Solving Non-Linear Arithmetic

Dejan Jovanović
New York University
New York, USA, 10012
dejan@nyu.edu

Leonardo de Moura
Microsoft Research
Redmond, USA, 98074
leonardo@microsoft.com

Abstract

We propose a new decision procedure for the existential theory of the reals. It performs a backtracking search for a model in $\mathbb{R}$, where the backtracking is powered by a novel conflict resolution procedure based on cylindrical algebraic decomposition. The initial experimental results are very encouraging. *The full article has been accepted at the 6th International Joint Conference on Automated Reasoning (IJCAR 2012).*

Summary. Solving polynomial constraints is one of the classic problems in computer algebra. In 1951, Tarski [8] showed that the theory of real closed fields admits elimination of quantifiers, and hence that a general decision procedure for solving polynomial constraints was indeed possible. Tarski's original procedure was unfortunately totally impractical but, as one would expect, it has consequently been much improved. Most notably, Collins [2] gave the first relatively effective method of quantifier elimination by cylindrical algebraic decomposition (CAD). The CAD procedure itself has gone through many revisions and improvements [5, 3, 1]. However, even with the improvements and various heuristics, its doubly-exponential worst-case behavior has remained as a serious impediment.

The CAD algorithm works by decomposing $\mathbb{R}^k$ into connected components such that, in each cell, all of the polynomials from the problem are sign-invariant. To be able to perform such a particular decomposition, CAD first performs a *projection* of the polynomials from the initial problem. This projection includes many new polynomials, derived from the initial ones, and these polynomials carry enough information to ensure that the decomposition is indeed possible. Unfortunately, the size of these projection sets grows exponentially in the number of variables, causing the projection phase, and its consequent impact on the search space, to be a key hurdle to CAD scalability.

We propose a new decision procedure for the existential theory of the reals that tries to alleviate the above problem. The new procedure performs a backtracking search for a model in $\mathbb{R}$, where the backtracking is powered by a novel conflict resolution procedure. Our approach takes advantage of the fact that each conflict encountered during the search is based on the current assignment and generally involves only a few constraints, a *conflicting core*. When in conflict, we project only the polynomials from the conflicting core and explain the conflict in terms of the current model. This means that we use projection conservatively, only for the subsets of polynomials that are involved in the conflict, and even then we reduce it further. As another advantage, the conflict resolution provides the usual benefits of a Conflict-Driven Clause Learning style [7] search engine, such as non-chronological backtracking and the ability to ignore irrelevant parts of the search space.

The website `http://cs.nyu.edu/~dejan/nonlinear/` contains a technical report, our prototype nlsat, and experimental results. The technical report contains a detailed description of our procedure, examples, additional references, and implementation details.

Table 1: Experimental results.

	meti-tarski (1006)		keymaera (421)		zankl (166)		hong (20)		kissing (45)		all (1658)	
solver	solved	time (s)	solved	time (s)	solved	time (s)	solved	time (s)	solved	time (s)	solved	time (s)
nlsat	1002	343.48	**420**	**5.73**	**89**	**234.57**	10	170.33	**13**	**95.62**	**1534**	**849.73**
Mathematica	**1006**	**796.90**	420	171.96	50	366.10	9	208.04	6	29.01	1491	1572.01
QEPCAD	991	2616.94	368	1331.67	21	38.85	6	43.56	4	5.80	1390	4036.82
Redlog-VTS	847	28640.26	419	78.58	42	490.54	6	3.31	10	275.44	1324	29488.13
Redlog-CAD	848	21706.75	363	730.25	21	173.15	6	2.53	4	0.81	1242	22613.49
iSAT	203	122.93	291	16.95	21	24.52	**20**	**822.01**	0	0.00	535	986.41

Experimental Results. In order to evaluate the new decision procedure we have implemented a new solver nlsat, the implementation being a clean translation of the decision procedure described in our technical report. We compare the new solver to the following solvers: Mathematica 8.0, QEPCAD 1.65, Redlog-CAD and Redlog-VTS; and the interval based iSAT. The nlsat main procedure and the polynomial and real algebraic number libraries were implemented from scratch in C++. We have reused parsers, simplifiers and basic data-structures from the z3 theorem prover [4]. The experimental results are summarized in Table 1.

The meti-tarski benchmarks are proof obligations extracted from the MetiTarski project, where the constraints are of high degree and the polynomials represent approximations of the elementary real functions being analyzed. The keymaera benchmark set contains verification conditions for hybrid systems. The zankl set of problems originating from attempts to prove termination of term-rewrite systems. We also have two crafted sets of benchmarks, the hong benchmarks, which are a parametrized generalization of the problem from [6], and the kissing problems that describe some classic kissing number problems, both sets containing instances of increasing dimensions.

References

[1] C. W. Brown. Improved projection for cylindrical algebraic decomposition. *Journal of Symbolic Computation*, 32(5):447–465, 2001.

[2] G. E. Collins. Quantifier elimination for real closed fields by cylindrical algebraic decomposition. In *Automata Theory and Formal Languages*, pages 134–183. Springer, 1975.

[3] G. E. Collins and H. Hong. Partial cylindrical algebraic decomposition for quantifier elimination. *Journal of Symbolic Computation*, 12(3):299–328, 1991.

[4] L. de Moura and N. Bjørner. Z3: An efficient SMT solver. *TACAS 2008*, pages 337–340, 2008.

[5] H. Hong. An improvement of the projection operator in cylindrical algebraic decomposition. In *Proceedings of the international symposium on Symbolic and algebraic computation*, pages 261–264. ACM, 1990.

[6] H. Hong. Comparison of several decision algorithms for the existential theory of the reals. 1991.

[7] J. P. M. Silva, I. Lynce, and S. Malik. Conflict-driven clause learning SAT solvers. In A. Biere, M. Heule, H. van Maaren, and T. Walsh, editors, *Handbook of Satisfiability*, volume 185 of *Frontiers in Artificial Intelligence and Applications*, pages 131–153. IOS Press, 2009.

[8] A. Tarski. A decision method for elementary algebra and geometry. Technical Report R-109, Rand Corporation, 1951.