The Identity Problem for Elementary Functions and Constants

Dan Richardson and John Fitch,
School of Mathematical Sciences,
University of Bath,
Bath, UK.
email : dsr@uk.ac.bath.maths *

Abstract

A solution for a version of the identity problem is proposed for a class of functions including the elementary functions. Given $f(x)$, $g(x)$, defined at some point β we decide whether or not $f(x) \equiv g(x)$ in some neighbourhood of β. This problem is first reduced to a problem about zero equivalence of elementary constants. Then a semi algorithm is given to solve the elementary constant problem. This semi algorithm is guaranteed to give the correct answer whenever it terminates, and it terminates unless the problem being considered contains a counterexample to Schanuel's conjecture.

1 Introduction

The *elementary functions* are, roughly, functions obtained by starting with polynomials and applying algebraic operations, exponentiation and logarithms finitely many times. In the field of computer algebra, complicated expressions for elementary functions are produced and manipulated. It is of fundamental importance to have a method to decide whether or not two elementary functions are equal, whether or not an elementary function is identically zero, or whether or not a given expression for an elementary function can be simplified. Some versions of this problem turn out to be undecidable[10, 2]; e.g. the identity problem is undecidable in the class of functions obtained from 1, π, x by closing under $+, -, *, e^x, logx, sinx, cosx$ and composition, considering all functions as partially defined real valued functions of a real variable.

Alternatively one could restrict attention to domains in which the functions are analytic. There are a bewildering number of possible formulations here. We consider now the local zero equivalence problem (and associated identity problem): *Given elementary function $f(x)$ and point α at which $f(x)$ is analytic, decide whether or not $f(x) \equiv 0$ in some neighbourhood of α.* Problems of this local sort have been considered by several authors. John Shackell [14] has shown that zero equivalence problems of this type can be reduced to the problem of deciding whether or not certain constants are zero. So he solved this problem with the help of a postulated oracle to deal with the constants.

All work on the constant problem so far is linked to *Schanuel's Conjecture*[1, 13]: If $z_1, ..., z_n$ are complex numbers which are linearly independent over the rationals, then $\{z_1, ..., z_n, e^{z_1}, ..., e^{z_n}\}$ has transcendence rank at least n.

This seems to imply that there are no unexpected identities among elementary constants. It has been shown, for larger and larger subsets of constants, that the zero equivalence problem is decidable provided that Schanuel's conjecture is true[11].

Here this development is continued by showing that the whole elementary constant problem is decidable if Schanuel's conjecture is true. The sensible reader may think that this is of no practical importance since we do not know if Schanuel's conjecture is true or not. However the situation is better than it seems at first. We have a semi-algorithm for the constant problem which always gives the correct answer whenever it terminates; also it always terminates unless the problem it is considering contains a counterexample to Schanuel's conjecture. If it seems unlikely that we will prove all of Schanuel's conjecture in the near future, it seems even more unlikely that we would find a counterexample.

2 Basic Definitions

An exponential system is a system of equations $(S = 0, E = 0)$, where S is a finite set of polynomials in $\mathbf{Q}[x_1, y_1 ..., x_n, y_n]$, and E is a subset of $\{y_1 - e^{x_1}, ..., y_n - e^{x_n}\}$.

Definition 1 *An* elementary point *is a point in C^{2n} which is a non-singular isolated solution of an exponential system $(S, E) = 0$; an* elementary number *is a complex number of the form $p(x_1, y_1, ..., x_n, y_n)$, where p is a polynomial with rational coefficients, and $(x_1, y_1, ..., x_n, y_n)$ is an elementary point.*

A rational point in C^{2n} is a point all of whose coordinates have real and imaginary parts which are rational. An elementary point can be specified by giving a rational point r, and a neighbourhood, $N_\epsilon(r)$ in C^{2n}, and an exponential system $(S = 0, E = 0)$, and a proof that this system has a unique non singular solution in $N_\epsilon(r)$. Such a proof can always be given in a standard way, by considering (S, E) as a map from $R^{4n} \to R^{4n}$, and calculating the topological degree of this map over $N_\epsilon(r)$.

A basic problem about the elementary numbers is how to decide, given a description, as above, of an elementary

*This paper was written with the support of CEC, ESPRIT BRA contract 6846 "POSSO"

ISAAC 94 - 7/94 Oxford England UK
© 1994 ACM 0-89791-638-7/94/0007..$3.50

number, whether or not the number is zero. This is called the elementary constant problem[11].

Assume the following ordering, by importance, on the variables $x_1 \prec y_1 \prec x_2 \prec ... \prec x_n \prec y_n$.

Let (S, E) be an exponential system, $S = (p_1, ..., p_s)$ and $E = (y_{i_1} - e^{x_{i_1}}, ...y_{i_r} - e^{x_{i_r}})$. Define the differential matrix of this system to be a $2n$ by $(r + s)$ matrix

$$\begin{pmatrix} \partial p_1/\partial x_1 & \partial p_1/\partial y_1 & ... & \partial p_1/\partial y_n \\ ... & ... & ... & ... \\ \partial p_s/\partial x_1 & \partial p_s/\partial y_1 & ... & \partial p_s/\partial y_n \\ 0 & ... - y_{i_1} & 1 & ...0 \\ ... & ... & ... & ... \\ 0 & ...0 & -y_{i_r} & 1 \end{pmatrix}$$

The columns of the differential matrix correspond to the $2n$ variables, listed in order of importance as follows: $x_1, y_1, x_2, y_2, ..., x_n, y_n$. The $(s + j)^{th}$ row has $-y_{i_j}$ in the x_{i_j} column and 1 in the y_{i_j} column, and zero in all other columns, corresponding to the differential equation $dy_{i_j} - y_{i_j} dx_{i_j} = 0$. The product of the differential matrix and the column vector $(dx_1, dy_1, ..., dx_n, dy_n)$ is the differential of the system.

Definition 2 *Let $(Z, W) = (x_1, y_1, ...x_n, y_n)$ with the first k of the variables, in order, in Z, and the other $2n - k$ variables in W. Let α be an elementary point in C^{2n} and $p(Z, W)$ a polynomial in $\mathbf{Q}[x_1, y_1, ..., x_n, y_n]$. We will say that a function*

$$f(Z) = p(Z, W(Z)) : C^k \rightarrow C$$

is implicitly defined by polynomial p and exponential system $(S, E) = 0$ near α *if*

1) $(S, E)(Z, W(Z)) \equiv 0$ in some neighbourhood of α

2) S is a set of s polynomials in $\mathbf{Q}[x_1, y_1, ..., x_n, y_n]$

3) E is a set of r terms among $y_1 - e^{x_1}, ..., y_n - e^{x_n}$

4) $k = 2n - (r + s)$ and the last $r + s$ columns of the differential matrix of (S, E) are linearly independent at α

In the situation described above, the variables Z will be called the *independent variables*, and the variables W will be called dependent. That W is defined implicitly as a function of Z by $(S, E) = 0$ near α is a consequence of the implicit function theorem. Note that these implicitly defined functions include all the usual elementary functions.

We claim to be able to solve the identity problem in the form: given two functions of this type $f(z_1, ..., z_k)$ and $g(z_1, ..., z_k)$, with the same number of independent variables, both defined around the same elementary point α, decide whether or not there exists a neighbourhood N of α in which $f \equiv g$. Since we can effectively do subtraction of functions, the problem reduces to the question of whether or not a given function is identically zero in some neighbourhood of the point around which it is defined.

First we define a normal form for exponential systems. Then the identity problem is solved for elementary constants, using Schanuel's conjecture. Finally the identity problem is solved for functions implicitly defined by exponential systems.

3 Extension of Wu's method to Exponential Systems

We use the algebraic methods of Wu Wen Tsun to get a normal form for exponential systems. Define an ascending set, S, of polynomials in $\mathbf{Q}[x_1, y_1, x_2, y_2, ..., x_n, y_n]$ as in Wu[15]. Also, if S is such an ascending set, and p is any polynomial in $\mathbf{Q}[x_1, y_1, ...x_n, y_n]$, let $Rem(S, p)$ be the pseudo remainder of p with respect to S, as defined by Wu.

Definition 3 *$(S = 0, E_1 = 0, E_2 = 0, I \neq 0, J \neq 0)$ is a* condition in normal form, *if the following properties hold.*

1) S is an ascending set in $\mathbf{Q}[x_1, y_1, x_2, y_2, ...x_n, y_n]$

2) (E_1, E_2) is a partition of the full exponential set E

3) I is the product of the leading coefficients of S, as in Wu.

4) $J \neq 0 \rightarrow (S, E_1)$ independent; J is the determinant of a maximal minor of the differential matrix. $Rem(S, J) \neq 0$. If there are several possibilities of maximal size, J is picked so that the set of dependent variables is as large as possible.

5) E_2 is such that if $C(t)$ is any smooth curve in C^{2n} on which $(S = 0, E_1 = 0, I \neq 0, J \neq 0)$, then any $y_i - e^{x_i}$ in E_2 is either identically zero on $C(t)$ or never zero.

The idea here is that the equations $(S = 0, E_1 = 0)$ should be independent, solution points should be required to be non singular, and the terms in E_2 play the same rôle as constants in differential algebra. The terms in E_2 will be called redundant. On a manifold defined by $(S = 0, E_1 = 0, I \neq 0, J \neq 0)$, the redundant terms will either be identically zero or never zero. Conditions in normal form are also called *triangular conditions*. Note that the solution set of a normal form condition is either empty or equidimensional; and in the neighbourhood of any point in the solution set the dimension can only be $2n - (r + s)$, where $r + s$ is the number of terms in (S, E_1).

Theorem 1 (Zero Decomposition:) The solution set in C^{2n} of any exponential system $(S = 0, E = 0)$ can be effectively expressed as the disjoint union of the solution sets of finitely many triangular conditions.

A proof of this theorem is in [12]. It is essentially the same as the Wu-Ritt zero structure theorem [15].

If an elementary point α is a solution of $(S = 0, E = 0)$, we can break (S, E) into finitely many triangular conditions $\Delta_1, ..., \Delta_t$, and we know that α satisfies just one of these. We can decide which of them it is if we can solve the elementary constant problem. The triangular condition which α satisfies will be called the *normal form* of $(S, E) = 0$ at α.

4 Proposed solution of the elementary constant problem

Suppose given exponential system (S, E_k) and neighbourhood N so that $(S = 0, E_k = 0)$ has a unique solution in N, and this solution α is non singular. $E_k = \{w_1 - e^{z_1}, ..., w_k - e^{z_k}\} \subseteq \{y_1 - e^{x_1}, ..., y_n - e^{x_n}\}$. Also suppose given polynomial p. We are interested in the constant $p(\alpha)$.

Define a *resolving matrix* for (S, E_k) at α to be an integral $d \times k$ matrix R, of rank d, *with d maximal*, so that $RX = 0$, where X is the column vector, evaluated at α, of the x variables $(z_1, z_2, ..., z_k)$ which occur in E_k.

The condition that d be maximal in this definition means that all linear dependencies over the integers of $(z_1, ..., z_k)$ at α are given by $RX = 0$. If one row is deleted from a resolving matrix, R, to give R', then R' is no longer resolving, although $R'X = 0$. Note that in case if we have $a_1 z_1 + ... + a_n z_n = 0$, with $(a_1, ..., a_n)$ integral, and $E_k = 0$ we also have $w_1^{a_1} w_2^{a_2} ... w_n^{a_n} = 1$. Thus dual to the linear equations $RX = 0$, we have a set of binomial equations in the y variables which will be written $Y^R = 1$.

In the following we consider algorithms which are supplied with oracles which, on request, will select an element at random from a countable set Σ of possibilities. We will say that such an algorithm *recognizes* a predicate $p(x_1, ..., x_n)$ if it is possible for the algorithm, given the arguments $x_1, ..., x_n$, and good guesses from its oracle, to terminate after finitely

many steps and say "yes" if and only if the predicate is true at the arguments. (It is possible that the algorithm, given bad guesses from the oracle, could go on forever, even though the predicate is true.) If a predicate and its negation are both recognizable in this sense, then the predicate is decidable. Among ways in which a predicate may be recognizable, some are relatively desirable. Especially good are the finite case and the generic case. For the finite case, the set Σ of possibilities can, without too much effort, be restricted to a not very large finite set. In the generic case, Σ is infinite or very large but almost any element of Σ is a good choice: so if a computation can possibly terminate, it almost always terminates, provided that the choice from Σ is sufficiently "random".

In the following algorithm there are $n+2$ branches, divided into three parts. It is claimed that in all cases one of the parts much occur, and that each part is recognizable.

Constant Solving Algorithm

Given α defined by $(S=0, E_k=0)$ in neighbourhood N, and polynomial p. We suppose E_k has k exponential terms in it. To decide whether or not $p(\alpha)=0$, we start $k+2$ processes in parallel.

A. (1 branch). Try to prove $p(\alpha)\neq 0$, by numerical approximation with error bounds.

B. (1 branch). Try to prove $S=0 \Rightarrow p=0$ in N, using algebraic techniques.

C. (n branches). For $d=1,...,k$: Try to guess a resolving matrix R of rank d. Having got a candidate matrix R, we use resolving matrix semi algorithm below to try to verify $RX=0$ at α. If this succeeds, it will give us a definition of α which uses less than k exponential terms. Interrupt all processes and start over with the simplified problem □

4.1 Part A: Numerical Approximation

We are given a definition of α as the solution, guaranteed non singular of $(S=0, E_k=0)$ in neighbourhood N. We need to generate good approximations to α, with error bounds. This can be used to generate a stream of contracting neighbourhoods, N_i, all containing the solution point, and the diameter of N_i tends to zero as i tends to infinity. From this we can construct increasingly good approximations, with error bounds, to $p(\alpha)$, and eventually recognize that $p(\alpha)\neq 0$ if this is the case.

There are two subcases, depending on how good an initial guess we have to α. Suppose our initial guess for an approximage value of α is x_0.

4.1.1 Newton's Method

It is well known that if x_0 is sufficiently close to a non singular solution α, we can verify numerically that there is a solution near x_0, and we can define an iterative proceedure which is guaranteed to converge rapidly to α. There are many different ways of doing this. A central result is the Kantorovich Theorem [9].

Let $F(x)=(S,E): C^{2n}\rightarrow C^{2n}$ be a function defined by an exponential system. Let $J(x)=F'(x)$ be the jacobian of $F(x)$. For matrices, M, define $\|M\|$ to be the smallest number d so that $|Mx|\leq d\,|x|$ for all x. Let D be an open set in C^{2n}. Define a sequence iteratively according to Newton's method: $x_{i+1}=x_i-J^{-1}(x_i)F(x_i)$

Theorem 2 *Kantorovich. Let x_0 be in D, and suppose $J^{-1}(x_0)$ exists, with $\|J^{-1}(x_0)(J(x)-J(y)\|\leq K\,|x-y|$ for all x and y in D. Also suppose $\|J^{-1}(x_0)F(x_0)\|\leq\eta$, and $h\equiv K\eta\leq 1/2$. Define*

$$\begin{aligned} r_0(h) &\equiv (1/h)(1-\sqrt{(1-2h)})\eta \\ r_1(h) &\equiv (1/h)(1+\sqrt{(1-2h)})\eta. \end{aligned}$$

Then if $\{x:|x-x_0|<r_0(h)\}\subseteq D$, the sequence of iterates defined by Newton's method exists, remains within distance $r_0(h)$ of the initial point x_0, and converges to x^* in D so that $F(x^*)=0$. If $h<1/2$, then x^* is the only root in D within distance $r_1(h)$ of x_0. The sequence of iterates satisfies the error bound $|x^*-x_n|\leq(1/2)^n(1-\sqrt{(1-2h)})^{2^n}(\eta/h)$

This guarantees that we can recognise numerically the existence of a non singular root of a system, provided we guess a sufficiently close initial value.

4.1.2 Computing Topological Degree

Suppose our given neighbourhood, N, is so large that we are not able to use the above technique immediately, i.e. we might not know how to make a good initial guess to the solution. We are given that $F(x)=0$ has only one solution, α in N and that $J(x)$ is non singular at α. So of course we could just try values in N until we get one that satisfies the Kantorovich Theorem, but if the neighbourhood is large, this is not one of the desirable kinds of recognition.

Another approach to this problem would be to recursively subdivide the neighbourhood and use interval arithmetic to prune the tree of sub-neighbourhoods.

Using topological degree offers an alternative infallible method of contracting N until we get to a stage in which we can use a more rapid iterative numerical technique. See [5, 3, 12, 6]. The topological degree of F over N is necessarily one, and if N is decomposed into the union of two neighbourhoods N_1 and N_2, and F is not zero on the intersection, then the solution to $F=0$ is in whichever of N_1 or N_2 has non zero topological degree.

4.2 Part B: Is $p(\alpha)$ algebraically zero?

From part (A) we are given a stream of contracting neighbourhoods, (N_i), converging to the solution point, α. If it happens that $S=0\Rightarrow p=0$ in N_i, for sufficiently large i, we wish to recognise this. We wait until the neighbourhoods are so small that we are able to use Newton's method to increase accuracy of the approximation.

The system S has $2n-k$ polynomials in it. We know that the differential matrix of S eventually has rank $2n-k$. Wait until this is true and then chop off the initial part of the stream. Pick out $2n-k$ linearly independent columns of the differential matrix of S. Rename the variables so that these columns correspond to variables $w_1,...,w_{2n-k}$; these will be called the dependent variables. Let the other variables be called independent, and rename them as $z_1,...,z_k$. Order the variables $z_1\prec z_2\prec ...\prec z_k\prec w_1\prec w_2\prec ...\prec w_{2n-k}$. Suppose N_i is so small that within N_i the dependent variables are defined implicitly as functions of the independent variables. Write this relationship as $W=F(Z)$.

To begin with, if p is not identically zero on the manifold defined by $S=0$ in the current neighbourhood, N_i, this fact can be recognised. We just pick a rational point Z_0 in the projection of the neighbourhood N_i onto the space of the independent variables, approximate $W_0=F(Z_0)$, using Newton's method on $S(Z_0,W)=0$, and evaluate p, with error bounds at (Z_0,W_0).

We now need to show that if p is identically zero on the solution manifold, this fact also can be recognised. We can find the partial derivatives of the dependent variables with respect to the independent ones from the differential matrix of S. Construct the partial derivatives of p with respect to the independent variables, regarding the dependent variables as functions of the independent variables. We may write these derivatives as rational functions in the variables. Let $A_1, ..., A_k$ be the numerators of these derivatives.

$S = 0$ defines a k dimensional manifold in N_i. If p is identically zero on this manifold, so are $A_1, ..., A_k$.

Form $\Delta = (S = 0, p = 0, A_1 = 0, ..., A_k = 0)$. Break this up into triangular conditions, $\Delta_1, ..., \Delta_s$. We have that $p \equiv 0$ on the solution manifold of $S = 0$ in N_i if and only if one of the k dimensional Δ_j conditions has a solution in N_i.

Discard all the Δ_j conditions which are not k dimensional. If there are none, then p is not zero on the solution manifold of $S = 0$. So stop.

Suppose there are some k dimensional Δ_j conditions remaining. In this case our strategy is to attempt to recognise that one of these has a solution in N_i.

Consider $\Delta_j = (S_j = 0, I_j \neq 0, J_j \neq 0)$. If we can show, using our current approximation to α that $S_j(\alpha) \neq 0$, then we discard Δ_j. Suppose this has not happened yet.

Next try to show $I_j(\alpha)J_j(\alpha) \neq 0$, using our approximation to α. If this succeeds, we just wait until our approximation to α is good enough to decide either $S_j(\alpha) \neq 0$, or, using the numerical technique above to prove that there is a solution of S_j in N_i, and that $I_j J_j$ is not zero anywhere in N_i.

It might possibly happen that Δ_j does have a solution in N_i, although $I_j(\alpha)J_j(\alpha) = 0$. This would still imply that $p \equiv 0$ on the solution manifold of $S = 0$. (It is just bad luck that α is not a generic point of the manifold.) So we need to start some other processes to recognise this case.

Let Z_α be the values of the independent variables at α. Pick rational Z_0 at random within the projection of N_i onto the independent variable space. For our original system of equations, $S = 0$, we have an implicitly defined solution $W = F(Z)$, which we can rapidly approximate with Newton's method within N_i to give the approximate $W_0 = F(Z_0)$. Now try to show that $I_j J_j$ is not zero at the point (Z_0, W_0). If this does not succeed, pick another random rational Z_0. (This is the generic type of good recognition.) If it does succeed, decide whether or not $S_j = 0$ at (Z_0, W_0). This can be done by waiting until it becomes clear that $S_j \neq 0$, or until it becomes clear that there is a solution to $S_j = 0$ which is so near to (W_0, Z_0) that it must be a solution to Δ_j which is also in N_i.

The algorithm described terminates in all cases, either deciding that $p \equiv 0$ on the solution manifold of $S = 0$ sufficiently near α, or deciding that this is not the case. But it could happen that $p(\alpha) = 0$ even though p is not identically zero on the solution manifold near α.

4.3 Part C: Finding a resolving Matrix

4.3.1 How to guess a resolving matrix R of rank d

We have an approximation to $z_1, ..., z_k$ at α. We could first look for one non trivial linear relationship among these numbers, and, having found it, drop one of the numbers which is approximately expressible as a rational combination of the others, and then continue with the smaller set.

To find the first linear relationship, pick a large number K and form

$$\begin{pmatrix} 1 & 0 & 0 & ... & 0 & Kz_1 \\ 0 & 1 & 0 & ... & 0 & Kz_2 \\ . & . & . & ... & . & . \\ . & . & . & ... & . & . \\ . & . & . & ... & . & . \\ 0 & 0 & 0 & ... & 1 & Kz_k \end{pmatrix}$$

and use the LLL algorithm to find a short vector in the lattice of integral combinations of the rows. In fact the MLLL algorithm[8] will give us a finite set of possible linear integral relationships. Every time there is a branch in the MLLL algorithm, depending on whether or not a combination is 0, *we take the zero branch*, until such time as we can prove the combination is not zero. (Of course the number of independent linear integral relationships is bounded by k; so if we have more than k independent possibilities, we know that we should just continue with our approximating process until the number is reduced. This is the finite type of good recognition.) Another method of solving this problem is to use the generalized Euclidean algorithm [4].

4.3.2 Resolving Matrix Semi Algorithm to recognize $RX = 0$ at α if R is a resolving matrix.

Given $k \times d$ integral matrix R of rank d, a possible resolving matrix, and given a stream of improving approximations to α, with error bounds, and a stream of contracting neighbourhoods N of α, and the definition of α as the solution of $(S = 0, E_k = 0)$ in N, using k exponential terms.

1) If $RX \neq 0$ at α, the algorithm should eventually stop and say this.

2) If $RX = 0$ *and R is a resolving matrix*, the algorithm should eventually be able to verify that $RX = 0$ at α.

3) If $RX = 0$ at α, but R is not a resolving matrix (due to not having maximal rank), the algorithm may evenutally verify that $RX = 0$ at α, or it may not terminate.

4) If the algorithm does verify that $RX = 0$, it also produces a definition of α $(S_i = 0, E_{i,1} = 0)$ which uses less than k exponential terms.

In order to be sure that if $RX \neq 0$ at α the algorithm eventually recognizes this, the algorithm must periodically try to prove $RX \neq 0$ using the latest approximation to α and the latest error bounds.

We suppose that α is defined by $(S = 0, E_k = 0)$ in N. We add the $2d$ equations associated with R: $RX = 0$ and $Y^R = 1$ to get

$$\Delta_R = (S = 0, RX = 0, Y^R - 1 = 0, E_k = 0)$$

We break this up into traingular parts, using the zero structure decomposition, obtaining $\Delta_1, ..., \Delta_t$. Set

$$Poss = \{\Delta_1, ..., \Delta_t\}$$

. Suppose that R is a resolving matrix for $(S = 0, E_k = 0)$ in N. Then one of the above triangular conditions must be satisfied at α. So consider each of the conditions in turn.

Until the set of possibilities , $Poss$, becomes empty:
Remove Δ_i from $Poss$.
$\Delta_i = (S_i = 0, E_{i,1} = 0, E_{i,2} = 0, I_i \neq 0, J_i \neq 0)$
Δ_i implies $(S = 0, E_k = 0)$. So if Δ_i is not zero dimensional, it can't be satisfied at α. In this case discard Δ_i.
Δ_i also implies Δ_R. So at least d of the exponential terms of E_k are redundant. Thus $E_{i,2}$ must have at least d exponential terms in it. If not, discard Δ_i.

Suppose $E_{i,2}$ has more than d exponential terms in it. Then $E_{i,1}$ has less than $k-d$ terms in it, and so S_i has more than $(2n-(k-d))$ polynomials in it. Thus the transcendence rank of α would be less than $(k-d)$ if α satisfied Δ_i. By

Schanuel's conjecture, there could not be $(k-d)$ linearly independent values in X at α. This would contradict our assumption that R is a resolving matrix. So in this case also, discard Δ_i.

We are left to consider Δ_i so that $E_{i,2}$ has d terms in it, $E_{i,1}$ has $(k-d)$ terms in it S_i has $(2n-(k-d))$ terms in it.

The $(k-d)$ terms of $E_{i,1}$ correspond to linearly independent columns of R. The differentials of terms in $E_{i,2}$ can all be written as linear combinations (with rational coefficients) of differentials of terms in $E_{i,1}$.

We suppose the terms in $E_{i,2}$ are $w_1 - e^{z_1}, ..., w_d - e^{z_d}$, and the terms in $E_{i,1}$ are $w_{d+1} - e^{z_{d+1}}, ..., w_k - e^{z_k}$. We have all of the variables in $E_{i,2}$ expressed in terms of the variables in $E_{i,1}$. For $s = 1, ..., d$ $m_s z_s = \sum_{d+1}^{k} a_{s,j} z_j$, $w_s^{m_s} = \prod_{d+1}^{k} w_{s,j}^{a_j}$ for some integral values $a_{s,j}, m_s$. These integer values are obtained just by solving $RX = 0$. We have $(S_i = 0, E_{i,1} = 0)$ implies $E_{i,2} = 0$.

We are now left with the problem of trying to verify that $\Delta_i = (S_i = 0, E_{i,1} = 0, E_{i,2} = 0, I_i \neq 0, J_i \neq 0)$ has a solution in N. We first try to show that $I_i \neq 0$ and $J_i \neq 0$ at α. If we can not do this with the current approximation to α, return Δ_i to *Poss*. Δ_i is not, at this stage, discarded.

Suppose, on the other hand that we do verify that I_i and J_i are not zero at α. We next try to prove that $S_i \neq 0$ or $E_{i,1} \neq 0$ at α, using our current approximation to α. If we succeed in doing this, we discard Δ_i. Suppose we do not succeed in doing this.

Consider $f = (S_i, E_{i,1}) : R^{4n} \rightarrow R^{4n}$, and consider N as a domain in R^{4n}. Assume N has been contracted sufficiently so that $f = 0$ has no solution on the boundary of N. We can verify that $f = 0$ has a solution in N either by using the Kantorovich theorem, or by calculating the topological degree $deg(N, f, 0)$ of f over N.

Since f is orientation preserving, if the degree is 0, there is not a solution in N. In this case we discard Δ_i.

If the degree is not zero, then $f = 0$ has a solution in N. Assuming that N has already been contracted so that $(S = 0, E_k = 0)$ has a unique solution in N and that is α, it must be that α also satisfies Δ_i. In this case we have verified that $RX = 0$ at α. We also have a new definition for α, namely as the solution of $(S_i = 0, E_{i,1} = 0)$ in N. This new definition uses d less exponential terms than the original one.

If all of the Δ_i have been discarded, we are not able to prove that $RX = 0$. In this case we just wait to see if it turns out that $RX \neq 0$, or if the algorithm is completed on some other branch. □.

5 Correctness of Solution to Constant Problem

Theorem 3 Suppose the constant solving algorithm is given α defined in N by $S = 0, E_k = 0)$, and polynomial p. If none of A,B,C in the Constant Solving Algorithm ever terminate, then $(x_1, ..., x_n)$ at α contains a counterexample to Schanuel's conjecture.

Proof. Branch A does not terminate means $p(\alpha) = 0$. Also suppose that branch B does not terminate. Assume N in branch B has been contracted far enough so that $S = 0$ defines a single manifold, of dimension $(2n-k)$ in N. Then the polynomial p is not identically zero on this manifold, and the zero set of p on this manifold is a union of lower dimensional manifolds. Thus the transcendence rank of $(S = 0, p = 0)$ in N is less than k, and the transcendence rank of X at α is less than k. By Schanuel's conjecture restricted to α, X at α must be linearly dependent over the rationals. Thus there exists a resolving matrix R for the system. This matrix R will eventually be guessed by one of the C branches of the algorithm. The resolving matrix semi algorithm now comes in to play. A set of triangular conditions $\Delta_1, ..., \Delta_t$ is generated. One of these conditions is satisfied at α. Suppose this condition is

$\Delta_i = (S_i = 0, E_{i,1} = 0, E_{i,2} = 0, I_i \neq 0, J_i \neq 0)$

Eventually we get a good enough approximation to α to verify that $I_i \neq 0$ and $J_i \neq 0$. The condition $E_{i,2} = 0$ is now implied by the others. So it is only necessary for the algorithm to check that $(S_i = 0, E_{i,1} = 0)$ has a solution in N. It infallibly does this using topological degree or, if the neighbourhood is small enough, by the Kantorovich theorem. So we get termination on branch C. □

6 The Identity problem for Implicitly Defined functions

Suppose we have a function defined as $f(Z) = p(Z, W(Z))$, where $W(Z)$ is implicitly defined near elementary point α by exponential system $(S, E) = 0$. We say $F(Z) \equiv 0$ if there is some neighbourhood of α in which $p(Z, W(Z)) \equiv 0$. We need to show that both $F(Z) \equiv 0$ and $f(Z) \not\equiv 0$ can be recognised.

We can find D, an open set in the domain of definition of $f(Z)$, i.e. in the space of the independent variables. It is clear that $f(Z) \not\equiv 0$ can be recognised. We just pick a generic point in D and evaluate. We need to show that $f(Z) \equiv 0$ can be recognised. Suppose that there are k variables in Z. Form $(S = 0, p = 0, E = 0)$

Break this up into a number of possible triangular conditions, $\Delta_1, ..., \Delta_m$. If $f(Z) \equiv 0$ is true one of these conditions, of dimension k, must be satisfied by any generic point in D. Discard all the triangular conditions which do not have dimension k. Pick a point with rational coordinates, at random, in D, say Z_Q. The point $(Z_Q, W(Z_Q))$ is elementary. Use the solution of the constant problem to decide whether or not one of the triangular conditions of dimension k is satisfied at this point.

7 What is needed for an implementation?

The work which needs to be done can be broken into four parts.

1. Implement the decomposition of exponential systems into triangular parts[12]. While not difficult, making it run quickly is quite hard. A prototype exists[7].

2. Implement numerical computation of topological degree [5, 3, 6]. This can be used to decide whether or not a non singular exponential system $(S = 0, E = 0)$ with $2n$ equations in $2n$ unknowns has a solution in a neighbourhood N. Algorithms to do this are known[6] but are computationally expensive. The topological degree computation should never be used where a standard iterative numerical technique can be used instead. It is a difficult problem efficiently to combine these two approaches.

3. Use the MLLL algorithm or some other method to guess a resolving matrix of rank d for a system $(S = 0, E = 0)$ in a neighbourhood N.

4. Implement the resolving matrix recognising algorithm of section 4.3.2.

References

[1] J. Ax. Schanuel's conjecture. *Ann Math*, 93:252–268, 1971.

[2] B. F. Caviness. On canonical forms and simplification. *Journal of the ACM*, 17(2):385–396, April 1970.

[3] J. Cronin. *Fixed Points and Topological Degree in Nonlinear Analysis.* American Mathematical Society, 1964.

[4] H. R. P. Ferguson and R.W. Forcade. Multidimensional euclidean algorithms. *J. Reine Ange. Math*, 33:171–181, 1982.

[5] N. G. Lloyd. *Degree Theory.* C.U.P., 1968.

[6] P. Moseley. Calculating topological degree. Technical report, Bath University School of Mathematical Sciences, 1993.

[7] W. Naylor. Master's thesis, School of Mathematical Sciences, University of Bath, 1993.

[8] M. Pohst. A modification of the LLL reduction algorithm. *J. Symbolic Computation*, 4:123–127, 1987.

[9] P. Rabinowitz, editor. *Numerical Methods for Nonlinear Algebraic Equations.* Gordon and Breach, 1970.

[10] D. Richardson. Some undecidable problems involving elementary functions of a real variable. *Journal of Symbolic Logic*, pages 514–520, 1968.

[11] D. Richardson. The elementary constant problem. In *Proceedings of ISSAC92, Berkeley, California.* SIGSAM, ACM, July 1992.

[12] D. Richardson. A zero structure theorem for exponential systems. In *Proceedings of ISSAC93, Kiev, Ukraine.* SIGSAM, ACM, July 1993.

[13] M. Rosenlicht. On Liouville's theory of elementary functions. *Pacific Journal of Mathematics*, 65(2):485–492, 1976.

[14] J. Shackell. A differential equations approach to functional equivalence. In G. Gonnet, editor, *ISSAC'89*, ISSAC, pages 7–10. ACM, ACM Press, 1989.

[15] W. T. Wu. Basic principles of mechanical theorem proving in elementary geometries. *J. Sys. Sci. and Math. Scis*, f(3):207–235, 1994.