様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成 ２７ 年　 ６ 月 １０ 日現在

機関番号：１３３０２
研究種目：基盤研究(B)
研究期間：2011～2014
課題番号：２３３００００５

研究課題名（和文）近似手法と数式処理の融合による実数多項式制約の効率化

研究課題名（英文）Optimization of polynomial constraint solving based on fusion of approximation and algebraix methods

研究代表者

小川　瑞史（Mizuhito, Ogawa）

北陸先端科学技術大学院大学・情報科学研究科・教授

研究者番号：４０３６２０２４

交付決定額（研究期間全体）：（直接経費）　　15,500,000円

研究成果の概要（和文）：本研究では、多項式制約解消アルゴリズムである区間制約伝播の拡張としてraSAT ループを提案し、SMTソルバ raSATとして実装を行った。制約解消の解は SAT（充足可能）かUNSAT（充足不能）だが、SAT検出はエラー検出、UNSAT検出はループ不変式生成に用いられる。数百変数程度の大規模な問題に対し、実質的に後者が解けるのはUNSATコア（小さな部分制約で充足不能となるもの）を発見した場合に限られ、前者はすべての制約の充足性の確認が必要なため、実用上より困難である。本研究ではSAT検出に焦点をあて、SMTlibベンチマーク上の実験で答えが未知であった複数の問題のSATを検出した。

研究成果の概要（英文）：This research extends the interval constraint propagation to the raSAT loop, which is implemented as an SMT solver raSAT. A polynomial constraint solving concludes either SAT (satisfiable) or UNSAT (unsatisfiable). raSAT is designed to intend the former, which is often used for error detection, where the latter is used for loop invariant generation. In practice, when tackling a larger problem with several hundred variables, UNSAT is detected only with the discovery of a small UNSAT core, whereas SAT is detected by finding an instance that satisfies all constraints, and often becomes a harder problem. In experiments, we newly found that several unsolved problems in SMTlib benchmark are SAT.

研究分野：理論計算機科学、形式手法

キーワード：ソフトウェア　仕様記述　仕様検証　制約解消　数式処理

１．研究開始当初の背景

形式手法において、その柔軟性から、制約解消系の一つである SMT ソルバが近年広く用いられている。しかし、多項式制約については、実装は限られており、いまだデファクトスタンダードとなるアルゴリズムは存在せず、さまざまなアルゴリズム（代数的数式処理手法の QE-CAD、区間制約伝播、線形化など）が試みられていた。各手法はそれぞれに長短があり、QE-CAD は変数数の増加に対し非効率（8 変数 10 次前後が限界）、区間制約伝播は充足不能性検出には比較的有効であるが充足性検出には非力であると同時に理論的な完全性・実装上の健全性が未解決であった。線形化は次数増加に対し甚だしく非効率であった。

２．研究の目的

本研究では、区間制約伝播アルゴリズムを基本として、充足性検出に強化する。さらに、数式処理手法との融合を図り、理論的完全性の強化を目的とする。さらに実装上の工夫により、検出結果の健全性を担保し、数百変数程度の多項式制約の制約解消を可能とする SMT ソルバの実装を目的とする。その際、SMT ソルバの応用を想定し、応用分野において有効な実用的な戦略や効率化を試みる。

３．研究の方法

(1) 区間制約伝播アルゴリズムに対し、テスト手法を組み合わせ、相互に精錬を行う raSAT ループアルゴリズムを用いる。

(2) 近似手法となる区間演算に対し、古典的な区間演算のみならず、アファイン区間演算およびその拡張を用いる。特に、アファイン区間表現により各変数の入力の影響度を評価する戦略を導入する。

(3) 理論的な完全性を保証するため、QE-CAD や Groebner 基底などの代数的手法を区間制約伝播に組み合わせる。ただし、一般に区間制約伝播の方が簡素で実用上の効率が良いことが多いので、制約の大部分を raSAT ループで解消し、限界的な部分のみを代数的手法による制約解消を適用を試みる。

(4) 区間制約伝播の欠点の一つが等式制約の扱いである。区間演算が近似手法であるため、そのままでは等式制約が扱えない。当初、直接に代数的手法（Groebner 制約など）の応用を想定したが、部分解ではあるが、よりシンプルな手法として、中間値の定理の応用を着想した。特に一変数の場合は知られていたが、多変数の場合に拡張した。

(5) 実用上、しばしば有効であるインクリメンタルなアルゴリズムを設計した。これは当初、区間を狭い範囲の探索、また分割の最小値を設定し探索の深さを制限して開始し、探索が失敗した場合に、順次、区間の拡大、分割の詳細化による探索の深化を行う。

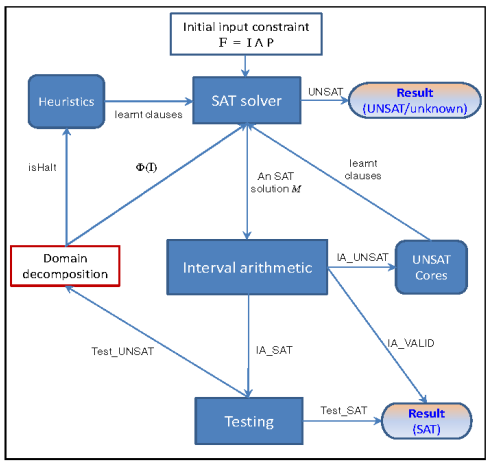
(6) これらのアイデアは SMT ソルバ raSAT として実装し、SMT-COMP (2005 年以来、毎年開催されている SMT ソルバの競技会 http://smtcomp.sourceforge.net）に参加し、評価する。

(7) SMT ソルバの応用として、量的情報流解析やセキュリティ解析への応用を想定し、応用手法について研究を進める。

４．研究成果

(1) raSAT ループ

区間制約伝播は、区間演算による真にとりうる値をカヴァーする近似を行い、区間の分割・細分化により近似を詳細化する。その結果が空である場合に充足不能（UNSAT)，結果が近似値すべてが制約を満たす場合に充足可能（SAT）を検出する。そのため、SAT の検出が遅い欠点がある。この欠点を補うため、SAT は１インスタンスの発見があればよいことに着目し、テスト手法を組み合わせた手法を提案した。いずれも SAT/UNSAT を決定できなかった場合、適切な戦略による区間分割を行い、精密化を結果が確定するまで繰り返す raSAT ループを提案した。

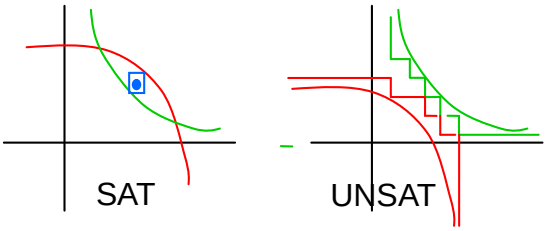


(2) アファイン区間演算の拡張および戦略の設計

アファイン区間演算は加減算における精度向上をめざし、部分的な記号処理と近似手法を組み合わせた演算であり、近似手法の導入の仕方により、さまざまな亜種が存在する。共通する特徴として、記号処理により、各変数に対する入力値の出力値への近似評価(sensitivity)を可能とする点があり、それを用いた二つの有効な SAT 検出のための近似尺度 SAT-likelyhood, sensitivity を提案した。戦略のアイデアはさまざまあるが、実際に試すと、殆どがランダム戦略と有意な差が生じない。これらを膨大なベンチマーク（11000 件）の実験を多数の戦略の組み合わせに対し実行し、最終的に、最小 SAT likelyhood と最大 sensitivity の組み合わ

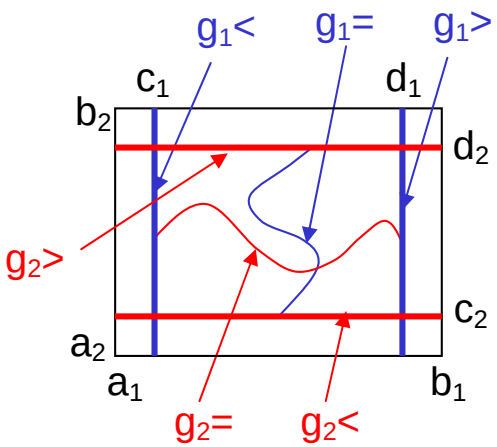
せが SAT 検出に有効であることを明らかにした。これは、いまだ基本戦略の決定にとどまり、今後の研究が必要である。

(3) 近似手法と代数的手法の組み合わせ
素朴な raSAT ループにおける主たる欠点は、理論的な完全性の保証ができないこと、等式制約の判定ができないことである。これらは関連した問題であり、完全性の保証ができないのは、無限遠点で収束する場合と、二つの境界が接する場合である。前者は、区間に適切な上限・下限を設けること、後者は本質的に等式制約判定に帰着する。



これらは、代数的手法で理論的解決は可能であるが、QE-CAD や Groebner 基底に基づく Mathematica,Maple/Synrac, REDUCE/redlog, QEPCAD などのツールなどからみてもスケーラビリティの追求が難しいと考え、最終的に部分的な代数的手法の利用を着想した。これは前者の区間の適切な上限・下限の設定は QE-CAD の分割を上限・下限付近のみに限ること、後者の等式制約は、中間値の定理を適用した後にも解けない限界的な場合にのみ適用するアイデアである。ただし、これらはいまだに着想段階であり、今後の研究によりアルゴリズムの明確化、実装を進める。

(4) 中間値の定理に基づく等式制約解消
多項式は連続関数であるので、多項式 f が f>0 および f<0 となる点をそれぞれ発見すれば、その中間に f=0 となる点の存在が示せる。（ただし具体的なインスタンスは決定されない。）このアイデアを多変数の場合に拡張した。制限として、変数の数が多項式の数以上の場合のみに適用可能である。



(5) インクリメンタルな探索アルゴリズム
探索開始時に注目する区間と、探索深化の制御のため、当初は探索対象の区間を小さく、また区間分割の詳細度を制限し、その範囲で解が決定されないとき、順次、拡大する。この手法については、現在、評価中であり、今後も実験による評価に基づき、決定する。

(6) SMT ソルバ raSAT の実装と SMT-COMP 参加
SMT ソルバ raSAT の実装は平成 26 年 1 月から初期バージョンを公開し、順次アップデートを続けている
http://www.jaist.ac.jp/~mizuhito/tools.html
SMT-COMP には 2014 年 7 月に QF_NRA（実数上の多項式制約）カテゴリに参加したが、事前の競技サーバー上でのドライラン不備などの準備不足のため、4 ツール参加のうち、最下位と振るわなかった。2015 年 7 月の競技会にも QF_NRA, QF_NIA（実数上および整数上の多項式制約）カテゴリにエントリしている。今回のドライランの結果は、QF_NRA 11540 件中 7965 件(結果が未知であった 37 件を含む)、QF_NIA 9389 件中 7898 件（結果が未知であった 14 件を含む）と良い成績を示している。（2014 年の各カテゴリの優勝ツールは QF_NRA は CVC3 10121 件中 3543 件、QF_NIA は AProve 8327 件中 8172 件であった。ただし、未参加であった Microsoft research の Z3 の参考データはそれぞれ 9927 件、8313 件であり、まだ最良の結果とはいえない。）特筆すべきは QF_NRA ベンチマークにおいて、結果が未知であった 100～200 変数の６つの制約の SAT を検出している点である。これは Z3 でも解けない規模の問題である。

(7) 量的情報流・セキュリティ解析への応用
量的情報流解析は、yes/no の離散値ではなく、エントロピーに基づく情報流出度の定量的評価に基づく新しい解析手法である。セキュリティ解析としては、主に XML データベースにおける攻撃や確定依存性などを対象として研究を進めた。

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計２件）

(1) Chittaphone Phonharath, Kenji Hashimoto, Hiroyuki Seki, Deciding Schema k-security for XML databses.
IEICE Transactions on Information and Systems, E96-D, pp.1268-1277(2013)査読有

(2) Kazuki Miyahara, Kenji Hashimoto, Hiroyuki Seki, Node quaey preservation for deterministic linear top-down tree transducers.
Electric Proceedings in Theoretical Computer Science, Vol.137, pp.27-37

(2013)査読有

〔学会発表〕(計８件)

(1) To Van Khanh, Mizuhito Ogawa, raSAT: SMT for polynomial inequality.
SMT workshop (SMT 2014), ウィーン、オーストリア（2014 年 7 月 17 日～18 日）

(2) Bao Trung Chu, Kenji Hashimoto, Hiroyuki Seki, Runtime control of a program based on quantitative information flow
IEICE SS2013-60, 豊田中央研究所、愛知県豊田市 （2014 年 1 月 31 日）

(3) Kenji Hashimoto, Ryuta Sawada, Yasunori Ishihara, Hiroyuki Seki, Toru Fujiwara, Determinacy and Subsumption for Single-valued Bottom-up Tree Transducers.
7th International Conference on Language and Automata Theory and Applications (LATA 2013), Springer LNCS 7810, pp.335-346, ビルバオ、スペイン (2013 年 4 月 2 日～5 日)

(4) To Van Khanh, Mizuhito Ogawa, SMT for Polynomial Constraints on Real Numbers.
Tools for Automatic Program Analysis (TAPAS 2012), Electrical Notes in Theoretical Computer Science, Vol.289, pp.27-40, ドゥービル、フランス（2012 年 9 月 14 日）

(5) Chittaphone Phonharath, Kenji Hashimoto, Hiroyuki Seki, Verification of the Security against Inference Attacks on XML Databases.
1st International Workshop on Trends in Tree Automata and Tree Transducers (TTATT2012) 名古屋大学　愛知県名古屋市（2012 年 6 月 2 日）

(6) 宮原 一喜, 橋本 健二, 関 浩之. 決定性線形下降木変換器における頂点問合せ保存
電子情報通信学会技術研究報告, SS2012-38, Vol.112, No.275, pp.13-18, 広島市立大学 広島県広島市 (2012 年 9 月 11 日)

(7) Dominik Klein, Nao Hirokawa, Confluence of Non-Left-Linear TRSs via Relative Termination.
18th International Conference on Logic for Programming, Artificial Intelligence and Reasoning (LPAR2012), Springer LNCS 7180, pp.258-273), メリダ、ベネズエラ (2012 年 3 月 11 日～15 日)

(8) Do Thi Bich Nogc, Mizuhito Ogawa, Positive-noise Affine Interval Arithmetic.
情報処理学会　第 86 回プログラミング研究会, 神奈川近代文学館　神奈川県横浜市（2011 年 11 月 1 日～2 日）

〔その他〕
ホームページ等
http://www.jaist.ac.jp/~mizuhito/tools.html

６．研究組織
(1)研究代表者
小川　瑞史　(OGAWA, Mizuhito)
北陸先端科学技術大学院大学・情報科学研究科・教授
研究者番号：40362024

(2)研究分担者
関　浩之　(SEKI, Hiroyuki)
名古屋大学・情報科学研究科・教授
研究者番号： 80196948

(3)研究分担者
廣川　直　(HIROKAWA, Nao)
北陸先端科学技術大学院大学・情報科学研究科・准教授
研究者番号：50467122

(4) 研究協力者
ヴ　シュアン　ツング (VU, Xuan Tung)

(5) 研究協力者
ト　ヴァン　カン　(To Van Khanh)