

科学研究費助成事業 研究成果報告書

平成 30 年 6 月 14 日現在

機関番号：13101

研究種目：基盤研究(C) (一般)

研究期間：2015～2017

課題番号：15K00003

研究課題名(和文)書き換えシステムの基底合流性自動証明の研究

研究課題名(英文)Study on Ground Confluence of Rewrite Systems

研究代表者

青戸 等人 (Aoto, Takahito)

新潟大学・自然科学系・教授

研究者番号：00293390

交付決定額(研究期間全体)：(直接経費) 3,500,000円

研究成果の概要(和文)：項書き換えシステムの基底合流性は、書き換えシステムに基づくソフトウェア検証法を構築する上で基礎となる性質である。本研究では、帰納的定理証明に用いられる書き換え帰納法に着目し、書き換え帰納法において束縛的変換可能性を保証すれば、基底合流性が成立することを示した。そして、束縛的変換可能性を保証する書き換え帰納法を設計して、その理論的な正当性の証明を与えた。また、書き換え規則の変換に基づく適切な関数定義の補完手法、順序付け不能な構成子規則を扱うための推論規則の拡張、基底合流性の反証法などの改良や拡張を考案した。そして、提案手法にもとづく基底合流性自動証明ツールAGCPを開発した。

研究成果の概要(英文)：Ground confluence of term rewriting systems is a property fundamental to establish software verification techniques based on rewrite systems. In this study, we have focused on rewriting induction which a method for inductive theorem proving, and have shown that bounded convertibility guarantees the ground confluence. We have designed a rewriting induction method for establishing bounded convertibility and have shown its correctness theoretically. We have also given a method to deal with the case in which suitable rules are not presented in the input system, a method to deal with non-orientable constructor rules, and a method to deal with disproving ground confluence. Based on the proposed methods we have implemented in ground confluence prover AGCP.

研究分野：プログラム理論

キーワード：項書き換えシステム 基底合流性

1. 研究開始当初の背景

合流性は項書き換えシステムの中心的な性質であり、長年研究が行われてきた。合流性がすべての項についてリダクションによる解の一意性を保証するのに比べ、基底合流性は、変数を含まない項（基底項）についてのみリダクションによる解の一意性を保証する性質である。基底合流性は、一般的にデータ構造に関する帰納法を用いて合流性を推論する必要があるため、通常の合流性よりも解析は困難である。このため、従来は合流性で近似されることが多く、研究においても合流性の方が優先されてきた。従って、合流性とは対照的に、基底合流性証明の理論はほとんど解明されていなかった。

2. 研究の目的

一般に、すべてのモデルについて性質が正しいことを保証する演繹的な妥当性の検証においては、合流性が重要な役割を果たす。一方、始代数において性質が正しいことを保証する帰納的な妥当性の検証においては、基底合流性で十分であることが知られている。特に、ソフトウェアにおける操作的な意味では、具体的なデータの入力に対する妥当性を議論するため、帰納的な妥当性が用いられる。このため、項書き換えシステムに基づくソフトウェア検証では、合流性ではなく、基底合流性がより根本的かつ重要な性質である。

そこで、本研究では、最新の合流性証明や帰納的定理証明の理論技法を応用し、基底合流性についての先行研究を整理・拡張するとともに、基底合流性証明の基盤理論を構築する。このために、Goebel および Becker の結果を抽象的な枠組みで整理するとともに、研究実施者らの考案したより強力な帰納的定理証明法を利用した手続きへ拡張する。また、研究実施者らが開発している強力な合流性自動証明システムと帰納的定理証明システムを利用することで、基底合流性自動証明システムを実現し、基底合流性自動証明の基盤技術を確立する。

3. 研究の方法

まず、基底合流性証明についての基礎理論の

構築と、それらの基礎理論に基づく証明手続きを実験・評価するための実験システムの開発を行う。現在、基底合流性の十分条件として Goebel の条件、一般的な基底合流性証明手続きとして Becker の手続きおよび Bouhoula の手続きが知られている。これらの先行研究をより詳しく調査するとともに、最新の合流性証明および帰納的定理証明の理論技法を応用してこれらの理論を整理し、見通しの良いより一般的な基礎理論の構築を行う。また、実験システムを開発し、これらの手法や証明手続きの評価を行う。その後、考案した基本的な証明手続きの実験評価や改良に取り組むとともに、研究実施者らの開発している強力な合流性証明システム ACP および帰納的定理証明システム sprint と組み合わせ、強力な基底合流性証明システムを構築する。

4. 研究成果

(1) 本研究では、始代数における妥当性を示す帰納的定理証明に用いられる自動証明法である書き換え帰納法に着目し、危険対が帰納的定理であることが書き換え帰納法により証明できるならば、基底合流性が成立するという予想をたてた。そして、書き換え帰納法において、束縛的変換可能性を保証すれば、基底合流性が成立することを見出した。そして、束縛的変換可能性を保証するような書き換え帰納法を設計して、その理論的な正当性の証明を与えた。また、順序付け不能な等式を扱えるよう、書き換え帰納法を拡張するとともに、構成子が自由でない場合へも拡張した。

(2) 研究実施者らの開発している強力な合流性証明システム ACP および帰納的定理証明システム sprint での経験やコードを組み合わせて、提案手法に基づく基底合流性自動証明ツール AGCP を開発した。AGCP は、多ソート項書き換えシステムを入力として与えることで、その多ソート項書き換えシステムが基底合流性をもつかを自動証明する。多ソート項書き換えシステムのフォーマットを設計する

ともに,合流性競技会にデモカテゴリに参加し,競技カテゴリへの昇格に参画した.

(3) 書き換え帰納法にもとづく基底合流性自動証明法をより強力にするため,書き換え規則の変換に基づく適切な関数定義の補完手法を開発した.書き換え帰納法を直接適用するには,入力項書き換えシステムの停止性が必須であるが,この手法によって,停止性がない場合に対応できるようにすることができた.また,順序付け不能な構成子規則を扱うための推論規則を考案し,それまで構成子規則については順序付けが必須であったが,その条件を緩和した.また,基底合流性の反証法を考案して,基底合流性をもたない場合に,基底合流性に対する反例を発見する手続きを考案した.

以上,従来ほとんど研究の進んでいなかった,項書き換えシステムの基底合流性について,その自動証明法の基礎理論を与えるとともに,その理論に基づく強力な基底合流性自動証明ツールを構築することができた.また,これらの結果を第1回,第2回国際会議 FSCD で報告した.また,第6回合流性競技会にて基底合流性カテゴリの創設に参画するとともに,基底合流性自動証明ツール AGCP は基底合流性カテゴリで第1位を獲得した.

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 8 件)

1) Kentaro Kikuchi, Takahito Aoto and Yoshihito Toyama, Parallel closure theorem for left-linear nominal rewriting systems, In Proceedings of the 11th International Symposium on Frontiers of Combining Systems (FroCoS 2017), Brasilia, Brazil, September 2017, pp.115-131, Lecture Notes in Computer Science, Vol.10483, Springer-Verlag. [doi:10.1007/978-3-319-66167-4_7] 査読

有

2) Takahito Aoto, Yoshihito Toyama and Yuta Kimura, Improving rewriting induction approach for proving ground confluence, In Proceedings of the 2nd International Conference on Formal Structures for Computation and Deduction (FSCD 2017), Oxford, UK, 2017, pp.7:1-7:18, Leibniz International Proceedings in Informatics, Vol.84, Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik. [doi:10.4230/LIPIcs.FSCD.2017.7] 査読有

3) 島貫健太郎, 青戸等人, 外山芳人, 書き換え規則の重なりに基づく到達可能性判定法, コンピュータソフトウェア, Vol.33, No.3, pp.93-107, 2016. [doi:10.11309/jssst.33.3_93] 査読有

4) Takahito Aoto and Kentaro Kikuchi, Nominal confluence tool, In Proceedings of the 8th International Joint Conference on Automated Reasoning (IJCAR 2016), Coimbra, Portugal, June-July 2016, pp.173-182, Lecture Notes in Computer Science, Vol.9706, Springer-Verlag. [doi:10.1007/978-3-319-40229-1_12] 査読有

5) Takahito Aoto and Yoshihito Toyama, Ground confluence prover based on rewriting induction, In Proceedings of the 1st International Conference on Formal Structures for Computation and Deduction (FSCD 2016), Porto, Portugal, June 2016, pp.33:1-33:12, Leibniz International Proceedings in Informatics, Vol.52, Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik.

[doi:10.4230/LIPIcs.FSCD.2016.33] 査読有

6) Takaki Suzuki, Kentaro Kikuchi, Takahito Aoto and Yoshihito Toyama, Critical pair analysis in nominal rewriting, In Proceedings of the 7th International Symposium on Symbolic Computation in Software Science (SCSS 2016), Tokyo, Japan, March, 2016, pp.156-168, EPiC Series in Computing, Vol.39, EasyChair. 査読有

7) Koichi Sato, Kentaro Kikuchi, Takahito Aoto and Yoshihito Toyama, Correctness of context-moving transformations for term rewriting systems, In Proceedings of 25th International Symposium on Logic-Based Program Synthesis and Transformation (LOPSTR 2015), Siena, Italy, July 2015, pp.331-345, Lecture Notes in Computer Science, Vol.9527, Springer-Verlag. [doi:10.1007/978-3-319-27436-2_20] 査読有

8) Takaki Suzuki, Kentaro Kikuchi, Takahito Aoto and Yoshihito Toyama, Confluence of orthogonal nominal rewriting systems revisited, In Proceedings of the 26th International Conference on Rewriting Techniques and Applications (RTA 2015), Warsaw, Poland, June-July 2015, pp.301-317, Leibniz International Proceedings in Informatics, Vol.36, Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik. [doi:10.4230/LIPIcs.RTA.2015.301] 査読有

[学会発表](計 3 件)

1) 加藤裕人, 青戸等人, 書き換え帰納法を利用した帰納的定理証明の補題生成法, 日本ソフトウェア科学会第 34 回大会, PPL4-1, 2017. 査読無

2) 萩原崇央, 青戸等人, 極大完備化に基づく等式定理の自動証明, 日本ソフトウェア科学会第 34 回大会, PPL2-1, 2017. 査読無

3) 菊池健太郎, 青戸等人, 外山芳人, 文脈移動法によるプログラム変換の正当性について, 日本ソフトウェア科学会第 32 回大会, PPL4-4, 2015. 査読無

6. 研究組織

(1) 研究代表者

青戸 等人 (AOTO, Takahito)
新潟大学・自然科学系・教授
研究者番号: 00293390

(2) 研究分担者

外山 芳人 (TOYAMA, Yoshihito)
東北大学・電気通信研究所・教授
研究者番号: 00251968