# How to Recognize Zero


Daniel Richardson,
Department of Mathematics, University of Bath.
email : dsr@maths.bath.ac.uk


July 10, 1997


**Abstract**

An elementary point is a point in complex $n$ space, which is an isolated, non singular solution of $n$ equations in $n$ variables, each equation being either or the form $p = 0$, where $p$ is a polynomial in $\mathbf{Q}[x_1, ..., x_n]$, or of the form $x_j - e^{x_i} = 0$. An elementary number is the polynomial image of an elementary point. In this article a semi algorithm is given to decide whether or not a given elementary number is zero. It is proved that this semi algorithm is an algorithm, i. e. that it always terminates, unless it is given a problem containing a counter example to Schanuel's conjecture.


## 1 Introduction

In computing, a *lazy sequence* is a finite initial segment of a sequence together with a process which generates more elements of the sequence, if desired. See, for example, Paulson (1991).

By analogy with this we may say that a lazy complex (or real) number is a bounded precision floating point complex (or real) number together with a process which could be used to increase the precision to any desired extent.

We will say that two such lazy numbers are equal if repeated application of their processes results in sequences which converge to the same ordinary number. (Of course there are other reasonable definitions of equality for lazy numbers. The one given here might be called standard equality.) It will be assumed in the following that real and complex numbers are given in lazy form, rather than as completed infinities of some kind.

The following fundamental question immediately presents itself:

*For which natural subsets of the real and complex numbers can we do exact computations?*

The computations of interest include the field operations, a test for equality among complex numbers, and determination of the sign of a real number.

It is clear that we can patch our approximations and processes together in order to effect addition, subtraction and multiplication. If two numbers are unequal, we will eventually be able to recognize this, by calculating them to sufficient precision. However, there may be problems recognizing equality.

If we could recognize zero, we could recognize equality, since we can do subtraction. If we can recognize zero, we can also avoid mistakes with division by zero, so we can do division. Also if we can recognize zero we can order real numbers effectively.

So the central part of the above problem reduces to: In which natural subsets of the real and complex numbers can we recognize zero?

In the following section a definition is given for a subset of the complex numbers which is called *elementary*. This set will be denoted by $\mathcal{E}$.

$\mathcal{E}$ is algebraically closed and is also closed under application of elementary functions, such as $e^x$, $sin(x)$, $cos(x)$. Also, isolated solutions of systems of equations involving elementary functions and polynomials with coefficients in $\mathcal{E}$ have coordinates which are in $\mathcal{E}$.

The main result below is that we can recognize zero among the elementary numbers, unless we are given a problem which contains a counterexample to Schanuel's conjecture. (The Schanuel conjecture is explained below.)

Let $\mathbf{Q}$ be the rational numbers.

If $B$ is a set of complex numbers and $z$ is complex, we will say that $z$ is algebraically dependent on $B$ if there is a polynomial

$p(t) = a_0 t^d + ... + a_d$

in $\mathbf{Q}[B][t]$ with $a_0 \neq 0$, $d > 0$ and $p(z) = 0$.

If $S$ is a set of complex numbers, a transcendence basis for $S$ is a subset $B$ so that no number in $B$ is algebraically dependent on the rest of $B$ and so that every number in $S$ is algebraically dependent on $B$.

The transcendence rank of a set $S$ of complex numbers is the cardinality of a transcendence basis $B$ for $S$. (It can be shown that all transcendence bases for $S$ have the same cardinality.)

**Schanuel's conjecture** If $z_1, ..., z_n$ are complex numbers which are linearly independent over $\mathbf{Q}$, then $\{z_1, ..., z_n, e^{z_1}, ..., e^{z_n}\}$ has transcendence rank at least $n$.

It is generally believed that this conjecture is true, but that it would be extremely hard to prove.

The history of the zero recognition problem is somewhat confused by the fact that many people do not recognize it as a problem at all.

In the algebraic case, the nature of the problem depends upon what we decide to accept as the definition of a complex algebraic number.

In general, our way of understanding the algebraic numbers has been influenced by the historical struggle to separate out the abstract algebra from interpretation in the complex numbers. From this point of view, it has been assumed that algebra should avoid floating point approximations. So it has been considered that the right way to do an algebraic computation is to put all the numbers involved into an algebraic number field, an abstract object in which there is a canonical form. See [Frohlich and Shepherdson, 1956]. (Note that we do not have a useful canonical form for the whole set of algebraic numbers, but only for the numbers in each particular finitely generated algebraic number field.)

If we are ultimately interested in floating point numbers, it is not clear that it is sensible to construct an enclosing algebraic number field in order to do one computation. But in any case this option disappears when we work with elementary numbers. There is at present no sufficiently developed theory of elementary number field. We do not, for example, know which abstract fields with exponentiation can be embedded into the complex numbers. The ideal of separation between algebra and geometric interpretation does not seem to work very well in this case.

The first good result about recognition of zero among non algebraic numbers is due to Caviness [ 1970 ]. Caviness shows, in essence, that if a weak version of the Schanuel conjecture is true it is possible to define a canonical form, and thus to solve the zero recognition problem in the set of numbers which are obtained by starting with the rationals and $i$ and closing under addition, subtraction, multiplication, and exponentiation. Of course, this set is probably not algebraically closed.

More recently, Wilkie and Macintyre have proved that if the Schanuel conjecture is true then the theory of $(R, e^x)$ is decidable, where $R$ is the ordered field of the reals.

In particular the Wilkie and Macintyre result solves the zero recognition problem for the (necessarily elementary) numbers in the minimal model for this theory. Their methods can be extended also to the theory of $(R, e^x, sin_{[0,1]}(x))$, where $sin_{[0,1]}(x)$ means $sin(x)$ restricted to the interval $[0,1]$, and defined to be 0 outside this interval. In this theory all the real elementary numbers are definable. The real and imaginary part of complex elementary numbers are real elementary. So the methods of Wilkie and Macintyre can be used to show that the zero recognition problem can be solved for the elementary numbers.

The work reported in this article is the result of a long independent development, however, the intention of which is ultimately to develop algorithms to solve problems in the real and complex numbers. [See Richardson 1969, 1971, 1991, 1992, 1993, 1994, 1995]. The techniques used here, i.e. Wu's method and the LLL algorithm, have their origins in computer algebra rather than in model theory.

## 2 Elementary points and numbers

**Definition 1** *An exponential system in variables* $x_1, ..., x_n$ *is* $(S_r, E_k)$*, where* $S_r = (p_1, ..., p_r)$ *is a list of* $r$ *polynomials in* $\mathbf{Q}[x_1, .., x_n]$*, and* $E_k = (w_1 - e^{z_1}, ..., w_k - e^{z_k})$ *is a list of* $k$ *terms,* $w_i - e^{z_i}$*, with* $\{w_1, ..., w_k, z_1, ..., z_k\} \subseteq \{x_1, ..., x_n\}$*.*

Let $C$ be the complex numbers.

In all the following, we will use $(S_r, E_k)$ to denote an exponential system, as described above. We will use $J(S_r, E_k)$ to denote the $r+k$ by $n$ matrix of partial derivatives $(\partial f_i/\partial x_j)$, where $(f_1, ..., f_r) = S_r$ and $(f_{r+1}, ..., f_{r+k}) = E_k$.

**Definition 2** *If $\alpha$ is a point in $C^n$, we will say that $(S_r, E_k)$ is non singular at $\alpha$ if $r+k=n$, and if the matrix $J(S_r, E_k)$ is non singular at $\alpha$.*

**Definition 3** *A point $\alpha$ in $C^n$ is* elementary *if there is an exponential system $(S_r, E_k)$, with $r+k=n$ so that $(S_r, E_k)(\alpha) = 0$, and so that $(S_r, E_k)$ is non singular at $\alpha$.*

**Definition 4** *A complex number $c$ is* elementary *if there is an elementary point $\alpha$ and a polynomial $q$ in $\mathbf{Q}[x_1, ..., x_n]$ so that $c = q(\alpha)$.*

At each stage in the following, we will assume that we have approximated some elementary numbers to within some tolerance $\epsilon = 10^{-prn}$. We will use $prn$ for the number of decimal places which are currently assumed to be known.

If $(x_1, ..., x_n)$ is in $C^n$, define $d(x_1, ..., x_n)$ to be the maximum of the absolute values of the real and imaginary parts of $x_1, .., x_n$, i.e.

$d(x_1, ..., x_n) = Max(\mid Re(x_1) \mid, \mid Im(x_1) \mid, ..., \mid Re(x_n) \mid, \mid Im(x_n) \mid)$.

For $\alpha$ in $C^n$, let $N_\epsilon(\alpha) = \{\beta : d(\alpha - \beta) \leq \epsilon\}$.

$N_\epsilon(\alpha)$ can be visualized as a coordinate aligned box in $R^{2n}$ around $\alpha$. We will use $\partial N_\epsilon(\alpha)$ to denote the boundary of $N_\epsilon(\alpha)$.

It is assumed that we have an interval arithmetic procedure for polynomials in $x_1, ..., x_n$, $e^{x_1}, ...., e^{x_n}$ with the following property: if $p$ is an expression for such a polynomial and $\alpha^*$ is an $n$ tuple of $prn$ precision complex floats, then the interval arithmetic procedure applied to $p$ over $N_\epsilon(\alpha^*)$ gives a pair of intervals $(I_r, I_i)$, with rational endpoints, so that the box which is the product of them in the complex plane is guaranteed to contain the image of $N_\epsilon(\alpha^*)$ under $p$. Furthermore, the procedure is such that the lengths of $I_r$ and $I_i$ tend to zero as $prn$ increases. [See Alefeld and Herzberger, 1983].

We will say $\vdash_{prn} p \neq 0$ in $N_\epsilon(\alpha^*)$ if the intervals $(I_r, I_i)$ produced by the interval arithmetic procedure do not both contain zero, i.e. if the complex 0 is not in the box which is the product of the intervals.

We will say $possible(p = 0, N_\epsilon(\alpha^*))$ in the complementary case in which the intervals $(I_r, I_i)$ produced by the interval arithmetic procedure do both contain zero.

Of course $\vdash_{prn} p \neq 0$ in $N_\epsilon(\alpha^*)$ depends on a particular expression for $p$, and not just on $p$ as a function, since we do not, for example assume that our interval arithmetic procedure obeys the distributive law.

$\vdash_{prn} p \neq 0$ in $N_\epsilon(\alpha^*)$ implies

$(\forall X \in N_\epsilon(\alpha^*))p(X) \neq 0$, but is much stronger. As an important special case of this, if $p$ is the (unsimplified) determinant of $J(S_r, E_k)$, with $r+k=n$, and if $\vdash_{prn} p \neq 0$ in $N_\epsilon(\alpha^*)$ , then the system of equations

$$(S_r, E_k) = 0$$

can have at most one solution in $N_\epsilon(\alpha^*)$. See Aberth[1994] for a discussion of this.

## 2.1 How is an elementary number given?

We will assume in all the following that an elementary number $c \in \mathcal{E}$ is given to us in the following way:

1. We are given an exponential system $(S_r, E_k)$ in $n$ variables, $x_1, ..., x_n$, with $r + k = n$.
2. We are given a neighbourhood $N_\epsilon(\alpha^*)$ , with $\epsilon = 10^{-prn}$ and $\alpha^*$ is an $n$ tuple of precision $prn$ complex floats. Let $J$ be the determinant of $J(S_r, E_k)$. We have $\vdash_{prn} J \neq 0$ in $N_\epsilon(\alpha^*)$
3. We are given a proof that there is a point $\alpha$ in the interior of $N_\epsilon(\alpha^*)$ so that $(S_r, E_k)(\alpha) = 0$.
4. The number $c$ is defined as $q(\alpha)$ where $q$ is a polynomial in $\mathbf{Q}[x_1, ..., x_n]$ and $\alpha$ is the elementary solution of $(S_r, E_k) = 0$ in $N_\epsilon(\alpha^*)$ .

We need to say some more about what kind of proofs might be acceptable for item 3 above. Suppose there is no solution of $(S_r, E_k) = 0$ in $\partial N_\epsilon(\alpha^*)$. In this case the topological degree of $(S_r, E_k)$ over $N_\epsilon(\alpha^*)$ is defined, and can be calculated by any one of a number of algorithms. One algorithm to calculate such a degree is in Aberth [1994]. This calculation will use floating point arithmetic but at a precision higher than *prn* and will also verify that there is no solution on the boundary of the box. Because of item 2 above, the only possible values for the degree are -1, 0, or +1, and there is a solution in the neighbourhood if and only if the degree is non zero.

Item 2 also implies that any solution in $N_\epsilon(\alpha^*)$ is necessarily non singular, and that there is at most one solution of $(S_r, E_k) = 0$ in $N_\epsilon(\alpha^*)$.

If *prn* is sufficiently large, we can use Newton's method to get a sequence of increasingly good approximations to $\alpha$:

$\alpha_0 = \alpha^*$

$\alpha_{i+1} = \alpha_i - J(S_r, E_k)^{-1}(S_r, E_k)(\alpha_i)$.

Not only is convergence of this guaranteed for sufficiently large *prn*, but there are also standard tests to verify convergence in $N_\epsilon(\alpha^*)$, provided, again, that *prn* is sufficiently large. One such is given by the Kantoravitch theorem in Rabinowitz [1970 ]. Others are given in Alefeld and Herzberger [1983], and in Richardson [1995]. These tests for Newton convergence can also be used, instead of computation of topological degree, to verify the existence of a solution in the neighbourhood.

In terms of giving the proofs required in item 3 above, it is not clear whether we should prefer topological degree computation, or a Newton convergence test, or some other method. All we are claiming here is that there exist feasible standard methods for giving such proofs. All these methods depend upon the fact that the number of equations is the same as the number of unknowns, and that we have a guarantee for the non singularity of the Jacobian in $N_\epsilon(\alpha^*)$.

Once we have a proof that there is a unique solution of $(S_r, E_k) = 0$ in $N_\epsilon(\alpha^*)$, we can use either Newton's method, or recursive subdivision and interval arithmetic to increase *prn*, reduce $\epsilon$ and improve our approximation $\alpha^*$. This method of giving the number $c$ is consistent with the lazy philosophy stated earlier.

Note that the proof is part of the presentation of an elementary number. If we are not given enough information, for example if the precision is not high enough to carry out either of the types of verification mentioned above, then we have not been given a correct specification of an elementary number.

## 2.2 A consequence of Schanuel's conjecture

We will say that a list of polynomials, $S_r = (p_1, ..., p_r)$, is independent at $\alpha$ in $C^n$ if the $r$ by $n$ matrix of partial derivatives $(\partial p_i / \partial x_j)$ has rank $r$ at $\alpha$, i.e. if the gradients of $p_1, ..., p_r$ are linearly independent at $\alpha$.

If there are $r$ independent polynomials, $S_r$, in $\mathbf{Q}[x_1, ..., x_n]$ at $\alpha$, then, by the implicit function theorem, the equation $S_r = 0$ implicitly defines $r$ of the coordinate variables as algebraic functions of the other variables in some neighbourhood of $\alpha$. In this case the transcendence rank of the coordinates of $\alpha$ can be at most $n - r$.

We have the following obvious consequence of Schanuel's conjecture.

**Proposition** (Assuming Schanuel's conjecture). *Suppose* $(S_r, E_k)(\alpha) = 0$ *and* $r + k > n$, *and* $E_k = (w_1 - e^{z_1}, ..., w_k - e^{z_k})$, *and* $S_r$ *is independent at* $\alpha$. *Then, at* $\alpha$, $z_1, ..., z_k$ *are linearly dependent over* $\mathbf{Q}$.

Proof. If $z_1, ..., z_k$ were linearly independent over $\mathbf{Q}$ at $\alpha$, then, by Schanuel's conjecture, $\{z_1, .., z_k, w_1, .., w_k\}$ would have transcendence rank at least $k$ at $\alpha$. Thus $\{x_1, ..., x_n\}$ would have transcendence rank at least $k$. In this case there could exist at most $n - k$ independent polynomials in $\mathbf{Q}[x_1, ..., x_n]$ which are also zero at $\alpha$. Since $r > n - k$ we have a contradiction.

$\square$.

As will be seen later, this implies that any identity among elementary numbers is either an algebraic consequence of their definitions or is explained by a linear relationship between numbers which appear in the definitions as arguments of the exponential function. So, in order to detect the presence of zero, we need to be able to detect linear relationships over $\mathbf{Q}$ among elementary numbers, and we also need a systematic way to make algebraic deductions. The first problem is solved below with the help of the LLL algorithm, and the second is solved subsequently using a variation of Wu's method.

# 3 Finding rational linear relationships among elementary numbers

Suppose we are given an elementary point $\alpha$ in $C^n$, as described above.

The point $\alpha$ is the unique solution of $(S_r, E_k) = 0$ in $N_\epsilon(\alpha^*)$, and $E_k = (w_1 - e^{z_1}, ..., w_k - e^{z_k})$.

We suppose that $(z_1, ..., z_k)$ and $(w_1, ..., w_k)$ are coordinate values of $\alpha$. These values are fixed, although we only currently know them approximately, as $\alpha^*$, with error no more than $\epsilon$. Using the values in $\alpha^*$ and the error bound, we get a z-box, containing $(z_1, ..., z_k)$ and a w-box, containing $(w_1, ..., w_k)$.

We wish to find, if possible, a non trivial sum $\sum n_i z_i$, with $n_1, ..., n_k$ integral, so that the sum is indistinguishable from zero, according to the current precision, i.e. so that

$possible(\sum n_i z_i = 0, N_\epsilon(\alpha^*))$.

A sum of this sort will be called a candidate sum.

Define the height of a sum $\sum n_i z_i$ to be $Max(\mid n_1 \mid, ..., \mid n_k \mid)$.

We prefer candidates with small height. Of course, if one of the $z_i$ is itself indistinguishable from zero, we can immediately find a candidate sum of height one. We assume in the following, therefore, that for all $z_i$

$\vdash_{prn} z_i \neq 0$.

This means that the z-box, containing the possible $z$ values is a product of intervals, none of which straddles zero. Let $m$ be the minimum of the absolute values of the coordinates of the z-box.

We will also suppose in the following that $prn$ is sufficiently large so that

**Condition 1:** $prn > 4k$, and $10^{-prn/4k} < m < 10^{prn/4k}$

Define $\mu_N(z_1, ..., z_k)$ to be the minimum of $\mid \sum n_i z_i \mid$ for non trivial sums of height $\leq N$.

Let $M$ be an upper bound for the mean of $\mid z_1 \mid, ..., \mid z_k \mid$.

There are $(2N+1)^k$ sums of height $\leq N$, and all such sums have absolute value no more than $NkM$.

Around each such point, put a circle of radius $2NkM/(2N+1)^{k/2}$. At least two of these small circles overlap, since the sum of the areas of the small circles is more than $\pi(NkM)^2$.

So there must be two such sums with different coefficients which differ by no more than $(4NkM)/(2N+1)^{k/2}$. If we subtract these two sums, we get a sum of height $\leq 2N$. We have

$\mu_{2N}(z_1, ..., z_k) \leq (4NkM)/(2N+1)^{k/2}$.

So if $N$ is even $\mu_N(z_1, ..., z_k) \leq (2NkM)/(N+1)^{k/2}$, and in general

$$\mu_N(z_1, ..., z_k) \leq (2NkM)/N^{k/2}$$

If $z_1, ..., z_k$ are all real, we get a better bound

$$\mu_N(z_1,...,z_k) \leq NkM/N^k$$

We also would like to have a lower bound for $\mu_N(z_1,...,z_k)$ but of course this depends on $z_1,...,z_k$. It is not clear to me how to estimate this lower bound, even when $z_1,...,z_k$ are chosen at random.

**Open Question:** *Suppose $z_1,...,z_k$ are chosen at random independently with uniform distribution in $(0,1)$. What is the expected value and variance of $\mu_N(z_1,...,z_k)$?*

There is some numerical evidence for the following.

**Conjecture:** *For almost all $z_1,...,z_k$ and for all sufficiently large $N$, $(m/N^{k+1} \leq \mu_N(z_1,...,z_k)$. )*

In view of this conjecture, we will say that a non trivial sum of height no more than $N$ is *surprisingly small* if $|\sum n_i z_i| < m/N^{2k}$.

We would like to calculate $prn$ and $N$ from the definition of $\alpha$ in such a way that

$$possible(\sum n_i z_i = 0, N_\epsilon(\alpha*)) \Rightarrow \sum n_i z_i = 0$$

if $\sum n_i z_i$ has height $\leq N$. In other words we would like some sort of gap theorem for elementary numbers. This is not available at present. So we impose the following somewhat arbitrary condition, derived from the concept of a surprisingly small sum mentioned above.

**Condition 2:** $N$ is the integer ceiling of $(10^{prn}m)^{1/2k}$

In order to find a candidate sum we can use the LLL algorithm as follows. Let $I_k$ be the $k$ by $k$ identity matrix. Let $Re_k$ be the column vector obtained by transposing $10^{prn/2}(Re(z_1^*),...,Re(z_k^*))$, where $z_1^*,...,z_k^*$ are the precision $prn$ floating point approximations to $z_1,...,z_k$. Similarly, let $Im_k$ be the column vector obtained by transposing $10^{prn/2}(Im(z_1^*),..,Im(z_k^*))$. Let $V_{k,k+2}$ be the $k$ by $k+2$ matrix of precision $prn/2$ floating point numbers whose first $k$ columns are the same as $I_k$ and whose last two columns are $Re_k$ and $Im_k$ respectively.

$$V_{k,k+2} = I_k Re_k Im_k$$

Suppose the rows of $V_{k,k+2}$ are $(v_1,...,v_k)$. Form a lattice $LV$ in $R^{k+2}$ with basis $v_1,...,v_k$. Now use the LLL algorithm to find a reduced basis $v_1*,...,v_k*$ for $LV$. See [Lenstra ].

Suppose $v_1*$ is $(n_1,...,n_k,\epsilon_1,\epsilon_2)$. Then $\sum n_i z_i$ is a possible candidate sum. We accept it as a candidate if it passes the tests, i.e. if its height is bounded by $N$ and if it is not distinguishable from zero using the current precision. If one of these tests fails, then our attempt to find a candidate has also failed. However, the following lemma shows that if $z_1,...,z_k$ actually are linearly dependent over $\mathbf{Q}$, then our method, applied on an increasing sequence of precisions, will eventually find a correct relationship.

**Lemma 1** *Suppose that, at $\alpha$, $z_1, ..., z_k$ are linearly dependent over* $\mathbf{Q}$. *If prn is sufficiently large, and $v_1^* = (n_1, ..., n_k, \epsilon_1, \epsilon_2)$ is the first vector in the reduced basis found by the LLL algorithm as described above, then*
$\sum n_i z_i = 0$ *at $\alpha$.*

Proof.
The idea of the proof is that as *prn* is increased, false candidates get pushed out of contention; eventually, the only possible initial vector in a reduced basis is a true candidate, if there is any such.
We rely on the following result about reduced bases.
*If vmin is a minimal length non zero vector in the lattice $LV$, then*
$| v_1^* |^2 \leq 2^k \mid vmin |^2$ .
See Lenstra.
Suppose $z_1, ..., z_k$ are linearly dependent over $\mathbf{Q}$. Then there is an upper bound $B$, valid for all *prn*, on the length of *vmin*, a minimal length non zero vector in the lattice. In other words, no matter how much *prn* is increased, there will be a non zero vector in the lattice of length no more than $B$. It follows that the first vector in a reduced basis must have length $\leq 2^k B$, no matter how large *prn* is. Since the initial part of $V_{k,k+2}$ is $I_k$, there are only $(2^k B + 1)^k$ vectors in the lattice which could possibly have length $\leq 2^k B$. The initial vector in a reduced basis must be one of these finitely many possibilities. But if *prn* is sufficiently large, all of these will have size bigger than $2^k B$, except for those which correspond to linear combinations of $z_1, ..., z_k$ which are actually zero at $\alpha$.
□
In fact it is also true that if there are $d$ independent linear relationships between $z_1, ..., z_k$ at $\alpha$ and if *prn* is sufficiently large, the first $d$ vectors in the reduced basis will give us $d$ correct relationships. So we could take more than one candidate from the reduced basis. This computationally useful possibility is ignored in the following, in order to simplify the exposition.
Suppose we have found a candidate sum $\sum_1^k n_i z_i$. Renumber $z_1, ..., z_k$ if necessary so that $n_k$ is non zero but is minimal, in absolute value, among the non zero coefficients. We now intend to use this to replace
$(w_1 - e^{z_1}, ..., w_k - e^{z_k}) = E_k = 0$
by
$(w_1 - e^{z_1}, ..., w_{k-1} - e^{z_{k-1}}) = E_{k-1} = 0$
together with the pair of algebraic conditions:
$n_k z_k = - \sum_1^{k-1} n_i z_i$
$w_k^{n_k} = \prod_1^{k-1} w_i^{-n_i}$
We assume *prn* is large enough to satisfy conditions 1 and 2 given earlier. As before we also assume that there is a solution of $(S_r, E_k) = 0$ in $N_\epsilon(\alpha *)$.
Let $(Z_1, ..., Z_k)$ be any point in the z-box, and let $(W_1, ..., W_k)$ be any point in the w-box. These are obtained by varying the numbers in $\alpha^*$ by no more than $\epsilon$.

**Lemma 2** *If* $W_1 = e^{Z_1}, ..., W_{k-1} = e^{Z_{k-1}}$, *and* $\sum_1^k n_i Z_i = 0$, *and* $1 - \prod_1^k W_i^{n_i}) = 0$, *then* $W_k = e^{Z_k}$.

Proof.

The problem is to exclude the possibility that $(W_k, Z_k)$ are on the wrong branch of the algebraic solution.

We have
$n_k Z_k = -\sum_1^{k-1} n_i Z_i$, and
$W_k^{n_k} = \prod_1^{k-1} W_i^{-n_i} = e^{n_k Z_k}$
So
$W_k = e^{Z_k}\eta$,
where $\eta$ is an $n_k$ th root of unity. We need to show that $\eta = 1$.
If $\eta \neq 1$, then

$$\mid 1 - \eta \mid \geq \pi / N$$

There are values $z_k$ and $w_k$, among the coordinates of $\alpha$, so that
$\mid Z_k - z_k \mid < 2\epsilon$
$\mid W_k - w_k \mid < 2\epsilon$
and $e^{z_k} = w_k$.
$\mid 1 - \eta \mid \mid e^{z_k} \mid$
$= \mid e^{z_k} - \eta e^{z_k} \mid$
$= \mid e^{z_k} - e^{Z_k} + e^{Z_k} - \eta e^{z_k} \mid$
$\leq e^{z_k} - e^{Z_k} \mid + \mid W_k - w_k \mid$
$\leq \mid e^{z_k} \mid 3\epsilon + 2\epsilon$.
If $\mid e^{z_k} \mid \geq 1$, we have $\mid 1 - \eta \mid < 5\epsilon$ and thus $\pi/N \leq 5\epsilon$, which is impossible.
On the other hand, if $\mid e^{z_k} \mid < 1$, we get
$m \mid 1 - \eta \mid < 5\epsilon$, and thus
$\pi/N \leq 5\epsilon/m$, which is also impossible, because $m > 10^{-prn/4k}$.
Thus $\eta = 1$ and $W_k = e^{Z_k}$.
$\square$.

# 4 Wu stratification

A subset $S$ of $C^n$ is a $d$ dimensional manifold if for every point $\alpha$ in $S$ there is a number $\epsilon > 0$ so that $S \cap B_\epsilon(\alpha)$ is diffeomorphic to an open ball in $C^d$, where $B_\epsilon(\alpha)$ is the open ball of radius $\epsilon$ around $\alpha$.

A stratification of a set is a decomposition of it into finitely many manifolds. The manifolds in a stratification are called strata.

An algorithm is given below which uses Wu's method for stratifying sets defined by polynomial equalities and inequalities.

## 4.1 Characteristic sets

The following definitions are taken from Wu, derived, in some cases, from the ideas of J.F. Ritt. Their purpose is to define a method of putting a system of polynomial equations into triangular form.

Suppose we are dealing with polynomials in $\mathbf{Q}[x_1, ..., x_n]$, and we order the variables by importance.

$x_1 \prec x_2 \prec ... \prec x_n$

The *leading variable* of a polynomial is the variable most important in the ordering among those which occur in the polynomial. We will write $lv(p)$ for the leading variable of $p$.

We assume here, unless otherwise stated, that polynomials are written, in normal form, as polynomials in their leading variable, with coefficients which are polynomials, also in normal form, in less important variables. So if $y$ is the leading variable of a polynomial $p$, $p$ would be in the form

$$C_n y^n + ... + C_0$$

where $n$ is called the *degree* of $p$, and $C_n$, assumed to be non zero, is called the *leading coefficient of* $p$. (Of course the leading coefficient may itself be a polynomial in variables below $y$ in the ordering.)

We will write $lc(p)$ for the leading coefficient of $p$.

If $p$ and $q$ are polynomials, $q$ is not a constant, and $y$ is the leading variable of $q$, we will say that *$p$ is reduced with respect to $q$* if the degree of $y$ in $p$ is less than the degree of $y$ in $q$. It may happen that $p$ is reduced with respect to $q$ although the leading variable of $p$ is more important than the leading variable of $q$.

For polynomials $p$ and $q$, we will say $p \prec q$ if the leading variable of $p$ is less important than the leading variable of $q$, or if the leading variables are the same and the degree of $p$ is less than the degree of $q$. If both the leading variables and the degrees of $p$ and $q$ are the same, we will say $p \sim q$.

Let $S_r = (p_1, ..., p_r)$ be a list of polynomials. We will say that $S_r$ is an ascending set if, for each $i < r$, the leading variable of $p_i$ is less important than the leading variable of $p_{i+1}$, and if, for all $j < i$, $p_i$ is reduced with respect to $p_j$.

The next step is to put an order on ascending sets. If $S_r = (p_1, ..., p_r)$ and $S_s = (q_1, ..., q_s)$ are ascending sets, we will say $S_r \prec S_s$ if, for some $k$, $p_1 \sim q_1$ and ... and $p_k \sim q_k$ and $p_{k+1} \prec q_{k+1}$, or if $s < r$ and $p_1 \sim q_1$ and ... and $p_s \sim q_s$.

Note that if we add a new polynomial to the end of an ascending set, the result, if it is an ascending set, is lower in the ordering than the original.

The ascending sets are well ordered by the ordering described above. This means that any descending sequence of ascending sets must be finite. This is useful to prove termination of algorithms. Any process which produces a descending sequence of ascending sets must eventually terminate. If we have a process which produces a tree in which the nodes are labelled with ascending sets and if the ascending sets on each branch are descending and if no node has more than finitely many children, then the tree itself must be finite.

Suppose $p$ and $q$ are polynomials and the leading variable of $p$ is $y$. The usual $pseudoremainder(p, q)$ is defined as follows. Suppose $p$ has degree $n$ in $y$ and $q$ has degree $m$ in $y$. In case $m < n$, we let $pseudoremainder(p, q) = q$. Otherwise, $pseudoremainder(p, q)$ is the remainder after dividing $p$ into $lc(p)^{m-n+1}q$, considering this as a polynomial in $y$ with coefficients in the other variables.

Suppose $S_r = (p_1, ..., p_r)$ is an ascending set , and $q$ is a polynomial. Define $Rem(S_r, q)$, which is called the Wu remainder of $q$ with respect to $S_r$, recursively in terms of the usual pseudoremainder by

$$Rem((p_1), q) = pseudoremainder(p_1, q)$$

in the case $r = 1$, and, for $r > 1$,

$$Rem((p_1, ..., p_{j+1}), q) = Rem((p_1, ..., p_j), pseudoremainder(p_{j+1}, q)).$$

It follows from this that $Rem(S_r, q)$ is reduced with respect to every polynomial in $S_r$, and satisfies an equation of the form

$$(\prod_{i \leq r} I_i^{n_i})q = \sum d_i p_i + Rem(S_r, q)$$

where each $I_i$ is the leading coefficient of $p_i$, and $n_1, ..., n_r$ are some natural numbers, and the $d_i$ are some polynomials.

If $S_r$ is ascending, and $Rem(S_r, q) = q$, we will say that $q$ is reduced with respect to $S_r$. If $S_r = (p_1, ..., p_r)$, then $q$ is reduced with respect to $S_r$ if, for each $i$, $q$ is reduced with respect to $p_i$, i.e. if the degree of the leading variable of $p_i$ in $q$ is less than it is in $p_i$.

Note that if $S_r = (p_1, ..., p_r)$ is ascending, then, for each $i$, the leading coefficient of $p_i$ is reduced with respect to $S_r$, and also the partial derivative of $p_i$ with respect to its leading variable is reduced with respect to $S_r$.

**Definition 5** *If $S$ is a set of polynomials in $\mathbf{Q}[x_1, ..., x_n]$ we will say that an ascending set $A$ is a characteristic set for $S$ if*

- *$A$ is contained in the ideal generated by $S$*
- *If $q$ is any polynomial in $S$, then $Rem(A, q) = 0$*

If $S$ is a set of polynomials, the notation $S = 0$ means the conjunction of the conditions $p = 0$ for all $p$ in $S$.

Note that if $A$ is characteristic for $S$, then $S = 0$ implies $A = 0$; and also $A = 0$ implies $S = 0$, provided that $I(A) \neq 0$, where $I(A)$ is the product of the leading coefficients of $A$.

If ascending set $A_1$ is contained in the ideal generated by $S$ but is not characteristic, then there must be a polynomial $q$ in $S$ so that $Rem(A_1, q) \neq 0$. In this case, suppose $Rem(A_1, q) = r$, and $A_1 = (p_1, ..., p_k)$. We can now use $r$ to construct an ascending set $A_2$ which is below $A_1$ in the ordering, but which is also contained in the ideal generated by $S$. If $r$ is a non zero constant, or if the leading variable of $r$ is less than or equal to all the leading variables of $A_1$, then we can take $A_2 = (r)$. Otherwise, pick $j$ maximal so that the leading variable of $p_j$ is less than the leading variable of $r$. Then let $A_2 = (p_1, ..., p_j, r)$.

**Wu's Characteristic set algorithm:**

We can, given any finite set $S$ of polynomials, find a characteristic set $A$ for $S$.

*First pick any ascending set, $A_1$, which is a subset of $S$ and, among ascending subsets of $S$, is minimal in the ascending set ordering. ($A_1$ can be constructed recursively, starting with the smallest polynomial in $S$.) Call such an $A_1$ a basic set for $S$. Note that $A_1$ may not be minimal in the ideal generated by $S$.*

*Then find Wu remainders of members of $S$ with respect to $A_1$. If all the Wu remainders are 0, then $A_1$ is characteristic. If not all Wu remainders are zero, use a non zero remainder to construct an ascending set $A_2$, as explained above, so that $A_2$ is in the ideal generated by $S$ but $A_2$ has lower order than $A_1$. Continue this process until a characteristic set is obtained.*

The ascending sets generated in this way are decreasing in order, and the ordering on ascending sets is well founded, so the process eventually terminates with a characteristic set.

## 4.2 Wu stratification algorithm

Let $A_r = (p_1, .., p_r)$ be an ascending set. Let $I(A_r)$ be the product of the leading coefficients of $p_1, ..., p_r$. (Recall that the leading coefficient of $p_i$ may be a polynomial in variables below the leading variable of $p_i$.) Let $D(A_r)$ be the product of the partial derivatives of $p_1, ..., p_r$ with respect to their leading variables, i.e.

$D(A_r) = \prod \partial p_i / \partial lv(p_i)$.

Note that there are $r$ distinct leading variables in $A_r$, and that $D(A_r)$ is the Jacobian determinant of the matrix of partial derivatives of $(p_1, ..., p_r)$ with respect to these leading variables. By the implicit function theorem, if $D(A_r)$ is not zero but $A_r = 0$, the leading variables are locally defined implicitly as functions of the other variables by $A_r = 0$.

Thus the condition $(A_r = 0, I(A_r) \neq 0, D(A_r) \neq 0)$ defines either the empty set or an $n - r$ (complex) dimensional manifold in $C^n$.

We can now use the Wu characteristic set algorithm as a tool to construct a stratification for the zero set of any finite set of polynomials, $S$. The stratification for the zero set of $S$ will be presented as a finite tree labelled with conditions $\Delta_1, ..., \Delta_k$, with each $\Delta_i$ defining either the empty set or a manifold in $C^n$. The zero set of $S$ will be the union of the manifolds defined by $\Delta_1, ..., \Delta_k$. The tree will be called $Wu - tree(S = 0)$, and it will be defined recursively.

**Wu stratification algorithm:**

*Suppose given finite set $S$ of polynomials. Let $A_r = (p_1, ..., p_r)$ be the characteristic set for $S$, obtained by the characteristic set algorithm.*

*If one of $p_1, ..., p_r$ is a non zero constant, $S = 0$ is inconsistent, and the $Wu - tree(S = 0)$ will be a single node labelled with the impossible condition* $1 = 0$.

*Otherwise, define $\Delta$ to be $(A_r = 0, I(A_r) \neq 0, D(A_r) \neq 0)$. Define $Wu - tree(S = 0)$ to be the tree which has root labelled with $\Delta$, and which has subtrees $T_1, ..., T_r, \tau_1, ..., \tau_r$, where, for $i = 1, ..., r$,*

$T_i = Wu - tree(S = 0, A_r = 0, lc(p_i) = 0)$

$\tau_i = Wu - tree(S = 0, A_r = 0, \partial p_i / \partial lv(p_i) = 0)$

This construction terminates because the characteristic sets obtained are descending in order on each branch. Note that even a basic set for $(S, A_r, lc(p_i))$ or for $(S, A_r, \partial p_i/\partial lv(p_i))$ must be below $A_r$ in the ordering. This is because each $p_i$ in $A_r$ is reduced with respect to $(p_1, ..., p_{i-1})$, and thus $Rem(A_r, lc(p_i)) = lc(p_i) \neq 0$. Similarly, if $p'_i = \partial p_i/\partial lv(p_i)$, then $Rem(A_r, p'_i) = p'_i$. If $p_i$ has degree one in its leading variable, then $p'_i$ is $lc(p_i)$. If $p_i$ has degree more than one in its leading variable, then $(p_1, p_2, ..., p_{i-1}, p'_i)$ is an ascending set which is below $A_r$ in the ordering.

**Warning:** We would hope that in a stratification tree the boundary of a set defined at a node would be the set defined by the subtree below the node. This does happen in nice cases with this algorithm. But sometimes it does not happen. In fact, the set defined at a node may have lower dimension than the sets defined at subtrees of the node. In exceptional cases, a node may be labelled with a condition which defines the empty set, but it may have subtrees which define non empty sets.

□

Jetender Kang at Bath has implemented this algorithm, using the Axiom computer algebra system. See Kang (1996).

It is not known what the average computational complexity of this algorithm is. In practice it seems to behave like the zero structure decomposition given by Wu.

The Wu stratification described above, together with the use of the LLL algorithm described previously, is sufficient to solve our problem. However, it seems that we do not need the full strength of the Wu stratification, and that it would be computationally useful to define a weaker, local version. This is done below.

### 4.3 Approximate local Wu stratification

If we are mainly interested in a stratification for a set in a certain bounded region of $C^n$, we can prune the Wu tree accordingly, and thus improve the computational behavior of the Wu stratification. This improvement may be especially dramatic if we have a point $\alpha$ in $C^n$ and we are only interested in the limiting case of a very small neighbourhood around $\alpha$. In this case we can pick a small neighbourhood of $\alpha$ and show, using interval arithmetic, that certain semi algebraic sets do not intersect with the neighbourhood; if that happens we do not need to consider branches of the tree corresponding to such sets.

As before we assume that we have a neighbourhood $N_\epsilon(\alpha^*)$ of $\alpha$, and $\epsilon = 10^{-prn}$, and $\alpha^*$ is an $n$ tuple of complex floating point numbers with precision $prn$.

Let $S$ be a finite set of polynomials. We assume $S(\alpha) = 0$, and we are looking for a stratification of the zero set of $S$ near $\alpha$.

In the construction of of $Wu - tree(S = 0)$ we can prune branches which include conditions $q = 0$ where $\vdash_{prn} q \neq 0$ in $N_\epsilon(\alpha^*)$.

We wish, however, to prune more radically. We will therefore adopt the following *eager annihilation rule* .

$$\frac{possible(q = 0, N_\epsilon(\alpha^*))}{q(\alpha) = 0}$$

This will only apply to polynomials which appear in conditions in $Wu - tree(S = 0)$.

A somewhat alarming disadvantage of this rule is that it may give incorrect results if the precision is not high enough. It has the advantage, however, that it collapses the Wu-tree into one node labelled with some condition $\Delta(S = 0)$. We *hope* that $\Delta(S = 0)$ will correctly describe the zero set of $S$ near $\alpha$. The rule will be used in a context in which incorrect results will eventually be recognized as incorrect, and this will force increase of the precision, which (as will be shown) will eventually imply that any results of the rule are correct.

**Approximate local Wu stratification algorithm**

*Suppose given finite set $S$ of polynomials and neighbourhood $N_\epsilon(\alpha^*)$, as explained above. Find characteristic set $A_r = (p_1, ..., p_r)$ for $S$. If, for $i = 1, ..., r$, we have*

$$\vdash_{prn} lc(p_i) \neq 0$$

*and*

$$\vdash_{prn} \partial p_i / \partial lv(p_i) \neq 0$$

*in $N_\epsilon(\alpha^*)$, then let $\Delta(S = 0)$ be $(A_r = 0, I(A_r) \neq 0, D(A_r) \neq 0)$.*

*Otherwise let* $S+$ *be the union of* $S$ *and* $\{p_1, ..., p_r\}$*, and* $\{lc(p_i) : (1 \leq i \leq r \wedge possible(lc(p_i)) = 0, N_\epsilon(\alpha^*)\}$ *and* $\{\partial p_i / \partial lv(p_i) : (1 \leq i \leq r \wedge possible(\partial p_i / \partial lv(p_i) = 0, N_\epsilon(\alpha^*))))\}$.

*Then define* $\Delta(S = 0) = \Delta(S+ = 0)$.

□

This algorithm, given a finite set $S$ of polynomials, produces a condition $\Delta(S = 0)$ of the form

$$(A_s = 0, I(A_s) \neq 0, D(A_s) \neq 0)$$

which either defines a manifold or the empty set, and which has the properties

- $Rem(A_s, q) = 0$ for all $q$ in $S$
- $\vdash_{prn} I(A_s) \neq 0$ and $\vdash_{prn} D(A_s) \neq 0$ in $N_\epsilon(\alpha^*)$.

If, therefore, $A_s(\alpha) = 0$ we have found a manifold which includes $\alpha$ and which is included in the zero set of $S$, which is what we want. In this case we will say that $\Delta(S = 0)$ is *correct* .

However, the algorithm may produce $A_s$ with $A_s(\alpha) \neq 0$. In this case we will say that the result is incorrect.

Suppose the set $S$ of polynomials is fixed.

**Lemma 3** *If the precision, prn is sufficiently large, the result* $\Delta(S = 0)$ *of the approximate local Wu stratification algorithm is correct.*

Proof. The ordering on ascending sets is well founded. The characteristic set algorithm given previously defines an effective map from finite sets of polynomials $S$ to their characteristic sets $ch(S)$, which, of course, are ascending. If the lemma were false, there would be a finite set $S0$ of polynomials so that

- The lemma is false for $S0$
- If $S$ is any set of polynomials with $ch(S) < ch(S0)$ in the ascending set ordering, then the lemma is true for $S$

Let $ch(S0) = A_r = (p_1, ..., p_r)$. We assume that $S0 = 0$ at $\alpha$. So it must happen that $A_r(\alpha) = 0$. If $I(A_r)(\alpha) \neq 0$ and $D(A_r)(\alpha) \neq 0$, then for *prn* sufficiently large, we will be able to prove this and the result of the algorithm will be

$$(A_r = 0, I(A_r) \neq 0, D(A_r) \neq 0)$$

which is correct.

Next suppose that some of the leading coefficients of $A_r$ or some of the leading partial derivatives are zero at $\alpha$. In this case, we can increase the precision until
$lc(p_i)(\alpha) \neq 0 \Leftrightarrow \vdash_{prn} lc(p_i) \neq 0$
$\partial p_i/\partial lv(p_i)(\alpha) \neq 0 \Leftrightarrow \vdash_{prn} \partial p_i/\partial lv(p_i) \neq 0$
in $N_\epsilon(\alpha^*)$ for $i = 1, ..., r$.

Form a sew set $S0+$ by adding the terms, $lc(p_i)$ or $\partial p_i/\partial lc(p_i)$ which do appear to vanish at $\alpha$, to $S0$, using this higher precision. The new set $S0+$ which is formed with this precision is zero at $\alpha$ and has characteristic set which is lower in the ordering than the characteristic set of $S0$. But $S0$ was a counterexample with minimal order characteristic set. So the result for $S0+$ and also for $S0$ will be correct for sufficiently large $prn$. We have a contradiction, and therefore the lemma is true.

□

# 5 Solution of the zero recognition problem among elementary numbers

Assume, as before that an elementary number $c$ is defined as $q(\alpha)$, and $\alpha$ is an elementary point satisfying the defining condition $\alpha \in N_\epsilon(\alpha^*)$ and $(S_r, E_k)(\alpha) = 0$.

The process described below will either show that $c \neq 0$, or will show that $c$ is zero as a consequence of the algebraic and numerical information which we already have; or, if this fails, will proceed by finding good candidate linear relationships and removing exponential terms. If it does not prove possible to verify the correctness of the candidates, it may be necessary eventually to backtrack, i.e. to reject the candidates, to increase the precision and start over with the original problem, replaceing the exponential terms which have been removed.

We assume that $prn$ is initially at some reasonably large value, for example 20.

**Zero recognition process**

Let $S$ be the union of $S_r$ and $\{q\}$. Calculate $A_s$, the characteristic set of $S$. We will use $d$ to denote the number of exponential terms which we have removed from the initial set $E_k$. Set $d = 0$ initially, so that $S_{r+d} = S_r$ and $E_{k-d} = E_k$.

1. Use Newton's method on $(S_{r+d}, E_{k-d})$ to decrease $\epsilon$ to below $10^{-prn}$, and reset $\alpha^*$.

2. If $\vdash_{prn} q \neq 0$ in $N_\epsilon(\alpha^*)$, then return $c \neq 0$.

3. Use approximate local Wu stratification to find $\Delta(S = 0)$, hopefully correct near $\alpha$. If the result is $A_s$ with $s = (n - (k - d))$, and if $\vdash_{prn} J \neq 0$

in $N_\epsilon(\alpha^*)$, where $J$ is the determinant of $J(A_s, E_{k-d})$, calculate the topological degree of

$$(A_s, E_{k-d})$$

over $N_\epsilon(\alpha^*)$. If the result is non zero, return $c = 0$. In all other cases continue.

4. Apply the LLL algorithm to look for non trivial integral linear combinations $\sum_1^{k-d} n_i z_i$ with height $\leq N$ so that

$$possible(\sum_1^{k-d} n_i z_i = 0, N_\epsilon(\alpha^*))$$

If such a candidate sum is found, renumber $z_1, ...., z_{k-d}$ so that $n_{k-d} \neq 0$ and $n_{k-d}$ is minimal in absolute value among the non zero coefficients. Expand $S$ by adding
$\sum_1^{k-d} n_i z_i$
and
$\prod_{(i \leq k-d \wedge n_i > 0)} w_i^{n_i} - \prod_{(i \leq k-d \wedge n_i < 0)} w_i^{-n_i}$
Set $d = d + 1$. Set $E_{k-d}$ to $\{w_1 - e^{z_1}, ..., w_{k-d} - e^{z_{k-d}}\}$. Go back to step 3) with new $(S, E_{k-d})$.

If no candidate sum is found, double $prn$, reset $d = 0$ and backtrack to step 1) with $S$ set to be the union of $S_r$ and $\{q\}$ and $A_s$, as initially calculated.

**Theorem 1** *If the zero recognition process given above terminates, it does so with the correct answer. If the process does not terminate, then* $(z_1, ..., z_k, e^{z_1}, ..., e^{z_k})$ *contains a counterexample to Schanuel's conjecture.*

Proof.

For the first part of the theorem we observe that the process can only terminate at step 2) or step 3). For correctness at step 2), we rely on the supposed correctness of our interval arithmetic procedure.

Suppose we get termination at step 3). This means that we have done approximate local Wu stratification near $\alpha$ and found $\Delta(S = 0)$ to be $(A_s = 0, I(A_s) \neq 0, D(A_s) \neq 0)$. $\Delta(S = 0)$ implies $S = 0$, and $S$ includes the original $S_r$ which was used to define the elementary point $\alpha$. The defining condition for $\alpha$ was

$$(S_r, E_k) = 0$$

in $N_\epsilon(\alpha^*)$

$E_{k-d}$ may not be currently equal to $E_k$ but by lemma 3.2,

$$S = 0, E_{k-d} = 0 \Rightarrow E_k = 0$$

in $N_\epsilon(\alpha^*)$. Thus $\Delta(S = 0), E_{k-d} = 0$ implies $(S_r, E_k) = 0$ in $N_\epsilon(\alpha^*)$.

The inequalities of $\Delta(S = 0)$ are always true in $N_\epsilon(\alpha^*)$. So

$$A_s = 0, E_{k-d} = 0 \Rightarrow (S_r, E_k) = 0$$

in $N_\epsilon(\alpha^*)$.

We have $\vdash_{prn} J \neq 0$, where $J$ is the Jacobian determinant of $(A_s, E_{k-d})$. This implies that the topological degree of $(A_s, E_{k-d})$ over $N_\epsilon(\alpha^*)$ is either plus or minus one or zero, and that the degree is non zero if and only if

$$(\exists \beta \in N_\epsilon(\alpha^*))(A_s, E_{k-d})(\beta) = 0$$

This $\beta$ must be the same as $\alpha$ since $\beta$ satisfies a condition which is stronger than the condition which we supposed uniquely defined $\alpha$. Since $q$ is also in $S$, we must have

$$q(\beta) = 0$$

and thus the conclusion $c = 0$ is correct.

In order to prove the second part of the theorem, assume that the process does not terminate. Each loop between step 3) and step 4) eliminates one exponential term, so there can never be more than $k$ such successive loops. Thus $prn$ is doubles an unbounded number of times in the non terminating computation. Since step 2) never succeeds, we must have $q(\alpha) = 0$ and thus $c = 0$.

Suppose that there are actually $d$ independent linear integral relationships among $z_1, ..., z_k$.

If $prn$ is sufficiently large, then after backtracking from step 4) to step 1), $d$ loops through steps 3) and 4) will, by lemma 3.1, produce $d$ correct candidate linear relationships. At this point $S(\alpha) = 0$ and the remaining $z_1, ..., z_{k-d}$, the arguments to the exponential function, are linearly independent over the rationals at $\alpha$.

After going into step 3), we get $\Delta(S = 0)$, which is
$(A_s = 0, I(A_s) \neq 0, D(A_s) \neq 0)$

Lemma 4.1) implies that if the precision is sufficiently high, these conditions are true at $\alpha$.

If $s > n - (k - d)$, we have a counterexample to Schanuel's conjecture, since $z_1, ..., z_{k-d}$ are linearly independent at $\alpha$.

It is not possible to have $s < n - (k - d)$ since $(A_s, E_{k-d}) = 0$ implies $(S_r, E_k) = 0$, and the latter has non singular Jacobian.

It is claimed that unless $z_1, ..., z_k$ is a counterexample to Schanuel's conjecture, it is also not possible to have $J(A_s, E_{k-d})$ singular at $\alpha$. For the sake of a contradiction, suppose this did happen.

Note here that $(A_s, E_{k-d}) = 0$ determines a single point in $N_\epsilon(\alpha^*)$.

Let $J$ be the result of replacing $e^{z_1}, ..., e^{z_{k-d}}$ by the variables $w_1, ..., w_{k-d}$ which are equal to them if $E_{k-d} = 0$. Suppose we found the Wu stratification of the solution set of $(A_s = 0, J = 0, S_r = 0)$. The point $\alpha$ is in this solution set. So $\alpha$ would be described by some condition of the form

$(B_r = 0, I(B_r) \neq 0, D(B_r) \neq 0)$

where $Rem(B_r, J) = 0$ and $Rem(B_r, q) = 0$ for all $q$ in $A_s$.

We can not have $r < s$ since the equations $A_s = 0$ are independent at $\alpha$. We can not have $r > s$ unless this is a counterexample to Schanuel's conjecture. Suppose $r = s$. $B_r = 0$ implies $J(A_s, E_{k-d})$ is singular. Since the $A_s$ are independent, this must mean that some $w_i - e^{z_i}$ in $E_{k-d}$ has a gradient in $N_\epsilon(\alpha^*)$ which is a linear combination of the gradients of $B_r$ and the rest of $E_{k-d}$ on the solution set of $B_r = 0$ near $\alpha$. Remove this dependent term from $E_{k-d}$ to get $E_{k-(d+1)}$. $(B_r, E_{k-(d+1)}) = 0$ at $\alpha$, and since there are less equations than variables, there must be a curve through $\alpha$ on which $B_r$ and $E_{k-(d+1)}$ are identically zero. $E_{k-d}$ is also identically zero on this curve, since it is zero at one point, and the curve is orthogonal to the gradients of the terms in $E_{k-d}$. $A_s$ is identically 0 on this curve since $A_s$ is reduced to zero by $B_r$. But this is impossible since we supposed that $(A_s, E_{k-d}) = 0$ determined a single point in $N_\epsilon(\alpha^*)$.

We have decided that $(A_s, E_{k-d})$ has non singular Jacobian at $\alpha$. For $prn$ sufficiently large, we can prove $\vdash_{prn} J \neq 0$ in $N_\epsilon(\alpha^*)$. The topological degree method will then apply, and will give termination.

Looking back over the discussion, we can see that the only case in which termination can be avoided is when $(z_1, ..., z_k, w_1, ..., w_k)$ is a counterexample to Schanuel's conjecture.

□

It follows from the above theorem that if Schanuel's conjecture is true, the elementary numbers are a computable field. Also, the real elementary numbers are a computable real closed field.

## 5.1 Implementation

There is a zero recognition program, written in Reduce. It does not use topological degree to show existence of non singular solutions of $n$ equations in $n$ unknowns, but instead applies standard tests for convergence of Newton sequences. The program has only been tried so far on about 50 examples, the most interesting of which is

$$c = 4atan(1/5) - atan(1/239) - \pi/4$$

which is zero, but which, we might say, is not obviously zero.

So far, on small problems of this type, termination (with the correct answer) has always been obtained within a few minutes.

The possibility of backtracking which is built in to the algorithm to ensure correctness has not yet been used. That is, it has not yet happened that a false candidate linear relationship has been produced by the LLL process. This suggests the following difficult and interesting problem in applied number theory: *how can we set the thresholds in such a way that no false candidate is ever produced?* From a theoretical point of view, this problem looks to be a little bit harder than settling the Schanuel conjecture.

Although the program has not failed yet on any small problems, it is clear that it is possible to create problems involving very large or very small numbers which will require such large precision that their solution will be infeasible.

There may be some other computational difficulties (such as counterexamples or near counterexamples to Schanuel's conjecture) but so far none such have appeared.

# References


[1] Aberth, O., Computation of Topological degree using Interval Arithmetic, and Applications, Mathematics of Computation, Jan 1994, pp 1-10

[2] Alefeld, G and J. Herzberger, Introduction to Interval Computation, translated by Jon Rokne, Academic Press, N.Y. 1983

[3] Ax, J., Schanuel's Conjecture, Ann Math 93 (1971), 252–68

[4] Baker, A., Transcendental Number Theory, Cambridge University Press, 1975

[5] Caviness, B. F., On canonical forms and simplification, Journal of the ACM, vol 17, no 2, April 1970, pp 385–396

[6] Caviness, B. F. and M. J. Prelle, A note on algebraic independence of logarithmic and exponential constants, SIGSAM Bulletin, vol 12, no 2, pp 18–20, 1978

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

[8] Ferguson, H.R.P., and R.W. Forcade, Multidimensional Euclidean Algorithms, J. Reine Ange. Math. 33, (1982), pp 171-181

[9] Frohlich, A., and J. C. Shepherdson, Effective Procedures in Field Theory, Phil. Trans. Roy. Soc Ser A 248 (1955-56), pp 149-167, 1956

[10] Gonzalez-Vega, L., and G. Trujillo, Topological degree methods determining the existence of a real solution for a polynomial system of equations, preprint, 1995. email: gvega@matsun1.unican.es

[11] Hastad, J., B. Just, J.C. Lagarias, C. P. Schnorr, Polynomial time algorithms for finding integer relations among real numbers, Procedings of STACS '86, *Lecture Notes in Computer Science*

[12] Kang,J., Wu stratification and retract decomposition, preprint, Bath University, submitted to MEGA 1996

[13] Lenstra, A. K., H. W. Lenstra, L. Lovasz, Factoring Polynomials with rational coefficients. Math Ann 261, pp 513-534

[14] Lloyd, N.G., Degree Theory, Cambridge University Press, 1978

[15] Macintyre, A.J. and A. J. Wilkie, On the decidability of the real exponential field, to appear

[16] O'Neal, T., and J. Thomas, The calculation of topological degree by quadrature, SIAM J. Numer Anal. 12, p 673-680, 1975

[17] Paulson, L.C., ML for the Working Programmer, CUP 1991, ch 5.

[18] Rabinowitz, P., (Ed), *Numerical Methods for Nonlinear Algebraic Equations*, Gordon and Breach, 1970

[19] Richardson, D., Solution of the identity problem for integral exponential functions, Zeitschr Mat Logic und Grund. d. Math., by 15, pp 333-340, 1969

[20] Richardson, D., The simple exponential constant problem, Zeitschr Mat Logik und Grund. d. Mat., Bd 17, 133-136, 1971

[21] Richardson, D., Finding roots of equations involving solutions of first order algebraic differential equations, pp 427–440 in Effective Methods in Algebraic Geometry, (Teo Mora and Carlo Traverso Eds), Birkhauser 1991

[22] Richardson,D., Wu's method and the Khovanskii finiteness theorem, Journal of Symbolic Computation, 1991, 12, pp 127–141

[23] Richardson, D., The Elementary Constant Problem, ISSAC 92.

[24] Richardson,D., A zero structure theorem for exponential systems, ISSAC '93

[25] Richardson, D. and J. P. Fitch, Simplification of elementary constants and functions, ISSAC 1994

[26] Richardson, D., A simplified method of recognizing zero among elementary constants, ISSAC 1995 pp 104-109

[27] Rosenlicht, M., On Liouville's Theory of Elementary Functions, Pacific Journal of Mathematics, vol 65, no 2, 1976, pp 485–492

[28] Wilkie, A.J., On the theory of the real exponential field, Illinois J. of Math, 33, No 3, pp 384-408

[29] Wilkie, A.J., Model completeness results for expansions of the real field , I: restricted Pfaffian functions, and II: the exponential function, to appear in Journal of the American Math. Soc.

[30] Chou, S.C., W. F. Schelter, and J. G. Yang, Characteristic Sets and Grobner Bases in Geometry Theorem Proving, Draft, Institute for Computing Science, The University of Texas, Austin, TX 78712

[31] Vrahatis,N., Solving systems of nonlinear equations using the nonzero value of the topological degree, ACM Transcations on Mathematical Software 14, 4, p 312-329, 1988

[32] Wu, W.T., Basic Principles of Mechanical Theorem Proving in Elementary Geometries, J. Sys. Sci. and Math. Scis, f(3), 1984, 207–235