氏　　名	Vu Xuan Tung		
学位の種類	博士(情報科学)		
学位記番号	博情第 391 号		
学位授与年月日	平成 30 年 6 月 22 日		
論文題目	SMT solving for polynomial constraints		
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
	緒方 和博	同	教授
	廣川 直	同	准教授
	関 浩之	名古屋大学	教授
	Pascal Fontaine	ロレーヌ大学	准教授

論文の内容の要旨

The need for solving non-linear arithmetic arises from many applications in artificial intelligence and formal methods. Although the full first-order theory of real numbers is decidable, the best well-known decision procedure for it, namely quantifier elimination by cylindrical algebraic decomposition, has the complexity of double exponential with respect to the number of variables. This remains as an impediment for a solver supporting non-linear arithmetic. This thesis aims at an efficient complete framework for solving existential fragment of polynomial constraints by first developing (incomplete) efficient procedures as heuristics and then combine them with a complete procedure. Two efficient procedures proposed are

- an extension of the raSAT loop, which is, in turn, an extension of interval constraint propagation (ICP) with testing, with the application of the intermediate value theorem (IVT), and
- subtropical satisfiability.

Distinct procedures and their combinations are further integrated into a satisfiability modulo theories (SMT) framework by supporting features of SMT solving such as unsat core computation.

While raSAT loop (an extension of the ICP with testing) aims at quickly detecting satisfiability of inequalities, the application of the IVT aims at showing satisfiability of equations. We propose a scheme to combine interval arithmetic, testing, and the IVT to show satisfiability of combinations of inequalities and equations. SAT-directed heuristics are also proposed for the framework to quickly detect satisfiability while not affecting performances of detecting unsatisfiability. Experimental data shows that the proposed extensions increase the number of solved problems and the heuristics improve the running time on solved problems and also increase the number of solved benchmarks. Comparing with other SMT solvers, except for weaknesses in completeness, **raSAT** shows comparable running time on problems it solved.

The second procedure, i.e. subtropical satisfiability, aims at finding an assignment for variables

which satisfies inequalities by examining the exponent vectors of polynomials appearing in the inequalities. From those exponent vectors, the method generates linear arithmetic constraints such that if they are satisfiable, then the original inequalities are also satisfiable. The solution of the generated linear constraints is further used to provide a witness for satisfiability of non-linear inequalities. Experimental results show that the procedure is quite fast at either detecting satisfiability or failing. In particular, it finds solutions for problems where other state-of-the-art non-linear arithmetic SMT solvers times out.

Both proposed procedures are incomplete and in order to produce a decision framework, we utilize quantifier elimination methods implemented in the computer algebra system Redlog/Reduce. We propose two kinds for combining the ICP-based methods and the quantifier elimination, namely lazy and less lazy approaches. While the lazy approach uses ICP-based methods as pre-processing steps for the quantifier elimination, the less lazy one invokes the quantifier elimination on every box generated by the ICP framework. In both approaches, subtropical satisfiability is utilized first as an attempt to find a model for inequalities. Experimentally, the lazy method performs better than the less lazy one but we expect some future improvements for the less lazy approach so that several unsatisfiable boxes can be all discarded once the quantifier elimination method detects the unsatisfiability of one box. Experimental results also show that our framework is an efficient decision procedure to solve non-linear arithmetic SMT problems and complementary to implementations in other SMT solvers.

Keywords: SMT solving, non-linear arithmetic, interval constraint propagation, subtropical satisfiability, complete efficient framework.

論文審査の結果の要旨

本博士論文では、ソフトウェア検証で広く用いられている制約解消器 SMT ソルバについて、従来、未開拓であった実数上の多項式制約 QFNRA (Quantifirer-Free Nonlinear Constraints over Reals)を対象とした raSAT の研究・開発を行ったものである。QFNRA は整数係数の多項式の等式または不等式の論理演算子による結合を制約とし、その制約が解をもつ（充足可能 SAT）か、解が存在しない（充足不能 UNSAT）を判定する。QFNRA は、理論的には CAD (Cyrindrical Algebraic Decomposition) により決定可能であることが知られているが、理論計算量が double exponential であり、また実用上の効率も、10 次以上で変数が 8 個を超えると、通常、解くことができない。

本研究では、実用上高速である区間演算を不等式制約解消の中心とし、テスト、中間値の定理、代数的手法の個別の手法を組み合わせることで、実用的に高速な SMT ソルバを構成できることを実装により示し、国際競技会 SMT-COMP に 2014 年より参加を通じて、高い実用性が得られることを実証した独自性の高い研究である。

具体的な貢献は、(1) 区間演算は近似計算であり、充足可能性が決定できなかった場合に、SAT 検出をテスト手法により加速する不等式制約を対象とする raSAT ループの提案・実

装、(2) raSAT ループに加え、等式制約判定を拡張中間値の定理を用いた拡張 raSAT ループの提案・実装、(3) 拡張 raSAT ループにおける有効なヒューリスティックスの発見・実装（以上は、国際会議 IJCAR2016 にて発表、および国際論文誌 FMSD b に 2017 年掲載）、(4) テストに代えて、特定の形の不等式制約に対し高速に SAT 検出を行う代数的手法 Subtropical Satisfiablity の提案・実装（国際会議 FroCos2017 にて発表）、(5) 個別手法・既存ツール(Reduce/Redlog)の独立性を高めつつ協調を容易にする、統一的設計および SMT ソルバフレームワーク VeriT 上での実装（投稿準備中）である。このうち(4),(5)は、主に 2016 年 6 月より 1 年間、ロレーヌ大学におけるインターン期間中になされた。

各論文の研究内容は、SMT ソルバ raSAT（2016 年より /www.jaist.ac.jp/~s1520002/raSAT/にて公開）、VeriT/raSAT として統合して実装されており、国際競技会 SMT-COMP の QFNRA 部門では 2016 年、2017 年と、Microsoft Research の開発する SMT ソルバ Z3 の姉妹ツールである SRI の開発する Yices2 に次ぐ 2 位を獲得している。特筆すべきは、raSAT は、独立性の高い個別手法・ツールの明快な組み合わせで、複雑に手法が交錯する Z3 / Yices2 に次ぐ性能を得ていることである。

以上、本学位論文は、上記研究を総括すると同時に、学術的に貢献するところが大きく、各学位論文審査員より高く評価をされた。よって博士（情報科学）の学位論文として高い価値を認める。