- Zeroness of solutions of hierarchical ADEs.
- no complexity is given

TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 336, Number 1, March 1993

ZERO-EQUIVALENCE IN FUNCTION FIELDS DEFINED BY ALGEBRAIC DIFFERENTIAL EQUATIONS

JOHN SHACKELL

ABSTRACT. We consider function fields obtained as towers over the field of rational functions, each extension being by a solution of an algebraic differential equation. On the assumption that an oracle exists for the constants, we present two algorithms for determining whether a given expression is functionally equivalent to zero in such a field. The first, which uses Gröbner bases, has the advantage of theoretical simplicity, but is liable to involve unnecessary computations. The second method is designed with a view to eliminating these.

1. INTRODUCTION

If we wish to perform symbolic computations involving transcendental functions there is a fundamental problem to be faced. Our object of study will be a domain, R, of functions, but it is not possible to compute directly with functions since they are abstract entities. We therefore need a domain Φ, consisting of expressions which represent the functions in R and a homomorphism $\rho: \Phi \to R$. In some cases, for example when R consists of elementary functions, suitable expressions are supplied by standard mathematical notation and there is no difficulty in extending this to cover the other cases. The problem lies in the fact that, trivial cases apart, ρ is not injective.

Such a situation is not uncommon in mathematics and would be of no great consequence here if we had sufficient knowledge of the kernel of ρ. Ideally we would like a set of representatives for the residue classes in $\Phi/\ker\rho$, and a good algorithm for finding the representative equivalent to a given element. This should be particularly simple for sums, products, quotients and functional composites of representatives. In other words we would like a *canonical simplifier* with good algebraic properties; see [6, 23, 8, 12].

Unfortunately no canonical simplifiers are known for the majority of function fields. A lesser requirement, and if we claim to compute with functions at all rather than representatives, a minimal one, is an algorithm to decide when a given element of Φ belongs to the kernel of ρ. Finding such an algorithm constitutes the problem of *zero-equivalence*.[1]

Received by the editors May 31, 1989 and, in revised form, November 30, 1990.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 68C20, 13N05.
Key words and phrases. Zero equivalence, functional equivalence, symbolic computation, computer algebra.

[1]Theoretically a zero-equivalence algorithm gives a canonical simplifier, but not generally one that is of any use [6].

One approach to zero-equivalence is derived from Hardy's work on asymptotic growth [15]. Hardy considered the function field generated from the functions x, $\exp(x)$ and $\log(x)$ by arithmetic operations and functional composition. He showed that a nonzero element of this field can have only a finite number of real zeros and hence such elements must tend either to infinity, minus infinity, or a finite limit. Richardson [27], and independently Macintyre [19], showed how to bound the number of zeros. Then if the given expression is found to vanish at more points than the bound allows it must be identically zero. As a zero-equivalence algorithm, such a procedure has a number of drawbacks both theoretical and practical. The practical problems are firstly that the number of evaluation points needed may be very large. Secondly the methods given by Richardson and Macintyre involve differentiating the given expression to a potentially high order. Since expressions involving transcendental functions generally grow very rapidly under repeated differentiation, these objections mean that the methods can only be considered practical for very simple expressions.

The theoretical problem, which is also a practical one, is that evaluation of an expression at a point requires a method of determining whether a constant is zero. This is clearly necessary anyway, since an algorithm to decide zero-equivalence must in particular be applicable to constant expressions. This *constants problem* is related to some old unsolved problems in transcendental number theory [1, 17, 7, 9] and looks very difficult. For this reason much of the existing work on zero-equivalence in transcendental function fields has proceeded from the (quite unwarranted) assumption that an oracle exists for the constants. We shall henceforth adopt this standpoint here, but the point should be made that because of the greater generality, this involves a somewhat larger assumption in our case. In particular, if the function field is generated by logarithms and exponentials only, constants may be dealt with by assuming the Schanuel conjecture, [17, 9]. This may be stated as follows:

> Let $\alpha_1, \ldots, \alpha_n$ be complex numbers which are linearly independent over the rational numbers, $\mathbf{Q}$. Then the field $\mathbf{Q}(\alpha_1, \ldots, \alpha_n, e^{\alpha_1}, \ldots, e^{\alpha_n})$ has transcendence degree at least n.

However we can hardly take refuge in such a conjecture here, and this leaves very much open the question of how one might deal with constants in practice; this point is discussed further in [31]. In connection with the constants problem see also [3, 12, 16, 20, 22, 25].

A second approach to functional equivalence (i.e., zero-equivalence in function fields) is founded on differential algebra. The idea is to determine the algebraic dependencies between the various (apparently) transcendental functions using the Risch Theorem or its generalisation due to Rothstein and Caviness. These techniques can be applied to fields built (via arithmetic operations and functional composition) using trigonometric functions, exponentials, and logarithms. With the Rothstein-Caviness theorem, it is also possible to include integration as a field-building operation, although there may be practical difficulties in some cases. For further details see [29, 7, 24].

These methods were developed primarily in connection with symbolic integration and there it is indeed necessary to know the algebraic dependencies

between functions. But to decide functional equivalence one does not need to know whether *there exist* polynomials in the given terms which are equivalent to zero, but merely whether this is true of the particular polynomial under consideration. From this viewpoint zero-equivalence should be an easier problem than integration in finite terms; the distinction between the two is somewhat akin to that between nondeterministic and deterministic algorithms in the theory of NP completeness [14]. In this paper we capitalise on the advantage by working directly with the given expression, rather than trying to determine algebraic dependencies.

Transcendental functions are specified by differential equations of the form

$$y^{(n)} = \frac{\tilde{\Lambda}(y, y', \ldots, y^{(n-1)})}{\tilde{\Omega}(y, y', \ldots, y^{(n-1)})}, \tag{1}$$

where $\tilde{\Lambda}$ and $\tilde{\Omega}$ are polynomials whose coefficients may contain other 'simpler' transcendental functions, and by initial conditions of the form $y(x_0) = c_0$, $y'(x_0) = c_1, \ldots, y^{(n-1)}(x_0) = c_{n-1}$. In this way we are able to handle towers of function fields with each new level of extension being by a function defined as a solution of an algebraic differential equation with coefficients in the existing field. In fact one does not gain any generality by taking coefficients in the field below, since the top-level functions must themselves satisfy an algebraic differential equation over $\mathbf{K}[x]$, where $\mathbf{K}$ is the field of constants. To see this, first note that y satisfies an algebraic differential equation over a field $\mathbf{F}$ if and only if the transcendence degree of $\mathbf{F}(y, y', \ldots)$ over $\mathbf{F}$ is finite. If this holds and in addition $\mathbf{F}(y, y', \ldots, z, z', \ldots)$ is of finite transcendence degree over $\mathbf{F}(y, y', \ldots)$ then $\mathbf{F}(y, y', \ldots, z, z', \ldots)$ is of finite transcendence degree over $\mathbf{F}$ (see [34, Chapter II]), and hence z satisfies an algebraic differential equation over $\mathbf{F}$.[2] However, it is nonetheless important to give the algorithm in terms of towers of extensions, since this fits in with the way in which expressions are generally encountered.

In fact we work with differential equations of first degree but this does not restrict the class of functions. This is because a solution of an algebraic differential equation of order n satisfies the first degree equation of order $n+1$ obtained by differentiating the former. In some cases at least, this is a more natural way of specifying the function. For example the sine function is more usually specified by the equation $y'' + y = 0$ than by $(y')^2 + y^2 = 1$. The device of differentiating to obtain a first-degree equation is also used to handle algebraic extensions.

In fact the theoretical existence of an algorithm for determining zero-equivalence in towers of function fields defined by algebraic differential equations has already been established by Denef and Lipshitz in [11] (see also [10]). However these authors were not concerned with obtaining practical algorithms. Their method would seem to require (among other things) factorization of a potentially large number of multivariate polynomials.

In some cases functional equivalence is well known to be undecidable. Let R_2 be the field generated by arithmetic operations and functional composition from the constants 1 and π, the variable x and the functions abs and sin. Then zero-equivalence in R_2 is recursively undecidable [8, 28]. It would be

[2] I am grateful to Chris Woodcock for drawing my attention to this argument.

nice to be able to contrast the situation in R_2, which has a single nondifferentiable function in its generating set, with that in the fields we shall be discussing in subsequent sections, but it may be that the constants problem is undecidable in both cases. However, the addition of the modulus function cannot be responsible for the undecidability of constants, for as pointed out in [27], if a constant is known to be nonzero, its sign may be determined by successive approximation. Then, if we can decide zero-equivalence of constant expressions which do not contain modulus signs, we can tackle those which do by successively removing the innermost modulus signs, having determined the sign of the expression they bound; cf. a similar argument, in a slightly different context, in [30]. It follows from this, that if the constants problem in R_2 is undecidable, then the Schanuel conjecture is false. This would be established if we could show how to decide functional equivalence in R_2 modulo constants, but none of the available methods seem applicable to this case.

In §2, we define the towers of extensions and the homomorphisms between them. In §3, we give a zero-equivalence algorithm in terms of Gröbner bases. However, the method has the drawback of requiring a relatively large number of differentiations and corresponding basis computations. In the next section, we give a sketch treatment of a more efficient 'gcd'-method applicable to the case when all the extensions are by first-order differential equations. Full details of this are given in [31]. A related, but slightly different treatment of this case is given in [26]. Also some similar ideas were used independently by F. Ulmer in [33].

The main results of the paper occur in §§5 and 6, where the first-order results of the previous section are generalised to higher orders. Theorem 3 allows us to identify factors in the given expression of the form $y - h$ where y defines the current extension and h satisfies the differential equation for y. Theorem 4 then gives a method of checking whether any such h also satisfies the initial conditions in the specification of y. These two results, together with Theorem 5 which generalises Theorem 3, form the bases of the main algorithms of the paper, Algorithms 3 and 4. A worked example illustrating these, is given in §7. Finally, in §8 we briefly consider expressions specified using functional composition, since this often occurs in practice and is catered for in the Richardson and Macintyre methods for example.

A number of people helped in the production of this paper. In particular, the author would like to thank Michael Singer and also Dan Richardson for some very valuable comments. The referee's keen insight helped to eliminate a number of errors and confusions. Also, as so often in the past, the author has benefited from a number of discussions with colleagues at the University of Kent at Canterbury. In particular, Chris Woodcock and John Merriman contributed a number of useful suggestions, and in addition, Tim Hopkins gave invaluable help with the use of the LaTeX document-preparation system.

2. Extension rings

We begin by constructing two towers of differential rings. One tower will contain rings of formal expressions, with the given expression belonging to the top-level ring. The rings of the other tower will contain the corresponding functions. We will also need various intermediate rings and differential homomorphisms.

First some notation. If R is any integral domain, we will denote the ring of polynomials in the indeterminates $a_1, \ldots, a_m$ by $R[a_1, \ldots, a_m]$. Its quotient field will be denoted by $R(a_1, \ldots, a_m)$. Now let $\mathbf{K}$ be any subfield of the field, $\mathbf{C}$, of complex numbers (e.g. $\mathbf{K}$ might be the rational number field) and let x_0 be a fixed element of $\mathbf{K}$. For $i = 0, \ldots, N$, we define recursively, differential rings Φ_i and R_i, and a differential epimorphism ρ_i. The elements of Φ_i will be formal expressions, and those of R_i the corresponding functions. The map ρ_i will take a formal expression to the function it represents.

Let Φ_0 be the formal polynomial ring $\mathbf{K}[x]$ and let R_0 be the ring of complex-valued polynomial functions with coefficients in $\mathbf{K}$. Let $\rho_0 \colon \Phi_0 \to R_0$ be the map which when applied to a formal expression gives the corresponding function (syntactically ρ_0 is the identity). Note that Φ_0 and R_0 are differential rings, with the obvious differentiation, and that ρ_0 is a differential isomorphism.

Now suppose that Φ_{i-1}, R_{i-1}, and ρ_{i-1} have been defined. Let n_i be a given positive integer (in fact n_i will be the order of the differential equation one of whose solutions defines the extension from R_{i-1} to R_i) and let

$$\tilde{\rho}_{i-1} \colon \Phi_{i-1}[y_i, y_i', \ldots, y_i^{(n_i-1)}] \to R_{i-1}[y_i, y_i', \ldots, y_i^{(n_i-1)}]$$

be the homomorphism obtained by applying ρ_{i-1} to the coefficients of polynomials in $\Phi_{i-1}[y_i, y_i', \ldots, y_i^{(n_i-1)}]$. We shall frequently write $\tilde{P}$ for the image of P under $\tilde{\rho}_{i-1}$. Denote the quotient field of R_{i-1} by F_{i-1} and let $c_{i,0}, c_{i,1}, \ldots, c_{i,n_i-1}$ be constant elements of F_{i-1}. Let $\chi_i \colon R_{i-1}[y_i, y_i', \ldots, y_i^{(n_i-1)}] \to F_{i-1} \cap \mathbf{C}$ be the homomorphism defined by the substitutions $x = x_0$, $y_i = c_{i,0}$, $y_i' = c_{i,1}, \ldots, y_i^{(n_i-1)} = c_{i,n_i-1}$.

We are now in a position to give the function which is used to define R_i as an extension of R_{i-1}. Let f_i denote the solution of the differential equation

$$y_i^{(n_i)} = \frac{\tilde{\Lambda}_i(y_i, y_i', \ldots, y_i^{(n_i-1)})}{\tilde{\Omega}(y_i, y_i', \ldots, y_i^{(n_i-1)})}, \tag{2}$$

which satisfies the initial conditions $y_i(x_0) = c_{i,0}$, $y_i'(x_0) = c_{i,1}, \ldots, y_i^{(n_i-1)} = c_{i,n_i-1}$. Here Λ_i and Ω_i are given polynomials in $\Phi_{i-1}[y_i, y_i', \ldots, y_i^{(n_i-1)}]$ such that $\tilde{\Lambda}_i$ and $\tilde{\Omega}_i$ have no common factors and $\chi_i(\tilde{\Omega}_i) \neq 0$. We note that f_i is uniquely specified in this way and is analytic in a neighbourhood of x_0; see, for example [2, Chapter V]. Let Φ_i be the ring obtained from $\Phi_{i-1}[y_i, y_i', \ldots, y_i^{(n_i-1)}]$ by introducing the inverse of Ω_i. In other words, Φ_i is the quotient of $\Phi_{i-1}[y_i, y_i', \ldots, y_i^{(n_i-1)}]$ by the multiplicative system $\{(\Omega_i)^r, r \in \mathbf{N}\}$; see [34, Chapter I]. As will soon be apparent, the negative powers of Ω_i are needed in connection with the differential structure to be defined on Φ_i. Now let R_i be the ring of functions which are polynomials in f_i, its derivatives, and $(\tilde{\Omega}_i(f_i, f_i', \ldots, f_i^{(n_i-1)}))^{-1}$, with coefficients in R_{i-1}. We note that $\tilde{\Omega}_i(f_i, f_i', \ldots, f_i^{(n_i-1)})$ does not have a zero at x_0 since $\chi_i(\tilde{\Omega}_i) \neq 0$. We use Υ_i to denote the quotient of $R_{i-1}[y_i, y_i', \ldots, y_i^{(n_i-1)}]$ by the multiplicative system $\{(\tilde{\Omega}_i)^r, r \in \mathbf{N}\}$. The map $\tilde{\rho}_{i-1}$ induces a homomorphism $\mu_i \colon \Phi_i \to \Upsilon_i$. Specifically, if $z \in \Phi_i$ we may write z in the form

$$z = z_0 + z_1/\Omega_i + \cdots + z_k/(\Omega_i)^k,$$

where $z_0, z_1, \ldots, z_k \in \Phi_{i-1}[y_i, y_i', \ldots, y_i^{(n_i-1)}]$. Then

$$\mu_i(z) = \tilde{z}_0 + \tilde{z}_1/\tilde{\Omega}_i + \cdots + \tilde{z}_k/(\tilde{\Omega}_i)^k .$$

Next we let $\nu_i\colon \Upsilon_i \to R_i$ be the homomorphism generated by substituting f_i and its derivatives for the formal parameters $y_i, y_i', \ldots, y_i^{(n_i-1)}$. Then $\rho_i\colon \Phi_i \to R_i$ is defined as $\rho_i = \nu_i \circ \mu_i$.

Our next task is to introduce the differential structure on the rings we have just defined. On R_i, the derivation is just normal differentiation with respect to x. Let $\lambda \in \Phi_{i-1}[y_i, y_i', \ldots, y_i^{(n_i-1)}]$ and let $\delta\lambda$ denote the polynomial obtained by applying the derivation of Φ_{i-1} to the coefficients of λ. We define

$$\lambda^* = \delta\lambda + \frac{\partial\lambda}{\partial y_i}y_i' + \frac{\partial\lambda}{\partial y_i'}y_i'' + \cdots + \frac{\partial\lambda}{\partial y_i^{(n_i-2)}}y_i^{(n_i-1)} + \frac{\partial\lambda}{\partial y_i^{(n_i-1)}}\frac{\Lambda_i}{\Omega_i}; \tag{3}$$

so $\lambda^* \in \Phi_i$. It is worth noting that this definition is equivalent, in the first-order case, to that of the derivation D in [32], used in connection with a problem on liouvillian first integrals of differential equations. If P is any element of Φ_i, we may regard P as a polynomial in $y_i, y_i', \ldots, y_i^{(n_i-1)}, t$ modulo the ideal generated by $t\Omega_i - 1$. The star derivative of P is then defined to be[3]

$$P^* = \delta P + \frac{\partial P}{\partial y_i}y_i' + \cdots + \frac{\partial P}{\partial y_i^{(n_i-2)}}y_i^{(n_i-1)} + \frac{\partial P}{\partial y_i^{(n_i-1)}}\frac{\Lambda_i}{\Omega_i} - \frac{\partial P}{\partial t}\frac{\Omega_i^*}{\Omega_i^2}. \tag{4}$$

It is easy to see that * is a derivation on Φ_i and that the natural inclusion $\Phi_{i-1} \hookrightarrow \Phi_i$ is a differential monomorphism. Moreover this is also true of $\Phi_{i-1}[y_i, y_i', \ldots, y_i^{(n_i-1)}] \hookrightarrow \Phi_i$, if we regard (3) as defining the derivation on $\Phi_{i-1}[y_i, y_i', \ldots, y_i^{(n_i-1)}]$. Similarly if $T \in R_{i-1}[y_i, y_i', \ldots, y_i^{(n_i-1)}]$, we define

$$T^* = \frac{\partial T}{\partial x} + \frac{\partial T}{\partial y_i}y_i' + \cdots + \frac{\partial T}{\partial y_i^{(n_i-2)}}y_i^{(n_i-1)} + \frac{\partial T}{\partial y_i^{(n_i-1)}}\frac{\tilde{\Lambda}_i}{\tilde{\Omega}_i}, \tag{5}$$

and for $X \in \Upsilon_i$, we let

$$X^* = \frac{\partial X}{\partial x} + \frac{\partial X}{\partial y_i}y_i' + \cdots + \frac{\partial X}{\partial y_i^{(n_i-2)}}y_i^{(n_i-1)} + \frac{\partial X}{\partial y_i^{(n_i-1)}}\frac{\tilde{\Lambda}_i}{\tilde{\Omega}_i} - \frac{\partial X}{\partial t}\frac{\tilde{\Omega}_i^*}{\tilde{\Omega}_i^2}. \tag{6}$$

Then $R_{i-1}[y_i, y_i', \ldots, y_i^{(n_i-1)}]$ and Υ are differential rings and the natural injection $R_{i-1}[y_i, y_i', \ldots, y_i^{(n_i-1)}] \hookrightarrow \Upsilon$ is a differential monomorphism.

Proposition 1. *The maps μ_i, ν_i, and ρ_i are differential ring epimorphisms.*

Proof of Proposition 1. It is trivial that ρ_0 is a differential epimorphism. Suppose then that the statement of the proposition holds when i is replaced by $i-1$. It is clear from the definitions and comparison of (3) with (5) and of (4) with (6), that μ_i is a differential epimorphism. Moreover ν_i is clearly surjective. Thus we need only show that ν_i commutes with the derivations.

Let $X \in \Upsilon$. Then from (6),

$$\nu_i(X^*) = \nu_i\left(\frac{\partial X}{\partial x} + \frac{\partial X}{\partial y_i}y_i' + \cdots + \frac{\partial X}{\partial y_i^{(n_i-2)}}y_i^{(n_i-1)} + \frac{\partial X}{\partial y_i^{(n_i-1)}}\frac{\tilde{\Lambda}_i}{\tilde{\Omega}_i} - \frac{\partial X}{\partial t}\frac{\tilde{\Omega}_i^*}{\tilde{\Omega}_i^2}\right).$$

[3] Strictly speaking P^* is the residue class of the expression on the right of (4).

Since ν_i is a homomorphism, the right side is equal to

$$\nu_i\left(\frac{\partial X}{\partial x}\right)+\sum_{j=0}^{n_i-2}\nu_i\left(\frac{\partial X}{\partial y_i^j}\right)f_i^{j+1}+\nu_i\left(\frac{\partial X}{\partial y_i^{(n_i-1)}}\right)\nu_i\left(\frac{\tilde{\Lambda}_i}{\tilde{\Omega}_i}\right)-\nu_i\left(\frac{\partial X}{\partial t}\frac{\tilde{\Omega}_i^*}{\tilde{\Omega}_i^2}\right).$$

However, since f_i satisfies the differential equation (2), we have $\nu_i(\tilde{\Lambda}_i/\tilde{\Omega}_i)=f_i^{(n_i)}$, and so

$$\nu_i(X^*)=\nu_i\left(\frac{\partial X}{\partial x}\right)+\sum_{j=0}^{n_i-1}\nu_i\left(\frac{\partial X}{\partial y_i^j}\right)f_i^{j+1}-\nu_i\left(\frac{\partial X}{\partial t}\frac{\tilde{\Omega}_i^*}{\tilde{\Omega}_i^2}\right)=\nu_i(X)^*,$$

by the chain rule. The conclusion for ρ_i now follows from that for μ_i and ν_i, and this completes the proof of Proposition 1.

We will also require the following result, which is a straightforward consequence of standard theorems.

Proposition 2. *The rings* Φ_i, R_i, *and* $R_{i-1}[y_i, y_i', \dots, y_i^{(n_i-1)}]$ *are Noetherian.*

Proof of Proposition 2. That $\mathbf{K}[x]$ is Noetherian follows immediately from the Hilbert Basis Theorem [34]. Suppose that Φ_{i-1} is Noetherian. Another application of the Hilbert Basis Theorem shows that $\Phi_{i-1}[y_i, y_i', \dots, y_i^{(n_i-1)}, t]$ is Noetherian. But Φ_i is a homomorphic image of this ring under the quotient map and so, by a standard result [34], must be Noetherian also. Thus, by induction, Φ_i is Noetherian for $i=1,\dots,N$. Since R_i is the homomorphic image of Φ_i by ρ_i, the conclusion follows for R_i and the Hilbert Basis Theorem again gives the result for $R_{i-1}[y_i, y_i', \dots, y_i^{(n_i-1)}]$ also. This completes the proof of Proposition 2.

3. A Gröbner basis algorithm

Suppose that we are given a rational expression in the functions $x, f_1, \dots, f_N$. This may be represented as the quotient of two polynomials each of which belongs to $\Phi_{N-1}[y_N, y_N', \dots, y_N^{(n_N-1)}]$; this ring we identify as a subring of Φ_N. Our task is then to find a suitable algorithm to determine when an element P of $\Phi_{N-1}[y_N, y_N', \dots, y_N^{(n_N-1)}]$ belongs to the kernel of ρ_N. We shall assume that such exists for constant elements of Φ_N and, inductively, for elements of Φ_{N-1}. Since we will have occasion to consider other inductions, we refer to the induction on N as the *outer induction.*

In order to simplify notation, we shall freely drop the subscript N from quantities such as y, Φ, Λ, n, etc. when no risk of confusion arises. In addition we shall use $\tilde{P}$ to stand for the image of P under μ; since μ and $\tilde{\rho}_{N-1}$ agree on $\Phi_{N-1}[y, y', \dots, y^{(n-1)}]$, this may be regarded as an extension of our previous convention. Finally, we write P^{*i} to denote the ith star derivative of P, and take this to be P itself in the case $i=0$.

Theorem 1. *Let* $P\in\Phi$. *If* $\rho(P)=0$ *then* $\chi(\tilde{P}^{*j})=0$ *for every* $j\geq 0$. *Conversely, if for some* $k>0$, $\tilde{P}^{*k}$ *belongs to the ideal in* Υ *generated by* $\tilde{P}, \tilde{P}^*, \dots, \tilde{P}^{*(k-1)}$ *and* $\chi(\tilde{P}^{*j})=0$ *for* $j=0,\dots,k-1$ *then* $\rho(P)=0$.

We note that the existence of such a k follows from Proposition 2.

Proof of Theorem 1. Let $\xi: R \to R \cap \mathbf{C}$ denote the homomorphism defined by the substitution $x = x_0$. It is then easy to see that the map χ factors as $\chi = \xi \circ \nu$. Now if $\rho(P) = 0$ then $\nu(\tilde{P}) = 0$. But ν is a differential homomorphism and hence

$$\chi(\tilde{P}^{*j}) = \xi(\nu(\tilde{P}^{*j})) = \xi((\nu(\tilde{P}))^{*j}) = 0.$$

Now suppose that $\tilde{P}^{*k} = \sum_{j=0}^{k-1} A_j \tilde{P}^{*j}$ with $A_j \in \Upsilon$ for $j = 0, \ldots, k-1$. On applying ν to this equation, we see that $Z = \nu(\tilde{P})$ satisfies the differential equation $Z^{(k)} = \sum_{j=0}^{k-1} \nu(A_j) Z^{(j)}$. If in addition $\chi(\tilde{P}^{*j}) = 0$ for $j = 0, \ldots, k-1$ then $\nu(\tilde{P})$ also satisfies the initial conditions $Z(x_0) = Z'(x_0) = \cdots = Z^{(k-1)}(x_0) = 0$. Since the elements of R are analytic at x_0, the uniqueness theorem for differential equations, [2], then implies that $\rho(P) = \nu(\tilde{P}) = 0$. This completes the proof of Theorem 1.

Theorem 1 will give an algorithm for deciding when $\rho(P)$ is zero once we have a method of determining when $\tilde{P}^{*k}$ belongs to the ideal generated by $\tilde{P}, \ldots, \tilde{P}^{*(k-1)}$. Problems of this type have been much studied and several methods are known [5, 18, 21, 23]. We shall give our algorithm in terms of Gröbner bases [5]. The Gröbner-basis calculations will be carried out in the ring Φ but the decisions as to whether to continue them or not are effectively taken in $R_{N-1}[y_N, y_N', \ldots, y_N^{(n_N-1)}]$. We shall use similar ideas elsewhere in the paper. The general principle is that where a computation in Φ requires only ring operations and decisions as to whether coefficients are zero, the ring calculations in Φ transfer via the homomorphism $\tilde{\rho}_{N-1}$ to $R_{N-1}[y_N, y_N', \ldots, y_N^{(n_N-1)}]$ and the decisions about the zero-equivalence of coefficients can effectively be taken in $R_{N-1}[y_N, y_N', \ldots, y_N^{(n_N-1)}]$, since by induction we can decide when elements of Φ_{N-1} belong to the kernel of ρ_{N-1}. In the present instance, suppose that P^{*j} is equal to Q_j modulo the ideal generated by $P, \ldots, P^{*(j-1)}$. By induction, we can decide whether $\tilde{Q}_j = \tilde{\rho}_{N-1}(Q_j)$ is zero. If it is, then $\tilde{P}^{*j}$ belongs to the ideal generated by $\tilde{P}, \ldots, \tilde{P}^{*(j-1)}$ since $\tilde{\rho}_{N-1}$ is a differential homomorphism.

Algorithm 1. *Given an element P of Φ, we must decide whether $\rho(P) = 0$.*

1. *Determine whether $\chi(\tilde{P}) = 0$. If not, then $\rho(P) \neq 0$. Otherwise let G_0 be the Gröbner basis consisting of the single polynomial P. Then carry out the procedure given below, for successive values of $j = 1, 2, \ldots$ until it is resolved whether or not $\rho(P) = 0$.*

2. *Compute P^{*j} and determine whether $\chi(\tilde{P}^{*j}) = 0$. If not then $\rho(P) \neq 0$. Otherwise reduce P^{*j} with respect to the Gröbner basis G_{j-1}, obtaining Q_j say. If $\tilde{Q}_j$ is the zero polynomial then $\rho(P) = 0$. If not, compute a reduced Gröbner basis for the ideal generated by G_{j-1} and P^{*j} and call the new basis G_j. Replace j by $j+1$ and repeat 2.*

One or two points still need to be made regarding the algorithm. Firstly, for the purpose of calculating Gröbner basis we identify Φ with the ring

$$\mathbf{K}[y_N^{(n_N-1)}, y_N^{(n_N-2)}, \ldots, y_N, y_{N-1}^{(n_{N-1}-1)}, \ldots, y_{N-1}, \ldots, y_1^{(n_1-1)}, \ldots, y_1]$$

and use a pure lexicographic order (i.e., $y_1 < \cdots < y_1^{(n_1-1)} < \cdots < y_N^{(n_N-1)}$). Secondly, we note that the termination of the algorithm follows from the fact

that Φ is Noetherian. Moreover if we find that $\widetilde{Q}_j = 0$, we will already have that $\chi(\widetilde{P}) = \chi(\widetilde{P}') = \cdots = \chi(\widetilde{P}^{(j-1)}) = 0$, and Theorem 1 then implies that $\rho(P) = 0$. Finally, it is necessary that differentiations be carried out in Φ rather than in $R_{N-1}[y, y', \ldots, y^{(n-1)}]$. In practice this means that the derivatives of y_i with $i < N$, which will be generated in the coefficients, must be identified as such, and not as new functions. Otherwise the possibility of nonterminating loops is introduced.

From a theoretical point of view, Algorithm 1 does all that is required. In practice however, the number of differentiations needed may be very large, and as already pointed out in connection with the methods of Richardson and Macintyre, this is likely to result in rapid growth in the size of the expression. One can alleviate the problem to some extent by reducing P^{*i} modulo G_i before applying the next star derivation. However consider the case when $P = (y - e^{x^2})(e^x + x^M)$, with $M > 0$, and y is defined by $y' = 2xy$, $y(0) = 1$. Even though it is obvious on inspection that $\rho(P) = 0$, Algorithm 1 will require $M+2$ differentiations, essentially because no derivative of the second factor of P before that of order $(M+2)$ is in the ideal generated by the previous derivatives. Yet this calculation is generated by a factor which is not involved in the vanishing of $\rho(P)$. The answer to the dilemma is to use a gcd algorithm. In the next section, we investigate this in the case when all the defining differential equations are of first order.

4. The first-order case

Full details of the algorithm presented in this section are covered in [31], so we give here a sketch treatment for the purposes of comparison with Algorithm 1, and of introducing the methods of the following sections.

Recall that we are assuming that, in equation (2), $n_i = 1$ for all i. We denote the algebraic closure of a ring Σ by Σ_{alg}. Note that if Σ is a differential ring, the derivation may be extended to Σ_{alg} [34]. For $Q \in \Upsilon$, we write $\pi(Q)$ for the polynomial $(\widetilde{\Omega})^r Q$, where r is the highest power of $(\widetilde{\Omega})^{-1}$ appearing in Q; so in the general case $\pi(Q) \in R_{i-1}[y_i, y_i', \ldots, y_i^{(n_i-1)}]$. Of course, $\nu(\widetilde{\Omega}) \neq 0$, and if we want to decide if $\nu(Q) = 0$, it suffices to consider $\pi(Q)$. The first-order algorithm is based on the following result.

Theorem 2. *Let $\widetilde{P}$ be a square-free element of $\widetilde{R}_{N-1}[y]$ and let g denote the gcd of $\widetilde{P}$ and $\pi(\widetilde{P}^*)$. If g contains a factor $y - h$, where $h \in (R_{N-1})_{\text{alg}}$, then h satisfies the equation*

$$y' = \widetilde{\Lambda}/\widetilde{\Omega}. \tag{7}$$

Conversely if h satisfies this equation and $\widetilde{P}(h) = 0$, then $y - h$ divides g.

The proof of this result (in a slightly different notation) is given in [31]; moreover a generalization will be proved in the next section. Theorem 2 allows us to remove 'extraneous' factors, such as $(e^x + x^M)$ in the above example, from P, by taking the gcd of $\widetilde{P}$ and $\pi(\widetilde{P}^*)$. This yields the following.

Algorithm 2. *To determine whether $\rho(P) = 0$, we proceed as follows:*

1. *Check that $\chi(\widetilde{P}) = 0$; if not, then $\rho(P) \neq 0$.*

2. *Check that* $\widetilde{P}$ *is not the zero polynomial. Assuming it is not, compute the gcd of* $\widetilde{P}$ *and* $\partial\widetilde{P}/\partial y$ *and divide it into* $\widetilde{P}$ *to make the latter square free.*

3. *Compute* $g = \gcd(\widetilde{P}, \pi(\widetilde{P}^*))$. *If* g *is independent of* y, *or if* $\chi(g) \neq 0$, *then* $\rho(P) \neq 0$.

4. *Otherwise substitute* $x = x_0$ *in* g *leaving* y *as an indeterminate. If this reduces* g *to the zero polynomial, keep differentiating partially with respect to* x *until this substitution no longer gives the zero polynomial. At this stage, substitute* $y = c_0$ *in addition to* $x = x_0$. *This will give zero if and only if* $\rho(P) = 0$.

One point to be made is that, to obtain g, the gcd computations are carried out in the ring Φ and remainders checked to see whether they reduce to zero under the map $\tilde{\rho}_{N-1}$. Similar remarks apply to the gcd calculations in stage 2. This matter is treated more fully in the next section; see in particular Subalgorithm 1. The reason for taking derivatives at stage 4, is that each coefficient of $\widetilde{P}$ might contain a factor which vanishes at x_0. This cannot be entirely avoided by removing common factors from coefficients since, for example, one term may contain a factor $x - x_0$ and another $\sin(x - x_0)$.

If we apply Algorithm 2 to the example $\widetilde{P} = (y - e^{x^2})(e^x + x^M)$, we need only one partial differentiation, one star derivation, two gcd computations and one set of substitutions. This compares very favourably with the $M+2$ differentiations and their associated Gröbner-basis calculations and substitutions required by Algorithm 1. The gain is not always so good; if $\widetilde{P}$ happens to be of the form $\prod_{j=1}^{k}(y - h_j)$ with each h_j satisfying the equation (7), then $g = \widetilde{P}$. Even here Algorithm 2 has the advantage of avoiding the Gröbner-basis calculations however.

5. Higher-order extensions

In this section, we consider towers of extentions of $\mathbf{K}[x]$ defined by higher order differential equations. Here we use a second *inner* induction within the outer induction.

Suppose then that $P \in \Phi_{N-1}[y, y', \ldots, y^{(n-1)}]$, as in §3. The inner induction is on the number s where $y^{(s)}$ is the highest derivative that actually appears in P. We consider first the case when $s = 0$. Although, as we shall see, there is a sense in which this is very nearly the general case, we do need to consider the case when $s > 0$. This is so even when the P in question contains no derivatives of y_i's, because our method involves taking star derivatives, and this introduces derivatives of the y_i, $i < N$, into coefficients. Thus the case $s > 0$ appears at the next depth of recursion.

For the moment however, let $P \in \Phi_{N-1}[y] \backslash \Phi_{N-1}$. Then for $1 \leq i \leq n-1$, we may write P^{*i} in the form

$$P^{*i} = y^{(i)}\frac{\partial P}{\partial y} + X_i, \tag{8}$$

with $X_i \in \Phi_{N-1}[y, y', \ldots, y^{(i-1)}]$. The equations $P^{*i} = 0$ therefore express $y^{(i)}$ as a quotient of two polynomials in $\Phi_{N-1}[y, y', \ldots, y^{(i-1)}]$. We substitute these expressions to successively eliminate $y^{(n-1)}$ down to y' from P^{*^n}. The justification for doing this is given in the next theorem. If $\check{\Omega}$ denotes the result of similarly eliminating $y^{(n-1)}, \ldots, y'$ from Ω, then the result of eliminating from P^{*^n} may be uniquely written as the quotient of two coprime

polynomials in $\Phi_{N-1}[y]$ with the denominator being a product of $\breve{\Omega}$ and a power of $\partial P/\partial y$. We denote the numerator by $\Xi(P)$, thus defining a map $\Xi\colon \Phi_{N-1}[y] \to \Phi_{N-1}[y]$. The following theorem is the basis of our algorithm for higher-dimensional extensions. It is a generalisation of Theorem 2.

Theorem 3. *Write* $T = \Xi(P)$ *and suppose that* $\widetilde{P}$ *is square free. Let* g *denote the gcd of* $\widetilde{P}$ *and* $\widetilde{T}$. *If* g *contains a factor* $y - h$ *with* $h \in (R_{N-1})_{\text{alg}}$, *then* h *satisfies the differential equation* (1). *Conversely if* h *satisfies* (1) *and* $\widetilde{P}(h) = 0$, *then* $y - h$ *divides* g.

Our proof of Theorem 3 will use the following.

Lemma 1. *Suppose* $y - h$ *divides* $\widetilde{P}$, *where* $h \in (R_{N-1})_{\text{alg}}$. *Then, for* $1 \le i \le n-1$, *the* X_i *of equation* (8) *have the property that*

$$(9)\quad \widetilde{X}_i = -h^{(i)}\frac{\partial \widetilde{P}}{\partial y} + (y^{(i-1)} - h^{(i-1)})W_1 + (y^{(i-2)} - h^{(i-2)})W_2 + \cdots + (y-h)W_i,$$

with $W_1, \ldots, W_i \in (R_{N-1})_{\text{alg}}[y, y', \ldots, y^{(i-1)}]$.

There is, of course, no reason to believe that h is differentiable at x_0. However we note here and for future reference that it will at least be analytic in a cut neighbourhood of x_0.

Proof of Lemma 1. Suppose $\widetilde{P} = (y-h)P_0$, where $P_0 \in (R_{N-1})_{\text{alg}}[y]$. For $1 \le i \le n-1$, we have, by Leibniz Theorem,

$$(10)\qquad \widetilde{P}^{*i} = (y^{(i)} - h^{(i)})P_0 + (y^{(i-1)} - h^{(i-1)})P_1 + \cdots + (y-h)P_i,$$

where $P_j \in (R_{N-1})_{\text{alg}}[y, y', \ldots, y^{(j)}]$, for $j = 1, \ldots, i$. In fact

$$(11)\qquad P_i = y^{(i)}\partial P_0/\partial y + U_i,$$

for some $U_i \in (R_{N-1})_{\text{alg}}[y, y', \ldots, y^{(i-1)}]$. Substituting (11) into (10) yields

$$\begin{aligned}\widetilde{P}^{*i} = {} & (y^{(i)} - h^{(i)})(P_0 + (y-h)\partial P_0/\partial y) + (y^{(i-1)} - h^{(i-1)})P_1 \\ & + \cdots + (y-h)(U_i + h^{(i)}\partial P_0/\partial y),\end{aligned}$$

and comparison of this with (8) gives the desired conclusion, since $\partial\widetilde{P}/\partial y = P_0 + (y-h)\partial P_0/\partial y$. This completes the proof of Lemma 1.

Proof of Theorem 3. If we take $i = n-1$ in (10) and apply the star derivative, we obtain

$$\widetilde{P}^{*n} = \left(\frac{\widetilde{\Lambda}}{\widetilde{\Omega}} - h^{(n)}\right)P_0 + (y^{(n-1)} - h^{(n-1)})Q_1 + \cdots + (y-h)Q_{n-1},$$

with $Q_1, \ldots, Q_{n-1} \in (R_{N-1})_{\text{alg}}[y, y', \ldots, y^{(n-1)}]$. On substituting for the derivatives of y using (8) and (9), we see that $\widetilde{T}$ takes the form

$$\widetilde{T} = P_0\{\widetilde{\Lambda}(h, \ldots, h^{(n-1)}) - h^{(n)}\widetilde{\Omega}(h, \ldots, h^{(n-1)})\}\left(\frac{\partial\widetilde{P}}{\partial y}\right)^r + (y-h)W,$$

where $W \in (R_{N-1})_{\text{alg}}[y]$ and $r \in \mathbf{N}$.

Now, since $\tilde{P}$ is square free, $(\partial\tilde{P}/\partial y)(h) = P_0(h) \neq 0$. Hence $y-h$ divides $\tilde{T}$ if and only if

$$\tilde{\Lambda}(h, \ldots, h^{(n-1)}) - h^{(n)}\tilde{\Omega}(h, \ldots, h^{(n-1)}) = 0;$$

i.e., if and only if h satisfies equation (1). This completes the proof of Theorem 3.

Theorem 3 gives us a means of discovering whether $\tilde{P}$ contains factors of the form $y-h$ with h satisfying (1). However we still need a way of finding out whether any such h also satisfies the initial conditions prescribed for f. We also need to deal with branch points. First some more notation.

Let $(R_{N-1})_{\text{alg}}\{y\}$ denote the differential ring generated by $(R_{N-1})_{\text{alg}}$ and y using the usual differentiation, not the star derivation; so an element of $(R_{N-1})_{\text{alg}}\{y\}$ is a polynomial in y and its derivatives of any order. Note that there is a natural identification $R_{N-1}[y] \hookrightarrow (R_{N-1})_{\text{alg}}\{y\}$. For $0 \leq j \leq n-1$, let $\eta_j : (R_{N-1})_{\text{alg}}\{y\} \to (\mathbf{C} \cap (R_{N-1})_{\text{alg}})\{y^{(j+1)}\}$ be the homomorphism defined by the substitutions $x = x_0$, $y = c_0, \ldots, y^{(j)} = c_j$. Let $\mathscr{H}_{x_0}$ denote the ring of germs of analytic functions at x_0. We extend the definition of ξ (the map given by $\kappa \to \kappa_0$) and η_j to $\mathscr{H}_{x_0}\{y\}$.

Let g be a polynomial in y whose coefficients are functions of x defined in a neighbourhood of x_0 and let $c_0, \ldots, c_{n-1}$ be given constants. A *lofting sequence* for g (with respect to $c_0, \ldots, c_{n-1}$) is a finite sequence of nonnegative integers $p_0(g) < p_1(g) < \cdots < p_J(g)$, $J \leq n-1$ with the properties:

(i) $\xi(g^{(i)}) = 0$ for $i < p_0(g)$, but $\xi(g^{(p_0)}) \neq 0$;

(ii) For $j = 1, \ldots, J$ we have $\eta_{j-1}(g^{(i)})$ is zero for $i < p_j(g)$ but not for $i = p_j(g)$.

We say that g has the *lofting property* if it possesses a lofting sequence $p_0, p_1, \ldots, p_J$ (this includes the assertion that the relevent derivatives exist at x_0) such that either

(a) $J = n-1$ and $\eta_{n-1}(g^{(p_{n-1})}) = 0$, or

(b) $\eta_j(g^{(p_J)}) \neq 0$ for $J \leq j \leq n-1$.

We define the *loft* of g to be n in case (a) and to be J in case (b); it is clear the loft is then uniquely defined.

In what follows we take x_0 to be 0 for convenience of notation. We proceed to obtain some results concerning the loft. Our eventual goal is to show that the g of Theorem 3 has the lofting property and that for such a g, the loft of g is equal to n if and only if $\tilde{\rho}_{N-1}(g) = 0$.

Lemma 2. *Let $a \in \mathscr{H}_0$. If $a \neq 0$ then a has the lofting property with loft 0. Also for any a in $\mathscr{H}_0$, the polynomial $y-a$ has the lofting property, and if $a(0) = 0$, so too does $ay-1$.*

The restriction $a(0) = 0$ is not in fact necessary for $ay-1$ to have the lofting property. This will follow from Lemma 4.

Proof of Lemma 2. To prove that a has the lofting property, with loft 0, we have only to take p_0 to be the least integer for which $a^{(p_0)} \neq 0$. For $y-a$, we take $p_i = i$ for $i = 0, 1, \ldots$ until $c_i \neq a^{(i)}(0)$ or $i = n-1$. Since $\xi(ay-1) = 1$, $ay-1$ has loft zero with $p_0(ay-1) = 0$.

Lemma 3. *Let* $g \in R_{N-1}[y]$ *be of degree at least two and irreducible over* $\mathscr{K}_0$. *Suppose that* g *satisfies the conditions of Theorem* 3, *i.e. if* $y - h$ *is any factor of* g, *with* $h \in (R_{N-1})_{\text{alg}}$, *then* h *satisfies the differential equation* (1).

Then g *has the lofting property with loft less than* n.

Proof of Lemma 3. Write d for the degree of g. It follows directly from the Theorem of Puiseux (see [13, §8.14] for example) that in a neighbourhood of the origin, g may be written in the form

$$g = A(x) \prod_{r=0}^{d-1} (y - \phi(\varepsilon_d^r x^{1/d})), \tag{12}$$

where $A(x)$ is analytic at 0, $x^{1/d}$ is defined on the branched Riemann surface, ε_d is the primitive dth root of unity and ϕ has a Laurent series with finite principal part, $\phi(\zeta) = \sum_{m=k}^{\infty} b_m \zeta^m$. Let α be the order of the zero of A at 0.

If we expand the right-hand side of (12) we obtain an expression of the form

$$g = A(x)(y^d + a_{d-1}(x)y^{d-1} + \cdots + a_0(x)), \tag{13}$$

where the a_i's are elementary symmetric functions of the $\phi(\varepsilon_d^r x^{1/d})$, and of course each Aa_i has a removable singularity at the origin. Suppose first that $k < 0$. Then since $\alpha + k$ is the order of the zero of Aa_0 at the origin, $\alpha + k \geq 0$. Moreover the functions Aa_i, $i > 1$ have zeros of larger order at 0. It follows that $\xi(g^{(j)}) = 0$ for $j < \alpha + k$ and $\xi(g^{(\alpha+k)}) = D^{\alpha+k}(Aa_0)(0) \neq 0$. Hence g has the lofting property with loft zero and $p_0(g) = \alpha + k$.

Now suppose that $k \geq 0$. By replacing y by $y + q(x)$ for some polynomial q and making the necessary adjustments to the constants $c_0, \ldots, c_{n-1}$ we can reduce to the case when k is not divisible by d. Choose $R \geq 0$ such that $dR < k < d(R+1)$. Then $\xi(g^{(j)})$ is equal to zero for $j < \alpha$ and to $A^{(\alpha)}(0)y^d$ for $j = \alpha$. Hence if $c_0 \neq 0$, it follows that g has loft 0 with $p_0(g) = \alpha$. Otherwise suppose that $c_i = 0$ for $i = 0, \ldots, I$ with $I < R$, and that we have already obtained $p_i(g) = \alpha + di$, for $i = 1, \ldots, I$. From (12), $g^{(j)}$ is a sum of terms of the form

$$A^{(\lambda)}(x) \prod_{r=0}^{d-1} (y^{(j_r)} - D^{j_r}(\phi(\varepsilon_d^r x^{1/d}))), \tag{14}$$

with $\lambda + \sum j_r = j$. Note that $D^{j_r}(\phi(\varepsilon_d^r x^{1/d}))$ has a zero of order $k/d - j_r$ at the origin. Hence the term in the expansion of (14) which is independent of y and its derivatives has a zero of order $\alpha - \lambda + k - \sum j_r = \alpha + k - j$ at 0. Similarly the coefficient of $y^{(j_{s_1})}y^{(j_{s_2})} \cdots y^{(j_{s_t})}$ has a zero of order at least $\alpha + k - j - kt/d + j_{s_1} + \cdots + j_{s_t}$. Any terms for which this order is negative must cancel out since the coefficients of g are analytic at 0. Moreover if any j_{s_i} is less than $I + 1$, the term in $y^{(j_{s_1})}y^{(j_{s_2})} \cdots y^{(j_{s_t})}$ will belong to the kernel of η_I since $c_0 = c_1 = \cdots = c_I = 0$. Any remaining terms will have coefficients with zeros of order at least $\alpha + k - j - kt/d + t(I+1)$. Since $t \leq d$ and $k > d(I+1)$, this order will certainly be positive if $j < \alpha + d(I+1)$. For $j = \alpha + d(I+1)$ however it will be positive except when $t = d$. This case occurs for just one of the summands (14) namely the one with $\lambda = \alpha$ and $j_r = I + 1$ for all r. This term has image $A^{(\alpha)}(0)(y^{(I+1)})^d$ under η_I, and indeed also under all η_i

with $i > I$. Now if $c_{I+1} \neq 0$, g has loft $I+1$ with $p_{I+1}(g) = \alpha + d(I+1)$. Otherwise we continue as before with I replaced by $I+1$.

Suppose that we reach the stage when $I = R$ and consider a term in $y^{(j_{s_1})}y^{(j_{s_2})} \cdots y^{(j_{s_t})}$ with each $j_{s_i} > R$. Its coefficient has a zero of order at least $\alpha + k - j + t(R + 1 - k/d)$, which is positive if $j < \alpha + k$. However for $j = \alpha + k$ all such terms belong to the kernel of η_R except the one with $t = 0$. Hence $\eta_R(g^{(\alpha+k)}) = D^{\alpha+k}(Aa_0)(0) \neq 0$ and so g has loft $R+1$ with $p_{R+1}(g) = \alpha + k$.

If $R \geq n-1$, the functions $\phi(\varepsilon_d^r x^{1/d})$ are $n-1$ times differentiable at 0. Since they also satisfy a differential equation of type (1) in a domain whose boundary includes the origin, they must in fact be analytic at 0 [2, Chapter V]. But this is contrary to our hypothesis that g is irreducible over $\mathscr{K}_0$. This completes the proof of Lemma 3.

Lemma 4. *Suppose that g_1 and g_2 have the lofting property and let $g = g_1 g_2$. Then g has the lofting property and its loft is equal to the maximum of the lofts of g_1 and g_2.*

Proof of Lemma 4. Let us write J and K for the respective lofts of g_1 and g_2. Let $m_i = p_i(g_1)$, $i = 0, \ldots, J$, and $n_i = p_i(g_2)$, $i = 0, \ldots, K$. Then for $i \leq \min(J, K)$, $p_i(g_1 g_2) = m_i + n_i$. To see this, note first that if $p < m_i + n_i$ then, by the Leibniz Theorem, $D^p(g_1 g_2)$ consists of a linear combination of terms of the form $D^r g_1 D^s g_2$ with at least one of the inequalities $r < m_i$, $s < n_i$ holding, and then $\eta_{i-1}(g_1 g_2) = 0$. On the other hand, if $p = m_i + n_i$, there is precisely one term in the Leibniz expansion of $D^p(g)$ for which neither of the inequalities $r < m_i$, $s < n_i$ holds. This term is $D^{m_i} g_1 D^{n_i} g_2$ and $\eta_{i-1}(D^{m_i} g_1 D^{n_i} g_2) \neq 0$. It follows that $\eta_{i-1}(D^{m_i+n_i} g) \neq 0$.

This situation continues until i reaches $\min(J, K)$. Suppose, without loss of generality, that this minimum is J. If $J = n$ then clearly the loft of g is also n. Otherwise $\eta_J(g_1^{(r)})$ is zero for $r < m_J$, but nonzero for $r = m_J$, and similarly for $\eta_j(g_1^{(r)})$ for $j > J$. If $K = J$, then $\eta_j(g_2^{(n_J)}) \neq 0$ for $j > J$ and so, by the above reasoning, $\eta_j(g^{(m_J+n_J)}) \neq 0$; hence the loft of g is equal to J. If $K > J$, consider the Leibniz expansion of $D^p(g_1 g_2)$. If $p < m_J + n_{J+1}$, any term must contain a derivative of g_1 of order less than m_J or a derivative of g_2 of order less than n_{J+1} and so will map to zero under η_J. For $p = m_J + n_{J+1}$, this holds for every term except $D^{m_J} g_1 D^{n_{J+1}} g_2$ and hence we take $p_{J+1}(g)$ equal to $m_J + n_{J+1}$. Similarly for $J + 1 < i \leq K$, we take $p_i(g) = m_J + n_i$. For $j \geq K$, it follows as above that $\eta_j(D^{m_J+n_K} g) = k\eta_j(D^{m_J} g_1)\eta_j(D^{n_K} g_2) \neq 0$, where k is a binomial coefficient. This suffices to establish Lemma 4.

The next result now follows easily.

Theorem 4. *Let $g \in R_{N-1}[y]$ be as in Theorem* 3; *i.e., if $y - h$ is any factor of g with $h \in (R_{N-1})_{\text{alg}}$, then h satisfies the differential equation* (1). *Then g has the lofting property and $\tilde{p}_{N-1}(g) = 0$ if and only if the loft of g is equal to n.*

Proof of Theorem 4. That g has the lofting property is a direct consequence of Lemmas 2, 3, and 4. It is also clear that g will have loft n if and only if it has a factor $y - h$ with h satisfying $h(x_0) = c_0$, $h'(x_0) = c_1, \ldots, h^{(n-1)}(x_0) = c_{n-1}$. Since, by hypothesis, such an h also satisfies the differential equation (1), it

follows that the loft of g is equal to n if and only if $\tilde{\rho}_{N-1}(g) = 0$. This completes the proof of Theorem 4.

We are now in a position to give our algorithm for the initial case of the inner induction.

Algorithm 3. *To determine whether* $\rho(P) = 0$ *when* $P \in \Phi_{N-1}[y]$, *we proceed as follows.*

1. *Check that* $\chi(\tilde{P}) = 0$; *if not then* $\rho(P) \neq 0$. *Then check that the coefficients of* $\tilde{P}$ *are not all zero, which by inductive assumption we are able to do.*

2. *Using Subalgorithm* 1 *below, compute a polynomial* $F \in \Phi_{N-1}[y]$ *such that* $\tilde{F}$ *is the gcd of* $\tilde{P}$ *and* $\partial\tilde{P}/\partial y$. *Then* $\tilde{P}/\tilde{F}$ *is square free and* $\rho(P) = 0$ *if and only if* $\rho(P/F) = 0$. *Replace* P *by* P/F.

3. *Compute the* i*th star derivative of* P *for* $i = 1, \ldots, n$. *Use the equations* $P^{*i} = 0$, $i = 1, \ldots, n-1$, *to eliminate the derivatives of* y *from* P^{*n}. *Multiply the result by the product of* $\check{\Omega}$ *and a suitable power of* $\partial P/\partial y$ *in order to clear denominators. (As before* $\check{\Omega}$ *denotes the result of eliminating* $y', \ldots, y^{(n-1)}$ *from* Ω *using the equations* $P^{*i} = 0$.) *Let* T *denote the result; so* $T \in \Phi_{N-1}[y]$.

4. *As in stage* 2, *compute an element* G *of* $\Phi_{N-1}[y]$ *such that* $\tilde{G}$ *is the gcd of* $\tilde{P}$ *and* $\tilde{T}$. *In practice this means making the gcd computations in* $\Phi_{N-1}[y]$ *but regarding elements of* Φ_{N-1} *belonging to the kernel of* ρ_{N-1} *as zero; cf. Subalgorithm* 1 *and also the remarks following Theorem* 1. *Write* $g = \tilde{G}$. *If* g *is independent of* y, *then* $\rho(P) \neq 0$.

5. *Otherwise compute the loft of* g *as follows. Check whether* g *reduces to zero under the substitution* $x = x_0$ *(with* y *remaining as an indeterminate). If it does, keep replacing* g *by its total derivative with respect to* x *until the substitution no longer gives the zero polynomial. Then substitute* $y = c_0$ *in addition to* $x = x_0$; *if this fails to give zero, then* g *has loft* 0 *and* $\rho(P) \neq 0$.

6. *Otherwise totally differentiate* g *until the result is no longer in the kernel of* η_0. *If the last expression fails to vanish when* c_1 *is substituted for* y', *then the loft is* 1 *and if* $n > 1$ $\rho(P) \neq 0$. *Otherwise apply keep differentiating until the result is no longer in the kernel of* η_1, *and so on. At the* j*th stage, differentiate until the result is not in the kernel of* η_{j-1}. *If the last expression fails to vanish when* c_j *is substituted for* $y^{(j)}$, *then the loft is* j *and* $\rho(P) \neq 0$; *otherwise continue differentiating. This continues until either we discover that* $\rho(P) \neq 0$ *or the loft has been found to be* n, *in which case* $\rho(P) = 0$.

This completes the algorithm, apart from Subalgorithm 1, *which we give below.*

Note first that checking $\chi(\tilde{P})$ at stage 1 is only for the purpose of efficiency. Most expressions are not functionally equivalent to zero and evaluation at x_0 will often reveal this without further ado. Secondly note that the last statement in stage 2 holds because $\rho(P)$ is zero if and only if $y - f$ is a factor of $\tilde{P}$, and removing repeated factors does not alter this.

Now for Subalgorithm 1. Let P and Q be two elements of $\Phi_{N-1}[y]$. The task is to find an element G such that $\tilde{G}$ is the gcd of $\tilde{P}$ and $\tilde{Q}$. We give here only a simple version based on pseudodivision gcd method, but more sophisticated gcd algorithms, such as the subresultant algorithm, [4], may also be adapted to the present needs.

Subalgorithm 1. *Let* P *and* Q *belong to* $\Phi_{N-1}[y]$. *We compute an element* G *of* $\Phi_{N-1}[y]$ *such that* $\tilde{G} = \gcd(\tilde{P}, \tilde{Q})$. *We may assume without loss of generality, that the degree of* P *in* y *is at least that of* Q *and that* $\mathrm{lc}(P)$, *the leading coefficient of* P, *does not belong to the kernel of* ρ_{N-1}.

1. *Check that* $\rho_{N-1}(\mathrm{lc}(Q)) \neq 0$; *if it is, remove this term from* Q *and check the new leading coefficient; of course* $\tilde{Q}$ *is unaffected by this. If* Q *is reduced to the zero polynomial by this process, take* $G = P$.

2. *While* $\deg(P) \geq \deg(Q)$ *do*

(i) *Divide* $\mathrm{lc}(Q).P$ *by* Q *and assign the remainder to* P;

(ii) *Remove terms from* P *as necessary until* $\rho_{N-1}(\mathrm{lc}(P)) \neq 0$.

3. *If* P *has been reduced to zero at stage* 2, *take* $G = Q$. *Otherwise, if* P *has been reduced to a nonzero element of* Φ_{N-1}, *take* $G = P$. *If neither of these is the case, interchange* P *and* Q *and return to stage* 2.

6. The inner induction

Suppose that

$$P \in \Phi_{N-1}[y, y', \ldots, y^{(s)}], \qquad s \leq n-1.$$

Let Ψ denote the ring $\Phi_{N-1}[y, y', \ldots, y^{(s-1)}]$ and write z for $y^{(s)}$. Then $\Phi_{N-1}[y, y', \ldots, y^{(n-1)}]$ may be identified with $\Psi(z, z', \ldots, z^{(n-s-1)})$, and $P \in \Psi[z]$. By induction, we may assume that we can decide when an element of Ψ belongs to the kernel of ρ. Let $\acute{\rho}_{N-1}$ denote the homomorphism from Φ to $R_{N-1}[f, f', \ldots, f^{(s-1)}]\{z\}$ obtained by composing $\tilde{\rho}_{N-1}$ with the map obtained by setting y to f, y' to $f', \ldots$, and $y^{(s-1)}$ to $f^{(s-1)}$. We write $\acute{P}$ for $\acute{\rho}_{N-1}(P)$.

The idea is to use a slight modification of Algorithm 3 with $\Phi_{N-1}[y]$ replaced by $\Psi[z]$. We form the polynomial T in a similar manner to that used in the case $s = 0$. Namely we use the equations $P^{*i} = 0$, $i = 1, \ldots, n-s-1$, to obtain expressions for $z^{(i)}$ and then use these to eliminate $z^{n-s-1}, \ldots, z'$ from P^{*n-s}. Denominators are then cleared to form $T \in \Psi[z]$. We then compute a polynomial $g \in \Psi[z]$ such that $\acute{g}$ is the gcd of $\acute{P}$ and $\acute{T}$. This we do by computing the gcd of P and T identifying to zero any elements of Ψ in the kernel of $\acute{\rho}_{N-1}$. The proof of the following theorem is almost word for word identical with that of Theorem 3.

Theorem 5. *Let* g *be as above and suppose that* $\acute{g}$ *contains a factor* $z - h$ *with* $h \in (R_{N-1}[f, f', \ldots, f^{(s-1)}])_{\mathrm{alg}}$. *Then* h *satisfies the differential equation*

$$z^{(n-s)} = \frac{\acute{\Lambda}(z, z', \ldots, z^{(n-s-1)})}{\acute{\Omega}(z, z', \ldots, z^{(n-s-1)})}. \tag{15}$$

Conversely if h *satisfies* (15) *and* $\acute{P}(h) = 0$, *then* $z - h$ *divides* g.

Theorem 4 now applies with R_{N-1} replaced by $R_{N-1}\{f\}$ and so gives a method of determining whether the factors of g contain a $z - h$ for which h satisfies the initial conditions $h(x_0) = c_s$, $h'(x_0) = c_{s+1}, \ldots, h^{(n-s-1)}(x_0) = c_{n-1}$. In practice, we need to be careful to distinguish derivatives of z, which are only substituted for when the appropriate member of the lofting sequence has been reached in the number of differentiations, from the derivatives of the function f which occur in coefficients and which are substituted at all stages.

This is because we are working in the ring $R_{N-1}\{f\}\{z\}$. The inner-induction algorithm is thus as follows.

Algorithm 4. *To determine whether* $\rho(P) = 0$ *when* $P \in \Psi[y^{(s)}]$, *we carry out the following steps.*

1. *Check that* $\chi(\tilde{P}) = 0$; *if not then* $\rho(P) \neq 0$. *Then substitute* z *for* $y^{(s)}$ *and check that the coefficients of* $\acute{P}$ *are not all zero, which by inductive assumption we are able to do.*

2. *Using Subalgorithm* 1, *compute a polynomial* $F \in \Psi[z]$ *such that* $\acute{F}$ *is the gcd of* $\acute{P}$ *and* $\partial\acute{P}/\partial z$. *Then* $\acute{P}/\acute{F}$ *is square free and* $\rho(P) = 0$ *if and only if* $\rho(P/F) = 0$. *Replace* P *by* P/F.

3. *Compute the* i*th star derivative of* P *for* $i = 1, \ldots, n - s$. *Use the equations* $P^{*i} = 0$, $i = 1, \ldots, n - s - 1$, *to eliminate the derivatives of* z *from* P^{*n-s}. *Clear denominators in order to obtain* $T \in \Psi[z]$.

4. *As in stage* 2, *compute an element* G *of* $\Psi[z]$ *such that* $\acute{G}$ *is the gcd of* $\acute{P}$ *and* $\acute{T}$. *In practice this means making the gcd computations in* $\Psi[z]$ *but regarding elements of* Ψ *belonging to the kernel of* $\acute{\rho}_{N-1}$ *as zero. Write* $g = \acute{G}$. *If* g *is independent of* z, *then* $\rho(P) \neq 0$.

5. *Compute the loft of* g *as follows. Check whether* g *reduces to zero under the substitution* $x = x_0$, *with* z *remaining as an indeterminate but* f *being substituted by* c_0, f' *by* c_1, *etc. If* g *does reduce to zero, keep replacing* g *by its total derivative with respect to* x *until the substitution no longer gives the zero polynomial. Then substitute* $z = c_s$ *in addition to the other substitutions. The values to be substituted for derivatives of* f *of order higher than* $n - 1$ *are calculated using the recurrence formula*

$$f^{(n+i)}(x_0) = D^i\left(\frac{\tilde{\Lambda}(f, f', \ldots, f^{(n-1)})}{\tilde{\Omega}(f, f', \ldots, f^{(n-1)})}\right)(x_0),$$

$i = 0, 1, \ldots$. *If substituting* $z = c_s$ *fails to give zero, then* g *has loft* 0 *and* $\rho(P) \neq 0$.

6. *Otherwise totally differentiate* g *until the result is no longer in the kernel of* η_s. *If the last expression fails to vanish when* c_{s+1} *is substituted for* z', *then the loft is* 1 *and if* $n > 1$ $\rho(P) \neq 0$. *Otherwise apply keep differentiating until the result is no longer in the kernel of* η_{s+1}, *and so on. At the* j*th stage, differentiate until the result is not in the kernel of* η_{s+j-1}. *If the last expression fails to vanish when* c_{s+j} *is substituted for* $z^{(j)}$, *then the loft is* j *and* $\rho(P) \neq 0$; *otherwise continue differentiating. This continues until either we discover that* $\rho(P) \neq 0$ *or the loft has been found to be* $n - s$, *in which case* $\rho(P) = 0$.

7. A WORKED EXAMPLE

We apply the techniques of the previous section to the expression $e^{2ix} - 2ie^{ix}\sin x - 1$. We take $y_1(x) = \sin x$ and define y_1 by $y_1'' = -y_1$, $y_1(0) = 0$, $y_1'(0) = 1$. Similarly, we define $y_2(x) = \exp(ix)$ by $y_2' = iy_2$, $y_2(0) = 1$. The polynomial for consideration is then

$$P = y_2^2 - 2iy_2y_1 - 1. \tag{16}$$

Our first task is to check that $\tilde{P}$ is square free. We have $\partial P/\partial y_2 = 2y_2 - 2iy_1$

and hence

$$P - \left(\frac{y_2}{2} - \frac{iy_1}{2}\right)\frac{\partial P}{\partial y_2} = y_1^2 - 1.$$

But $\tilde{\rho}_1(y_1^2 - 1) \neq 0$, since substituting $x = 0$, $y_1 = 0$ gives -1. Thus $\gcd(\widetilde{P}, \partial\widetilde{P}/\partial y_2) \neq 0$ and so $\widetilde{P}$ is square free. We have

$$P^* = 2iy_2^2 - 2iy_2y_1' + 2y_2y_1. \tag{17}$$

Our next task is to compute $\gcd(\widetilde{P}, \widetilde{P}^*)$. Let $Q = iP - P^*/2$. Then $Q = y_2(iy_1' + y_1) - i$. We observe that $\tilde{\rho}_1(iy_1' + y_1) \neq 0$, since substituting $x = 0$, $y_1 = 0$, $y_1' = 1$ gives a nonzero result. Next

$$-(iy_1' + y_1)P + y_2Q = y_2\{2iy_1(iy_1' + y_1) - i\} + (iy_1' + y_1).$$

On multiplying through by $iy_1' + y_1$, we obtain

$$\begin{aligned} &-(iy_1' + y_1)^2P + y_2(iy_1' + y_1)Q \\ &\quad = y_2(iy_1' + y_1)(-2y_1'y_1 + 2y_1'^2 - i) + (iy_1' + y_1)^2. \end{aligned} \tag{18}$$

Also

$$\begin{aligned} &(-2y_1'y_1 + 2iy_1^2 - i)Q \\ &\quad = y_2(iy_1' + y_1)(-2y_1'y_1 + 2y_2'^2 - i) - i(-2y_1'y_1 + 2iy_1^2 - i). \end{aligned} \tag{19}$$

On subtracting (19) from (18), we obtain on the right-hand side

$$(iy_1' + y_1)^2 + i(-2y_1'y_1 + 2iy_1^2 - i) = -y_1'^2 - y_1^2 + 1.$$

Let $S = -y_1'^2 - y_1^2 + 1$. To determine whether $\widetilde{S} = 0$, we use the inner induction. We write $z = y_1'$, so that $S = -z^2 - y_1^2 + 1$. We have $S^* = 2zy_1 - 2y_1z = 0$ and so $\gcd(S, S^*) = S$. This establishes that S contains a factor of the form $z - h$, $h \in (\mathbf{Q}[x][y_1])_{\text{alg}}$, where h satisfies the differential equation for z, i.e., $z' = -y_1$. In fact, as we can see, there are two choices for h, namely $\pm\sqrt{1 - y_1^2}$. Next we must make the substitutions. We substitute $x = 0$, $y_1 = 0$, but keep z as an indeterminate; under these substitutions, $S \to -z^2 + 1$. Now putting $z = 1$ reduces S to zero, and hence $\widetilde{S} = 0$.

However S was the remainder obtained on reducing P modulo Q, and hence $\widetilde{Q} = \gcd(\widetilde{P}, \widetilde{P}^*)$. Then $i(iy_1' - y_1)^{-1}$ satisfies the differential equation $y_2' = iy_2$, as follows from the definition of Q.[4] Finally, the substitutions need to be applied to Q. First, on putting $x = 0$, $y_1 = 0$, $y_1' = 1$, we see that $Q \to iy_2 - i$. Putting $y_2 = 1$ then does give zero, and we are now entitled to conclude that $\widetilde{P} = 0$.

8. Functional composition

The viewpoint of this paper has been that transcendental functions are specified by differential equations of the form (1) together with initial conditions. While this may be a reasonable standpoint, it is nonetheless often convenient to specify functions using functional composition. We take a brief look at this in the present section.

Suppose then that f is a nonconstant function satisfying (1) and the associated initial conditions and that g is another nonconstant function similarly

[4]The reader may verify that $i(iy_1' + y_1)^{-1} = \exp(ix)$.

specified, with f analytic on a domain which has nontrivial intersections with the range of g. We have (cf. [10]) $f' \circ g = (f \circ g)'/g'$ and hence

$$f'' \circ g = (f' \circ g)'/g' = \frac{(f \circ g)''}{(g')^2} - \frac{(f \circ g)' g''}{(g')^3}.$$

In general suppose that we have established that

$$(20)\quad f^{(j)} \circ g = Q_j((f \circ g)', (f \circ g)'', \ldots, (f \circ g)^{(j)}, g', \ldots, g^{(j)})/(g')^{2j-1},$$

where Q_j is a polynomial. Then

$$f^{(j+1)} \circ g = \frac{(f^{(j)} \circ g)'}{g'} = \left(\frac{Q_j((f \circ g)', \ldots, (f \circ g)^{(j)}, g, \ldots, g^{(j)})}{(g')^{2j-1}}\right)' \frac{1}{g'}$$
$$= \frac{Q_{j+1}((f \circ g)', \ldots, (f \circ g)^{(j+1)}, g, \ldots, g^{(j+1)})}{(g')^{2j+1}}.$$

Since f satisfies (1),

$$(21)\quad \{f^{(n)}\tilde{\Omega}(f, f', \ldots, f^{(n-1)}) - \tilde{\Lambda}(f, f', \ldots, f^{(n-1)})\} \circ g = 0.$$

The expressions (20) can then be substituted into (21) and the result multiplied through by $(g')^{2n-1}$ to yield a differential equation $p(Y, Y', \ldots, Y^{(n)}) = 0$ for $f \circ g$. Inspection shows that the coefficient of $(f \circ g)^{(n)}$ in $p(f \circ g, \ldots, (f \circ g)^{(n)})$ is equal to $(g')^{n-1}.\tilde{\Omega}(f, \ldots, f^{(n-1)}) \circ g$ and so we need to determine a point x_0 at which this quantity is nonzero in order to obtain initial conditions for $f \circ g$.

Suppose that g is analytic at $\bar{x}$ and f at $g(\bar{x})$. One way of finding a suitable x_0 is to take a strictly monotonic sequence $x_1, x_2, \ldots$ tending to $\bar{x}$ and evaluate $(g')^{n-1}.\tilde{\Omega}(f, \ldots, f^{(n-1)}) \circ g$ at each successive x_n until one is found at which it is not zero. This must happen eventually since $(g')^{n-1}.\tilde{\Omega}(f, \ldots, f^{(n-1)}) \circ g$ cannot have a limit point of zeros at $\bar{x}$. The method might even be a successful one in practice, but it is somewhat unsatisfactory to have no estimate of when it will terminate. Another possible approach is to try to use cylindrical decomposition. Richardson [26] showed how this can be done with expressions defined by towers of *first-order* equations of the form (1), but so far as the author is aware there is no corresponding method for higher-order equations. Finally a rather promising suggestion, first made to the author by Michael Singer, is to use the results of Denef and Lipshitz [11]. These give one uniqueness of power-series solutions of (1) about points at which $\tilde{\Omega}$ has a zero; the price to be paid is that many more derivatives may need to be specified in the initial conditions.

We hope to examine the problems associated with functional composition more fully in a later paper.

References

1. A. Baker, *Transcendental number theory*, Cambridge Univ. Press, Cambridge, 1975.
2. G. Birkoff and G. C. Rota, *Ordinary differential equations*, Ginn, 1962.
3. W. S. Brown, *Rational exponential expressions and a conjecture concerning* π *and* e, Amer. Math. Monthly **76** (1969), 28–34.
4. W. S. Brown and J. F. Traub, *On Euclid's algorithm and the theory of subresultants*, J. Assoc. Comput. Mach. **18** (1971), 505–514.

5. B. Buchberger, *Gröbner bases: an algorithmic method in polynomial ideal theory*, Multidimensional Systems Theory (N. K. Bose, ed.), Reidel, Dordrecht, 1985, pp. 184–232.
6. B. Buchberger and R. Loos, *Algebraic simplification*, Computer Algebra: Symbolic and Algebraic Computation (B. Buchberger, G. E. Collins, and R. Loos, eds.), 2nd ed., Springer-Verlag, Wien/New York, 1983, pp. 11–43.
7. B. F. Caviness, *Methods for symbolic computation with transcendental functions*, Proc. Conf. on Symbolic Computational Methods and Applications (A. Visconti, ed.), St. Maximin, France, 1977, pp. 16–43.
8. ____, *On canonical forms and simplification*, J. Assoc. Comput. Mach. **17** (1970), 385–396.
9. B. F. Caviness and M. J. Prelle, *A note on algebraic independence of logarithmic and exponential constants*, SIGSAM Bull. **12** (1978), 18–20.
10. J. Denef and L. Lipshitz, *Decision problems for differential equations*, J. Symbolic Logic **54** (1989), 941–950.
11. ____, *Power series solutions of algebraic differential equations*, Math. Ann. **267** (1984), 213–238.
12. J. P. Fitch, *On algebraic simplification*, Comput. J. **17** (1973), 23–27.
13. O. Forster, *Lectures on Riemann surfaces*, Springer-Verlag, New York, 1981.
14. M. R. Garey and D. S. Johnson, *Computers and intractability: a guide to the theory of NP-completeness*, Freeman, New York, 1979.
15. G. H. Hardy, *Orders of infinity*, Cambridge Univ. Press, Cambridge, England, 1910.
16. S. C. Johnson, *On the problem of recognizing zero*, J. Assoc. Comput. Mach. **18** (1971), 559–565.
17. S. Lang, *Transcendental numbers and diophantine approximation*, Bull. Amer. Math. Soc. **77** (1971), 635–677.
18. D. Lazard, *Résolutions des systèmes d'equations algébriques*, Theoret. Comput. Sci. **15** (1981), 77–110.
19. A. J. Macintyre, *The laws of exponentiation*, Model Theory and Arithmetic (C. Berline, K. McAloon, and J. P. Rossayre, eds.), Springer-Verlag, New York, 1981, pp. 185–197.
20. W. A. Martin, *Determining the equivalence of algebraic expressions by hash coding*, J. Assoc. Comput. Mach. **18** (1971), 549–558.
21. F. Mora, *An algorithm to compute the equations of tangent cones*, EUROCAM '82 Proceedings, Springer-Verlag, Berlin and New York, 1982, pp. 158–165.
22. J. Moses, *Algebraic simplification: a guide for the perplexed*, Comm. Assoc. Comput. Mach. **14** (1971), 527–537.
23. ____, *Solution of a system of polynomial equations by elimination*, Comm. Assoc. Comput. Mach. **9** (1966), 634–637.
24. A. C. Norman, *Computing in transcendental extensions*, Computer Algebra: Symbolic and Algebraic Computation, 2nd ed. (B. Buchberger, G. E. Collins, and R. Loos, eds.), Springer-Verlag, Wien/New York, 1983, pp. 11–43.
25. A. Oldehoeft, *Analysis of constructed mathematical responses by numeric tests for equivalence*, Proc. ACM 24th Nat. Conf., 1969, pp. 117–124.
26. D. Richardson, *Finding roots of equations involving solutions of first order algebraic differential equations*, Proc. Conf. Effective Methods in Algebraic Geometry, MEGA, 1990.
27. ____, *Solution of identity problem for integral exponential functions*, Z. Math. Logik Grundlag. Math. **15** (1969), 333–340.
28. ____, *Some undecidable problems involving elementary functions of a real variable*, J. Symbolic Logic **33** (1968), 514–520.
29. M. Rothstein and B. F. Caviness, *A structure theorem for exponential and primitive functions*, SIAM J. Comput. **8** (1979), 357–367.
30. J. R. Shackell, *Asymptotic estimation of oscillating functions using an interval calculus*, ISSAC '88 Proceedings (P. Gianni, ed.), Springer-Verlag, Rome, pp. 481–489.

31. ____, *A differential-equations approach to functional equivalence*, ISSAC '89 Proceedings (G. Gonnet, ed.), A.C.M. Press, Portland, Oregon, 1989, pp. 7–10.
32. M. F. Singer, *Liouvillian first integrals of differential equations*, (extended abstract), ISSAC '88 Proceedings (P. Gianni, ed.), Springer-Verlag, 1988, pp. 57–63.
33. F. Ulmer, *Representing functions by differential equations*, private communication, 1989.
34. O. Zariski and P. Samuel, *Commutative algebra*, vols. I, II, Van Nostrand, 1960.

Department of Mathematics, University of Kent at Canterbury, Canterbury, England
E-mail address: jrs@ukc.ac.uk