Towards Automatic Proofs of Inequalities Involving Elementary Functions

Behzad Akbarpour and Lawrence C. Paulson

Computer Laboratory, University of Cambridge

Abstract

Inequalities involving functions such as sines, exponentials and logarithms lie outside the scope of decision procedures, and can only be solved using heuristic methods. Preliminary investigations suggest that many such problems can be solved by reduction to algebraic inequalities, which can then be decided by a decision procedure for the theory of real closed fields (RCF). The reduction involves replacing each occurrence of a function by a lower or upper bound (as appropriate) typically derived from a power series expansion. Typically this requires splitting the domain of the function being replaced, since most bounds are only valid for specific intervals.

1 Introduction

Decision procedures are valuable, but too many problems lie outside of their scope. Linear arithmetic restricts us to the language of $=$, $<$, $\leq$, $+$ and multiplication by integer constants, combined by Boolean connectives. In their formalization of the Prime Number Theorem [2], Avigad and his colleagues spent much time proving simple facts involving logarithms. We would like to be able to prove inequalities involving any of the so-called elementary functions: sine, cosine, arctangent, logarithm and exponential. Richardson's theorem tells us that this problem is undecidable [11], so we are left with heuristic methods.

In this paper, we outline preliminary work towards such heuristics. We have no implementation nor even a definite procedure, but we do have methods that we have tested by hand on about 30 problems. Our starting point is that the theory of real closed fields—that is, the real numbers with addition and multiplication—is decidable. Our idea is to replace each occurrence of an elementary function by an algebraic expression that is known to be an upper or lower bound, as appropriate. If this results in a purely algebraic inequality, then we supply the problem to a decision procedure for the theory of real closed fields.

Complications include the need for case analysis on the arguments of elementary functions, since many bounds are only valid over restricted intervals. If these arguments are complex expressions, then identifying their range requires something like a recursive application of the method. The resulting algebraic inequalities may be too difficult to be solved efficiently. Even so, the method works on many problems.

Paper outline. We begin by reviewing the basis of our work, namely existing decision procedures for polynomials and prior work on verifying inequalities involving the elementary functions (Sect. 2). To illustrate the idea, we present a simple example involving the exponential function (Sect. 3) and then a more complex example involving the logarithm function (Sect. 4). We conclude by presenting a list of solved problems and outlining our next steps (Sect. 5).

2 Background

Our work relies on the existence of practical, if not always efficient, decision procedures for the theory of real closed fields (RCF). According to Dolzmann et al. [3], Tarski found the first quantifier elimination procedure in the 1930s, while Collins introduced the first feasible method in 1975. His *cylindrical algebraic decomposition* is still doubly exponential in the worst case. Dolzmann et al. proceed to survey several quantifier elimination algorithms and their applications. One freely-available implementation is QEPCAD [5], a decision procedure that performs partial cylindrical algebraic decomposition. The prover HOL Light provides a simpler quantifier elimination procedure for real closed fields [8]. Also in HOL Light is an implementation of Parrilo's method [10] for deciding polynomials using sum-of-squares decompositions; less general than any quantifier elimination procedure, it is dramatically more efficient.[1] Some polynomial inequalities can also be tackled using heuristic procedures such as those of Hunt et al. [6] and Tiwari [12].

Our second starting point is the work of Mũnoz and Lester [9], on proving real number inequalities that may contain the elementary functions, but no variables. The example they give is

$$\frac{3\pi}{180} \le \frac{g}{v}\tan\left(\frac{35\pi}{180}\right),$$

where g and v are constants. Their method for proving such ground inequalities relies on upper and lower bounds for the elementary functions, coupled with interval arithmetic. The absence of variables makes the problem much simpler; in particular, if we need to establish the range of the argument x in $\tan(x)$, we simply call the procedure recursively.

These methods might be expected to work for some problems containing variables. Interval arithmetic should be able to prove some inequalities involving a variable x say, if we know that $0 \le x \le 1$. However, the method fails on some easy-looking problems; as Mũnoz and Lester note, interval arithmetic can

[1] Harrison has mentioned this implementation [4], but as yet no documentation exists.

lose information rapidly. For example, if $x \in [0,1]$, interval arithmetic cannot prove the trivial $x - x \geq 0$: we get $[0,1] - [0,1] = [0,1] + [-1,0] = [-1,1]$, and neither $[-1,1] \leq 0$ nor $[-1,1] \geq 0$ hold. This is a well-known issue and there are some techniques that can reduce its impact, such as (obviously) reducing $x - x$ to 0 before applying interval arithmetic. But, in some cases, when we wanted to prove $E \leq 0$, the best we could do with interval arithmetic was to prove that $E \leq \epsilon$ for an arbitrary small, but positive, ϵ. A method based on a decision procedure for real closed fields ought to be more general and effective.

3 A Simple Example Concerning Exponentials

Figure 1 presents a family of upper and lower bounds for the exponential function. Mũnoz and Lester [9] give similar bounds, but we have corrected errors in the first two and altered the presentation. All conventions are as in the original paper. The lower bound is written $\underline{\exp}(x,n)$ and the upper bound is written $\overline{\exp}(x,n)$, where n is a non-negative integer. For all x and n, they satisfy

$$\underline{\exp}(x,n) \leq e^x \leq \overline{\exp}(x,n).$$

As n increases, the bounds converge monotonically to the target function, here exp. As n increases, the bounds get tighter and the RCF problems that must be decided get harder; in return, we should be able to prove harder inequalities involving exponentials.

Case analysis on the value of x in $\exp(x)$ cannot be avoided. Clearly no polynomial could serve as an upper bound, or as an accurate lower bound, of the exponential function. The role of m in these bounds is to segment the real line into integers, with separate bounds in each segment. These case analyses will complicate our proofs. In particular, unless the argument of the exponential function has a finite range, these bounds are useless, since they would require the examination of infinitely many cases.

For a simple demonstration of our idea, let us prove the theorem

$$0 \leq x \leq 1 \Longrightarrow e^x \leq 1 + x + x^2.$$

Here it suffices to replace the function e by an upper bound:

$$0 \leq x \leq 1 \Longrightarrow \overline{\exp}(x,n) \leq 1 + x + x^2.$$

We have a lower bound if $0 < x \leq 1$, so we need to perform a simple case analysis.

- If $x = 0$ then $\overline{\exp}(0,n) = 1 \leq 1 + 0 + 0^2 = 1$, trivially.

- If $0 < x \leq 1$, then by equations (5) and (1)

$$\overline{\exp}(x,n) = \left(\sum_{i=0}^{2(n+1)+1} \frac{(-x)^i}{i!} \right)^{-1}$$

$$\underline{\exp}(x,n) = \sum_{i=0}^{2(n+1)+1} \frac{x^i}{i!} \qquad \text{if } -1 \le x < 0 \tag{1}$$

$$\overline{\exp}(x,n) = \sum_{i=0}^{2(n+1)} \frac{x^i}{i!} \qquad \text{if } -1 \le x < 0 \tag{2}$$

$$\underline{\exp}(0,n) = \overline{\exp}(0,n) = 1 \tag{3}$$

$$\underline{\exp}(x,n) = \frac{1}{\overline{\exp}(-x,n)} \qquad \text{if } 0 < x \le 1 \tag{4}$$

$$\overline{\exp}(x,n) = \frac{1}{\underline{\exp}(-x,n)} \qquad \text{if } 0 < x \le 1 \tag{5}$$

$$\underline{\exp}(x,n) = \underline{\exp}(x/m,n)^m \quad \text{if } \ x < -1,\ m = -\lfloor x \rfloor \tag{6}$$

$$\overline{\exp}(x,n) = \overline{\exp}(x/m,n)^m \quad \text{if } \ x < -1,\ m = -\lfloor x \rfloor \tag{7}$$

$$\underline{\exp}(x,n) = \overline{\exp}(x/m,n)^m \quad \text{if } \ 1 < x,\ m = \lfloor -x \rfloor \tag{8}$$

$$\overline{\exp}(x,n) = \underline{\exp}(x/m,n)^m \quad \text{if } \ 1 < x,\ m = \lfloor -x \rfloor \tag{9}$$

Figure 1: Bounds for the Exponential Function

and putting $n = 0$, it suffices to prove

$$\left(1 + (-x) + \frac{(-x)^2}{2} + \frac{(-x)^3}{6}\right)^{-1} \le 1 + x + x^2.$$

This last inequality is non-trivial, but as it falls within RCF, it can be proved automatically. Existing tools require us first to eliminate the division, reducing the problem to the two inequalities

$$0 < 1 - x + \frac{x^2}{2} - \frac{x^3}{6} \quad \text{and} \quad 1 \le \left(1 + x + x^2\right)\left(1 - x + \frac{x^2}{2} - \frac{x^3}{6}\right).$$

HOL Light has two separate tools that can prove these. Sean McLaughlin's quantifier elimination package [8] can prove the pair of inequalities in 351 seconds, while John Harrison's implementation of the sum-of-squares method [10] needs only 0.48 seconds.[2]

Let us check these inequalities ourselves. The first one is clear, since $x^{k+1} \le x^k$ for all k. Multiplying out the second inequality reduces it to

$$0 \le \frac{x^2}{2} - \frac{2x^3}{3} + \frac{x^4}{3} - \frac{x^5}{6}.$$

[2] All timings were done on a dual 3GHz Pentium equipped with 4GB of memory.

Multiplying both sides by 6 and factoring reduces this inequality to

$$0 \le x^2(1-x)(3-x+x^2)$$

when it is obvious that all of the factors are non-negative.

This proof is not obvious, and its length shows that we have much to gain by automating the procedure. That involves performing the case analysis, substituting the appropriate bounds, calling an RCF decision procedure, and in case of failure, retrying with a larger value of n.

4 An Extended Example Concerning Logarithms

Figure 2 presents the bounds for the logarithm function. They are again taken from Mũnoz and Lester [9], while correcting several errata. The next example will demonstrate how a complicated derivation can arise from a simple-looking inequality:

$$-\frac{1}{2} < x \le 3 \Longrightarrow \ln(1+x) \le x.$$

We re-express the condition on x in terms of $1+x$, which is the argument of ln, when substituting in the lower bound:

$$\frac{1}{2} < 1+x \le 4 \Longrightarrow \overline{\ln}(1+x,n) \le x$$

As with the exponential function, to obtain reasonably tight bounds requires considering rather small intervals. Our problem splits into four cases:

$$\frac{1}{2} < 1+x < 1 \quad \text{or} \quad 1+x=1 \quad \text{or} \quad 1<1+x\le 2 \quad \text{or} \quad 2<1+x\le 4$$

Let us leave the first case for last, as it is the most complicated, and consider the other three cases.

If $1+x=1$, then $x=0$ and trivially $\overline{\ln}(1+x,n) = \overline{\ln}(1,n) = 0 \le x$.

If $1<1+x\le 2$, then

$$\overline{\ln}(1+x,n) = \sum_{i=1}^{2n+1}(-1)^{i+1}\frac{((1+x)-1)^i}{i} = \sum_{i=1}^{2n+1}(-1)^{i+1}\frac{x^i}{i}$$

by equation (11). Setting $n=0$ yields $\overline{\ln}(1+x,n)=x$ and reduces our inequality to the trivial $x\le x$.

If $2<1+x\le 4$, then we have to apply equation (16). That requires finding a positive integer m and some y such that $1+x=2^m y$ and $1<y\le 2$. Clearly $m=1$. In this case, putting $n=0$, we have

$$\begin{aligned}\sum_{i=1}^{2n+1}(-1)^{i+1}\frac{(2-1)^i}{i} + \sum_{i=1}^{2n+1}(-1)^{i+1}\frac{(y-1)^i}{i} &= 1+(y-1)\\ &= y\\ &\le 2y-1\\ &= x.\end{aligned}$$

$$\underline{\ln}(x,n) = \sum_{i=1}^{2n} (-1)^{i+1} \frac{(x-1)^i}{i} \qquad \text{if } 1 < x \leq 2 \tag{10}$$

$$\overline{\ln}(x,n) = \sum_{i=1}^{2n+1} (-1)^{i+1} \frac{(x-1)^i}{i} \qquad \text{if } 1 < x \leq 2 \tag{11}$$

$$\underline{\ln}(1,n) = \overline{\ln}(1,n) = 0 \tag{12}$$

$$\underline{\ln}(x,n) = -\,\overline{\ln}\left(\frac{1}{x},\, n\right), \qquad \text{if } 0 < x < 1 \tag{13}$$

$$\overline{\ln}(x,n) = -\,\underline{\ln}\left(\frac{1}{x},\, n\right), \qquad \text{if } 0 < x < 1 \tag{14}$$

$$\underline{\ln}(x,n) = m\,\underline{\ln}(2,n) \;+\; \underline{\ln}(y,n) \quad \text{if } x > 2,\, x = 2^m y,\, 1 < y \leq 2 \tag{15}$$

$$\overline{\ln}(x,n) = m\,\overline{\ln}(2,n) \;+\; \overline{\ln}(y,n) \quad \text{if } x > 2,\, x = 2^m y,\, 1 < y \leq 2 \tag{16}$$

Figure 2: Bounds for the Logarithm Function

Now, let us turn to that postponed first case. If $\frac{1}{2} < 1+x < 1$, then $1 < 1/(1+x) < 2$. Putting $n = 1$, we have

$$\begin{aligned}
\overline{\ln}(1+x,n) &= -\,\underline{\ln}\left(\frac{1}{1+x},\, n\right) \\
&= -\sum_{i=1}^{2n} (-1)^{i+1} \frac{(\frac{1}{1+x}-1)^i}{i} \\
&= \sum_{i=1}^{2n} \frac{(-1)^i}{i} \left(\frac{-x}{1+x}\right)^i \\
&= \left(\frac{x}{1+x}\right) + \left(\frac{1}{2}\right)\left(\frac{-x}{1+x}\right)^2.
\end{aligned}$$

Now

$$\begin{aligned}
\left(\frac{x}{1+x}\right) + \left(\frac{1}{2}\right)\left(\frac{-x}{1+x}\right)^2 \leq x &\iff \\
x(1+x) + \frac{1}{2}x^2 \leq x(1+x)^2 &\iff \\
x + \frac{3}{2}x^2 \leq x + 2x^2 + x^3 &\iff \\
-\frac{1}{2}x^2 \leq x^3 &\iff \\
-\frac{1}{2} \leq x &
\end{aligned}$$

which holds because $\frac{1}{2} < 1 + x$. Note that putting $n = 0$ would have required us to prove $0 \le x$, which fails.

This derivation reveals some limitations. We should have been able to prove this result with looser bounds on x, since $\ln(1 + x) \le x$ holds for $x > -1$. We could not do this because our upper bound, $\overline{\ln}(x, n)$, introduces the value m in equation (16). This formulation allows the upper bound to be tight, but for our purposes we need to seek looser bounds that have less restrictive range conditions.

The bounds for the exponential function have a similar problem. An alternative lower bound, valid for all $x \ge 0$, comes directly from its Taylor expansion:

$$\underline{\exp}(x, n) = \sum_{i=0}^{n} \frac{x^i}{i!}.$$

This series for the logarithm [1] also suggests a lower bound, for $x \ge 1$:

$$\underline{\ln}(x, n) = \sum_{i=1}^{n} \frac{(x-1)^i}{i x^i}.$$

Finding upper and lower bounds for elementary functions that work well with RCF decision procedures is one of our first tasks.

5 Conclusions

Our preliminary investigations are promising. We have used the method described above to solve the problems shown in Fig. 3. (Note that some of these split into several problems when the absolute value function is removed and chains of inequalities are separated.) We manually reduced each problem to algebraic form as described above, then tried to solve the reduced problems using three different tools.

- QEPCAD solved all of the problems, usually taking less than one second.
- HOL Light's sum-of-squares tool (`REAL_SOS`) solved all of the problems but two, again usually in less than a second.
- HOL Light's quantifier elimination tool (`REAL_QELIM_CONV`) solved all of the problems but three. It seldom required more than five seconds. The 351 seconds we reported above is clearly exceptional.

The simplest bound using $n = 0$ was sufficient for all but one of the problems, which required $n = 1$.

Much work remains to be done before this procedure can be automated. We need to experiment with a variety of upper and lower bounds. Case analyses will still be inevitable, so we need techniques to automate them in the most common situations. We need to tune the procedure by testing on a large suite of problems, and we have to evaluate different ways of deciding the RCF problems that are finally generated.

$$-\frac{1}{2} \leq x \leq 3 \Longrightarrow \frac{x}{1+x} \leq \ln(1+x) \leq x$$

$$-3 \leq x \leq \frac{1}{2} \Longrightarrow \frac{-x}{1-x} \leq \ln(1-x) \leq -x$$

$$0 \leq x \leq 3 \Longrightarrow |\ln(1+x) - x| \leq x^2$$

$$-3 \leq x \leq 0 \Longrightarrow |\ln(1-x) + x| \leq x^2$$

$$|x| \leq \frac{1}{2} \Longrightarrow |\ln(1+x) - x| \leq 2x^2$$

$$|x| \leq \frac{1}{2} \Longrightarrow |\ln(1-x) + x| \leq 2x^2$$

$$0 \leq x \leq 0.5828 \Longrightarrow |\ln(1-x)| \leq \frac{3x}{2}$$

$$-0.5828 \leq x \leq 0 \Longrightarrow |\ln(1+x)| \leq -\frac{3x}{2}$$

$$\frac{1}{2} \leq x \leq 4 \Longrightarrow \ln x \leq x - 1$$

$$0 \leq x \leq 1 \Longrightarrow e^{(x-x^2)} \leq 1 + x$$

$$-1 \leq x \leq 1 \Longrightarrow 1 + x \leq e^x$$

$$-1 \leq x \leq 1 \Longrightarrow 1 - x \leq e^{-x}$$

$$-1 \leq x \leq 1 \Longrightarrow e^x \leq \frac{1}{1-x}$$

$$-1 \leq x \leq 1 \Longrightarrow e^{-x} \leq \frac{1}{1+x}$$

$$x \leq \frac{1}{2} \Longrightarrow e^{-x/(1-x)} \leq 1 - x$$

$$-\frac{1}{2} \leq x \Longrightarrow e^{x/(1+x)} \leq 1 + x$$

$$0 \leq x \leq 1 \Longrightarrow e^{-x} \leq 1 - \frac{x}{2}$$

$$-1 \leq x \leq 0 \Longrightarrow e^x \leq 1 + \frac{x}{2}$$

$$0 \leq |x| \leq 1 \Longrightarrow \frac{1}{4}|x| \leq |e^x - 1| \leq \frac{7}{4}|x|$$

Figure 3: Problems Solved

Acknowledgements

The research was funded by the EPSRC grant EP/C013409/1, *Beyond Linear Arithmetic: Automatic Proof Procedures for the Reals.* R. W. Butler, D. Lester, J. Harrison and C. Muñoz answered many questions. A. Chaieb commented on this paper.

References

[1] M. Abramowitz and I. A. Stegun. *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables.* Wiley, 1972.

[2] J. Avigad, K. Donnelly, D. Gray, and P. Raff. A formally verified proof of the prime number theorem. *ACM Trans. Comput. Logic*, in press.

[3] A. Dolzmann, T. Sturm, and V. Weispfenning. Real quantifier elimination in practice. Technical Report MIP-9720, Universität Passau, D-94030, Germany, 1997.

[4] J. Harrison. A HOL theory of Euclidean space. In Hurd and Melham [7], pages 114–129.

[5] H. Hong. QEPCAD — quantifier elimination by partial cylindrical algebraic decomposition. On the Internet at `http://www.cs.usna.edu/~qepcad/B/QEPCAD.html`. Web site includes sources and documentation.

[6] W. A. Hunt, Jr., R. B. Krug, and J. Moore. Linear and nonlinear arithmetic in ACL2. In D. Geist and E. Tronci, editors, *Correct Hardware Design and Verification Methods (CHARME)*, LNCS 2860, pages 319–333, 2003.

[7] J. Hurd and T. Melham, editors. *Theorem Proving in Higher Order Logics: TPHOLs 2005*, LNCS 3603. Springer, 2005.

[8] S. McLaughlin and J. Harrison. A proof-producing decision procedure for real arithmetic. In R. Nieuwenhuis, editor, *Automated Deduction — CADE-20 International Conference*, LNAI 3632, pages 295–314. Springer, 2005.

[9] C. Muñoz and D. Lester. Real number calculations and theorem proving. In Hurd and Melham [7], pages 195–210.

[10] P. A. Parrilo. Semidefinite programming relaxations for semialgebraic problems. *Mathematical Programming*, 96(2):293–320, 2003.

[11] D. Richardson. Some undecidable problems involving elementary functions of a real variable. *Journal of Symbolic Logic*, 33(4):514–520, Dec. 1968.

[12] A. Tiwari. Abstraction based theorem proving: An example from the theory of reals. In C. Tinelli and S. Ranise, editors, *PDPAR: Workshop on Pragmatics of Decision Procedures in Automated Deduction*, pages 40–52. INRIA, Nancy, 2003.