氏　　名	TO, Khanh Van			
学位の種類	博士(情報科学)			
学位記番号	博情第 278 号			
学位授与年月日	平成 25 年 6 月 24 日			
論文題目	SMT for polynomial constraints and its applications (多項式制約のための SMT とその応用)			
論文審査委員	主査	小川　瑞史	北陸先端科学技術大学院大学	教授
		平石　邦彦	同	教授
		廣川　直	同	准教授
		番原　睦則	神戸大学	准教授
		穴井　宏和	株式会社富士通研究所	主任研究員

論文の内容の要旨

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., $f_i \geq 0$ is transformed to $f_i > 0$ for proving satisfiability, and for proving unsatisfiability $f_i \geq 0$ is transformed to $f_i > -\delta_i$ for $\delta_i > 0$.

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

論文審査の結果の要旨

多項式制約解消とは、$\exists x_1 \in (a_1,b_1) \cdots x_n \in (a_n,b_n).\ \wedge f(x_1,\cdots,x_m) \sim 0$ ($\sim \in \{>, \geqq, =\}$) の形をした制約の真偽を判定し、真の場合には具体的な解を与えることをいう。多項式制約解消は、整数上では Hilbert の第十問題として決定不能であることが知られており、実数上では決定可能であることが 1930 年に Tarski により示されている。近年、丸め誤差エラー検出、ループ不変式生成、停止性検証、制御変数設計など、多くの実用的問題が多項式制約に還元され、適用されている。

その解法として QE-CAD (Collins, 1975) に基づく数式処理に基づく実装 (mathematica, reduce,

QEPCAD 等）が知られている。しかし計算量は DEXPTIME であり、7〜8 変数で 10 次程度の問題がスーパーコンピュータで 20〜30 時間を要し、変数をさらに増やすと解けない例が報告されている。

一方、近年、命題論理式の充足可能性を判定する SAT ソルバの急速な発達（スケーラビリティ）に基づき、背景論理を加えた SMT (SAT modulo theory) の研究・利用が盛んであり、Z3, yices, CVC3 など多くのツール実装が知られる。しかし背景論理は線形制約がポピュラーであり、多項式制約は最近、bit blasting や場合分けに基づく線形制約への還元などの手法が試みられている。

本研究は、多項式制約を不等式に制限することで、十分条件・必要条件による近似の双方とその近似を精錬する手法を提案し、さらに十分条件近似として区間演算、必要条件近似としてテスト、近似精錬として区間分割を用いた SMT raSAT を実装した（国際ワークショップ TAPAS2013 発表）。多項式制約の大きさの尺度として、多項式の次数、多項式の数、多項式制約の変数の数があるが、他の手法でしばしば主要な困難となる次数は、区間演算・テストのいずれでも困難にはならない。しかし変数の数は、他の手法同様に困難となる。ここでは、未充足な多項式間に依存関係に基づく動的ソーティングにより、ターゲットの多項式を選択する戦略を導入している。その結果、SMT-lib ベンチマークのうち、不等式制約のみを対象とした実験結果は、既存の数式処理・SMT のツールで現状最強の Z3 4.3 に次ぐ性能を示している（国際会議 ASE 2013 投稿予定）。また現在、等式制約への拡張として中間値の定理の応用を検討しており今後の拡充が期待される（国際会議投稿予定）。

以上、本論文で提案した多項式不等式制約のための SMT raSAT は、既存手法とは異なる新たな手法を提案し実用上の大きな可能性を示している。学術的に貢献するところが大きく、博士（情報科学）の学位論文として十分価値のあるものとして認めた。