OVERCOMING INTRACTABLE COMPLEXITY IN AN AUTOMATIC THEOREM PROVER FOR REAL-VALUED FUNCTIONS

PROF. LAWRENCE C. PAULSON

Real quantifier elimination, first established by Tarski [8] and later refined by Collins [2] and others, implies the decidability of first-order formulas involving the familiar arithmetic operations over the real numbers. Giving necessary and sufficient conditions for the existence of real roots of polynomials amounts to quantifier elimination. A classic example is the quadratic equation $ax^2 + bx + c = 0$, which has a real solution subject to surprisingly complicated conditions:

$$\exists x\, [ax^2 + bx + c = 0] \iff b^2 \geq 4ac \wedge (c = 0 \vee a \neq 0 \vee b^2 > 4ac).$$

We are accustomed to simply $b^2 \geq 4ac$ as a sufficient condition, but the full formula covers the degenerate cases $a = 0$ and $b = 0$. Even in this trivial example, eliminating a quantifier greatly increases the formula's Boolean complexity. Quantifier elimination is possible regardless of the degrees of the polynomials or the logical complexity of the formula. Given the tremendous power of this procedure, it is hardly surprising to learn that its complexity is intractable [4]: the length of the resulting quantifier-free formula can be doubly exponential in the number of quantified variables.

Researchers have made strenuous efforts to design efficient quantifier elimination procedures for well-behaved problem classes. Literature surveys include Dolzmann et al. [5] and Passmore [6]. The decision problem is called RCF, for "real-closed fields": fields that are elementarily equivalent to the field of real numbers.

Augmenting the language of polynomials with real-valued functions such as ln, exp, sin, cos, $\tan^{-1}$ obviously makes the decision problem even more difficult. Few decision procedures exist for such extended languages, regardless of complexity. This suggests the use of heuristic methods.

MetiTarski is an automatic theorem prover for first-order logic including polynomials and real-valued special functions. It solves problems in this extended language using a combination of resolution theorem proving and RCF decision procedures [1]. The key idea is to provide upper and lower bounds for each function of interest. Such bounds will typically be polynomials or rational functions obtained from power series or continued fraction expansions [3]. Inevitably, we need families of bounds, valid over various intervals, and trading accuracy against simplicity. Resolution uses these bounds (supplied as axioms) to reduce a problem involving special functions to problems involving rational functions, and ultimately to problems in RCF, which can then be solved by a decision procedure.

Despite the terrible complexity of real quantifier elimination, MetiTarski uses it as a subroutine. And in many cases, MetiTarski can prove difficult theorems in a couple of seconds. Here is an example:

$$\begin{aligned}&\forall\, t > 0, v > 0\\ &\qquad((1.565 + 0.313\, v)\, \cos(1.16\, t) + (.0134 + .00268\, v)\, \sin(1.16\, t))\, e^{-1.34\, t}\\ &\qquad\qquad - (6.55 + 1.31\, v)\, e^{-0.318\, t} + v \,\geq\, -10\end{aligned}$$

MetiTarski actually outputs a proof, not one that a mathematician would want to read, but a detailed formal deduction in the resolution calculus.

The complexity of real quantifier elimination imposes strict limits on the number of variables allowed in a problem. This is largely dependent on the choice of RCF decision procedure. Early work used only QEPCAD, and theorems in more than two variables could seldom be proved. More recently, we have incorporated Mathematica, and proved theorems with up to 5 variables. The latest work uses the decision procedure Z3, which now supports non-linear arithmetic. With the help of heuristics specialised to MetiTarski [7], theorems with up to 9 variables can be proved.

Acknowledgements. The developers of MetiTarski include Behzad Akbarpour, James Bridge and Grant Passmore. The research was supported by the Engineering and Physical Sciences Research Council [grant numbers EP/C013409/1, EP/I011005/1 and EP/I010335/1].

References

[1] Behzad Akbarpour and Lawrence Paulson. MetiTarski: An automatic theorem prover for real-valued special functions. *Journal of Automated Reasoning*, 44(3):175–205, March 2010.

[2] George E. Collins. Hauptvortrag: Quantifier elimination for real closed fields by cylindrical algebraic decomposition. In H. Barkhage, editor, *Automata Theory and Formal Languages*, volume 33 of *LNCS*, pages 134–183. Springer, 1975.

[3] A. Cuyt, V. Petersen, B. Verdonk, H. Waadeland, and W.B. Jones. *Handbook of Continued Fractions for Special Functions*. Springer, 2008.

[4] J. H. Davenport and J. Heintz. Real quantifier elimination is doubly exponential. *J. Symbolic Comp.*, 5:29–35, 1988.

[5] Andreas Dolzmann, Thomas Sturm, and Volker Weispfenning. Real quantifier elimination in practice. Technical Report MIP-9720, Universität Passau, D-94030, Germany, 1997.

[6] Grant Olney Passmore. *Combined Decision Procedures for Nonlinear Arithmetics, Real and Complex*. PhD thesis, University of Edinburgh, 2011.

[7] Grant Olney Passmore, Lawrence C. Paulson, and Leonardo de Moura. Real algebraic strategies for MetiTarski proofs. In Johan Jeuring, editor, *Conferences on Intelligent Computer Mathematics — CICM 2012*. Springer, 2012. In press.

[8] Alfred Tarski. A decision method for elementary algebra and geometry. Technical Report R-109, RAND Corporation, 1948.

Computer Laboratory, Univ. of Cambridge, England
E-mail address: lp15@cl.cam.ac.uk