thus, though one needs only $O(1)$ operations to determine the Nth coefficients from a few previous ones, and these operations are only additions and multiplications (divisions) by small integers (size $O(\log N)$), the storage requires $O(1)$ terms in the expansion, each of which is of size $O(N)$. Thus typically it seems that though the Nth coefficient can be determined very fast for a very large N, this coefficient can be impossible to display or to keep in the memory for a reasonably large N (say, of the order $N \sim 10^7$). Moreover the size of N has to be even smaller, if symbols (say, constants) are present in the expansion. However, in many cases one has to compute coefficients of the expansion of algebraic functions with large indices. Since the only limitation we have is that of storage, a significant number of terms can be computed fast and kept in the memory, whenever the sizes of the coefficients that one needs to store are bounded. These are the cases of (a) computations in finite fields, and (b) multiprecision computations with fixed precision. In case (a) we compute, say, coefficients mod n for a fixed n, so that the sizes of stored numbers never exceed $O(\log n)$, independent of N.

Applications of our algorithms should include the criteria of p-integrality of coefficients of solutions of linear differential equations (as necessary for the Grothendieck conjecture (Chudnovsky and Chudnovsky, 1984b, 1985a, b); applications to diophantine geometry, especially to Abel's theorem and explicit laws of addition on Jacobians of algebraic curves; computations with algebroid formal groups over $\overline{\mathbb{Q}}$ and $\mathbb{Q}_p$ including applications to primality testing (Chudnovsky and Chudnovsky, 1985a, c).

Investigation of the complexity problem is far from being completed. Ideally, one would hope to achieve the polynomial complexity—$O(\log N)$ operations to compute the Nth term in the expansion of an algebraic function—at least for simple functions and in the case where computations are done mod n or in finite fields (mod p). Such a possibility would be spectacular and hardly possible even for the simplest algebraic functions. Indeed, take $y(x) = \sqrt{1 - 4x}$ near $x = 0 : y(x) = \Sigma_{N=0}^{\infty} \binom{2N}{N} x^N$. If one could compute $\binom{2N}{N}$ mod n in polynomial time, then, as is well known, the factorization of integers could be achieved in polynomial time. In fact, the numbers $\binom{2N}{N}$ carry complete information on the distribution of primes (G. V.

Chudnovsky, 1983). This does not mean that polynomial complexity cannot be achieved under special conditions; we hope to present corresponding results ourselves, when p is fixed and we compute mod p^n, or N and p are related (e.g., $\binom{2N}{N}$ mod p for $N = (p-1)/2$, $N = (p \pm 1)/4$, etc.).

The complexity discussion above relates to the obvious sequential implementation of our algorithms. These algorithms can also be implemented in a parallel (sequential/parallel) manner. The parallelization of these algorithms depends on the parallelization of solutions of recurrences, generating the coefficients of power series expansions. In this way one can compute N first coefficients of the power (Puiseux) series expansions of an algebraic function in $O(\log N)$ parallel steps with $O(N)$ processors. We will report further on parallel algorithms of power series computations and on methods of analytic continuation of solutions of algebraic and linear differential equations based on power series computations.

The main purpose of this paper is to serve as a manual in the implementation of power series computations in the SCRATCHPAD II (IBM) system.

After the power series package is sufficiently developed, various continued fraction and Padé approximation algorithms will be added to it. Their complexity will match that of power series manipulation routines. One hopes, however, that continued fraction expansion and Padé approximation computations for algebraic functions are significantly faster than those of power series expansion computations.

The complexity of computations of the Nth element in continued fraction expansion is, in fact, polynomial (in $\log N$), if an algebraic function belongs, e.g., to a hyperelliptic algebraic function field $C(x, \sqrt{P(x)})$. We will report elsewhere on classes of algebraic functions for which the complexities of continued fraction expansions and Padé approximations are polynomial.

1. Linear Differential Equations Satisfied by All Branches of an Algebraic Function

We want to compute the nth coefficient (or n first coefficients) in the (Puiseux) expansion of an algebraic function over $\mathbb{A}(x)$, where $\mathbb{A}$ is $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{Q}_p$, $\mathbb{F}_p$, or $\mathbb{R}$ or $\mathbb{C}$ (in the two latter cases one speaks of multiple precision computations). As stated in the Introduction, we find an efficient algorithm to compute an expansion of an algebraic function by replacing an original algebraic equation by a linear differential equation satisfied by all branches of a given algebraic function. Thus we are reducing the problem of expansion of algebraic functions to a larger and, surprisingly, easier, problem of expansion of functions satisfying linear differential equations with rational function coefficients (possessing the regularity, or Fuchsianity, property). It is therefore necessary to provide an algorithm that will associate to an algebraic

function a Fuchsian linear differential equation of the smallest possible order that this algebraic function and all its branches satisfy.

We present this algorithm in several forms including two different proofs of its existence.

Our first argument is based on a purely algebraic method. To establish the existence of the algorithm, it is sufficient to note that an arbitrary function field K, which is a finite extension of a rational function field $k(x)$, is a differential field. Hence for an arbitrary element $f = f(x)$ of K (read: for an algebraic function f from K), its derivative $f' = df/dx$ is again an element of K, and so on. If m is the degree of K over $k(x)$, then there are at most m elements of K, linearly independent over $k(x)$. Since $f, f', f'' = d^2f/dx^2, \ldots, f^{(m)} = d^mf/dx^m$ are all elements of K, and there are $m + 1$ of them, they are linearly dependent over $k(x)$. The linear relation connecting them,

$$a_m f^{(m)} + a_{m-1} f^{(m-1)} + \cdots + a_1 f' + a_0 f = 0,$$

for $a_i \in k(x)$ $(i = 0, \ldots, m)$, and a_i, not all zeros simultaneously, is the linear differential equation satisfied by the function $f = f(x)$ from K. This, merely existence, result was made into an actual algorithm by Tannery.

We start with an algebraic equation

$$P(x, y) = 0, \tag{1.1}$$

where $P(x, y)$ is a polynomial from $A[x, y]$ of degree m in y. An equation (1.1) defines an algebraic function (or, rather, branches of an algebraic function) $y = y(x)$. We are assuming momentarily that a polynomial $P(x, y)$ does not have multiple factors (say, is not divisible by the square of a polynomial nontrivially depending on y). This assumption is significantly weaker than an assumption of irreducibility of $P(x, y)$. The assumption that $P(x, y)$ does not have multiple roots (as a polynomial in y), means that two polynomials (in y), $P = P(x, y)$ and $P_y = \partial P/\partial y$, are "relatively prime." The latter term means that the resultant $r = r(x)$ of P and P_y, as polynomial in y, is nonzero. At this point, it is wise to rely on one of the subroutines of a computer algebra system that compute gcd's of polynomials. The corresponding subroutine, called, say,

SOLVEDIOPHANTINE (P, Q)

for two polynomials P, Q in y, provides a triplet (A, B, r) where

$$A \cdot P + B \cdot Q = r,$$

$$r = \gcd(P, Q)$$

and coefficients of A and B are polynomials in coefficients of P and Q. If we apply the subroutine SOLVEDIOPHANTINE to two polynomials P and

$Q = P_y$, considered as polynomials in y with coefficients that are polynomials in x, we obtain as an output

$$(A(x, y), B(x, y), r(x)).$$

Here $A(x, y)$ and $B(x, y)$ are polynomials in x and y from $\mathbb{A}[x, y]$ of degrees, correspondingly, $m - 2$ and $m - 1$ in y; $r(x)$ is a polynomial from $\mathbb{A}[x]$; and

$$r(x) = A(x, y) \cdot P(x, y) + B(x, y) \cdot P_y(x, y). \tag{1.2}$$

Now let $y(x)$ be any solution of (1.1). Then it follows from (1.2) that

$$r(x) = B(x, y(x)) \cdot P_y(x, y(x)),$$

while differentiating (1.1) we obtain $P_x(x, y(x)) + (dy/dx) \cdot P_y(x, y(x)) = 0$, or

$$\frac{dy}{dx} = -\frac{P_x(x, y(x))}{P_y(x, y(x))}.$$

Consequently,

$$\frac{dy}{dx} = -\frac{B(x, y(x)) \cdot P_x(x, y(x))}{r(x)}. \tag{1.3}$$

Taking into account the algebraic equation (1.1) we can eliminate from the numerator in the right-hand side of (1.3) all powers of $y(x)$ higher than $m - 1$. Consequently, we get

$$\frac{dy}{dx} = \frac{R_1}{r(x)}, \tag{1.4}$$

where $R_1 = R_1(x, y)$ is a polynomial in y of degree $m - 1$ with coefficients being *rational functions* in x. Iterating (1.4) we obtain

$$\frac{d^2y}{dx^2} = \frac{1}{r(x)^2}\left\{R_1 \cdot \frac{\partial R_1}{\partial y} + r(x)\frac{\partial R_1}{\partial x} - R_1\frac{\partial r(x)}{\partial x}\right\}.$$

Again we use (1.1) to eliminate all powers of $y(x)$ of degree higher than $m - 1$. Thus we obtain

$$\frac{d^2y}{dx^2} = \frac{R_2}{r(x)^2}.$$

Repeating this procedure $m - 2$ times more we obtain a system of equations

$$\frac{d^i y}{dx^i} = \frac{R_i}{r(x)^i} : i = 1, \ldots, m, \tag{1.5}$$

where $R_i = R_i(x, y)$ $(i = 1, \ldots, m)$ are polynomials in y of degrees in y at most $m - 1$ with coefficients rational in x. We obtain m equations

$$R_i = \frac{d^i y}{dx^i} \cdot r(x)^i : i = 1, \ldots, m, \tag{1.6}$$

and thus we can eliminate (say by Gauss' elimination method) powers $y^0, y^1, \ldots, y^{m-1}$ of y in the left side of (1.6). In this way we obtain a linear relation

$$c_0 y = \sum_{i=1}^{m} c_i \frac{d^i y}{dx^i} r^i,$$

where $c_0, c_1, \ldots, c_m$ are rational functions in x. Multiplying this relation by the common denominator of $c_0, c_1, \ldots, c_m$, we obtain a linear differential equation on y with polynomial coefficients in x:

homogeneous

$$\sum_{i=0}^{m} b_i(x) \frac{d^i y}{dx^i} = 0. \tag{1.7}$$

Equation (1.7) corresponds to the algebraic equation (1.1), and is independent of the choice of its solution y (since we used only Eq. (1.1) to eliminate high powers of y). The order of (1.7) is at most m, and we can claim only that one of the coefficients $b_0(x), \ldots, b_m(x)$ is nonzero.

In fact, this algorithm provides a linear differential equation corresponding to (1.1) of the smallest possible order. For this it is enough to determine the rank of the matrix formed from the coefficients at powers of $y(x)$ of polynomials R_i $(i = 1, \ldots, m)$. Indeed, let

$$R_i = \sum_{j=0}^{m-1} R_{i,j} y^j, \tag{1.8}$$

where $R_{i,j}$ are rational functions in $x : j = 0, \ldots, m - 1; i = 1, \ldots, m$. Form an $(m + 1) \times m$ matrix $M = (M_{i,j} : i = 0, \ldots, m; j = 0, \ldots, m - 1)$ with rational function entries, such that

$$M_{i,j} = \begin{cases} \delta_{1,j} & \text{for } i = 0 \\ R_{i,j} \cdot r(x)^{-i} & \text{for } i = 1, \ldots, m \end{cases}$$

for $i = 0, \ldots, m; j = 0, \ldots, m-1$. Let $k \leq m$ be the minimal integer (≥ 0) such that $k+1$ first rows $\overline{M}_i = (M_{i,j} : j = 0, \ldots, m-1; i = 0, \ldots, k)$ of M are *linearly dependent* (clearly $k \leq m$ exists as rank of M is at most m). Then there are (rational functions in x) $c_0, \ldots, c_k$ such that c_k is *nonzero* (as $\overline{M}_0, \ldots, \overline{M}_{k-1}$ are linearly independent) and

$$\sum_{i=0}^{k} c_i \overline{M}_i = 0.$$

The last equation is equivalent to the linear differential equation

$$\sum_{i=0}^{k} c_i \frac{d^i y}{dx^i} = 0, \tag{1.9}$$

satisfied by *all* m solutions of (1.1). According to the definition of k, Eq. (1.9) is a linear differential equation of minimal order, satisfied by all solutions of (1.1). This equation is unique up to multiplication by an invertible rational function.

Though for a "generic" algebraic equation (1.1) the order of a differential equation (1.9) is equal to the degree m of (1.1), we can see that a simple linear transformation can reduce the order of a linear differential equation corresponding to (1.1) from m to $m-1$. To do this let us assume for the moment that in the polynomial expansion of $P(x, y)$ in powers of y the coefficient at y^{m-1} is equal to zero. Then the order of the differential equation (1.9), corresponding to (1.1), is at most $m-1$. Indeed, it is sufficient to note that under these assumptions on $P(x, y)$, the rank of the matrix M above is at most $m-1$. An alternative proof of this statement is given below in connection with Wronskians.

This remark on the reduction of the order of a linear differential equation (1.9), if $P(x, y)$ has a special form, can be applied to an arbitrary algebraic function. Indeed, let $P(x, y)$ be an arbitrary polynomial of degree m in y as in (1.1), and let $p_m = p_m(x)$ and $p_{m-1} = p_{m-1}(x)$ be coefficients at y^m and y^{m-1}, respectively, in $P(x, y)$. Then the transformed polynomial $P_1(x, y) = P(x, y + p_{m-1}/mp_m) \cdot m^m \cdot p_m^{m-1}$ has the coefficient at y^{m-1} equal to zero. Thus if $y(x)$ is an arbitrary solution of (1.1), then there exists a linear differential equation of order at most $m-1$ satisfied by $y(x) + p_{m-1}(x)/mp_m(x)$. This equation has the form (1.9) for $k \leq m-1$ if one constructs M from a polynomial $P_1(x, y)$ instead of $P(x, y)$ in (1.1).

The above algorithm can be realized using computer algebra systems (particularly, using SCRATCHPAD and SCRATCHPAD II) possessing codes for (a) resultants or gcd's of polynomials; (b) differentiation of polynomials; and (c) solution of linear equations with symbolic (polynomial) entries.

The only assumption of the polynomial $P(x, y)$ made above was that P and P_y are "relatively prime" in the sense that the resultant $r(x)$ of P and P_y is not zero. If it is zero, then P, as a polynomial in y, possesses multiple roots. To rid ourselves of this possibility, we have to consider gcd of P and P_y in a polynomial ring and treat separately two polynomials: (a) $P/\gcd(P, P_y)$ and (b) $\gcd(P, P_y)$ (dividing P_y). In case (a) we arrive at a polynomial without multiple roots to which the above algorithm is applied. In case (b) we obtain a polynomial of degree at most $m - 1$. If the polynomial does not have multiple roots, then the above algorithm is applied to it separately and we obtain two scalar linear differential equations corresponding to an algebraic equation (1.1). If the polynomial in (b) has multiple roots, we apply to it the same process that we applied to P, . . . , etc. If it is possible to factorize $P(x, y)$ completely using a given computer algebra system, then it is easier to apply the above algorithm to each of its irreducible factors.

The second method that we propose is based on Wronskians instead of resultants, and this method is more convenient when several first terms of the Puiseux expansions of branches of an algebraic function are known. These terms can be determined, say, directly from Eq. (1.1) and its Newton diagram.

For convenience we work in extensions of a differential field K over a field of constants k. Typically, K is a rational function field over k (or, perhaps, an algebraic function field). To each homogeneous scalar linear differential equation of order d over K

$$y^{(d)} + a_{d-1}y^{(d-1)} + \cdots + a_1 y' + a_0 y = 0 \tag{1.10}$$

with $a_i \in K$ $(i = 1, \ldots, d - 1)$, there corresponds a Picard–Vessiot extension L of K (Kolchin, 1973; Kaplansky, 1957), generated by a fundamental system of solutions of (1.10). If $y_1, \ldots, y_d$ is a fundamental system of solutions of (1.10) from L, then the left-hand side of Eq. (1.10), denoted symbolically by $L[y]$, can be represented as a ratio of two Wronskian determinants:

$$L[y] = \frac{\begin{vmatrix} y & y_1 & \cdots & y_d \\ y' & y_1' & \cdots & y_d' \\ \vdots & \vdots & \vdots & \vdots \\ y^{(d)} & y_1^{(d)} & \cdots & y_d^{(d)} \end{vmatrix}}{\begin{vmatrix} y_1 & \cdots & y_d \\ y_1' & \cdots & y_d' \\ \vdots & & \vdots \\ y_1^{(d-1)} & \cdots & y_d^{(d-1)} \end{vmatrix}} \cdot (-1)^d. \tag{1.11}$$

(To prove (1.11), note that the denominator in the right-hand side of (1.11) is nonzero, because $y_1, \ldots, y_d$ are linearly independent over k; see the main

property of Wronskians (Kolchin, 1973; Kaplansky, 1957). Thus the right-hand side of (1.11) is well defined. Also, every solution of (1.10) is a linear combination of $y_1, \ldots, y_d$ with coefficients from k. Consequently, for every solution y of (1.10), the determinant in the numerator in the right-hand side of (1.11) is zero. The right side of (1.11) is, obviously, a linear differential equation of order d in y, with leading coefficient one, with coefficients from K and having, as we proved, $y_1, \ldots, y_d$ as its solutions. Thus the difference between the right and left sides in (1.11) is a differential operator of order at most $d - 1$ with d linearly independent solutions, and this is identically zero.)

Expressions in the right-hand side of (1.11) for various $y_1, \ldots, y_d$ can be used, therefore, to construct linear differential equations (Chudnovsky and Chudnovsky, 1983, 1984a). If $y_1, \ldots, y_d$ are lying in some differential extension V of K, the crucial question is whether the coefficients of the corresponding linear differential equation lie in K. The answer is given by the following trivial

LEMMA 1.1. *Let V be an arbitrary Picard–Vessiot extension of K and let $y_1, \ldots, y_d$ be elements of V, linearly independent over the field k' of constants of K and such that the vector space $k'\{y_1, \ldots, y_d\}$ over k' generated by $y_1, \ldots, y_d$ is closed under the action of the Picard–Vessiot group of V/K. Then an expression*

$$L[y] = (-1)^d \frac{W(y, y_1, \ldots, y_d)}{W(y_1, \ldots, y_d)}$$

in a differential undetermined y is a linear differential operator of order d with coefficients from K.

Proof. It is enough to show that the differential operator $L[y]$ is invariant under the action of the Picard–Vessiot group of V/K. However, since the action of the Picard–Vessiot group on $y_1, \ldots, y_d$ is always a linear one, the ratio of two determinants in the definition of $L[y]$ is always unaltered. ■

Lemma 1.1 is sufficient to construct linear differential equations satisfied by algebraic functions. To see the relationship between differential fields and algebraic function fields, which are differential fields, as remarked above, we remind the reader that the Picard–Vessiot group of a Picard–Vessiot extension of a differential field is a Galois group of this extension. Henceforth, if one looks for the Galois group of an algebraic function field, one gets its Picard–Vessiot group. If the ground field (field of constants) is a complex number field, then the action of the Galois group of an algebraic function field coincides with the action of the monodromy group on a Riemann surface corresponding to the model of the function field. It is well known that in this case, the actions of the Galois, monodromy, and Picard–Vessiot groups are the same (cf. Markus,1959–1960).

To derive a linear differential equation over $k(x)$ having minimal order and satisfied by all roots $y = y(x)$ of an algebraic equation (1.1), let us assume that we have m distinct roots $y_1 = y_1(x), \ldots, y_m = y_m(x)$ of (1.1). (Here again we momentarily invoked an assumption that (1.1) does not have multiple roots in y.) Let us choose a subset of $\{y_1, \ldots, y_m\}$ with the maximal number of functions linearly independent over k. To do this it is enough to examine the rank of the Wronskian *matrix*

$$W = \begin{pmatrix} y_1 & \cdots & y_m \\ y_1' & \cdots & y_m' \\ \cdots & \cdots & \cdots \\ y_1^{(m-1)} & \cdots & y_m^{(m-1)} \end{pmatrix}$$

(with $y_i^{(j)} = d^j y_i / dx^j$). The rank of the matrix W over k is equal to the maximal number d of functions among $\{y_1, \ldots, y_m\}$, linearly independent over k. In these notations, the first d rows of W are linearly independent over k, while the $d + 1$ are linearly dependent over k. Also in this case there is a nonzero $d \times d$ minor of W of the form $\det(y_{k_i}^{(j)} : i, j = 0, \ldots, d-1)$ and $1 \le k_0 < \cdots < k_{d-1} \le m$. Without loss of generality (simply by renumbering) we can assume that $k_0 = 1, k_1 = 2, \ldots, k_{d-1} = d$, i.e., that functions $y_1, \ldots, y_d$ are linearly independent over k. In these notations we obtain

PROPOSITION 1.2. *The expression*

$$L[y] = (-1)^d \frac{W(y, y_1, \ldots, y_d)}{W(y_1, \ldots, y_d)} \tag{1.12}$$

is a linear differential operator with rational coefficients from $k(x)$ and the leading coefficient 1, *such that all solutions $y = y(x)$ of an algebraic equation (1.1) are solutions of a linear differential equation $L[y] = 0$, and, conversely, any solution of a linear differential equation $L[y] = 0$ is a linear combination (with coefficients from a field of constants k) of roots of an algebraic equation (1.1).*

Proof. First, the expression $L[y]$ is nontrivial, as $y_1, \ldots, y_d$ are linearly independent over k. As expression of $L[y]$ shows solutions of $L[y] = 0$ are exactly linear combinations (with coefficients from k) of $y_1, \ldots, y_d$. Since, by the choice of $\{y_1, \ldots, y_d\}$, the linear closure over k of $\{y_1, \ldots, y_d\}$ coincides with that of $\{y_1, \ldots, y_m\}$, solutions of $L[y] = 0$ are exactly linear combinations of roots of (1.1). Also $L[y]$ is a linear differential operator of minimal order with the same property, because $y_1, \ldots, y_d$ are linearly independent. ■

It follows from the discussion above (on the coincidence of the Galois and Picard–Vessiot groups) and Lemma 1.1 that the expression $L[y]$ has coefficients from the rational function field $k(x)$. It is preferable to give an independent proof of it, without using any information on the structure of Picard–Vessiot extensions.

To check that the coefficients of the operator $L[y]$ in (1.12) (see also (1.11)) are rational functions with the coefficients from $k(x)$, it is sufficient to remark that the coefficients of (1.12) lie in the Galois closure K of $k(x, y_1, \ldots, y_d)/k(x)$. An action of the Galois group of K on $\{y_1, \ldots, y_m\}$ is given by appropriate permutations. Since $y_1, \ldots, y_m$ are expressed linearly over k in terms of $y_1, \ldots, y_d$, an action of the Galois group of K on $\{y_1, \ldots, y_d\}$ is given by linear transformations $\mathbf{y} \to A \cdot \mathbf{y}$ for $\mathbf{y} = (y_1, \ldots, y_d)$ and $A \in GL_d(k)$. Then the action of the Galois group on the coefficients of the differential operator (1.12) is trivial, since any nonsingular linear transformation $\mathbf{y} \to A \cdot \mathbf{y}$ affects both Wronskians in (1.12) in the same way: $W(y_1, \ldots, y_d) \to \det(A) \cdot W(y_1, \ldots, y_d)$; $W(y, y_1, \ldots, y_d) \to \det(A) \cdot W(y, y_1, \ldots, y_d)$. This shows that the operator $L[y]$ is defined over $k(x)$.

Proposition 1.2 uniquely defines a linear differential equation of minimal order with rational function coefficients, satisfied by all m roots of Eq. (1.1). This equation, $L[y] = 0$, coincides with Eq. (1.9) if one normalizes (1.9) with $c_k = 1$, where, of course, $k = d$ is the order of (1.12). The identification between Eq. (1.9) and the operator (1.12) is useful, e.g., for proof of the statement above that the order of an equation (1.9) is at most $m - 1$ whenever the coefficient at y^{m-1} of $P(x, y)$ is zero. Indeed, in this case, for m solutions $y_1, \ldots, y_m$ of (1.1), we have $y_1 + \cdots + y_m = 0$, and thus $d \leq m - 1$, i.e., $k \leq m - 1$.

For computational purposes, Proposition 1.2 seems to be unsuitable as an algorithm of construction of a minimal linear differential equation associated with (1.1), unlike the first algorithm proposed above. The main reason for this lies in the ambiguity of the definition of "functions $y_1 = y_1(x), \ldots, y_m = y_m(x)$ that are solutions of (1.1)." This ambiguity, and with it Proposition 1.2, can be clarified, if one assumes that instead of functions $y_i = y_i(x)$ we consider approximations to them given by the sum of leading N terms in their Puiseux expansions at some point $x = x_0$ in $\mathbb{CP}^1$, for an appropriate large integer N. In this case the word "functions" is computationally justified and we understand by "functions" their approximations, given by the sum of initial terms in the Puiseux expansion of $y_i(x)$. We denote an Mth-order approximation to "true solutions" $y_i = y_i(x)$ of (1.1) by the finite list $Y(x; x_0, M) = (y_i(x'; x_0, M) : i = 1, \ldots, m)$, where $y_i(x; x_0, M)$ are finite Laurent series in a variable $(x - x_0)^\nu$ for an appropriate $\nu \in \mathbb{Q}$ and such that $\operatorname{ord}_{x=x_0}(y_i(x) - y_i(x; x_0, M)) \geq M$ for all $i = 1, \ldots, m$.

To generate a list $Y(x; x_0, M)$ of approximations to $y_i(x)$ up to order at least M, one can use any of the existing (even slow) algorithms of computation of

the first terms in the Puiseux expansions of all branches of solutions of (1.1) at $x = x_0$. The standard method based on Newton diagrams of (1.1) is presented in Walker (1950) and efficient versions of this algorithm are presented in Kung and Traub (1978). We refer readers to Part II, Section 7 (Chudnovsky and Chudnovsky, 1987) for remarks concerning the Newton diagram method.

We indicate now how to recover a linear differential equation (1.9) from an approximation $Y(x; x_0, M)$ to solutions of (1.1). First we have to determine d, the maximal number of solutions of (1.1) linearly independent over k, the field of constants. Having a list of approximations $Y(x; x_0, M)$, it is easy to find linearly independent (Laurent) polynomials among $y_i(x; x_0, M) : i = 1, \ldots, m$ by considering a scalar matrix of their coefficients. (This does not even require a computer algebra system.) If approximations of order M to y_i are linearly independent, then, clearly, the corresponding functions $y_i(x)$ are linearly independent as well, whatever M is. The converse to this statement is correct only for large M. To determine the lower bound on such M, let us assume that the linear dependence relation between approximations $y_i(x; x_0, M) - \sum_{i=1}^{m} c_i y_i(x; x_0, M) \equiv 0$ for constants $c_1, \ldots, c_m$ (not all zero) does not materialize as a linear dependence relation between functions $y_i(x)$. Then we have a nonzero algebraic function $y_0 \overset{\text{def}}{=} \sum_{i=1}^{m} c_i y_i(x)$, which has a zero at $x = x_0$ of order at least $M : \operatorname{ord}_{x=x_0} y_0 \geq M$. One must now consider the algebraic equation satisfied by $y_0 = y_0(x)$,

$$Q(x, y_0) \overset{\text{def}}{=} \sum_{j=0}^{m'} q_j(x) y_0^j = 0; \qquad q_0(x) \not\equiv 0, \tag{1.13}$$

for polynomials $q_j(x)$ $(j = 0, \ldots, m')$. The simplest way to generate such an equation is to look at an equation satisfied by all *nonzero* functions of the form $\sum_{j=1}^{m} c_j y_{\pi(j)}$ for all permutations π of $\{1, \ldots, m\}$. We are *not* interested in the explicit form of (1.13) but only in the upper bound on the degree of $q_0(x) : \deg(q_0) \leq D_0$. D_0 can be trivially estimated from the above discussion in terms of the degree d_x of $P(x, y)$ with respect to x independently of $c_i : D_0 \leq d_x m!$. From (1.13) and $\operatorname{ord}_{x=x_0} y_0 \geq M$ it follows that whenever $q_j(x)$ are regular at $x = x_0$ (i.e., $x_0 \neq \infty$), $\operatorname{ord}_{x=x_0} q_0(x) \geq M$. Thus $D_0 < M$ implies that $y_0(x) \equiv 0$. Consequently for positive M and $M > D_0$ the linear independence of approximations $y_i(x; x_0, M)$ is *equivalent* to the linear independence of $y_i(x)$. (The arguments can be properly modified to include the case $x_0 = \infty$.)

Once d is found using the approximation $Y(x; x_0, M)$, we can determine similarly the linear differential equation (1.9). For this let us expand a linear operator $L[y]$ from (1.12) linearly in $y^{(j)} : j = 0, 1, \ldots, d$. We have

$$L[y] = y^{(d)} + a_{d-1} y^{(d-1)} + \cdots + a_1 y' + a_0 y, \tag{1.14}$$

where $a_i \in k(x)$ $(i = 0, \ldots, d-1)$ according to Proposition 1.2 and a_i can be expressed as

$$a_i = \frac{M_i}{W}, \tag{1.15}$$

where $W = W(y_1, \ldots, y_d)$ and M_i is an appropriate $d \times d$ minor of $W(y, y_1, \ldots, y_d) : M_i = \pm\det(y_i^{(j)} : i = 1, \ldots, d, j = 0, \ldots, d; j \neq 1) : i = 0, \ldots, d-1$. In (1.15) we understand M_i and W as differential polynomials in $y_1, \ldots, y_d : M_i = M_i(y_1, \ldots, y_d)$, $W = (y_1, \ldots, y_d) : i = 0, \ldots, d-1$.

Hence we can substitute approximations $y_i(x; x_0, M)$ into M_i and W and obtain approximate coefficients $a_i(x; x_0, M)$—as power series in an appropriate local parameter at $x = x_0$. For large M, these coefficients are *rational functions* and *coincide* with $a_i = a_i(x)$ from (1.14). To determine the rationality of $a_i(x; x_0, M)$ we suggest Padé approximations of order up to $M/2$. The precise bound on M for which the Padé approximations to $a_i(x; x_0, M)$ *coincide* with rational functions $a_i(x) : i = 0, \ldots, d-1$ can be easily determined in terms of degrees d_x and m of $P(x, y)$. However, instead of this bound, in practical terms it is enough to look at Padé approximations to $a_i(x; x_0, M)$ and note the first instances when Padé approximations become nonnormal (i.e., continued fraction expansions become nonnormal.) As results and conjectures predict (Chudnovsky and Chudnovsky, 1984a), if nonnormality persists (say, for about $O(m)$ steps), then the corresponding Padé approximations are, in fact, correct rational functions. The approach to the construction of (1.9) from approximations to algebraic functions can be implemented whenever the proper power series facility allows.

In construction of the linear differential equation satisfied by an algebraic function, an uncertainty lies in the order of this differential equation, as compared to the degree of an algebraic equation satisfied by this algebraic function. Though for a "generic" algebraic function this order is equal to the degree of the equation, there are numerous important algebraic functions satisfying linear differential equations of orders significantly smaller than their degree. For example, any algebraic function $y = x^{1/n}$ of degree n satisfies a homogeneous first-order linear differential equation $nxy' - y = 0$. (The word "generic" means, as usual, that the coefficients of the algebraic equation defining a function lie in an open Zarisky set.)

Though we proposed an algorithm (either the first or the second one) that determines the precise order of a linear differential equation satisfied by an algebraic function, it is important to present an alternative method of finding linear differential equations associated with algebraic functions, where the order of a differential equation is easier to determine. This method is based on a construction of a matrix first-order linear differential equation satisfied by algebraic functions. It should be remembered that though one can always

pass from the matrix form of a linear differential equation to a scalar one and vice versa, some information is lost/gained, particularly concerning apparent singularities (cf. D. V. Chudnovsky, 1980; G. V. Chudnovsky, 1980a, Sect. 5). Matrix linear differential equations are useful, when one chooses a particular basis of an algebraic function field. In this case many invariants connected with the function field can be computed directly from a matrix linear differential equation.

As above, let us start with an algebraic equation

$$P(x, y) = 0, \tag{1.1}$$

where $P(x, y)$ is a polynomial with coefficients from k and of degree m in y. Now we make the following assumption:

There are no multiple roots in Eq. (1.1) in y.

See the discussion above after the presentation of the first algorithm on what to do if there is a multiple root in Eq. (1.1).

Let $y_i = y_i(x) : i = 1, \ldots, m$ be m distinct roots of (1.1). We want to construct a matrix $m \times m$ first-order homogeneous linear differential equation

$$\frac{d}{dx}(\overline{w}^t) = A \cdot \overline{w}^t, \tag{1.16}$$

for $\overline{w} = (w_1, \ldots, w_m)$ and $A \in M_n(k(x))$ with a transposition operator t, such that m linearly independent solutions of (1.16) are

$$\overline{w}_i = (1, y_i, y_i^2, \ldots, y_i^{m-1}) : i = 1, \ldots, m.$$

First, m vectors $\overline{w}_i : i = 1, \ldots, m$ are linearly independent; this follows from the expression for the Vandermonde determinant. Consequently, if a linear differential equation (1.16) with the desired properties exists, it is, essentially, unique, up to multiplication by a rational function from $k(x)$. To obtain this differential equation we use a method identical to (1.2)–(1.4). Using the language of commands in a Computer Algebra system we apply the operation SOLVEDIOPANTINE $(X, Y) = (A, B)$, where $A \cdot X + B \cdot Y = \gcd(X, Y)$ applied to two polynomials $X = P(x, y)$ and $Y = P_y(x, y)$ as polynomials *in* y with coefficients from k[x]. That is, we find two polynomials $A = A(x, y)$ and $B = B(x, y)$ such that $A \cdot P + B \cdot P_y = r(x)$ (and $r(x)$ is, of course, a resultant (= discriminant of $P(x, y)$ in y) of P and P_y in y). Then for any $y = y_i$, $P(x, y_i) = 0$, and

$$\frac{dy_i}{dx} = -\frac{B(x, y_i) \cdot P_x(x, y_i)}{r(x)} : i = 1, \ldots, m.$$

Similarly, we have

$$\frac{d}{dx}(y_i^k) = \frac{-k \cdot y_i^{k-1} \cdot B(x, y_i) \cdot P_x(x, y_i)}{r(x)} \tag{1.17}$$

for any $k = 0, \ldots, m-1$ and $i = 1, \ldots, m$. Taking into account the defining equation $P(x, y_i) = 0$, we can express in (1.17) all powers of y_i with exponents higher than $m-1$ in terms of $1, y_i, y_i^2, \ldots, y_i^{m-1}$ with coefficients from $k(x)$. Then from (1.17) we obtain

$$\frac{d}{dx}(y_i^k) = \frac{R_k(x, y_i)}{r(x)} : i = 1, \ldots, m, \tag{1.18}$$

where $R_k(x, y_i) = \sum_{j=0}^{m-1} r_{k,j}(x) y_i^j$ and $r_{k,j}(x) \in k(x) : k, j = 0, \ldots, m-1$. We note that $r_{k,j}(x) \cdot a(x)^K$ are polynomials from $k[x]$ for an appropriate K (depending only on m) : $k, j = 0, \ldots, m-1$. Consequently the matrix linear differential equation (1.16) has matrix coefficients of the form

$$A = (A_{i,j})_{i,j=1}^m \qquad \text{and} \qquad A_{i,j} = r_{i-1,j-1}(x)$$

for $i, j = 1, \ldots, m$. Note that in order to obtain expressions for $A_{i,j}$ it is enough to simplify the expression $-(i-1)y^{i-1}B(x, y)P_x(x, y)$ by means of the identity $P(x, y) \equiv 0$.

2. Criteria of Fuchsianity of Linear Differential Equations

A solution of a Fuchsian linear differential equation with rational function coefficients can be defined over the complex numbers as a multivalued function in the extended complex plane, regular everywhere but at finitely many points (called regular singularities), near which the function exhibits algebraic behavior. For detailed definitions and criteria of Fuchsianity see Forsyth (1959), Fuchs (1900–1906), Ince (1959), Theorem 2.1 and Proposition 2.2 below, and Section 3.

Thus the scalar linear differential equation $L[y] = 0$ from (1.9) or (1.12) associated with an algebraic equation (1.1) is a Fuchsian linear differential equation. Indeed, as we remarked above, an analytic criterion of Fuchsianity states that if all of the solutions of a linear differential equation are analytic in $\mathbb{CP}^1 \backslash S$ for a (fixed) finite set S and algebraic behavior near any singularity from S, then the linear differential equation is a Fuchsian one (see Proposition 2.2). Since all solutions of $L[y] = 0$ are, according to Proposition 2.2, algebraic functions, an equation $L[y] = 0$ is, according to this criterion, a Fuchsian one. From the point of view of applications to the construction of multivariable expansions of algebraic functions of several variables, we need

a generalization of the criterion of Fuchsianity for the case of linear differential equations in several variables (as in the microlocal calculus). It is therefore important to review briefly the corresponding result on the relationship between the structure of singularities of functions of several complex variables and linear differential equations they satisfy. For details we refer the reader to Björk (1979), Kashiwara and Kawai (1979), Nilsson (1963–1965), and Deligne (1970). Instead of multivalued functions with algebraic singularities only, we consider Nilsson class functions. According to Nilsson, a function $f = f(z_1, \ldots, z_n)$ belongs to a Nilsson class if there exists a nonzero polynomial $q = q(z_1, \ldots, z_n) \in \mathbb{C}[z_1, \ldots, z_n]$ without multiple factors such that for the hypersurface in $\mathbb{C}^n$, $M(q) = \{(z_1, \ldots, z_n) \in \mathbb{C}^n : q(z_1, \ldots, z_n) = 0\}$, the function f is multivalued on $\mathbb{C}^n \backslash M(q)$, and is of tempered growth. The tempered (at most algebraic) growth condition means that on some polydisk Δ around $z \in M(q)$ we have $f = \Sigma \varphi_{\alpha,h} \cdot z_i^{\alpha} (\log z_i)^h (h \geq 0, \alpha \in \mathbb{C}, h \in \mathbb{Z})$, where locally $q \sim z_i$ near $M(q)$. We can restate this by saying that f has at worst a polynomial growth near singularities and the vector space over k of all analytic continuations of f is finite dimensional. The last condition is known as the finite-dimensional determination condition, and means that the fundamental group of $\mathbb{C}^n \backslash M(q)$ has a finite-dimensional representation as a monodromy group of f. Clearly, algebraic functions belong to the Nilsson class. It turns out that any functions of the Nilsson class (and only they) satisfy a system of Fuchsian linear differential equations with polynomial coefficients. We can associate with any Nilsson class function f a polynomial ideal L_f of all linear differential equations with polynomial coefficients satisfied by f:

$$L_f = \left\{ l \in \mathbb{C}[z_1, \ldots, z_n]\left[\frac{\partial}{\partial z_1}, \ldots, \frac{\partial}{\partial z_n}\right] : l \cdot f = 0 \right\}.$$

If $A_n = \mathbb{C}[z_1, \ldots, z_n][\partial/\partial z_1, \ldots, \partial/\partial z_n]$ (the Weyl algebra of differential operators with polynomial coefficients), then the A_n-module $A_n \cdot f = \{l \cdot f : l \in A_n\}$ is naturally isomorphic to A_n/Lf. An algebraic characterization of multidimensional Fuchsian linear differential equations is the following.

THEOREM 2.1. (Kashiwara and Kawai, 1979; Deligne, 1970). *For an arbitrary Nilsson class function f, the A_n-module $A_n \cdot f$ is Fuchsian along the principal ideal generated by q : $(q) = \mathbb{C}[z_1, \ldots, z_n] \cdot q$. This means that for every derivative $\partial \in \mathrm{Der}_{\mathbb{C}}(\mathbb{C}[z_1, \ldots, z_n])$ such that $\partial q \in (q)$, there exists $m \in \mathbb{Z}$, $m \geq 0$ and $a_0, \ldots, a_{m-1} \in \mathbb{C}[z_1, \ldots, z_n]$ such that*

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

In particular, f satisfies a Fuchsian linear differential equation along any straight line in $\mathbb{C}^n$. That is, there exists $m_1 \geq 1$ such that

$$\left\{\left(\frac{\partial}{\partial z_i}\right)^{m_1} + a_{m_1-1,i}\left(\frac{\partial}{\partial z_i}\right)^{m_1-1} + \cdots + a_{0,i}\right\} f = 0$$

for $a_{j,i} \in \mathbb{C}[z_1, \ldots, z_n] : j = 0, \ldots, m_1 - 1$ and $i = 1, \ldots, n$.

The coefficients in the Fuchsian linear differential equations are not arbitrary polynomials, and their structure can be determined from the Nilsson class conditions. In the one-dimensional case this algebraic criterion of Fuchsianity belongs to Fuchs. We present Fuchs' criterion locally and globally. The local Fuchs' criterion is particularly useful, because it allows us to expand solutions of arbitrary linear differential equations, even though they do not belong to the Fuchsian class, in the neighborhood of a point that is a regular singular point for the equation. We formulate this condition for linear differential equations with arbitrary, not necessarily rational, function coefficients.

PROPOSITION 2.2. (Fuchs, 1900–1906; Ince, 1959). *A point $x = x_0$ is a regular singular point of the equation (i.e., it is a regular singularity for all its solutions)*

$$\frac{d^m y}{dx^m} + a_{m-1}(z)\frac{d^{m-1}y}{dx^{m-1}} + \cdots + a_1(x)\frac{dy}{dx} + a_0(x)y = 0$$

if and only if $a_i(x) = (x - x_0)^{-(m-i)} \cdot A_i(x) : i = 0, \ldots, m - 1$, where $A_i(x) : i = 0, \ldots, m - 1$ are regular at $x = x_0$.

In the case where the coefficients $a_i(x)$ are given as Laurent power series in $x - x_0$, the condition of regularity of $A_i(x)$ at $x = x_0$ means that $A_i(x)$ are formal power series in $x - x_0$.

If all points in extended complex plane $\mathbb{CP}^1 = \mathbb{C} \cup \{\infty\}$ are regular singular points of the linear differential equation, this equation is called Fuchsian. If there are only finitely many singularities, then this Fuchsian equation has rational function coefficients. Alternatively, according to Theorem 2.1, the Fuchsianity of a linear differential equation means that all its solutions are multivalued functions everywhere at $\mathbb{CP}^1$ minus the singularities, with algebraic behavior everywhere. Proposition 2.2 gives the following characterizations of coefficients of a Fuchsian linear differential equation with rational function coefficients:

PROPOSITION 2.3. (Forsyth, 1959; Fuchs, 1900–1906; Ince, 1959). *Fuchsian linear differential equations of order m with rational function coefficients, and only they, have the form*

$$\frac{d^m y}{dx^m} + \frac{P_{m-1}(x)}{P(x)} \cdot \frac{d^{m-1}y}{dx^{m-1}} + \cdots + \frac{P_1(x)}{P(x)^{m-1}} \cdot \frac{dy}{dx} + \frac{P_0(x)}{P(x)^m} y = 0,$$

where $P(x) = \prod_{j=1}^{k} (x - a_j)$ *is a polynomial without multiple roots, and* $P_i(x)$ *are polynomials of degrees at most* $(m - i)(k - 1) : i = 0, \ldots, m - 1$.

3. Fundamental Systems of Solutions of Fuchsian Linear Differential Equations

Let us consider a linear differential equation of order n with rational function coefficients

$$y^{(m)}(x) + a_{m-1}(x)y^{(m-1)}(x) + \cdots + a_0(x)y(x) = 0 \tag{3.1}$$

for $y^{(i)}(x) = d^i y/dx^i$ and $a_i(x) \in \mathbb{C}(x) : i = 0, \ldots, m$ $(a_m(x) \equiv 1)$.

We are interested in Eqs. (3.1) with regular singularities only. First, all singularities of solutions are singularities of $a_j(x) : j = 0, \ldots, m - 1$. We remind the reader that the singularity of the system (3.1) is called *apparent* (D. V. Chudnovsky, 1980) if it is a singularity of some of the $a_j(x) : j = 0, \ldots, m - 1$ but not of the solutions of (3.1). The notion of a regular singularity for (3.1) is defined in many equivalent ways. The simplest way is described by the roots of an indicial equation (Forsyth, 1959; Ince, 1959):

Definition 3.1. Let $x = x_0$ be a singularity of (3.1), i.e., a singularity of one of the $a_j(x) : j = 0, \ldots, m - 1$. We look for formal solutions $y(x)$ of (3.1) of the form

$$y(x) = (x - x_0)^r \cdot y_0(x) = (x - x_0)^r \cdot (a_0 + a_1(x - x_0) + \cdots), \tag{3.2}$$

$a_0 \neq 0$, where $y_0(x)$ is an invertible element of $\mathbb{C}[[x - x_0]]$. Substituting $y(x)$ from (3.2) into (3.1), we obtain some algebraic equation $P_{x_0}(r) = 0$ characterizing possible values of r. This equation is called an indicial equation of (3.1) at $x = x_0$ and has degree $\leq n$. If the degree $P_{x_0}(r)$ is exactly n, then $x = x_0$ is called a regular singularity of (3.1).

If $x = x_0$ is a regular singularity of (3.1), then a fundamental system of solutions of the form (3.2) exists. However, one must be aware of the case when the roots of $P_{x_0}(r)$ differ by rational integers and logarithmic terms may appear in the expansion of $y(x)$ (see Forsyth, 1959; Fuchs, 1900–1906; Ince, 1959). Using the methods of G. Frobenius (1968) and L. Fuchs (1900–1906), one obtains the fundamental set of solutions at $x = x_0$ of (3.1) as products of $(x - x_0)^r \log^k (x - x_0)$ by a convergent power series at $x = x_0$.

Theorem 3.2. (Frobenius, 1968; Fuchs, 1900–1906). *Let* $x = x_0$ *be a regular singularity of (3.1), and let* $r_1, \ldots, r_m$ *be roots of an indicial equation* $P_{x_0}(r) = 0$ *of (3.1) at* $x = x_0$. *Let* $\{r_{1,1}, \ldots, r_{1,k_1}\}, \ldots, \{r_{l,1}, \ldots, r_{l,k_l}\}$ *be* l *blocks of elements of* $\{r_1, \ldots, r_m\}$, $m = k_1 + \cdots + k_l$, *such that in each block* $\{r_{i,1}, \ldots, r_{i,k_i}\}$ *elements are equivalent*

(mod $\mathbb{Z}$) *and elements of different blocks are nonequivalent* (mod $\mathbb{Z}$), *i.e.*, $r_{i,p} - r_{j,q} \in \mathbb{Z}$ *if and only if* $i = j$ *for* $p = 1, \ldots, k_i$; $q = 1, \ldots, k_j$. *Let the order of* $r_1, \ldots, r_m$ *be chosen in such a way that* $r_{i,1} \geq \cdots \geq r_{i,k_i}$: $i = 1, \ldots, l$. *Then there exists a fundamental system of solutions of* (3.1) *having the form*

$$y_{i,p}(x) = (x - x_0)^{r_{i,p}} u_{i,p}^p(x) + (x - x_0)^{r_{i,p+1}} \cdot \log(x - x_0) \cdot u_{i,p+1}^p(x) + \cdots + (x - x_0)^{r_{i,k_i}} \log^{k_i - p}(x - x_0) \cdot u_{i,k_i}^p(x), \tag{3.3}$$

where $u_{i,q}^p(x)$ *are analytic functions at* $x = x_0$: $p \leq q \leq k_i$; $p = 1, \ldots, k_i$; $i = 1, \ldots, l$.

The origin of the partition of $\{r_1, \ldots, r_m\}$ into blocks is connected with the normal form of the monodromy matrix of the system of (3.1) at $x = x_0$ (Lappo-Danilevski, 1953; Markus, 1959–1960). Exactly, let $\mathbf{y}(x) = (y_1(x), \ldots, y_m(x))$ be the fundamental system of solutions of (3.1). We consider now any simple closed contour γ surrounding x_0, and not containing any singularity of (3.1) other than x_0. Let the system of functions $\mathbf{Y}(x) = (Y_1(x), \ldots, Y_m(x))$ be the result of the analytic continuation of $\mathbf{y}(x)$ after x has described the circuit γ. Since the coefficients $a_j(x) : j = 0, \ldots, m - 1$ are unaltered by the description of the circuit γ (they are rational functions), Eq. (3.1) is unchanged. Thus $\mathbf{Y}(x)$ is expressed in terms of $\mathbf{y}(x)$:

$$\mathbf{Y}(x)^t = V_\gamma \cdot \mathbf{y}(x)^t. \tag{3.4}$$

Following from (3.2) and (3.4) is the well-known (Ince, 1959; Fuchs, 1900–1906; G. V. Chudnovsky, 1980b) relationship between the roots r_j of the indicial equation (3.1) at $x = x_0$ and the eigenvalues μ_j of the (local) monodromy matrix V_γ in (3.4):

$$\mu_j = e^{2\pi\sqrt{-1}r_j} : j = 1, \ldots, m, \tag{3.5}$$

Now let the canonical Jordan form of the monodromy matrix V_γ be the matrix

$$S_\gamma V_\gamma S_\gamma^{-1} = \begin{pmatrix} J_{\lambda_1} & & 0 \\ & \ddots & \\ 0 & & J_{\lambda_l} \end{pmatrix},$$

where J_{λ_i} is a Jordan block corresponding to the eigenvalue λ_i of size $k_i : i = 1, \ldots, l$ and $k_1 + \cdots + k_l = m$. Then the Fuchs–Hamberger rule (Forsyth, 1959; Fuchs, 1900–1906; G. V. Chudnovsky, 1980 a) $\{r_1, \ldots, r_m\}$ of the indicial equation of (3.1) at $x = x_0$ are divided into l

groups corresponding to l Jordan blocks J_{λ_i} of $S_\gamma V_\gamma S_\gamma^{-1}$ according to the formula

$$\lambda_i = e^{2\pi\sqrt{-1}r_{i,p}} : p = 1, \ldots, k_i; i = 1, \ldots, l. \tag{3.6}$$

That is, in each group $\{r_{i,1}, \ldots, r_{i,k_i}\}$ of k_i roots of an indicial equation at $x = x_0$, roots differ by integers.

As we mentioned in Section 2, there is an analytic characteristic of a regular singularity of Eq. (3.1) due to L. Fuchs (1900–1906):

PROPOSITION 3.3. *Equation (3.1) has a regular singularity at $x = x_0$ if and only if all its solutions are at most regular singular at $x = x_0$ and if and only if $a_i(x) = (x - x_0)^{-(m-i)} \times p_i(x)$ for $p_i(x)$ analytic at $x = x_0 : i = 0, \ldots, m - 1$.*

Linear differential equations (3.1) having only regular singularities in the extended x-plane $\mathbb{CP}^1$ (including $x = \infty$ with a local parameter $1/x$ instead of $x - x_0$ at a finite x_0) are called *Fuchsian*. Their characterization was presented in Proposition 2.3. According to this proposition (Ince, 1959; G. V. Chudnovsky, 1980a; Forsyth, 1959; Fuchs, 1900–1906), Fuchsian linear differential equations of order n have the form

$$\frac{d^m y}{dx^m} + \frac{P_{m-1}(x)}{P(x)} \cdot \frac{d^{m-1}y}{dx^{m-1}} + \cdots + \frac{P_1(x)}{P(x)^{m-1}} \cdot \frac{dy}{dx} + \frac{P_0(x)}{P(x)^m} y = 0, \tag{3.7}$$

where $P(x) = \prod_{j=1}^{l} (x - a_j)$ is a polynomial without multiple roots, and $P_i(x)$ are polynomials of degrees at most $(m - i)(k - 1) : i = 0, \ldots, m - 1$.

Now we make a few remarks about the local monodromy of Fuchsian linear differential equations. Due to the form (3.3) of the fundamental system of solutions of (3.1), we call the roots $\{r_1, \ldots, r_n\}$ of the indicial equation of (3.1) at $x = x_0$ *local exponents* of (3.1) corresponding to $x = x_0$ that are independent of the choice of the fundamental solution of (3.1).

We have the set of *all* singularities of (3.7) as the set $\{a_0, \ldots, a_k\}$, possibly including ∞. If

$$\frac{P_{m-i}(x)}{P(x)^i} = \sum_{s=1}^{k} \frac{P_{i,s}}{(x - a_s)^i} + \frac{Q_i'(x)}{P(x)^{i-1}} : i = 1, \ldots, m,$$

then the indicial equation corresponding to $x = a_s$ has the form

$$(r)_m + \sum_{i=1}^{m} P_{is}(r)_{m-i} = 0,$$

where $(r)_k = r \ldots (r - k + 1)$. We denote by $\alpha_i^{(a_s)} : i = 1, \ldots, m$ local exponents of (3.7) at $x = a_s : s = 1, \ldots, l$, and by $\alpha_i^{(\infty)} : i = 1, \ldots, m$

the local exponents of (3.7) at $x = \infty$ (with the local parameter $1/x$ for a large x). Then we have

$$P_{1s} - \frac{n(n-1)}{2} = -\sum_{i=1}^{m} \alpha_i^{(a_s)} : s = 1, \ldots, k$$

and

$$\sum_{s=1}^{k} P_{1s} - \frac{n(n-1)}{2} = \sum_{i=1}^{m} \alpha_i^{(\infty)}.$$

COROLLARY 3.4. *The total sum of all local exponents of (3.7) corresponding to all singularities at* $\mathbb{CP}^1$ *is* $(k-1) \cdot (m(m-1)/2)$:

$$\sum_{s=1}^{k} \sum_{i=1}^{m} \alpha_i^{(a_s)} + \sum_{i=1}^{m} \alpha_i^{(\infty)} = (k-1) \cdot \frac{m(m-1)}{2}. \tag{3.8}$$

Identity (3.8) is called the Fuchs identity, and has many nontrivial consequences (cf. G. V. Chudnovsky, 1980b; Chudnovsky and Chudnovsky, 1983) in number theory and quantum field theory, because it is the only algebraic identity relating various accessory parameters of Fuchsian equations (3.7). We suggest using the Fuchs identity (3.8) as a necessary check of any implementation that computes local exponents of Fuchsian equations.

ACKNOWLEDGMENTS

We thank R. Jenks, B. Trager, B. Sutor, and other members of the Computer Algebra Group at the T. J. Watson Research Center (IBM) for their help and support. We thank J. Traub and H. Wozniakowski for their advice and interest.

REFERENCES

BJÖRK, J. -E. (1979), "Rings of Differential Operators," North-Holland Mathematical Library Series, North-Holland, Amsterdam.

BRENT, R. P., AND KUNG, H. T. (1978), Fast algorithms for manipulating formal power series, *J. Assoc. Comput. Mach.* **25,** 581–595.

BRENT, R. P., AND TRAUB, J. F. (1980), On the complexity of composition and generalized composition of power series, *SIAM J. Comput.* **9,** 54–66.

CHUDNOVSKY, D. V. (1980), Riemann monodromy problem, isomonodromy deformation equations and completely integrable systems (Cargese Lectures, July 1979), *in* "Bifurcation Phenomena in Mathematical Physics and Related Topics," pp. 385–447, Riedel, Boston.

CHUDNOVSKY, G. V. (1980a), Rational and Padé approximations to solutions of linear differential equations and the monodromy theory (Les Houches Lectures, September 1979), *in* "Proceedings, Les Houches International Colloquium on Complex Analysis and Relativistic Quantum Field Theory," pp.136–169, Lecture Notes in Physics, Vol. 126, Springer–Verlag, New York.

CHUDNOVSKY, G. V. (1980b), Padé approximations and the Riemann monodromy problems (Cargese Lectures, June 1979), *in* "Bifurcation Phenomena in Mathematical Physics," pp. 448–510, Riedel, Boston.

CHUDNOVSKY, G. V. (1983), Number theoretic applications of polynomials with rational coefficients defined by extremality conditions, *in* "Arithmetic and Geometry," pp. 67–107, Progress in Mathematics, Vol. 35, Birkhauser, Boston.

CHUDNOVSKY, D. V., AND CHUDNOVSKY, G. V. (1983), "The Wronskian Formalism for Linear Differential Equations. The Effectivization of Roth's and Schmidt's Theorem," IBM Research Report RC9864 (No. 93707), March 3.

CHUDNOVSKY, D. V., AND CHUDNOVSKY, G. V. (1984a), The Wronskian formalism for linear differential equations and Padé approximations, *Adv. in Math.* **53,** 28–54.

CHUDNOVSKY, D. V., AND CHUDNOVSKY, G. V. (1984b), "p-Adic Properties of Linear Differential Equations and Abelian Integrals," IBM Research Report RC10645 (No. 47741), July 26.

CHUDNOVSKY, D. V., AND CHUDNOVSKY, G. V. (1985a), Padé approximations and diophantine geometry, *Proc. Nat. Acad. Sci. U.S.A.* **82,** 2212–2216.

CHUDNOVSKY, D. V., AND CHUDNOVSKY, G. V. (1985b) "Applications of Padé Approximations to the Grothendieck Conjecture on Linear Differential Equations," IBM Research Report RC 11121 (No. 49938), April 19; *in* "Proceedings, New York Number Theory Seminar," pp. 85–167, Lecture Notes in Mathematics, Vol. 1135, Springer–Verlag, New York.

CHUDNOVSKY, D. V., AND CHUDNOVSKY, G. V. (1985c), "Sequences of Numbers Generated by Addition in Formal Groups and New Primality and Factorization Tests," IBM Research Report, CR11262 (No. 50739), July 12; *Adv. in Math.* **7,** 187–237.

CHUDNOVSKY, D. V., AND CHUDNOVSKY, G. V. (1987), On expansion of algebraic functions in power and Puiseux series, II, *J. Complexity* **3,** in press.

DELIGNE, P. (1970), "Equations differentielles à points singuliers reguliers," Lecture Notes in Mathematics, Vol. 163, Springer–Verlag, New York.

FORSYTH, A. R. (1959), "Theory of Differential Equations," Vols. I–VI, reprint, Dover, New York.

FROBENIUS, F. G. (1968), "Gesammelte Abhandlungen," Bd. 1, Springer–Verlag, New York.

FUCHS, L. (1900–1906) "Gesammelte mathematische Werke," Bd. 1–3, Berlin.

INCE, I. L. (1959), "Ordinary Differential Equations," Dover, New York.

KAPLANSKY, I. (1957), "An Introduction to Differential Algebra," Hermann, Paris.

KASHIWARA, M. AND KAWAI, T. (1979), *in* "Seminar on Micro-Local Analysis," Princeton Univ. Press, Princeton, N. J.

KNUTH, D. E. (1981), "The Art of Computer Programming," 2nd ed., Vol. 2, Addison–Wesley, Reading, Mass.

KOLCHIN, E. R. (1973), "Differential Algebra and Algebraic Groups," Academic Press, New York.

KUNG, H. T., AND TRAUB, J. F. (1978), All algebraic functions can be computed fast, *J. Assoc. Comput. Mach.* **25,** 245–260.

LAPPO-DANILEVSKI, J. A. (1953), "Mémoires sur la théorie des systèmes des équations différentielles linéaires," Chelsea, New York.

MARKUS, L. (1959–1960), Group theory and differential equations, Lecture notes, University of Minnesota.

NILSSON, N. (1963–1965), Some growth and ramification properties of certain integrals on algebraic manifolds, *Ark. Mat.* **5,** 527–540.

SIEGEL, C. L. (1966), *in* "Gesammelte Abhandlungen," Vol. 3, pp. 178–187, Springer–Verlag, New York.

WALKER, R. J. (1950), "Algebraic Curves," Princeton Univ. Press, Princeton, N. J.