Counterexamples to Witness Conjectures

Joris van der Hoeven

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

Abstract

Consider the class of exp-log constants, which is constructed from the integers using the field operations, exponentiation and logarithm. Let z be such an exp-log constant and let n be its size as an expression. Witness conjectures attempt to give bounds $\varpi(n)$ for the number of decimal digits which need to be evaluated in order to test whether z equals zero. For this purpose, it is convenient to assume that exponentials are only applied to arguments with absolute values bounded by 1. In that context, several witness conjectures have appeared in the literature and the strongest one states that it is possible to choose $\varpi(n) = O(n)$. In this paper we give a counterexample to this conjecture. We also extend it so as to cover similar, polynomial witness conjectures.

1. Introduction

Consider the class of exp-log constant expressions, which is constructed from the integers using the field operations, exponentiation and logarithm. An important problem in computer algebra is to test whether an exp-log constant expression c represents zero. A straightforward approach is to evaluate c up to a certain number of decimal digits and test whether this evaluation vanishes. Witness conjectures attempt to give bounds $\varpi(n)$ for the number of decimal digits which are necessary as a function of the size n of the expression c.

Of course, exponentials can be used in order to produce massive cancellations, like in

$$\mathrm{e}^{\mathrm{e}^{\mathrm{e}^{10}}+\mathrm{e}^{-\mathrm{e}^{\mathrm{e}^{10}}}} - \mathrm{e}^{\mathrm{e}^{\mathrm{e}^{10}}} - 1 \approx 0.$$

[⋆] The paper was originally written using GNU TeXmacs (see `www.texmacs.org`). Unfortunately, Elsevier insists on the use of LaTeX with its own style files. Any insufficiencies in the typesetting quality should therefore be imputed to Elsevier.

Email address: `vdhoeven@texmacs.org` (Joris van der Hoeven).

Preprint submitted to Elsevier Science *17 April 2006*

For this reason, it is appropriate to allow only for exp-log expressions such that $|s| \leqslant 1$ for all subexpressions of the form e^s. In that context, several witness conjectures appeared in the literature [van der Hoeven (1997, 2001a,b); Richardson (2001)], and the strongest one states that we may take $\varpi(n) = O(n)$.

In this paper we give a counterexample to this strong witness conjecture. The counterexample is based on the observation that it suffices to find a counterexample for the power series analogue of the problem [van der Hoeven (2001b)] and a suggestion made by D. Richardson. In Section 4, we will generalize our technique and give counterexamples to all witness conjectures with $\varpi(n) = n^{O(1)}$. However, for this generalization, we need to extend the notion of exp-log constants so as to include algebraic numbers.

In what follows, we will freely use Hardy's notations $\varphi \prec \psi$ for $\varphi = o(\psi)$ and $\varphi \preccurlyeq \psi$ for $\varphi = O(\psi)$. We also write $\varphi \asymp \psi$ if $\varphi \preccurlyeq \psi \preccurlyeq \varphi$ and $\varphi \sim \psi$ if $\varphi - \psi \prec \varphi$. Finally, given a field $\mathbb{K}$, we denote $\mathbb{K}^{\neq} = \mathbb{K} \setminus \{0\}$.

2. Notations

Let $\mathcal{E}$ be the set of admissible constant expressions built up from $\mathbb{Z}, +, -, \times, /, \exp$ and log. Here a constant is said to be admissible if it evaluates to a real number. Given $c \in \mathcal{E}$, we denote by $\sigma(c) \in \mathbb{N}$ its size (the number of inner nodes in the corresponding expression tree plus the number of digits which are needed to write the integers at the leaves) and by $\bar{c} \in \mathbb{R}$ its evaluation. We denote by $\mathcal{C} \subseteq \mathcal{E}$ the subset of all expressions c, such that $|\bar{s}| \leqslant 1$ for all subexpressions of the form e^s.

Consider the ring $\mathcal{R} = \mathbb{Q}[[z]]$ of formal power series. A series $f = f_0 + f_1 z + \cdots \in \mathcal{R}$ is said to be *infinitesimal* if $f_0 = 0$. If $f \neq 0$, then its *valuation* is the smallest number $v(f) \in \mathbb{N}$ with $f_{v(f)} \neq 0$. Let $\mathcal{S}$ be the set of series expressions built up from z, elements in $\mathbb{Q}$, the ring operations and left composition of expressions which represent infinitesimal series by one of the series

$$
\begin{aligned}
I &= z/(1-z)\\
L &= \log(1+z)\\
E &= \exp(z) - 1
\end{aligned}
$$

Given such an expression $f \in \mathcal{S}$, we denote by $\sigma(f) \in \mathbb{N}$ its size (the number of nodes of the corresponding expression tree) and by $\bar{f} \in \mathcal{R}$ the represented series. We also denote by $\#_z f$ the number of occurrences of z in f and by $v(\bar{f})$ the valuation of $\bar{f}$.

Given $f \in \mathcal{S}$ and $g \in \mathcal{S}$ with $v(\bar{g}) > 0$, the substitution of g for z in f yields another series expression $f \circ g$ in $\mathcal{S}$ and we have

$$
\begin{aligned}
\sigma(f \circ g) &= \sigma(f) + (\#_z f)(\sigma(g) - 1)\ ; &(1)\\
v(\overline{f \circ g}) &= v(\bar{f}) v(\bar{g}). &(2)
\end{aligned}
$$

Similarly, given $f \in \mathcal{S}$ and $c \in \mathcal{C}$, such that $|\bar{c}|$ is sufficiently small, the substitution of c for z in f yields a constant expression $f(c) \in \mathcal{C}$ of size

$$
\sigma(f(c)) = \tilde{\sigma}(f) + (\#_z f)(\sigma(c) - 1), \qquad (3)
$$

where $\tilde{\sigma}(f)$ is the number of inner nodes of f plus the sizes of the rational numbers on the leaves. For $\bar{c} \to 0$, we also have

$$\log|\overline{f(c)}| \sim v(\bar{f}) \log|\bar{c}|.$$

Proposition 1 *Given $f \in \mathcal{S}$ with $v(\bar{f}) > 0$ and $k \in \mathbb{N}$, we have*

$$\sigma(f^{\circ k}) = (\sigma(f) - \#_z f)\frac{(\#_z f)^k - 1}{\#_z f - 1} + (\#_z f)^k \; ; \tag{4}$$

$$v(\overline{f^{\circ k}}) = v(\bar{f})^k. \tag{5}$$

If $c \in \mathcal{C}$ is such that $|\bar{c}|$ is sufficiently small, then we also have

$$\sigma(f^{\circ k}(c)) = (\tilde{\sigma}(f) - \#_z f)\frac{(\#_z f)^k - 1}{\#_z f - 1} + (\#_z f)^k \sigma(c). \tag{6}$$

Proof This follows from (1), (2) and (3) by a straightforward induction. □

3. The strong witness conjecture

Consider

$$\Phi = 2\log(1 - \log(1 - z/2)) - z \in \mathcal{S}.$$

We have $\sigma(\Phi) = 11$, $\#_z \Phi = 2$ and $v(\bar{\Phi}) = 3$, since

$$\bar{\Phi} = \frac{1}{24} z^3 + O(z^4).$$

Theorem 1 *Let ϖ be a witness function with $\varpi(n) = O(n^\alpha)$ and $\alpha < \log 3/\log 2$. Then there exists an expression $\Omega \in \mathcal{S}$ of size n with $\bar{\Omega} \neq 0$ and $v(\bar{\Omega}) \geqslant \varpi(n)$.*

Proof By Proposition 1, we have $n := \sigma(\Phi^{\circ k}) = 10 \cdot 2^k - 9 \asymp 2^k$ and $v(\overline{\Phi^{\circ k}}) = 3^k$. It therefore suffices to take $\Omega = \Phi^{\circ k}$ for a sufficiently large k. □

Theorem 2 *Let ϖ be a witness function with $\varpi(n) = O(n^\alpha)$ and $\alpha < \log 3/\log 2$. Then there exists a constant expression $c \in \mathcal{C}$ of size n with $\bar{c} \neq 0$ and $|\bar{c}| \leqslant \mathrm{e}^{-\varpi(n)}$.*

Proof On the interval $[0, \frac{1}{2}]$, we notice that $\bar{\Phi}$ satisfies $0 \leqslant \bar{\Phi}(c) \leqslant c^3$. Hence, $|\overline{\Phi^{\circ k}(\frac{1}{2})}| \leqslant 2^{-3^k}$ for all k. By Proposition 1, we also have $n := \sigma(\Phi^{\circ k}(\frac{1}{2})) \asymp 2^k$ for large k. Therefore, it suffices to take $c = \Phi^{\circ k}(\frac{1}{2})$ for a sufficiently large k. □

4. Polynomial witness conjectures

Let $\hat{\mathcal{E}}$, $\hat{\mathcal{C}}$ and $\hat{\mathcal{S}}$ be the analogues of $\mathcal{E}$, $\mathcal{C}$ and $\mathcal{S}$, if we replace $\mathbb{Z}$ and $\mathbb{Q}$ by the set of algebraic numbers $\hat{\mathbb{Q}}$ in their respective definitions. The size of an algebraic number c is defined to be the minimal size of a polynomial equation satisfied by c. After choosing a suitable determination of log, the evaluations of constants in $\hat{\mathcal{E}}$ are complex numbers. The analogues of all observations in Section 2 remain valid.

Given $l > 2$ and $\boldsymbol{a} = (a_0, \ldots, a_l) \in (\hat{\mathbb{Q}}^{\neq})^{l+1}$, we denote

$$\Psi_{\boldsymbol{a}} = (a_0 z) \circ \log(1+z) \circ (a_1 z) \circ \cdots \circ (a_{l-1} z) \circ \log(1+z) \circ (a_l z) \in \hat{\mathcal{S}}.$$

Lemma 1 *Given $\boldsymbol{a}, \boldsymbol{b} \in (\hat{\mathbb{Q}}^{\neq})^{l+1}$ with $\boldsymbol{b} \neq \boldsymbol{a}$, we have $\Psi_{\boldsymbol{b}} \neq \Psi_{\boldsymbol{a}}$.*

Proof Let i be maximal such that $b_i \neq a_i$. Modulo postcomposition of both sides of the equation $\Psi_{\boldsymbol{b}} = \Psi_{\boldsymbol{a}}$ with

$$\log(1+z) \circ (a_{i+1} z) \circ \cdots \circ \log(1+z) \circ (a_l z)]^{\circ -1},$$

we may assume without loss of generality that $i = l$. Then $\Psi_{\boldsymbol{b}}$ admits a singularity above $z = -b_l^{-1}$, near to which $\Psi_{\boldsymbol{b}} \asymp \log^{\circ l}(z + b_l^{-1})$. On the other hand, the number of nested logarithms in the logarithmic transseries expansion of $\Psi_{\boldsymbol{a}}$ near any point above $z = -b_l^{-1}$ cannot exceed $l-1$. Therefore, we must have $\Psi_{\boldsymbol{b}} \neq \Psi_{\boldsymbol{a}}$. □

Lemma 2 *There exist $\boldsymbol{a}, \boldsymbol{b} \in (\hat{\mathbb{Q}}^{\neq})^{l+1}$ with $\Phi = \Psi_{\boldsymbol{b}} - \Psi_{\boldsymbol{a}} \neq 0$ and $v(\Phi) \geqslant l$.*

Proof The mapping ξ from $(\hat{\mathbb{Q}}^{\neq})^{l+1}$ into $\hat{\mathbb{Q}}^l$, which maps $\boldsymbol{a}$ to the first l Taylor coefficients of $\Psi_{\boldsymbol{a}}$, is polynomial. Since $\dim(\hat{\mathbb{Q}}^{\neq})^{l+1} > \dim \hat{\mathbb{Q}}^l$, this mapping cannot be injective. We conclude by the previous Lemma. □

Theorem 3 *Let ϖ be a witness function with*

$$\varpi(n) = O(n^{\alpha \log n})$$
$$\alpha < \frac{2\log 2 - \log^3 2}{4}$$

Then there exists an expression $\Omega \in \hat{\mathcal{S}}$ of size n with $\bar{\Omega} \neq 0$ and $v(\bar{\Omega}) \geqslant \varpi(n)$.

Proof With Φ as in Lemma 2, consider $\Omega = \Phi^{\circ k}$ for large $l \in \mathbb{N}$ and

$$k = \left\lceil \frac{\log 2}{2 - \log^2 2} \log l \right\rceil.$$

Since $\sigma(\Phi) = 6l + 7$, $v(\bar{\Phi}) \geqslant l$ and $\#_z \Phi = 2$, Proposition 1 implies

$$n := \sigma(\Omega) = (6l+9)(2^k - 1) + 2^k \asymp l 2^k \asymp l^{\frac{2}{2-\log^2 2}} \tag{7}$$

and

$$v(\bar{\Omega}) \geqslant l^k = \mathrm{e}^{\frac{\log 2}{2-\log 2}\log^2 l + O(\log l)}. \tag{8}$$

From (7) it follows that

$$\log n = \frac{2}{2 - \log^2 2} \log l + O(1).$$

Plugging this into (8), we obtain

$$v(\bar{\Omega}) \geqslant \mathrm{e}^{\alpha \log^2 n + O(\log n)},$$

which clearly implies the Theorem, by choosing l large enough. □

Theorem 4 *Let ϖ be a witness function with $\varpi(n) = O(n^\alpha)$ and $\alpha \in \mathbb{R}^>$. Then there exists an expression $c \in \hat{\mathcal{C}}$ of size n with $\bar{c} \neq 0$ and $|\bar{c}| \leqslant \mathrm{e}^{-\varpi(n)}$.*

Proof With Φ as in Lemma 2, choose l such that $\log l / \log 2 > \alpha$. Then for $r \in \mathbb{Q}^> \cap [0, \frac{1}{2}]$ sufficiently small, the closed disk $B_r = \{z \in \mathbb{C} : |z| \leqslant r\}$ is mapped into itself and $|\bar{\Phi}(z)| \leqslant z^l$ for $z \in B_r$. Now Proposition 1 implies $n := \sigma(\Phi^{\circ k}(r)) \asymp 2^k$ and $|\overline{\Phi^{\circ k}(r)}| \leqslant r^{l^k}$ for large k. Therefore, $c = \Phi^{\circ k}(r)$ yields the desired counterexample for a sufficiently large k. □

5. Algebraic counterexamples

The technique from the previous Section may also be used in order to produce algebraic counterexamples. Indeed, given $l > 0$ and $\boldsymbol{a} = (a_0, \ldots, a_l) \in (\hat{\mathbb{Q}}^{\neq})^{l+1}$, let

$$\Psi_{\boldsymbol{a}} = (a_0 z) \circ \sqrt{1+z} \circ (a_1 z) \circ \cdots \circ (a_{l-1} z) \circ \sqrt{1+z} \circ (a_l z)$$

Then we have the following analogue of Lemma 1:

Lemma 3 *Given $\boldsymbol{a}, \boldsymbol{b} \in (\hat{\mathbb{Q}}^{\neq})^{l+1}$ with $\boldsymbol{b} \neq \boldsymbol{a}$, we have $\Psi_{\boldsymbol{b}} \neq \Psi_{\boldsymbol{a}}$.*

Proof Consider the Riemann surface of $\Psi_{\boldsymbol{a}}$ admits an algebraic singularity at

$$z = z_l = -\frac{1}{a_l}$$

of degree 2. On one of the two leaves, we again have an algebraic singularity at

$$z = z_{l-1} = -\frac{1}{a_l} + \frac{1}{a_l a_{l-1}^2}$$

of degree 2, and so on for the $z_{l-2}, \ldots, z_1$ given by

$$z_i = \left(\frac{z}{a_l} \circ (z^2 - 1) \circ \frac{z}{a_{l-1}} \circ \cdots \circ \frac{z}{a_{i+1}} \circ (z^2 - 1) \circ \frac{z}{a_i} \right) (-1).$$

We conclude by the observation that the mapping $(a_1, \ldots, a_l) \mapsto (z_1, \ldots, z_l)$ is injective. □

6. Conclusion

We have given counterexamples to the most optimistic kind of witness conjectures. In the power series context, we previously proved a witness conjecture for a doubly exponential witness function ϖ [Shackell and van der Hoeven (2001)]. Hopefully, this technique may be extended in order to yield Khovanskii-like bounds $\varpi(n) = \mathrm{e}^{O(n^2)}$ [Khovanskii (1991)]. If this turns out to be possible indeed, the next challenge would be to study what happens for growth rates between $\mathrm{e}^{O(\log^2 n)}$ and $\mathrm{e}^{O(n^2)}$. In particular, it would be very useful for practical applications if the witness conjecture would hold for a witness function of exponentiality 0 (i.e., $\log^{\circ k} \circ \varpi \circ \exp^{\circ k} \sim \mathrm{Id}$ for sufficiently large k).

It might also be interesting to further investigate the proof technique used in this paper. For instance, can we do without algebraic numbers? Would it be possible to replace Φ by $\Psi_{\boldsymbol{a}} - z$ in Lemma 2? Can we make Theorem 4 as strong as Theorem 3? Does there exist an approximation theory for power series by expressions of the form $\Psi_{\boldsymbol{a}}$ (analogous to Padé approximation)?

References

Borwein, J., Borwein, P., 1992. Strange series and high precision fraud. American Mathematical Monthly 99, 622–640.

Khovanskii, A., 1991. Fewnomials. Vol. 88 of Translations of Mathematical Monographs. A.M.S., Providence RI.

Richardson, D., 1997. How to recognise zero. JSC 24, 627–645.

Richardson, D., 2001. The uniformity conjecture. In: Lecture Notes in Computer Science. Vol. 2064. Springer Verlag, pp. 253–272.

Richardson, D., Elsonbaty, A., 2006. Counterexamples to the uniformity conjecture. Computational Geometry, theory and applications 33, 58–64.

Richardson, D., Langley, S., July 2002. Some observations on familiar numbers. In: Mora, T. (Ed.), Proc. ISSAC '02. Lille, France, pp. 214–220.

Shackell, J., van der Hoeven, J., 2001. Complexity bounds for zero-test algorithms. Tech. Rep. 2001-63, Prépublications d'Orsay, accepted for publication in JSC.

van der Hoeven, J., 1997. Automatic asymptotics. Ph.D. thesis, École polytechnique, France.

van der Hoeven, J., 2001a. Fast evaluation of holonomic functions near and in singularities. JSC 31, 717–743.

van der Hoeven, J., 2001b. Zero-testing, witness conjectures and differential diophantine approximation. Tech. Rep. 2001-62, Prépublications d'Orsay.