Title	多項式制約のためのSMTとその応用
Author(s)	To, Van Khanh
Citation	
Issue Date	2013-06
Type	Thesis or Dissertation
Text version	ETD
URL	http://hdl.handle.net/10119/11445
Rights	
Description	Supervisor:小川　瑞史，情報科学研究科，博士

Abstract

Solving polynomial constraints plays an important role in program verification, e.g., checking roundoff and overflow errors with fixed point or floating point arithmetic, measures for proving termination, and linear loop invariant generation. Tarski proved that polynomial constraints over real numbers (algebraic numbers) are decidable, and later Collins proposed Quantifier Elimination by Cylindrical Algebraic Decomposition, which is nowadays implemented in Mathematica, Maple/SyNRAC, Reduce/Redlog, and QEPCAD. However, it is DEXPTIME with regard to the number of variables, and works fine in practice up to 5 variables and lower degrees. For instance, 8 variables with degree 10 may require 20–30 hours by a supercomputer.

Motivated from numerous applications of polynomial constraint solving, this thesis aims to propose an approach and develop an *SMT solver* for *solving polynomial constraints*. First, we focus on *polynomial inequality constraints* coming from following reasons.

(a) In constructive analysis, solving equality constraints on real numbers is in general undecidable (decidable only for algebraic numbers), whereas solving inequality is decidable. In other words, $a > b$ is computable, whereas $a = b$ is not computable.

(b) Inequality allows approximations.

(c) Solving polynomial inequality on real numbers is reduced to that on rational numbers. The reduction to rational numbers allows avoiding roundoff-errors in implementations.

Our approach and contributions in the thesis are summarized as follows:

(i) We propose an approach of *iterative approximation refinement* for solving constraints, which is formalized as an *abstract DPLL(T) procedure* for *over/under-approximations* and *refinements* under a background theory T. An under approximation is sound for proving in the background theory T, and an over approximation is sound for disproving. When they neither prove nor disprove, *refinements* are applied to decompose an atomic formula of the input formula, i.e., ψ to $\psi_1 \vee \psi_2$ such that $\psi \Leftrightarrow \psi_1 \vee \psi_2$. The proposed approach combined DPLL(T) procedure with over/under-approximations and refinements is sound and complete for solving polynomial inequality constraints under certain restrictions.

(ii) We instantiate *interval arithmetic* to over approximation and *testing* to under approximation. A new form of affine interval, called *Chebyshev Affine Interval*, is proposed. Chebyshev Affine Interval has an advantage over current *affine intervals* such that it can keep sources of computation for high degree variables, which would be useful for guiding refinements.

(iii) The proposed approach is implemented as the SMT solver **raSAT**, which applies *interval arithmetic* (over-approximation, aiming to decide unsatisfiability), *testing* (under-approximation, aiming to decide satisfiability), and *refinements* on interval decompositions.

(iv) We propose UNSAT cores of polynomial constraints that can improve efficiency in theory propagation of SMT. Computation of UNSAT cores in polynomial constraints allows inferring other unsatisfiable domain when a particular domain is detected as unsatisfiable. We propose an approach for incremental test data generation which would be useful when performing a large number of test data (i.e., a large number of variables).

(v) We propose strategies for refinements such that choices of intervals to decompose and methods to decompose an interval into smaller intervals. These strategies are guided from interval arithmetic, testing results, test data, and polynomials.

(vi) The proposed approach is also extended for *greater-than-or-equal* ($\geq$) constraints, i.e., $\bigwedge_i f_i \geq 0$ is transformed to $\bigwedge_i f_i > 0$ for proving satisfiability, and for proving unsatisfiability $\bigwedge_i f_i \geq 0$ is transformed to $\bigwedge_i f_i > -\delta_i$ for $\delta_i > 0$.

(vii) We propose a non-constructive method for solving polynomial constraints including *equalities* based on *intermediate value theorem*.

Key words: interval arithmetic, affine arithmetic, SAT Modulo Theories - SMT, polynomial constraints, testing, abstract DPLL.