Zero-testing, witness conjectures and differential diophantine approximation

BY JORIS VAN DER HOEVEN

Dépt. de Mathématiques (bât. 425)
Université Paris-Sud
91405 Orsay CEDEX
France

November 14, 2001

Abstract

Consider a class of constants built up from the rationals using the field operations and a certain number of transcendental functions like exp. A central problem in computer algebra is to test whether such a constant, which is represented by an expression, is zero.

The simplest approach to the zero-test problem is to evaluate the constants up to a certain number of decimal digits. Modulo certain precautions, we will make it likely that this approach is actually a valid one. More precisely, one may for instance restrict oneself to certain subsets of expressions in order to avoid "high precision fraud". For such subsets, we will state witness conjectures, which propose reasonable lower bounds for non zero constants as a function of the minimal sizes of expressions that represent them.

Unfortunately, such witness conjectures are extremely hard to prove, since they are really far reaching generalizations of results in diophantine approximations. Nevertheless, we will also discuss their counterparts for formal power series, which are more accessible.

1 Introduction

Zero-testing an important issue in mathematics and more specifically in computer algebra. Standard mathematical notation provides a way of representing many transcendental functions. However, trivial cases apart, this notation gives rise to the following problems:

- Expressions may not be defined: consider $1/0$, $\log(0)$ or $\log(e^{x+y} - e^x e^y)$.
- Expressions may be ambiguous: what values should we take for $\log(-1)$ or $\sqrt{z^2}$?
- Expressions may be redundant: we have the functional equation
$$\sin^2 x + \cos^2 x = 1,$$
although $\sin^2 x + \cos^2 x$ and 1 are different as expressions. Similarly,
$$\sqrt[3]{\sqrt[5]{32/5} - \sqrt[5]{27/5}} = (1 + \sqrt[5]{3} - \sqrt[5]{9})/\sqrt[5]{25}.$$

The first two problems can usually be solved by restricting oneself to an appropriate setting. Remains the third and most difficult problem, which is known as the zero-test or zero-equivalence problem, since we are usually interested in expressions that represent functions in a ring.

As a reflex, most mathematicians tend to deal with the zero-test problem by restricting their attention to expressions of a certain form and proving a structure theorem for such expressions. Some successes of this approach are the following:

- Computations in algebraic extensions of a field using Groebner basis techniques. In this case an element of the algebraic extension is represented uniquely by its reduction modulo the Groebner basis.

- The Risch structure theorem [Ris75] allows computations in differential field extensions by exponentials, logarithms, or integrals. This technique may be adapted to a few other cases [SSC85].
- Richardson designed a zero-test for elementary constants (i.e. constants which may be defined implicitly using rational numbers, the field operations and exponentiation), which assumes Schanuel's conjecture [Ric94], [Ax71].
- More recently, Ecalle has proved several structure theorems for generalized polylogarithms and zeta functions. One may expect the design of fast algorithms for dealing with such functions on the basis of his results.

However, it should be stressed that a structure theorem explicitly describes *all* relations which hold for the class of expressions being considered. Such a theorem is much more powerful than a zero-test algorithm, which just provides a method to test whether a *particular* expression represents zero.

It is therefore recommended to treat the zero-test problem independently from the problem of establishing a complete structure theorem. Indeed, we have just stressed that the zero-test problem is less ambitious, so it may be solved for larger classes of expressions. Secondly, even if a structure theorem exist, a special purpose zero-test may be more efficient than a zero-test derived from the theorem, which may be very complicated.

Now engineers have a very simple solution to the zero-test problem for constants: evaluate the constant with double precision and test whether the result vanishes. The advantage of this method, which works most of the time, is that it is very fast. However, double precision is not always sufficient to ensure the correctness of the answers. This problem can not merely be solved by considering quadruple or higher fixed precisions. Instead, it rises an interesting theoretical question: what is the required precision of evaluation *as a function of* the size of the input expression in the zero-test.

Now there are some well-known examples of small, but non-zero expressions, like

$$e^{\pi\sqrt{163/9}} - 640320, \tag{1.1}$$

or

$$e^{e^{e^{10}} + e^{-e^{e^{10}}}} - e^{e^{e^{10}}} - 1. \tag{1.2}$$

Essentially, we conjecture that such examples always come down to the substitution of a very small number in a non-zero power series with high valuation. This is clear in the second example, but may necessitate some extra work in other cases. For other nice examples of "high precision fraud", we refer to [BB92].

In order to develop reliable zero-tests, we thus have to search for a setting in which high precision fraud is impossible. In the case of exp-log constants, one possible approach is to limit the modules of certain subexpressions. In such a setting an expression like 10^{100} might become invalid and need to be rewritten as $10 \times \cdots \times 10$, which increases its size. Then it is reasonable to expect that there exist bounds from below for the absolute values of non-zero constants as a function of the sizes of their representing expressions. Such "witness conjectures" were first stated in [vdH97, vdH01], and later by Richardson [Ric01], who has also done some numerical computations which tend to confirm our expectations.

In this paper, we study several possible formulations of witness conjectures and we consider more general transcendental functions, defined by differential equations and initial conditions. We will also discuss some analogue conjectures for formal power series, on which we some progress has already been made [Kho91, SvdH01].

Witness conjectures may be interpreted as far reaching generalizations of existing conjectures and results in diophantine approximation [Lan71]. Indeed, this theory is concerned with finding good rational approximations of real numbers x, which is equivalent to minimizing

$$|p\,x - q|$$

for large $p, q \in \mathbb{Z}$. More generally, diophantine approximation is concerned with minimizing $|P(x)|$ for polynomials $P \in \mathbb{Z}[X]$. In our case, we are interested in even more general expressions, which involve transcendental functions defined by differential equations and initial conditions. The theory of minimizing the absolute values of such more general expressions might therefore be baptized as "differential diophantine approximation".

We finally want to stress the interest of our approach for transcendental number theory. One major problem in this area is that it is already very hard to just state something like a generalization of the Schanuel conjecture for more general transcendental functions. The reason of this difficulty is that this conjecture is a result of the "structure theorem" approach. In order to state such a generalization, one thus has to anticipate the structure theorems which hold in the more general setting. By contrast, our "witness conjecture" approach directly applies to more general settings and it is legitimate to hope that some of the tools developed in this context can also be applied elsewhere.

2 Witness conjectures for constants

2.1 Exp-log constants

Let $\check{\mathcal{E}}$ be the set of exp-log constant expressions, i.e. the expressions formed from $\{0, 1\}$ using $+, -, \times, /$, exp and log. We will denote by $\mathcal{E}$ the set of real numbers which can be represented by an expression in $\check{\mathcal{E}}$ and by $x \in \mathcal{E}$ the real number represented by an expression $\check{x} \in \check{\mathcal{E}}$. We will denote by $\sigma(\check{x})$ the size of an expression $\check{x} \in \check{\mathcal{E}}$ (i.e. the number of nodes when interpreting the expression as a tree). Given a rational number $N \geqslant 3$, we denote by $\check{\mathcal{E}}_N$ the set of all expressions $\check{x} \in \check{\mathcal{E}}$, such that $N^{-1} \leqslant |y| \leqslant N$ for all subexpressions $\check{y}$ of $\check{x}$. In [vdH97], we stated the first *witness conjecture*:

Conjecture 2.1. *There exists a function ϖ of one of the forms*

a) $\varpi(\sigma) = K\,\sigma$*;*

b) $\varpi(\sigma) = K^{\sigma}$*,*

where $K \geqslant 1$ depends on N, such that

$$|x| \geqslant e^{-\varpi(\sigma(\check{x}))}. \tag{2.1}$$

for all $\check{x} \in \check{\mathcal{E}}_N$ with $x \neq 0$.

Actually, we conjectured the b-part and we remarked that the conjecture might even hold for smaller *witness functions* ϖ, such as in the a-part. We will call the a-part a *strong witness conjecture* and the b-part a *weak witness conjecture*. It is also possible to consider intermediate witness conjecture, by taking $\varpi(\sigma) = \sigma^K$, for instance. In general, we call a weakness conjecture strong, if $\log_l \varpi(\exp_l \sigma) \sim \sigma$, for some $l \in \mathbb{N}$, where $\log_l$ and $\exp_l$ denote the l-th iterates of log and exp. In what follows, we will only state strong witness conjectures with linear witness functions, but it might turn out in the future that other witness functions are necessary.

A slightly different setting was first considered (in a more general form) in [vdH01]. Given a rational number $N > 1$, let $\check{\mathcal{E}}'_N$ be the class of all expressions $\check{x}$ in $\check{\mathcal{E}}$, such that for each subexpression $\check{y}$ of $\check{x}$ of the form $\check{y} = \exp \check{z}$ we have $|z| \leqslant N$, and such that for each subexpression $\check{y}$ of $\check{x}$ of the form $\check{y} = \log \check{z}$ we have $1/N \leqslant z \leqslant N$.

Conjecture 2.2. *There exists a witness function of the form $\varpi(\sigma) = K\,\sigma$, where $K \geqslant 1$ depends on N, and such that for all $\check{x} \in \check{\mathcal{E}}'_N$, we either have $x = 0$ or $|x| \geqslant e^{-\varpi(\sigma(\check{x}))}$.*

It should be noticed that this conjecture holds for all N as soon as it holds for a particular N. Indeed, for $N' \leqslant N$ we may take $\varpi_{N'} = \varpi_N$. For $N' > N$ we may take

$$\varpi_{N'}(\sigma) = \varpi_N(\lceil N'/N \rceil\,(\sigma + K)) \tag{2.2}$$

for some constant K, since any $y = \exp z$ with $N < |z| \leqslant N'$ may be rewritten as

$$y = \exp \frac{z}{\lceil N'/N \rceil} \overset{\lceil N'/N \rceil \text{ times}}{\cdots} \exp \frac{z}{\lceil N'/N \rceil}.$$

In a similar way, if $y = \log z$ with $1/N' \leqslant z < 1/N$ or $N < z \leqslant N'$, then we may decompose

$$z = r^k\,z', \tag{2.3}$$

where $r, z' \in (1/N, N)$ and $k \in \mathbb{Z}$, so that

$$y = k \log r + \log z'.$$

Moreover, by selecting r to be a fixed rational number of small size close to N, we may bound $|k|$ by a fixed constant, which explains (2.2).

Obviously, conjecture 2.1 is implied by conjecture 2.2. We do not know at present whether the inverse is also true. Yet another variant of conjecture 2.2 is obtained by dropping the requirement on the arguments to logarithms. Using (2.3), this variant can again be reduced to conjecture 2.2, but the witness function may change in a non linear way, since $|k|$ can no longer be bound from above by a fixed constant, but only by $O(\varpi(\sigma(\check{z})))$.

2.2 Values of differentially algebraic functions

In [vdH01], we have generalized the witness conjectures for exp-log constants to so called "holonomic constants". Such constants are formed from the rationals, using the field operations and holonomic functions (i.e. functions that satisfy a linear differential equation over $\mathbb{Q}[x]$). The approach actually easily generalizes to more general constants, which arise as values of differentially algebraic functions.

Let $\mathcal{C} \subseteq \mathbb{C}$ be a certain field of constants and let f be a function which is analytic in 0. We say that f is differentially algebraic over $\mathcal{C}$ with initial conditions in $\mathcal{C}$, if f satisfies a differential equation

$$f^{(r)} = \frac{P(f, \ldots, f^{(r-1)})}{Q(f, \ldots, f^{(r-1)})},$$

with $P, Q \in \mathcal{C}[F, \ldots, F^{(r-1)}]$ and where $f(0), \ldots, f^{(r-1)}(0) \in \mathcal{C}$ are such that

$$Q(f(0), \ldots, f^{(r-1)}(0)) \neq 0.$$

We will consider values of such functions f in points $z \in \mathcal{C}$, such that $|z|$ is strictly smaller than the radius of convergence ρ_f of f.

We may now construct a huge class of constants as follows. We start with $\mathcal{D}_0 = \mathbb{Q}$. Assuming that $\mathcal{D}_h$ has been constructed, we let $\mathcal{D}_{h+1}$ be the set of all possible values in elements of $\mathcal{D}_h$ of differentially algebraic functions over $\mathcal{D}_h$ with initial conditions in $\mathcal{D}_h$. It can be shown that each $\mathcal{D}_{h+1}$ is a field, which contains $\mathcal{D}_h$. Finally, we take $\mathcal{D} = \mathcal{D}_0 \cup \mathcal{D}_1 \cup \cdots$. Elements in $\mathcal{D}$ may be represented by expressions as follows. Let $\check{\mathcal{D}}$ be the smallest set of expressions such that

- $0, 1 \in \check{\mathcal{D}}$.
- $\check{u} + \check{v}, \check{u} - \check{v}, \check{u}\,\check{v}, \check{u}/\check{v} \in \check{\mathcal{D}}$ for all $\check{u}, \check{v} \in \check{\mathcal{D}}$.
- Let f be a differentially algebraic function as above, such that $f(0), \ldots, f^{(r-1)}(0)$ are represented by $\check{c}_0, \ldots, \check{c}_{r-1} \in \check{\mathcal{D}}$ and such that P and Q are represented by expressions in $\check{\mathcal{D}}[F, \ldots, F^{(r-1)}]$. Given $\check{u} \in \check{\mathcal{D}}$ with $|u| < \rho_f$, the expression $\heartsuit(\check{P}, \check{Q}, \check{c}_0, \ldots, \check{c}_r, \check{u}) \in \check{\mathcal{D}}$ then represents $f(z)$.

From the expressiveness point of view, it is not really necessary to have special expressions for the field operations (if we take $\mathbb{Q} \subseteq \check{\mathcal{D}}$). However, we do need them in order to keep the sizes of expressions reasonably small.

2.3 Corrected size functions

In order to state witness conjectures for constants in $\mathcal{D}$, several approaches are possible. One approach, which will be developed in the section 2.4, is to restrict ones attention to representations by expressions in $\check{\mathcal{D}}$ of a special form, like we did in the case of exp-log constants.

Another approach, which was introduced in [vdH01], is to redefine the size of an expression in such a way that expressions like e^{100} have a large size. In the present setting, this comes down to defining the "size" $\sigma^*(\check{z})$ of an expression $\check{z} \in \check{\mathcal{D}}$ as follows:

- If $\check{z} = 0$ or $\check{z} = 1$, then $\sigma^*(\check{z}) = 1$.
- If $\check{z} = \check{u} + \check{v}, \check{z} = \check{u} - \check{v}, \check{z} = \check{u}\,\check{v}$ or $\check{z} = \check{u}/\check{v}$, then $\sigma^*(\check{z}) = \sigma^*(\check{u}) + \sigma^*(\check{v}) + 1$.
- If $\check{z} = \heartsuit(\check{P}, \check{Q}, \check{c}_0, \ldots, \check{c}_{r-1}, \check{u})$, then
$$\sigma^*(\check{z}) = \sigma^*(\check{f}) + \sigma^*(\check{u}) + \log\left(\sup_{|v| \leqslant |u|} |f(v)| + 1\right),$$
where
$$\sigma^*(\check{f}) = \sigma^*(\check{P}) + \sigma^*(\check{Q}) + \sigma^*(\check{c}_0) + \cdots + \sigma^*(\check{c}_{r-1}) + 1$$
and
$$\sigma^*(\check{P}) = \sum_{i_0 \leqslant \deg_F \check{P}} \cdots \sum_{i_{r-1} \leqslant \deg_{F^{(r-1)}} \check{P}} \sigma^*(\check{P}_{i_0, \ldots, i_{r-1}})$$
and similarly for $\sigma^*(\check{Q})$.

For example, in the case of the exponential function, we have $f' = f$ and $f(0) = 1$, so that $\sigma^*(\exp) = 5$ and $\sigma^*(\exp \check{u}) = \sigma^*(\check{u}) + 5 + \log(e^{|u|} + 1)$. Hence, $\sigma^*(\exp \check{u}) \approx \sigma^*(\check{u}) + 5 + |u|$ for large u. Because of the corrective term $|u|$, an expression like e^{100} will therefore have a large size.

Conjecture 2.3. *There exists a witness function $\varpi(\sigma) = K\sigma$ with $K \geqslant 1$, such that for all $\check{z} \in \check{\mathcal{D}}$, we either have $z = 0$ or $|z| \geqslant e^{-\varpi(\sigma^*(\check{z}))}$.*

Remark 2.4. It is easy to show by structural induction that we also have the upper bound
$$|z| \leqslant e^{\varpi(\sigma^*(\check{z}))}$$

for all $\check{z} \in \check{\mathcal{D}}$, if the conjecture holds. Notice also that this bound holds independently from the conjecture, if we disallow expressions of the form $\check{u}/\check{v}$.

2.4 Admissible expressions

The second approach in order to state witness conjectures for $\check{\mathcal{D}}$ is to use the usual size function σ, which is defined recursively as the corrected size function σ^* by omitting the corrective term $\log\left(\sup_{|v| \leqslant |u|} |f(v)| + 1\right)$, but to restrict our attention to a subset of admissible expressions of $\check{\mathcal{D}}$.

Let $\lambda \in (0,1)$ be a rational parameter. We recursively define the subset $\check{\mathcal{D}}_\lambda$ in a similar way as $\check{\mathcal{D}}$, but each time that $\check{z} \in \check{\mathcal{D}}_\lambda$ is of the form $\check{z} = \heartsuit(\check{P}, \check{Q}, \check{c}_0, \ldots, \check{c}_{r-1}, \check{u})$, we require that $|u| \leqslant \lambda$, $Q(f(v)) \neq 0$ for all $|v| \leqslant \lambda$, and $|f_k| \leqslant 1$ for each Taylor coefficient f_k of f. We first claim that each constant in $\mathcal{D}$ may be represented by an expression in $\check{\mathcal{D}}_\lambda$. This follows from the following two observations:

- The Taylor coefficients of any analytic function f in 0 satisfy a bound of the form $|f_k| \leqslant \alpha\, \beta^k$, with $\alpha, \beta \in \mathbb{Q}$ (and β^{-1} as close to ρ_f as we wish). If f is also differentially algebraic over $\mathcal{C}$ with initial conditions in $\mathcal{C}$, then so is $g(z) = \alpha^{-1} f(\beta^{-1} z)$. We may therefore assume without loss of generality that $|f_k| \leqslant 1$ for all k when constructing constants in $\mathcal{D}$.
- If we want to evaluate f in a point z with $|z| > \lambda$, then we may use analytic continuation: taking
$$g(z') = f\left(\lambda \tfrac{z}{|z|} + z'\right),$$
g satisfies a similar algebraic differential equation as f, whose initial conditions correspond to evaluations of f and its derivatives in $(\lambda\, z)/|z|$. Assuming that we chose β^{-1} sufficiently close to ρ_f in the first observation, and repeating the analytic continuation argument, we may finally evaluate f in z.

We notice that the analytic continuation procedure in the second observation is very close to rewriting $e^{n x} = e^x \cdots e^x$, as we did before.

Conjecture 2.5. *Let $\lambda \in (0,1)$. Then there exists a witness function $\varpi(\sigma) = K\, \sigma$, where $K \geqslant 1$ depends on λ, and such that for all $\check{z} \in \check{\mathcal{D}}_\lambda$, we either have $z = 0$ or $|z| \geqslant e^{-\varpi(\sigma(\check{z}))}$.*

Because of the analytic continuation argument, conjecture 2.5 holds for all $\lambda \in (0,1)$ as soon as it holds for a particular λ. It is not hard to see that conjecture 2.2 is also implied by conjecture 2.5. Indeed, the coefficients of the Taylor series of exp in 0 are all bounded by 1 in module, so if $\check{x} \in \check{\mathcal{D}}_\lambda$ and $\check{y} \in \check{\mathcal{E}}'_\lambda$ represent the same number $x = y$ with $|x| \leqslant \lambda$, then $\heartsuit(F, 1, 1, \check{x}) \in \check{\mathcal{D}}_\lambda$ and $\exp \check{y} \in \check{\mathcal{E}}'_\lambda$ both represent e^x and we have $\sigma(\heartsuit(F, 1, 1, \check{x})) = \sigma(\check{x}) + O(1)$ as well as $\sigma(\exp \check{y}) = \sigma(\check{y}) + O(1)$. Logarithms may be handled in a similar fashion.

Let us now show that conjecture 2.5 is implied by conjecture 2.3. Indeed, an analytic function f, such that $|f_k| \leqslant 1$ for all k, satisfies the bound
$$\sup_{|z| \leqslant \lambda} |f(z)| \leqslant \frac{1}{1 - \lambda}.$$
Consequently, the corrective terms in the corrected sizes $\sigma^*(\check{z})$ of expressions $\check{z} \in \check{\mathcal{D}}_\lambda$ are uniformly bounded. We conclude that $\sigma^*(\check{z}) = O(\sigma(\check{z}))$ for $\check{z} \in \check{\mathcal{D}}_\lambda$, which implies our claim.

Actually, conjecture 2.3 seems to be slightly stronger than conjecture 2.5. When using
$$\log\left(\sup_{|v| \leqslant \lambda^{-1}|u|} |f(v)| + 1\right)$$

as a corrective term for some rational $\lambda \in (0, 1)$ instead of the usual one, both conjectures are equivalent. Indeed, in this case we may normalize $g(u') = M^{-1} f(u' u / \lambda)$ and replace $f(u)$ by $M g(\lambda)$, where M is a good rational upper approximation of $\sup_{|v| \leqslant \lambda^{-1}|u|} |f(v)|$. Performing this trick recursively in expressions in $\check{\mathcal{D}}$ of corrected size σ^*, we end up with expressions in $\check{\mathcal{D}}_\lambda$ of usual size $\sigma = O(\sigma^*)$.

2.5 More general constants

Witness conjectures may also be stated for more general types of constants, such as

- Constants that arise as values of solutions to partial differential equations, whose boundary conditions recursively satisfy partial differential equations in less variables.
- Constants that arise during the process of accelero-summation [É92] of divergent solutions to algebraic differential equations, or as limits of such solutions in singular points, if these limits exist. This may for instance be done using the approach from section 2.3, but where the supremum in the corrective term for $\sigma^*(\check{z})$ is taken over a sector instead of a disk.
- Constants that arise as values of solutions to more general functional equations. Of course, one has to be much more careful in this setting, since it is much easier to construct examples of high-precision fraud in this setting, by considering equations such as

$$f(x) = \frac{1}{x} + f(e^x)$$

  for $x \to \infty$.

3 Witness conjectures for power series

3.1 Exp-log series

Consider the ring of formal power series $C[[z]]$ over a field C of characteristic zero. Let $\check{\mathcal{E}}$ be the smallest set of expressions $\check{f}$ that represent series $f \in C[[z]]$, such that

- $z \in \check{\mathcal{E}}$.
- $c \in \check{\mathcal{E}}$, for all $c \in C$.
- $\check{f} + \check{g}$, $\check{f} - \check{g}$ and $\check{f}\check{g}$ are in $\check{\mathcal{E}}$, for all $\check{f}, \check{g} \in \check{\mathcal{E}}$.
- $\frac{1}{1+\check{f}}$, $\exp \check{f}$ and $\log(1 + \check{f})$ are in $\check{\mathcal{E}}$ for all $\check{f} \in \check{\mathcal{E}}$ with $f_0 = 0$.

The set $\mathcal{E}$ of series represented by expressions in $\check{\mathcal{E}}$ is called the set of *exp-log series* in z. We will denote by $v(f)$ the valuation of a series $f \in C[[z]]$.

Conjecture 3.1. *There exists a constant $K \geqslant 1$, such that for all $\check{f} \in \check{\mathcal{E}}$, we either have $f = 0$ or $v(f) \leqslant K \sigma(\check{f})$.*

We observe that the coefficients of $f \in \mathcal{E}$ are polynomials with rational coefficients in the constants of C which occur in a representing expression $\check{f} \in \check{\mathcal{E}}$ of f. Consequently, it suffices to check conjecture 3.1 in the case when C is the field of algebraic numbers.

Let us now show that conjecture 3.1 is implied by conjecture 2.2(a) in the case when $C=\mathbb{Q}$. Indeed, assume that there exists a counterexample $\check{f}\in\check{\mathcal{E}}$ to conjecture 3.1 for each K with $f\neq 0$ and $v(f)>K\sigma(\check{f})$. Then for $n\in\mathbb{N}$ sufficiently large, we may represent $f(e^{-n})$ by an expression in $\check{\mathcal{E}}_\lambda'$ whose size is bounded by $B_\lambda n\sigma(\check{f})$. Moreover, since $\check{f}$ is a counterexample to conjecture 3.1, there exists a constant M, such that $f(e^{-n})\neq 0$ and

$$|f(e^{-n})|<M e^{-nK\sigma(\check{f})}\leqslant M e^{-(K/B_\lambda)\sigma(\widetilde{f(e^{-n})})}.$$

This yields a counterexample to conjecture 2.2(a), for sufficiently large K.

The above argument suggests that, in order to prove numerical witness conjectures, it may be good to start proving their power series equivalents. Although this project seems still to be out of reach for linear witness functions, we were able to prove the following weak witness theorem [SvdH01]; this result is based on a careful complexity analysis of the zero-test algorithm from [Sha89].

Theorem 3.2. *For all $\check{f}\in\check{\mathcal{E}}$, we either have $f=0$ or $v(f)\leqslant\varpi(\sigma(\check{f}))$, with $\varpi(\sigma)=(4\sigma)^{9^\sigma}$.*

Recently, we have been made aware of the work of Khovanskii [Kho91], which seems to imply even better bounds of the form $\varpi(\sigma)=\sigma^{O(1)}2^{\sigma^2}$. We are still studying this work and trying to prove similar bounds with our techniques. Our main reason for doing this is that the techniques from [SvdH01] are better suited for generalizations.

3.2 Differentially algebraic series

Let $\mathcal{R}$ be a differential subring of $C[[z]]$. In analogy with section 2.2, we define a series $f\in C[[z]]$ to be differentially algebraic over $\mathcal{R}$, if f satisfies an algebraic differential equation

$$f^{(r)}=\frac{P(f,\ldots,f^{(r-1)})}{Q(f,\ldots,f^{(r-1)})},\tag{3.1}$$

with $P,Q\in\mathcal{R}[F,\ldots,F^{(r-1)}]$ and where $f(0),\ldots,f^{(r-1)}(0)$ are such that

$$Q(f(0),\ldots,f^{(r-1)}(0))\neq 0.$$

Starting with $\mathcal{D}_0:=C$, we may again recursively construct $\mathcal{D}_{h+1}$ to be the ring of differentially algebraic power series over $\mathcal{D}_h$, and define $\mathcal{D}:=\mathcal{D}_0\cup\mathcal{D}_1\cup\cdots$. Power series in $\mathcal{D}$ may be represented in a similar way as in section 2.2 and we have the following power series analogue of conjectures 2.3 and 2.5.

Conjecture 3.3. *There exists a witness function $\varpi(\sigma)=K\sigma$ with $K\geqslant 1$, such that for all $\check{f}\in\check{\mathcal{D}}$, we either have $f=0$ or $v(f)\geqslant\varpi(\check{f})$.*

In [SvdH01], we proved the above conjecture for $\varpi(\sigma)=(4\sigma)^{9^\sigma}$ in the case of differential equations (3.1) of order $r=1$. We believe to have found a generalization of this theorem to higher orders, but this still has to be worked out in detail. In the first order case, better bounds of the form $\varpi(\sigma)=\sigma^{O(1)}2^{\sigma^2}$ seem to result from [Kho91].

3.3 Multivariate series

Actually, there is no reason to restrict ourselves to formal power series in one variable in sections 3.1 and 3.2, so that we may very well replace $C[[z]]$ by $C[[z_1,\ldots,z_k]]$. In the construction of $\check{\mathcal{E}}$, given $\check{f}\in\check{\mathcal{E}}$, we then have to assume that $f_{0,\ldots,0}=0$, for $1/(1+\check{f})$, log $(1+\check{f})$ or $e^{\check{f}}$ to be in $\mathcal{E}$. Similarly, the differential equation (3.1) should be replaced by a system of partial differential equations

$$\frac{\partial^{r_i}f}{\partial z_i^r}=\frac{P_i(f,\ldots,\partial^{r_i-1}f/\partial z_i^{r-1})}{Q_i(f,\ldots,\partial^{r_i-1}f/\partial z_i^{r-1})},\tag{3.2}$$

for $i = 1, \ldots, k$, such that the polynomials P_i, Q_i satisfy

$$Q_i(f(0, \ldots, 0), \ldots, \partial^{r_i - 1} f / \partial z_i^{r-1}(0, \ldots, 0)) \neq 0.$$

One might also investigate other ways to present the partial differential equations (3.2), such as coherent autoreduced systems.

Now given such a multivariate setting, it is interesting to study the dependence of the witness conjectures on the parameter k. The following result has been proved in [SvdH01]; better bounds might follow from [Kho91].

Theorem 3.4. *For all $\check{f} \in \check{\mathcal{E}}$, we either have $f = 0$ or $v(f) \leqslant \varpi(\sigma(\check{f}))$, where $\varpi(\sigma) = (4\, k\, \sigma)^{9^\sigma}$.*

3.4 Finer size parameters

Technically speaking, it turns out that the exponential behavior in $\sigma(\check{f})$ in theorem 3.2 is due to the "differential part" of $\check{f}$. More precisely, if we consider a non zero power series f in a fixed polynomial ring $C[g_1, \ldots, g_n]$ with $g_1, \ldots, g_n \in \mathcal{E}$, then there exists a polynomial bound for $v(f)$ in $d = \max \{\deg_{g_1} f, \ldots, \deg_{g_n} f\}$. This observation seems to generalize to higher order differential power series.

As a first step to the proofs of stronger witness conjectures for differential power series, it may therefore be a good idea to find more subtle size parameters for expressions in $\check{\mathcal{E}}$, such as n and d above. It may also be interesting to consider other interesting classes of power series, such as rings of the form

$$C[z, e^{P_1(z)}, \ldots, e^{P_n(z)}],$$

where $P_1, \ldots, P_n \in C[z]$. Can the exponential bound in n be further improved for such rings?

It might also be interesting to do some computer algebra experiments for expressions of a simple form and small size. For instance, one might consider all expressions formed using z, formal parameters λ_1, λ_2, ..., additional, multiplication and exponentiation of infinitesimals. Given a power series represented by such an expression, one may set the first n coefficients to zero (this puts constraints on the parameters $\lambda_1, \lambda_2, \ldots$) and study the number of remaining free parameters as a function of n. Doing this for all expressions up to a certain size, one may collect concrete evidence for the witness conjectures and determine the "worst case expressions".

4 Differential diophantine approximation

4.1 Classical results in diophantine approximation

Now we have stated different types of witness conjectures, it is interesting to investigate what is already known on this subject. Probably, the classical theory of diophantine approximation, which is concerned with the approximation of a given real number x by rationals, comes closest to our subject. Equivalently, one may ask how small $|n\, x - m|$ can get for large n, $m \in \mathbb{Z}$. More generally, an interesting question is to know how small $|P(x)|$ can get as a function of $P \in \mathbb{Z}[X] \setminus \{0\}$. Even more generally, one may consider complex numbers $z_1, \ldots, z_k$ and ask how small $|P(z_1, \ldots, z_k)|$ can get as a function of $P \in \mathbb{Z}[Z_1, \ldots, Z_k] \setminus \{0\}$.

Let us first consider an algebraic number z, with $P(z) = 0$ for some polynomial $P \in \mathbb{Z}[Z]$ of minimal degree $n \geqslant 2$ and minimal leading coefficient $c \in \mathbb{N}^*$. Let

$$P = c\,(Z - \alpha_1) \cdots (Z - \alpha_n)$$

be the factorization of P with $z=\alpha_1$ and $\alpha_i\neq\alpha_j$ for all $i\neq j$. Given $p/q\in\mathbb{Q}$ close to z (say $|p/q-z|<|p/q-\alpha_i|$ for all $i\neq 1$), we then have

$$\left|z-\frac{p}{q}\right|=\frac{\left|P\left(\frac{p}{q}\right)\right|}{c\left|\alpha_2-\frac{p}{q}\right|\cdots\left|\alpha_n-\frac{p}{q}\right|}\geqslant\frac{1}{2^{n-1}\,c\,|\alpha_2-\alpha_1|\cdots|\alpha_n-\alpha_1|\,q^n},$$

since $q^n\,P(p/q)\in\mathbb{Z}^*$. This bound, which is due to Liouville, shows that $|z-p/q|$ can be bounded from below by an expression of the form β/q^n, where β can be expressed as a function of the polynomial P (and actually as a function of its size). This seems to give some evidence for a strong witness conjecture for algebraic numbers.

Actually, the above bound can be sharpened in an asymptotical way. Given a real number x, let $\|x\|$ be the distance between x and the closest point in $\mathbb{Z}$. The following theorem is due to Roth [Rot55], based on previous work by Schneider [Sch36].

Theorem 4.1. *Given an algebraic irrational number x and $\varepsilon>0$, there are only a finite number of solutions to the inequality $\|q\,x\|<1/q^{1+\varepsilon}$, for $q\in\mathbb{N}^*$.*

Unfortunately, asymptotic bounds are not really suited for establishing witness theorems, because such theorems do not accommodate exceptions, even if finite in number. Nevertheless, they contribute to the likeliness of witness conjectures. Another, very general, probabilistic and asymptotic result is the following [Khi61]:

Theorem 4.2. *Let ψ be a positive function, such that $\sum_{q=1}^{\infty}\psi(q)$ converges. Then for almost all numbers x (for the Lebesgue measure), the equation $\|q\,x\|<\psi(x)$ admits only a finite number of solutions.*

We refer to [Lan71] for a more detailed survey on diophantine approximation and in particular on the diophantine approximation of transcendental constants like e, logarithms and exponentials of algebraic numbers and so on. Unfortunately, the scope of the actual theory is very limited from our point of view, since it lacks effectiveness and no general results exist for, say, the exp-log constants.

4.2 Differential diophantine approximation

In the light of witness conjectures, there is no good reason to restrict oneself to the approximation of transcendental constants by rational or algebraic numbers. On the contrary, we might consider the approximation by more general constants, like exp-log constants or differentially algebraic constants. Equivalently, given complex numbers $z_1,\ldots,z_k$ and a class of multivariate analytic functions $\mathcal{F}$, one might be interested in lower bounds for $|f(z_1,\ldots,z_k)|$ as a function of the size of an expression which represents $f\in\mathcal{F}$.

Several classical questions in diophantine approximations have natural analogues. For instance, is there an analogue of theorem 4.2? We expect this to be so, since we will usually only consider countable sets of constants. Similarly, one may search for analogues of asymptotic results like theorem 4.1. It would also be interesting to have effective analogues for continued fraction expansions. By preference, such expansions should have more structure than the successive approximations found by, say, the LLL-algorithm [LLL82].

Finally, it is worth it to investigate the power series counterpart of differential diophantine approximation. In this context, there is a need for transfer principles back to the numeric setting. Of course, such transfer principles would also be useful for proving witness conjectures or designing zero-tests for constants. In the case of zero-tests, one might for instance wonder how to represent a constant which is suspected to be zero by the value of a function which can be proved to vanish globally.

5 Applications that rely on witness conjectures

The main application of witness conjectures is zero-testing. However, it is not recommended to directly apply the witness conjectures in all circumstances. For instance, if we want to test whether the expression (1.2) from the introduction vanishes, then conjecture 2.1 would give a very bad bound for the number of digits that we need to evaluate. Nevertheless, using asymptotic expansion techniques, it is easy to detect that (1.2) does not vanish.

In this section, we briefly discuss two zero-test algorithms which only indirectly rely on witness conjectures. In both cases, the witness conjectures enable us to obtain reasonable complexity bounds for such zero-tests, something which is impossible for algorithms that rely on structure theorems [Ric94].

We should also mention that it is not necessary to wait for proofs of the witness conjecture in order to base zero-test algorithms on them. Indeed, since most general purpose zero-tests implemented so far are either based on non reliable heuristic or are limited to relatively small classes of constants, we think that the mere statement of a precise conjecture already forms a progress, since such a conjecture can be used as a reliable and efficient heuristic.

5.1 Linear combinations of exponentials

In [vdH01], we considered linear combinations of the form

$$c_1 e^{z_1} + \cdots + c_r e^{z_r}, \tag{5.1}$$

where $c_1, \ldots, c_r, z_1, \ldots, z_r$ are "holonomic constants". Such expressions naturally occur when computing with solutions to linear differential equations near singularities. We proved a theorem, which implies the following one for "sufficiently regular" witness functions ϖ:

Theorem 5.1. *Assume conjecture 2.3. Then we may test whether* (5.1) *vanishes in a time bounded by*

$$(\sigma \log^3 \sigma \log \log \sigma) \circ (C\, r\, \varpi(\sigma))^{\circ r}$$

for some constant $C > 0$, and where $c_1, \ldots, c_r, z_1, \ldots, z_r$ can be represented by expressions of size $\leqslant \sigma$.

The following points should be noticed about this result:

- The left composition with $\sigma \log^3 \sigma \log \log \sigma$ is due to the cost of the evaluation of (5.1) up to $(C\, r\, \varpi(\sigma))^{\circ r}$ digits. If the class of holonomic constants is replaced by a larger one, such as $\mathcal{D}_\lambda$, then one should rather compose on the left by $\sigma^2 \log^2 \sigma \log \log \sigma$.

- There is a big difference between strong and weak witness conjectures as to the behavior of the r-th iterate of $C\, r\, \varpi(\sigma)$. Indeed, if $C\, r\, \varpi(\sigma)$ has exponentiality zero in σ, then so has its r-th iterate (see [vdH97] for a definition of exponentiality; examples of such functions are $\varpi(\sigma) = K \sigma$, $\varpi(\sigma) = \sigma^K$ or $\varpi(\sigma) = e^{\log^K \sigma}$). Moreover, the growth of $(C\, r\, \varpi(\sigma))^{\circ r}$ in r is bounded by an iterated exponential in this case.

  On the other hand, as soon as ϖ has exponentiality > 0, the r-th iterate of $C\, r\, \varpi(\sigma)$ has an extremely bad behavior for large r, since it is not longer bounded by any iterated exponential. It is therefore of the *greatest practical interest* to prove witness conjectures for witness functions of exponentiality 0; unfortunately, even in the power series setting, the existing techniques do not allow us to do so.

5.2 Exp-log constants

In [vdH95] we described the first efficient zero-test for real exp-log constants. At the time, we were not able to give any complexity bound for our algorithm, and this was one of our main motivation for the statement of witness conjectures.

Using the more powerful asymptotic expansion algorithms from [vdH97], which rely on Cartesian representations, and the more powerful zero-tests for multivariate exp-log series from [SvdH01], we also designed a more efficient zero-test for real exp-log constants in collaboration with J. Shackell. This algorithm, which will be detailed in a forthcoming paper, is expected to satisfy a similar complexity bound as in theorem 5.1 in the sense that it again involves an iterate of the witness function ϖ.

Bibliography

[Ax71] J. Ax. On Schanuel's conjecture. *Ann. of Math.*, 93:252–268, 1971.

[BB92] J.M. Borwein and P.B. Borwein. Strange series and high precision fraud. *Mathematical Monthly*, 99:622–640, 1992.

[É92] J. Écalle. *Introduction aux fonctions analysables et preuve constructive de la conjecture de Dulac*. Hermann, collection: Actualités mathématiques, 1992.

[Khi61] A. Ya. Khinchin. *Continued fractions*. Fizmatgiz, Moscow, 1961. English transl., Univ. of Chicago Press, Chicago, Ill., 1964, MR 28 #5037.

[Kho91] A. G. Khovanskii. *Fewnomials*. American Mathematical Society, Providence, RI, 1991.

[Lan71] S. Lang. Transcendental numbers and diophantine approximation. *Bull. Amer. Math. Soc.*, 77/5:635–677, 1971.

[LLL82] A.K. Lenstra, H.W. Lenstra, and L. Lovász. Factoring polynomials with rational coefficients. *Math. Ann.*, 261:515–534, 1982.

[Ric94] D. Richardson. How to recognise zero. *J. Symbol. Comput.*, 24(6):627–646, 1994.

[Ric01] D. Richardson. The uniformity conjecture. In *Lecture Notes in Computer Science*, volume 2064, pages 253–272. Springer Verlag, 2001.

[Ris75] R.H. Risch. Algebraic properties of elementary functions in analysis. *Amer. Journ. of Math.*, 4(101):743–759, 1975.

[Rot55] K. Roth. Rational approximations to algebraic numbers. *Mathematika*, 2:1–20, 1955. Corrigendum, 168, MR 17, 242.

[Sch36] T. Schneider. Über die approximation algebraischer zahlen. *J. Reine Angew. Math.*, 175:110–128, 1936.

[Sha89] J.R. Shackell. A differential-equations approach to functional equivalence. In G. Gonnet, editor, *ISSAC '89 Proceedings*, pages 7–10, Portland, Oregon, 1989. A.C.M. Press.

[SSC85] M.F. Singer, B.D. Saunders, and B.F. Caviness. An extension of Liouville's theorem on integration in finite terms. *SIAM J. Comp.*, 14:966–990, 1985.

[SvdH01] J.R. Shackell and J. van der Hoeven. Complexity bounds for zero-test algorithms. Technical Report 2001-63, Prépublications d'Orsay, 2001.

[vdH95] J. van der Hoeven. Automatic numerical expansions. In J.-C. Bajard, D. Michelucci, J.-M. Moreau, and J.-M. Müller, editors, *Proc. of the conference "Real numbers and computers", Saint-Étienne, France*, pages 261–274, 1995.

[vdH97] J. van der Hoeven. *Asymptotique automatique*. PhD thesis, École Polytechnique, Laboratoire d'Informatique, École Polytechnique, Paris, France, 1997.

[vdH01] J. van der Hoeven. Fast evaluation of holonomic functions near and in singularities. *JSC*, 31:717–743, 2001.