Zero Tests for Constants in Simple Scientific Computation

Daniel Richardson,
Computer Science, Bath University,
Bath BA2 7AY, UK
email: masdr@bath.ac.uk

July 6, 2007

Abstract

It would be desirable to have an algorithm to decide equality among the constants which commonly occur in scientific computing. We do not yet know whether or not this is possible. It is known, however, that if the Schanuel conjecture is true, then equality is Turing decidable among the closed form numbers, that is, the complex numbers built up from the rationals using field operations, radicals, exponentials and logarithms. An algorithm based on the Schanuel conjecture is described in this article to decide equality among these numbers, presented as expressions. The algebraic part of this algorithm is simpler than those which have been given previously to solve related problems.

1 Introduction

Scientific computing is supported by a rich legacy of algorithms, many of which depend at crucial points on tests for equality of real or complex numbers. The mathematical notion of equality depends on the quite subtle mathematical notion of **R** and **C** as infinite objects. We would of course like our computational work to be closely related to our mathematical understanding. For this reason, it would be desirable to have a subset, D, of the complex numbers with the following properties (at least):

1. We should have a finite unambiguous notation for every element of D.
2. We should have a reasonably efficient way to approximate any element of D.
3. Given any $x \in D$, we should have a method to decide whether or not $x = 0$. Such a method is called a zero test.
4. D should be closed under application of some standard functions, including, at least, field operations, radicals, exponentials and logarithms.

Such a field D of complex numbers could be called a domain for scientific computing. It is an embarrassing fact that we do not know whether or not there is *any* such domain, even though the minimal form of the closure condition given above is very mild. We do not know how to solve the quite basic problems in this area; on the other hand we also have no evidence that these problems are especially difficult. That is to say, we do not possess any significantly difficult examples.

It is true that we have some moderately difficult examples, which are all essentially algebraic. For example, the following, due to Ramanujan:

Example 1. $(1/25)^{1/5} + (3/25)^{1/5} - (9/25)^{1/5} - (1/25)^{1/5}(1 + 3^{1/5} - 3^{2/5}) = 0$ *?*

All such algebraic problems can be solved in a systematic way. See for example, the work of Chen Li and Chee Yap [11], based on classical ideas of Liouville and Mahler. One of the basic ideas is Mahler measure.

Suppose $p(x) \in \mathbf{Z}[x]$. Let the degree of $p(x)$ be $d > 0$. Then $p(x) = a_d x^d + ... + a_0 = a_d(x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_d)$, where $\alpha_1, \dots, \alpha_d$ are the roots of $p(x)$, and $a_d \neq 0$. We define the Mahler measure of $p(x)$ to be

$\mid a_d \mid \prod_{i=1\dots d} Max(1, \mid \alpha_i \mid)$

For an algebraic number α we define $M(\alpha)$, the Mahler measure of α to be $M(p)$ where p is the minimal defining polynomial for α in $\mathbf{Z}[x]$. Mahler measure has often been used to solve the zero problem for algebraic quantities. Some of the properties of Mahler measure are:

1. If α is algebraic but not zero,
   (a) $1/M(\alpha) \leq \mid \alpha \mid \leq M(\alpha)$
   (b) $M(\alpha) = M(1/\alpha)$
   (c) If k is a positive integer, $M(\alpha^{1/k}) \leq M(\alpha)$
2. If α and β are algebraic with degrees d_1 and d_2 respectively, then
   (a) $M(\alpha\beta) \leq M(\alpha)^{d_2} M(\beta)^{d_1}$
   (b) $M(\alpha + \beta) \leq 2^{d_1 d_2} M(\alpha)^{d_2} M(\beta)^{d_1}$

Condition 1a) above allows us to prove that $\alpha = 0$ by finding an upper bound M for the Mahler measure of α and showing that $\mid \alpha \mid < 1/M$. The other conditions allow us to compute an upper bound for Mahler measure of an algebraic number given its presentation as an expression built up from the rationals using field operations and radicals. These estimates have been, in many cases, improved in, for example, [11], leading to easier zero tests.

In spite of successes in the algebraic area, many people consider these problems, in their general form, unrealistically hard. This is perhaps related to the situation with the Turing computable numbers.

Define the Gaussian rationals to be numbers of the form $X + iY$ where X and Y are rational. We will say that a Turing machine computes a complex number Z if for every natural number n the machine finds Gaussian rational Z_n so that $\mid Z_n - Z \mid \leq 10^{-n}$.

It is not possible to have a computable zero test among computable real or complex numbers, as was pointed out by Turing. The notation for computable real and complex numbers is also unsatisfactory, since, although we do have a notation for Turing machines, the question of whether or not a given Turing machine actually computes a real or complex number is undecidable.

In response to this, there have been very serious and sophisticated attempts to develop an effective analysis, which takes the computable numbers as its domain, and which must omit equality tests between real and complex numbers from its algorithms. See for example the book by Klaus Weihrauch [22]. The algorithms developed in this field are a useful contribution to science. However all these algorithms have the property that the outputs are continuous functions of the inputs (since computable functions among computable numbers must be continuous). But reality has actual discontinuities. So it seems fair to say that effective analysis must blur some aspects of reality. The notion of an uncountable continuum is rather odd but perhaps it really does contribute to clarity of understanding.

In the following, we look at a minimal subset D of the complex numbers satisfying conditions 1), 2) and 4) above, and we will then discuss the zero problem for this subset. The D in this case is the smallest subfield of $\mathbf{C}$ closed under radicals, exponentials and logarithms. This famous collection of numbers has been given various names. In this article, following T. Chow [8], we will call them the closed form numbers.

Let $\mathcal{E}$ be the smallest set of expressions which contains the usual canonical representations for the rational numbers, and so that if A and B are in $\mathcal{E}$, so are $(A+B), (A-B), (A*B), (A/B)$, and if A is in $\mathcal{E}$ then so are $exp(A)$ and $\log(A)$, and if A is in $\mathcal{E}$ and n is a natural number, then $A^{1/n}$ is in $\mathcal{E}$.

The value of an expression E as a real or complex number may not be defined. If defined, it may depend on a choice of branches for the multivalued functions such as logarithms or radicals. Where a value is defined for expression E, we will denote it as $V(E)$. How the branches are chosen, and the values are defined, is discussed in more detail in the next section.

Progress in proving completeness of equality recognising processes, or axioms for equality, for the closed form numbers (and implicitly defined numbers related to these) has been made using the Schanuel conjecture. This is stated below.

We will say that complex numbers $z_1, \ldots, z_k$ are algebraically independent over $\mathbf{Q}$ if the only polynomial $p \in \mathbf{Z}[x_1, \ldots, x_k]$ such that $p(z_1, \ldots, z_k) = 0$ is the identically zero polynomial.

It follows from this that if α is any algebraic function, defined with integral coefficients, and if $z_1, \ldots, z_k$ are algebraically independent over $\mathbf{Q}$ then either α is identically zero or $\alpha(z_1, \ldots, z_k) \neq 0$. That is, algebraically independent numbers can be used to test whether or not algebraic functions are identically zero.

Schanuel Conjecture. If $x_1, \ldots, x_k$ are complex numbers which are linearly independent over $\mathbf{Q}$, then $\{x_1, \ldots, x_k, e^{x_1}, \ldots, e^{x_k}\}$ contains at least k algebraically independent numbers.

This has been used to solve zero problems, related to the problem for the closed form numbers, by Caviness and Prelle [7], by Wilkie and Macintyre [13] and also by Richardson [14].

Let $x_1, \ldots, x_k$ be given complex numbers. An integer relation for $(x_1, \ldots, x_k)$ is a vector of integers $m = (a_1, \ldots, a_k) \neq 0$ so that $a_1 x_1 + \cdots + a_k x_k = 0$.

The PSLQ algorithm, developed by H. Ferguson and others [9] can be used to find integer relations, and is therefore a natural computational partner of the Schanuel conjecture. All it assumes about $(x_1, \ldots, x_k)$ is that we have the ability to approximate these numbers as precisely as we wish. The implemented PSLQ algorithm has two parameters, a precision m, and a bound M on the absolute values of integers in its search space. The error bound corresponding to precision m is $\epsilon = 10^{-m}$. The search space corresponding to the bound M is $\{(a_1, \ldots, a_k) :\mid a_i \mid \leq M \ for \ i = 1, \ldots, k\}$. All the computation in PSLQ is done in floating point arithmetic with precision m. The input of PSLQ is $x = (x_1, \ldots, x_k)$ represented as a vector of floating point numbers. On termination, PSLQ will either exclude the possibility of any integer relation for x in the search space, or it will return a candidate integer relation $(a_1, \ldots, a_k)$. The candidate is not guaranteed actually to be an integer relation. All we are guaranteed is that precision m floating point computation is consistent with the possibility that $a_1 x_1 + \cdots + a_k x_k = 0$. In order to check that the candidate $(a_1, \ldots, a_k)$ really is an integer relation, a separate verification method must be used.

It can be shown that if there is an integer relation for x in the search space, then PSLQ will find it provided that m is sufficiently large. If we were totally unconcerned with computation time, we could just enumerate the search space and check each possibility using floating point arithmetic. The PSLQ algorithm returns a result which could also have been found in this brute force way, but does so relatively quickly. The computation time for PSLQ increases only polynomially in $k, \log M$ and m. See [9] for discussion of this.

The zero test described below in section 5) is based on the Schanuel conjecture and has the following basic structure. Suppose given expression E in $\mathcal{E}$. Form an expression $\eta(E)$ for an algebraic function by replacing each distinct exponential or logarithmic subexpression in E by a new variable. We can decide whether or not $\eta(E)$ represents the zero function. If so, then $V(E) = 0$. However, if $\eta(E)$ does not represent the zero function, but $V(E) = 0$, the Schanuel conjecture implies that there must be some integer linear relation between the numbers represented in E by logarithmic expressions or by arguments of the exponential expressions. Suppose these numbers are $(x_1, \ldots, x_k)$. We can use PSLQ to pick out candidate integer relations $(a_1, \ldots, a_k)$ for $(x_1, \ldots, x_k)$. This means only that we suspect it might be true that $a_1 x_1 + \cdots + a_k x_k = 0$. We then use a separate, algebraic technique to verify $a_1 x_1 + \cdots + a_k x_k = 0$, if this is the case. Once this verification has been done, the integer relation can be used to simplify the original expression E, reducing the number of exponential or logarithmic subexpressions. If a candidate is found but not verified, the PSLQ working precision is increased, and the search continues.

The method used here is simpler than the zero test given previously in [14], mainly because the use of Wu's method is avoided.

2 Expression Trees and Partial Evaluations

We will not distinguish between expression in $\mathcal{E}$ and expression trees corresponding to them. We will consider an expression to be a subexpression of itself. The nodes in the expression tree for E correspond to the subexpressions of E. The nodes labelled with radical signs, *exp* or log are called radical, exponential or logarithmic nodes (or subexpressions). The nodes at the leaves are labelled with rational numbers written in canonical form.

There are a number of related problems about evaluating an expression E in $\mathcal{E}$.

1. Is the value of E defined?
2. If defined, how can we approximate $V(E)$?
3. In case E contains radical or logarithmic subexpressions, how can we specify which branches are intended?
4. If the value of E is defined, is $V(E) = 0$?

In this article, we approach this complex of problems by assuming that we are given an expression E in which problems 1), 2), and 3), restricted to E and its subexpressions, have already been solved, so that we are left with problem 4). Our basic assumption is that some preparatory work has already been done on expression E giving it a partial evaluation, as defined below. This implies that the value of the expression is defined, and can be approximated.

We do not assume in advance that the problems 1), 2), and 3) are solved in general for all E in $\mathcal{E}$. We only suppose that we are given a particular expression E, such as the one of example 1) above, so that these three problems are solved for E and its subexpressions.

Define an approximating box to be a subset of $\mathbf{C}$ of the form $\{x + iy : | x - x_0 | \leq 10^{-k}, | y - y_0 | \leq 10^{-k}\}$, where k is some natural number and x_0 and y_0 are rational. Define the size of such a box to be 10^{-k}. As a limiting case, we allow approximating boxes of size zero, of the form $\{x_0 + iy_0\}$ where x_0 and y_0 are rational numbers. All the approximating boxes are closed sets.

Definition 1. *We will say that an expression tree E is partially evaluated if*

1. *Each node n of the expression tree E has associated with it an approximating box $b(n)$. Identical subexpressions have identical approximating boxes.*

2. *Each function symbol at each node has its standard representation as a single valued analytic function defined on an open set containing the Cartesian product of the approximating boxes of its children and taking values in its own approximating box. If the function symbol at node n is a radical or a logarithm, the approximating box $b(n)$ is so small that only one of the branches of the multivalued function can take values in $b(n)$.*
3. *We have an approximation procedure which will refine all the approximating boxes of size greater than zero in the tree, reducing the sizes as much as desired below any given positive value, modifying the functions only by restricting them to the new domains, and maintaining properties 1) and 2) above.*

Since the functions are required to be analytic, the approximating boxes of the children of radical and logarithmic nodes must not contain zero. Similarly, the denominator of a division node must have an approximating box which does not contain zero. Since the functions are required to be single valued, one of the branches is chosen in the multivalued cases.

The approximation procedure can be based on interval arithmetic as explained in, for example, the book by Alefeld and Herzberger [1]. For a more recent discussion of validated approximation, see [25].

In all the following, we will consider expressions E which have an associated partial evaluation. For such an expression, the value $V(E)$ is defined and can be approximated.

We can define length for expressions in $\mathcal{E}$ by taking the number of digits in the decimal representation to be the length for rational numbers and defining $length((A+B)) = length((A-B)) = length((A*B)) = length((A/B)) = length(A) + length(B) + 1$, and $length(exp(A)) = length(\log(A)) = length(A)+1$ and $length(A^{1/n}) = length(A) + length(n) + 1$.

Two other quantities of interest are $d(E)$, the depth of nesting of E and $h(E)$, the integral height of E. These are defined as follows. For a natural number n in canonical decimal form, we define $d(n)$ to be 1 and $h(n)$ to be the number of digits in n. We let $h(-n) = h(n)$, and $d(-n) = d(n)+1$. For rational numbers a/b in canonical form, we define $d(a/b) = 1+Max(d(a), d(b))$, and $h(a/b) = Max(h(a), h(b))$. In general, we define $d((A+B)) = d((A-B)) = d((A*B)) = d((A/B)) = 1 + Max(d(A), d(B))$; and $h((A+B)) = h((A-B)) = h((A*B)) = h((A/B)) = Max(h(A), h(B))$. We define $d(exp(A)) = d(\log(A)) = d(A^{1/n}) = 1 + d(A)$. We define $h(exp(A)) = h(\log(A)) = h(A)$. We define $h(A^{1/n}) = Max(h(A), h(n))$.

Suppose, given expression E, we could compute a natural number $m(E)$ so that

$| V(E) | < 10^{-m(E)} \rightarrow V(E) = 0$

Such a function has been considered by a number of researchers, including Joris van der Hoeven, Daniel Richardson, Chen Li, Sylvain Pion and Chee Yap. See [12]. If the zero problem is decidable at all, there must exist a computable function $m(E)$ with the above property. It is called a gap function or a witness function or a Liouville bound.

If E is built up using radicals only, we can construct the Liouville bound using Mahler measure and the work of Chen Li and Chee Yap. When E contains exponential or logarithmic terms, we must depend on conjectures. There have been a number of these, called uniformity conjectures or witness conjectures, attempting to bound $m(E)$ by some function of the length of E. For example, the uniformity conjecture stated that $m(E)$ could be taken to be a small multiple of the length of E, for those expressions in which all the arguments of the exponential function were restricted to the unit ball around zero. Some of the conjectures (including the uniformity conjecture) have turned out to be false. Of course, also, a number of conjectures of this type survive, up to this point in time. An example of a surviving conjecture of this type is the following.

Conjecture 1. *Let E be a partially evaluated expression in $\mathcal{E}$ in which all the arguments of the exponential function are restricted to the unit ball around zero. Then*

$$\mid V(E) \mid \leq 10^{-h(E)2^{d(E)}} \rightarrow V(E) = 0$$

For discussion, see [19, 20, 21, 16, 17].

3 Recognising Some Equalities Algebraically

Let $\iota : \mathcal{E} \rightarrow \mathbf{N}$ be some enumeration of the closed form expressions. For each E in $\mathcal{E}$ we can construct an expression $\eta(E)$ by replacing each distinct exponential or logarithmic subexpression by a new variable, chosen according to the enumeration ι. We will use variables of the form X_j to replace logarithmic expressions, and variables of the form Y_j to replace exponential expressions. The expression $\eta(E)$ will represent an algebraic function built up from the variables and rational numbers using field operations and radicals.

If E is $exp(A)$, we define $\eta(E)$ to be $Y_{\iota(A)}$. If E is $\log(A)$, we define $\eta(E)$ to be $X_{\iota(A)}$. So exponential and logarithmic expressions map into variables, via the enumeration ι. If E is $A^{1/n}$, we define $\eta(E)$ to be $(\eta(A))^{1/n}$. We also define $\eta((A+B)) = (\eta(A)+\eta(B))$, $\eta((A-B)) = (\eta(A)-\eta(B))$, $\eta(A*B) = (\eta(A)*\eta(B))$, and $\eta((A/B)) = (\eta(A)/\eta(B))$.

Suppose E is partially evaluated, and has distinct exponential or logarithmic subexpressions $A_1, \ldots, A_k$, which are replaced in $\eta(E)$ by variables $w_1, \ldots, w_k$. (Here w_i is a name we are using for the variable which replaces A_i.) We take the domains of the variables $w_1, \ldots, w_k$ to be the approximating boxes which were given to expressions $A_1, \ldots, A_k$ respectively in the partial evaluation of E.

$\eta(E)$ will be called the algebraic precursor of E. It is an expression built using radicals and field operations. We will write $f_{\eta(E)}$ for the algebraic function defined by $\eta(E)$, in the domain obtained from the partial evaluation of E.

Theorem 1. *If $f_{\eta(E)} \equiv 0$ then $V(E) = 0$.*

This follows from the observation, using the previous notation, that $V(E)$ is $f_{\eta(E)}(V(A_1), \ldots, V(A_k))$.

It can happen, however, that $V(E) = 0$ although $f_{\eta(E)}$ is not identically zero. One way in which this can occur is that the arguments of the exponential function and the values of the logarithm function can be linearly dependent over the rationals. For example

Example 2. $exp(3^{1/2}) * exp(3^{1/2}) - exp(12^{1/2})$
with algebraic precursor $Y_1^2 - Y_2$
or
$\log(9) - 2\log(3)$
with algebraic precursor $X_1 - 2X_2$.

It turns out to be a consequence of the Schanuel conjecture that whenever $V(E) = 0$ but $f_{\eta(E)}$ is not identically zero this is a consequence of an integral linear dependence among the arguments of the exponential function and the values of the logarithm function inside the expression. This situation is discussed in more detail in section 4).

Suppose, as above, that we are given $\eta(E)$, depending on variables $w_1, \ldots, w_k$ and approximating boxes for the expression tree for $\eta(E)$. We wish to decide whether or not $\eta(E) \equiv 0$.

Assume that the domains of $w_1, \ldots, w_k$ are $b_1, \ldots, b_k$ respectively. There are now a number of ways to solve this algebraic zero recognition problem.

A probabilistic method to decide whether or not $f_{\eta(E)}(w_1, \ldots, w_k) \equiv 0$ would be to pick Gaussian rationals $\alpha_1, \ldots, \alpha_k$ at random in domains $b_1, \ldots, b_k$ respectively, to compute the Mahler measure for $f_{\eta(E)}(\alpha_1, \ldots, \alpha_k)$, by working recursively up the expression tree, as described in [10], and then approximating until the question is decided. If we discover that $f_{\eta(E)}(\alpha_1, \ldots, \alpha_k) \neq 0$, then certainly $f_{\eta(E)}$ is not identically zero. On the other hand, if $f_{\eta(E)}$ is zero at this randomly chosen point, we have at least strong evidence that the function is identically zero. If we want more evidence, we could choose another point at random.

Suppose that $f_{\eta(E)}$ is not identically zero. We will say that a point $(\alpha_1, \ldots, \alpha_k)$ is bad if $f_{\eta(E)}(\alpha_1, \ldots, \alpha_k) = 0$. Assume that the algebraic function $y = f_{\eta(E)}$ has defining polynomial $p(y, w_1, \ldots, w_k) = 0$, with $w_1, \ldots, w_k$ having degrees bounded by $d(w_1), \ldots, d(w_k)$ respectively. Suppose we consider N choices from each of the domains $b_1, \ldots, b_k$, with $d(w_i)/N < \epsilon$ for each i. The probability of a bad choice of $(\alpha_1, \ldots, \alpha_k)$ is bounded by $p_1 + p_2$, where p_1 is the probability of choosing $w_k = \alpha_k$ so that $p(0, w_1, \ldots, w_{k-1}, \alpha_k) \equiv 0$, and p_2 is the probability of a bad choice of $(w_1, \ldots, w_{k-1})$ in case $p(0, w_1, \ldots, w_{k-1}, \alpha_k)$ is not identically zero. From this, it follows that the probability of choosing a bad point is bounded by $k\epsilon$. So, for example, if we have ten variables, and N is more than any of the degrees by a factor of 10^6, then the probability of a bad choice is bounded by 10^{-5}.

Suppose we find that the function is zero at one or more points in the domain, but we are unhappy with a probabilistic result. There are several ways to check deterministically if the function really is identically zero.

One approach involves observing that the radical subexpressions of $\eta(E)$ are defined by a Pfaffian chain of differential equations. List these subexpressions in order of complexity, so that each is defined by a Pfaffian differential equation involving previous, simpler ones. Treating $\eta(E)$ as a polynomial in these radical subexpressions, replace $\eta(E)$ by its square free part. Then formally differentiate $\eta(E)$ with respect to one of the variables, w_i, obtaining an expression for $(\partial/\partial w_i)f_{\eta(E)}$; and then use the resultant and GCD constructions (regarding the expressions as polynomials in their radical subexpressions) to obtain an expression R which is simpler than $\eta(E)$ and so that f_R is identically zero iff $f_{\eta(E)}$ is identically zero; and then continue recursively to decide whether or not f_R is identically zero.

A good discussion of these symbolic methods can be found in the book by John Shackell [5]. See especially the algorithm 2) in chapter 2) of [5].

4 Reducing Non Algebraic Questions to Algebraic Questions

Definition 2. *An ascending sequence of closed form definitions is a list $G_1, G_2, \ldots, G_n$ of partially evaluated expressions in $\mathcal{E}$ so that, for all $i \leq n$, if H is a subexpression of G_i, then $H = G_j$ for some $j \leq i$. We assume that $G_i = G_j$ only when $i = j$, and that that any two equal expressions or subexpressions in the sequence have the same partial evaluation.*

Let E be a partially evaluated expression in $\mathcal{E}$. Consider the usual left to right bottom up traversal of the tree E. If we list the subexpressions in this order, omitting duplicates, we get an ascending sequence of closed form definitions. This will be called the ascending sequence associated with the expression E. We are able to omit duplicates since, as stated earlier, we assume that any two equal subexpressions of E have the same partial evaluation.

In all the following, let $G_1, \ldots, G_n$ be an ascending sequence of closed form definitions associated with partially evaluated expression E. We will give the ascending sequence by giving E and assuming the default order of traversal mentioned above. (We would not like to write out an ascending sequence of definitions explicitly, since, as pointed out by one of the referees of this paper, it contains much redundancy and tends to increase in size exponentially.)

A radical, exponential or logarithmic expression is one of the form $A^{1/m}, exp(A)$ or $\log(A)$ respectively. Let the radical, exponential, or logarithmic expressions among $G_1, \ldots, G_n$ be $G_{h(1)}, \ldots, G_{h(m)}$ where $h(1) < h(2) < \ldots < h(m)$. Define $H_1, \ldots, H_m$ as $G_{h(1)}, \ldots, G_{h(m)}$.

We remark that corresponding to ascending sequence $G_1, \ldots, G_n$, there exists a tower of fields of closed form numbers

$\mathbf{Q} = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_m$

constructed by taking $F_{i+1} = F_i(V(H_i))$ for all $i < m$. For each i, either $H_i = A_i^{1/n_i}$, or $H_i = exp(A_i)$, or $H_i = \log(A_i)$, where $V(A_i) \in$

F_i. So each F_{i+1} is given as either a radical, an exponential or a logarithmic extension of F_i. The fact that the fields are arranged in this simple increasing sequence underlies the inductive structure of the proofs given later.

Suppose now that among $H_1, \ldots, H_m$ there are k distinct exponential or logarithmic expressions

$H_{j(1)}, \ldots, H_{j(k)}$,

where $j(1) < j(2) < \cdots < j(k)$. Define $P_1, \ldots, P_k$ as $H_{j(1)}, \ldots, H_{j(k)}$. We form a sequence of k pairs of closed form numbers $(x_1, y_1), \ldots, (x_k, y_k)$ as follows:

For $i = 1$ up to k, if $P_i = exp(Q_i)$, then let $x_i = V(Q_i), y_i = V(P_i)$; but if $P_i = \log(Q_i)$ then let $x_i = V(P_i), y_i = V(Q_i)$. Note that we have $y_i = e^{x_i}$ in all cases.

All of this is based on the original ascending sequence of definitions $G_1, \ldots, G_n$. Define the order of $G_1, \ldots, G_n$ to be k, the number of distinct logarithmic or exponential subexpressions. We will also define the order of E to be k. The list $(x_1, y_1), \ldots, (x_k, y_k)$ is called the fundamental list of exponential points associated with the partially evaluated expression E, or with $G_1, \ldots, G_n$.

Definition 3. *We will say that the ascending sequence of closed form definitions $G_1, \ldots, G_n$ is reduced if $x_1, \ldots, x_k$ are linearly independent over the rational numbers, where $(x_1, y_1), \ldots, (x_k, y_k)$ is the associated fundamental list of exponential points..*

Example 3. *The ascending sequence of definitions*

$1, \log(1), 1000, exp(1000), exp(exp(1000)), exp(-exp(exp(1000)))$,

with $V(\log(1)) = 2\pi i$, is reduced if the Schanuel conjecture is true. This can be proved by induction on the length of an initial segment of the sequence. (x_1, x_2, x_3, x_4) is $(2\pi i, 1000, exp(1000), -exp(exp(1000)))$. In this case, the algebraic precursor of the expression at the end of the ascending sequence of definitions is just a single variable and the associated function is obviously not identically zero.

Comment: There are a number of cases of this kind in which it is possible to prove directly, using the Schanuel conjecture, that an ascending sequence of closed form definitions is reduced.

Theorem 2. *(Assuming the Schanuel conjecture) Let E be a partially evaluated expression in $\mathcal{E}$. If $G_1, \ldots, G_n$ is a reduced ascending sequence of closed form definitions with $V(E) = V(G_n)$ then $V(E) = 0$ if and only if $f_{\eta(G_n)} \equiv 0$.*

Proof. Let $(x_1, y_1), \ldots, (x_k, y_k)$ be the fundamental list of exponential points associated with $G_1, \ldots, G_n$. The sequence of definitions is reduced; this means that $x_1, \ldots, x_k$ are linearly independent over $\mathbf{Q}$. According to the Schanuel conjecture, there are at least k numbers in $\{x_1, \ldots, x_k, y_1, \ldots, y_k\}$ which are algebraically independent over $\mathbf{Q}$. Using the notation developed above, the numbers $V(P_1), \ldots, V(P_k)$ are all in this set. But also every number in this set, and even every $V(G_j)$ for $j \leq n$ is algebraic in $V(P_1), \ldots, V(P_k)$. So $V(P_1), \ldots, V(P_k)$ are algebraically independent over $\mathbf{Q}$. So

$f_{\eta(G_n)} \equiv 0 \leftrightarrow f_{\eta(G_n)}(V(P_1), \ldots, V(P_k)) = 0$.

But $V(E) = f_{\eta(G_n)}(V(P_1), \ldots, V(P_k))$. So $V(E) = 0$ if and only if $f_{\eta(G_n)} \equiv 0$, proving the theorem.

Corollary 1. *Suppose $H_1, \ldots, H_m$ is a reduced ascending sequence of closed form definitions.*

1. *If E is an expression obtained from $H_1, \ldots, H_m$ and $\mathbf{Q}$ using $+, -, *$, then $V(E) = 0$ if and only if $f_{\eta)E)} \equiv 0$.*
2. *The evaluation map which takes $f_{\eta(H_i)}$ to $V(H_i)$ for $i = 1, \ldots, m$ extends to an isomorphism of the fields $\mathbf{Q}(f_{\eta(H_1)}, \ldots, f_{\eta(H_m)})$ and $\mathbf{Q}(V(H_1), \ldots, V(H_m))$.*

Proof. For the first part, we note that all the exponential and logarithmic expressions which occur in E already occur in $H_1, \ldots, H_m$. Using $H_1, \ldots, H_m$ and $\mathbf{Q}$ and $+, -, *$, we can construct an ascending sequence of closed form definitions $G_1, \ldots, G_n$ with $G_n = E$, and such that all the exponential and logarithmic expressions in $G_1, \ldots, G_n$ already occur in $H_1, \ldots, H_m$. The fundamental sequence of exponential points for $G_1, \ldots, G_n$ is either the same as or is a subsequence of the fundamental sequence of exponential points for $H_1, \ldots, H_m$. Since $H_1, \ldots, H_m$ is reduced, $G_1, \ldots, G_n$ is also reduced. Theorem 2) now applies to give the stated result.

For the second part of the corollary, we use the fact that the first part implies isomorphism of the rings $\mathbf{Q}[f_{\eta(H_1)}, \ldots, f_{\eta(H_m)}]$ and $\mathbf{Q}[V(H_1), \ldots, V(H_m)]$, extending the evaluation map. The fields are just the quotient fields of the rings, and so they are also isomorphic, extending the same map.

Definition 4. *Let $(x_1, y_1), \ldots, (x_k, y_k)$ be the fundamental list of exponential points associated with partially evaluated expression E. We will say that the vector of integers $(a_1, \ldots, a_j)$ is reducing for E or for the associated ascending sequence of closed form definitions $G_1, \ldots, G_n$ if $a_j \neq 0$, and $a_1 x_1 + \cdots + a_j x_j = 0$.*

The next step is to state a procedure, based on Theorem 1), which, in some cases, will verify that $(a_1, \ldots, a_j)$ is reducing for E. We assume E is partially evaluated, and that $a_j \neq 0$. The return values for the procedure are either "SUCCESS" or "FAILURE".

Procedure $verify(E, (a_1, \ldots, a_j))$

Let $(x_1, y_1), \ldots, (x_k, y_k)$ be the fundamental list of exponential points associated with E. Let $G_1, \ldots, G_n$ be the ascending sequence of closed form definitions associated with E.

Let $x_1, \ldots, x_j$ be defined by $A_1, \ldots, A_j$ in the sequence $G_1, \ldots, G_n$, and $y_1, \ldots, y_j$ by $B_1, \ldots, B_j$. Either $B_j = exp(A_j)$ or $A_j = \log(B_j)$.

Check if

$a_1 f_{\eta(A_1)} + \cdots + a_j f_{\eta(A_j)} \equiv 0$.

If so, the verification succeeds, and the value "SUCCESS" is returned. Otherwise, check if

$f_{\eta(B_1)}^{a_1} \cdots f_{\eta(B_j)}^{a_j} \equiv 1$.

If this is false then the verification fails, and the value "FAILURE" is returned.

Otherwise, if the identity is true, it follows that $y_1^{a_1} \dots y_j^{a_j} = 1$. And therefore $a_1 x_1 + \cdots + a_j x_j = 2k\pi i$ for some integer k. This implies that the sum either has absolute value zero, or has absolute value larger than 2.

Now approximate $a_1 x_1 + \cdots + a_j x_j$. If we find $\mid a_1 x_1 + \cdots + a_j x_j \mid > 1/2$, then the verification fails, and the value "FAILURE" is returned. However if we find $\mid a_1 x_1 + \dots a_j x_j \mid < 1$ then the verification succeeds, and the value "SUCCESS" is returned.

Note that in the last step we only need a rough approximation since $\mid 2k\pi i \mid < 1$ and k integral implies $k = 0$.

If the verification procedure succeeds, the result is always correct, whether or not the Schanuel conjecture is true. That is, whenever "SUCCESS" is returned, the procedure has proved that $(a_1, \dots, a_j)$ is reducing for E. Correctness of this verification procedure depends only on Theorem 1). On the other hand, the return value "FAILURE" means only that the procedure was not able to decide whether or not $(a_1, \dots, a_j)$ is reducing for expression E.

The point of the next theorem is that if the Schanuel conjecture is true than the verification will succeed for a reducing vector of smallest dimension.

Theorem 3. *(Assuming the Schanuel conjecture) Let $E \in \mathcal{E}$ be a partially evaluated expression. Let $(x_1, y_1), \dots, (x_k, y_k)$ be the fundamental list of exponential points associated with E. If $(a_1, \dots, a_j)$ is reducing, with j minimal, then we can effectively verify that $a_1 x_1 + \dots a_j x_j = 0$ by calling the procedure $verify(E, (a_1, \dots, a_j))$*

Proof.

Let $G_1, \dots, G_n$ be the ascending sequence of closed form definitions associated with E. Let $x_1, \dots, x_j$ be defined by $A_1, \dots, A_j$ in the sequence $G_1, \dots, G_n$, and $y_1, \dots, y_j$ by $B_1, \dots, B_j$. Either $B_j = exp(A_j)$ or $A_j = \log(B_j)$. Since we suppose that $(a_1, \dots, a_j)$ is reducing, it is true that $a_1 x_1 + \cdots + a_j x_j = 0$.

Case 1). Suppose $B_j = exp(A_j)$. B_j must occur in the ascending sequence. Suppose B_j is G_a. Since j is minimal, $G_1, \dots, G_{a-1}$ is reduced.

$A_1, \dots, A_j$ are all in this reduced sequence. By The corollary to Theorem 2),

$a_1 x_1 + \dots + a_j x_j = 0 \leftrightarrow a_1 f_{\eta(A_1)} + \cdots + a_j f_{\eta(A_j)} \equiv 0$. So in this case the verification succeeds.

Case 2). Suppose $A_j = \log(B_j)$. Suppose that A_j is G_a. Since j was minimal, the sequence of definitions $G_1, \dots, G_{a-1}$ is reduced. And $B_1, \dots, B_j$ are all in this reduced sequence. So, once again, by the corollary to Theorem 2), the verification succeeds.

Theorem 4. *Suppose we are given a partially evaluated expression E in $\mathcal{E}$ of order k, and also given a reducing vector $(a_1, \dots, a_j)$. Then we can effectively construct another expression $\hat{E}$ so that $V(E) = V(\hat{E})$, and $\hat{E}$ has order $k - 1$.*

Proof. Refine the approximations if necessary so that the approximating boxes for the exponential subexpressions do not contain zero.

Let $G_1, \ldots, G_n$ be the ascending sequence of closed form definitions associated with E. Let $x_1, \ldots, x_j$ be defined by $A_1, \ldots, A_j$ in the sequence $G_1, \ldots, G_n$, and $y_1, \ldots, y_j$ by $B_1, \ldots, B_j$. Either $B_j = exp(A_j)$ or $A_j = \log(B_j)$.

Case 1). Suppose $B_j = exp(A_j)$. We have $y_j = V(B_j) = e^{x_j}$. Since $a_1 x_1 + \ldots a_j x_j = 0$, we also have $y_1^{a_1} \ldots y_j^{a_j} = 1$. So y_j is defined by a radical expression in $y_1, \ldots y_{j-1}$. In fact

$y_j = (y_1^{-a_1} \ldots y_{j-1}^{-a_{j-1}})^{1/a_j}$

Let D be an expression built up by field operations from $B_1, \ldots, B_j$ and having the same meaning as $B_1^{-a_1} \ldots B_{j-1}^{-a_{j-1}}$. To obtain the new, lower order, expression $\hat{E}$, we replace every instance of B_j in E by D^{1/a_j}. The approximating box for D^{1/a_j} will be the same as the approximating box for B_j. Since $V(D^{1/a_j}) = V(B_j)$, we also have $V(E) = V(\hat{E})$. The expression $\hat{V}$ has order $k-1$ since one exponential term has been replaced.

Case 2). Suppose $A_j = \log(B_j)$. We have $V(A_j) = x_j = (-1/a_j)(a_1 x_1 + \cdots + a_{j-1} x_{j-1})$. Let D be an expression built up by field operations from $A_1, \ldots, A_{j-1}$ which has the same meaning as $(-1/a_j)(a_1 A_1 + \cdots + a_{j-1} A_{j-1})$. In E replace every instance of A_j by D to obtain $\hat{E}$. As before, the value is unchanged, but the order is reduced by one.

5 Zero Tests for Closed Form Numbers

Using the above ideas, we can construct a variety of zero tests for closed form numbers. We get a number of possibilities, depending on whether or not we wish to include the use of a Liouville bound, such as the one given above in Conjecture 1), or whether or not we use some way to prove that an ascending sequence of definitions is reduced.

We first give a procedure which uses PSLQ to search for reducing vectors for a given expression E. Suppose E has associated ascending sequence of closed form definitions $G_1, \ldots, G_n$, and order k.

Let m be the initial precision to be used by PSLQ, and let M be the initial bound on the absolute values of integers in the search space.

Procedure $Search(E, m, M)$

Let $(x_1, y_1), \ldots, (x_k, y_k)$ be the fundamental list of exponential points associated with partially evaluated expression E.

Step 1) For $j = 1, \ldots, k$ use PSLQ with parameters m and M to search for a candidate reducing vector $(a_1, \ldots, a_j)$ for $(x_1, \ldots, x_j)$. If such a candidate is found, call $verify(E, (a_1, \ldots, a_j))$ to attempt to verify it. If the verification succeeds, return the reducing vector $(a_1, \ldots, a_j)$, and halt. If the verification fails, break out of the loop and go to step 2).

Step 2) Call $Search(E, 2m, M^2)$. Return the result, if any is ever obtained, and then halt.

The Search procedure will continue forever if E is already reduced.

Otherwise there must be a reducing vector $(a_1, \ldots, a_j)$ with j minimal. Assuming that the Schanuel conjecture is true, such a reducing vector can be verified, as shown in Theorem 3).

The PSLQ algorithm is guaranteed to find an integer relation if one exists. In our context that means that the search will eventually find a reducing vector if one exists, and if the Schanuel conjecture is true.

Zero Test

Suppose given partially evaluated expression E in $\mathcal{E}$. To decide whether or not $V(E) = 0$, we start two processes **P1)** and **P2)**, as described below. These processes run in parallel until one or the other halts with conclusion $V(E) \neq 0$ or $V(E) = 0$.

P1)

For $n = 1, 2, 3, \ldots.$ use the approximation procedure to find Gaussian rational Z_n so that $\mid V(E) - Z_n \mid < 10^{-n}$. If $\mid Z_n \mid > 10^{-n}$ then halt and conclude $V(E) \neq 0$.

[If we have available some Liouville bound $m(E)$ for E and we find $\mid V(E) \mid < 10^{-m(E)}$, then halt and conclude $V(E) = 0$.]

P2)

1. *Test if $f_{\eta(E)} \equiv 0$. If so, halt and conclude $V(E) = 0$.*
2. *[Otherwise, if we are able to show that $G_1, \ldots, G_n$ is reduced, then halt and conclude $V(E) \neq 0$.]*

   *Otherwise look for a reducing vector by calling $Search(E, 10\,k, 10^6)$, where k is the order of E. If this returns a reducing vector $(a_1, \ldots, a_j)$ then use this to simplify E to $\hat{E}$ with lower order, as explained in theorem 4). Begin process **P2)** again with $\hat{E}$ replacing E. Whatever is concluded about $\hat{E}$ should also be concluded about E.*

The parts of the test in square brackets are optional. With or without these parts, the test always eventually terminates, unless E and its subexpressions define a counterexample to the Schanuel conjecture. If $V(E) \neq 0$ then **P1)** will eventually discover this by approximation. On the other hand, suppose $V(E) = 0$. We can prove that **P2)** terminates, using the Schanuel conjecture, by induction on the order of the ascending sequence of definitions $G_1, \ldots, G_n$ associated with E. If the sequence is already reduced, then the Schanuel conjecture implies that $f_{\eta(E)} \equiv 0$, as shown in Theorem 2), and this algebraic identity can be verified. On the other hand, if the sequence is not reduced, the search algorithm will find a reducing vector, which will then be used to simplify E and to reduce the order.

A result returned by the test without the optional parts is correct, whether or not the Schanuel conjecture is true. Correctness of a result returned by **P1)** follows from the presumed correctness of our approximation technique. Correctness of **P2)** can be proved by induction on order. Suppose that this has been shown for partially evaluated expressions E of order less than k. Assume that E has order k. It may be that **P2)** terminates immediately, by finding that $f_{\eta(E)} \equiv 0$. In this case, theorem 1) implies that $V(E) = 0$. Otherwise, the search procedure is called. This comes back, if at all, with a reducing vector $(a_1, \ldots, a_j)$, which has been verified. **P2)** then constructs $\hat{E}$ which has order less than k and so that $V(E) = V(\hat{E})$. If **P2** terminates, concluding that that $V(\hat{E}) = 0$, the induction hypothesis implies that $V(\hat{E})$ is zero. Therefore $V(E) = 0$ is also correct.

Example 4. *Let E be $exp(3^{1/2}) * exp(3^{1/2}) - exp(12^{1/2})$.*

We take the positive branch of the square roots.

Since $V(E)$ is zero and, as we suppose, our approximation method is correct, the first part of the zero test, **P1)** *will not terminate.*

The second part of the zero test, **P2)** *will terminate. The fundamental list of exponential points is $(3^{1/2}, exp(3^{1/2}), (12^{1/2}, exp(12^{1/2}))$. Call this $(x_1, y_1), (x_2, y_2)$. We discover the reducing vector $(2, -1)$, and this reduces E to an expression which is algebraically zero.*

Example 5. $4\ arctan(1/5) - arctan(1/239) - \pi/4 = 0$

taking $arctan(x) = (i/2)\log((i + x)/(i - x))$, $i = \sqrt(-1)$, and $\pi = \log(-1)/\sqrt(-1)$ with appropriate partial evaluations to determine branches. If we take $x_1 = i\pi$, $x_2 = \log((i + 1/5)/(i - 1/5))$, $x_3 = \log((i+1/239)/(i-1/239))$, we get reducing vector $(1, 8, -2)$ for (x_1, x_2, x_3). The corresponding multiplicative identity can be verified algebraically.

6 Discussion

Definition 5. *A Schanuel bound for closed form numbers $x_1, \ldots, x_k$ is a number B so that if there is an integer relation for $x_1, \ldots, x_k$ there is one with norm no larger than B.*

The computational complexity of the above zero test could be bounded if we could compute explicit Schanuel bounds for closed form numbers $x_1, \ldots, x_k$.

It turns out, not surprisingly, that the essential problem is to bound norms of smallest integer relations for either vectors of algebraic numbers or for vectors of logarithms of algebraic numbers.

In [15] some upper bounds are found of this type by computing canonical forms in the associated algebraic fields.

A useful result in this connection is the following, given in notes of a course by C.L. Stewart. See Theorem 6) and the proof of Theorem 6') in [18]. Let $M(\alpha)$ denote Mahler measure of algebraic number α.

Theorem 5. *Let $\alpha_1, \ldots, \alpha_n$ be nonzero algebraic numbers and suppose that $\log\alpha_1, \ldots \log\alpha_n$ are linearly dependent over $\mathbf{Q}$. Suppose that $A_j = max(M(\alpha_j), e^{|\log\alpha_j|/d}, e)$ for $j = 1, \ldots, n$ where $d = [\mathbf{Q}(\alpha_1, \ldots, \alpha_n) : \mathbf{Q}]$. Then there exist integers $t_1, \ldots, t_n$ not all zero for which $t_1 \log\alpha_1 + \cdots + t_n \log\alpha_n = 0$ with*

$| t_i | \leq (11(n-1)d^3)^{n-1} \log A_1 \ldots \log A_n / \log A_i$

for $i = 1, \ldots, n$.

This theorem, greatly superior to anything in [15], can be used to bound in advance the sizes of the integers needed in a reducing vector for problems such as the one in the example 5) immediately above.

References

[1] G. Alefeld and J. Herzberger. *Introduction to Interval Computation*, Academic Press, 1983

[2] A. Baker. *Transcendental number theory*, CUP, 1975.

[3] J. M. Borwein and P. B. Borwein. On The Complexity of Familiar Functions and Numbers, SIAM Review, vol. .30, No 4, December 1988, pp. 589-601.

[4] Richard P. Brent. Multiple-precision zero- finding methods and the complexity of elementary functions, Analytic Computational Complexity, J.F.Traub ed., Academic Press 1975, pp. 151-176.

[5] J. R. Shackell. *Symbolic Asymptotics*, Springer, 2004

[6] C. Burnikle, S. Funke, K. Mehlhorn, S. Schirra and S. Schmitt. A separation bound for real algebraic expressions, Lecture Notes in Computer Science, pp. 254-265, Springer, 2001.

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

[8] T. Y. Chow. What is a Closed-Form Number?, American Mathematical Monthly, vol. 106, No 5, 1999, pp. 440-448.

[9] H. R. P. Ferguson, D. H. Bailey, and S. Arno. Analysis of PSLQ, An Integer Relation Finding Algorithm, Mathematics of Computation, vol. 68, number 225, January 1999, pp. 351-359

[10] C. Li. *Exact Geometric Computation: Theory and Applications*, Ph.D. Thesis, Department of Computer Science, New York University, 2001.

[11] C. Li and C.K. Yap. A new constructive root bound for algebraic expressions, In *12th ACM-SIAM Symp. on Discrete Algorithms*, pp. 496-505, Jan. 2001.

[12] C. Li, S. Pion and C. K. Yap. Recent Progress in Exact Geometric Computation, Journal of Logic and Algebra Programming, vol. 64, issue 1, 2005, pp. 85-111.

[13] A. Macintyre, A. Wilkie. On the decidability of the real exponential field, in *Kreiseliana, About and Around Georg Kreisel*, A.K. Peters, 1996, pp. 441-467.

[14] Daniel Richardson. How to Recognise Zero, J. Symbolic Computation (1997), 24, pp. 627-645.

[15] Daniel Richardson. Multiplicative Independence of Algebraic Numbers and Expressions, Journal of pure and applied algebra, 164, 2001, pp. 231-245

[16] Daniel Richardson. The Uniformity Conjecture, Proceedings of Computability and Complexity in Analysis, CCA2000, September 17-19, Swansea, Wales. Also in associated Springer lecture notes in computer science vol. 2064, pp. 253-272.

[17] Daniel Richardson and Ahmed Elsonbaty. Counterexamples to the Uniformity Conjecture, Computational Geometry, Theory and Applications 33, issue 1-2, January 2006, pp. 58-64, Elsevier ISSN 0925-7721

[18] C.L. Stewart. Linear Forms in Logarithms and Diophantine Equations, Notes by D. Wolczuk. See www.math.uwaterloo/PM_Dept/Homepages/Stewart/Course_Notes/Stewart.notes_1.pdf

[19] Joris Van Der Hoeven. Automatic Numerical Expansions, in J.-C. Bajard, D. Michelucci, J.-M. Moreau, and J.-M. Muller, editors, Proc. of the conference "Real numbers and computers", Saint-Etienne, France, pp. 261-274, 1995.

[20] Joris Van Der Hoeven. *Automatic Asymptotics*, Ph.D. thesis, Ecole Polytechnique, 1997.

[21] Joris Van Der Hoeven. Zero-testing, witness conjectures and differential diophantine approximation, Preprint. See www.math.u-psud.fr/ ~ vdhoeven.

[22] K. Weihrauch. *Computable Analysis, an Introduction*, Springer-Verlag, Berlin, 2000

[23] C. K. Yap. Robust Geometric Computation in Handbook of Discrete and Computational Geometry (eds. J. E. Goodman and J. O'Rourke) Chapman & Hall/CRC, Boca Raton, Florida. 2nd Edition. pp. 927-952, 2004

[24] C. K. Yap. *Fundamental Problems of Algorithmic Algebra*, Oxford University Press, 2000.

[25] C. K. Yap. On Guaranteed Accuracy Computation, in *Geometric Computation*, World Scientific Publishing, pp. 322-373, 2004