Equality handling and efficiency improvement of SMT for non-linear constraints over reals

Vu Xuan Tung (1310007)

School of Information Science,
Japan Advanced Institute of Science and Technology

February 12, 2015

Keywords: Polynomial Constraints, Interval Arithemic, Testing, abstract DPLL.

Solving polynomial constraints is raised from many applications of Software Verification such as roundoff/overflow error analysis, automatic termination proving or loop invariant generation. Although in 1948, Tarski proved the decidability of polynomial constraints over real numbers, the current complete method named Quantifier Elimination by Cylindrical Algebraic Decomposition has the complexity of doubly-exponential with respect to the number of variables which remains as an impediment. Interval Constraint Propagation (ICP) which uses the inequalities/equations to contract the interval of variables by removing the unsatisfiable intervals is an efficient methodology because it uses floating point arithmetic. However the number of boxes (combination of intervals of variables) may grow exponentially.

This thesis presents strategies for efficiency improvement and extensions of an SMT solver named **raSAT** for polynomial constraints. **raSAT** which initially focuses on polynomial inequalities over real numbers follows ICP methodology and adds testing to boost satisfiability detection. In this work, in order to deal with exponential exploration of boxes, several heuristic measures, namely *SAT likelyhood*, *sensitivity*, and *the number of unsolved polynomial inequalities*, are proposed. From the experiments on standard SMT-LIB benchmarks, **raSAT** is able to solve large constraints

(in terms of the number of variables) which are difficult for other tools. In addition to those heuristics, extensions for handling equations using the Intermediate Value Theorem and handling constraints over integer number are also presented in this thesis. The contributions of this work are as follows:

1. Because the number of boxes (products of intervals) grows exponentially with respect to the number of variables during refinement (interval decomposition), strategies for *selecting one variable* to decomposed and *selecting one box* to explore play a crucial role in efficiency. We introduce the following strategies:

   - **Selecting one box.** The box with more possiblity to satisfy the constraint is selected to explore, which is estimated by several heuristic measures, called *SAT likelyhood*, and *the number of unsolved polynomial inequalities*.
   - **Selecting one variable.** The most influential variable is selected as priority in approximation and refinement process. This is estimated by *sensitivity* which is determined during the approximation process.

2. Two schemes of *incremental search* are proposed for enhancing solving process:

   - **Incremental deepening**. raSAT follows the depth-first-search manner. In order to escape local exhaustive search, it starts searching with a threshold that each interval will be decomposed no smaller than it. If neither satisfiability nor unsatisfiability is detected, a smaller threshold is taken and raSAT restarts.
   - **Incremental widening**. Starting with a small intervals, if **raSAT** detects UNSAT, it enlarges input intervals and restarts. This strategy is effective in detecting satisfiability of constraints because small intervals reduce the number of boxes after decomposition.

3. *Satisfiability confirmation* step by an error-bound guaranteed floating point package **iRRAM**[2], to avoid soundess bugs caused by roundoff

[2] `http://irram.uni-trier.de`

errors.

4. This work also implemented the idea of using Intermediate Value Theorem to show *the satisfiability of multiple equations* which was suggested in our previous work.

5. **raSAT** is also extended to *handle constraints over integer numbers* by simple extension in the approximation process.