科学研究費助成事業　　研究成果報告書

平成　２６　年　　６　月　　６　日現在

機関番号：　１１３０１
研究種目：　基盤研究(C)
研究期間：　2011～2013
課題番号：　２３５００００２

研究課題名（和文）定理自動証明における補題発見法に関する研究

研究課題名（英文）Lemma Generation in Inductive Theorem Proving

研究代表者
青戸　等人（aoto, takahito）

東北大学・電気通信研究所・准教授

研究者番号：００２９３３９０

交付決定額（研究期間全体）：（直接経費）　　3,900,000円、（間接経費）　　1,170,000円

研究成果の概要（和文）：書き換えシステムに基づく帰納的定理の自動証明における補題生成法について、補題候補の発見法や補題決定に有効な技術に資する成果を得た。主な研究成果としては、発散を生じる等式を解析するための基礎理論として、正則項の単一化および書き換え理論、半単一化についての理論について新しい知見を与えた。補題の決定手続きに適した書き換え帰納法の決定理論を拡張するとともに、書き換え帰納法において有効な補題決定手続きについて、始代数を用いるアプローチに基づく新しい手続きを考案した。また、書き換えシステムにおける末尾再帰を用いた関数定義において、自動証明に適した関数定義を得るための補題を抽出する手法を考案した。

研究成果の概要（英文）：Our focus in this project is inductive theorem proving based on term rewriting systems. We are interested in identifying lemmas that leads the whole inductive theorem proving procedure to success. Our first attempt to this problem lies in how to extract information from divergence of proving procedure. For this, we investigated theories of unification and rewriting of regular terms and semi-unification that suits for expressing and detecting looping structures. We extended decision procedure for inductive theorems based on rewriting induction, and also we give a novel decision procedure of inductive theorems based on a new approach employing decision procedures for validity in initial algebras. We also studied how one can extract suitable properties from tail-recursive function definition for translating them to equivalent simple recursive one.

研究分野：　総合領域

科研費の分科・細目：　情報学・情報学基礎

キーワード：　項書き換えシステム　自動定理証明　帰納的定理　補題発見

１．研究開始当初の背景

プログラムの性質はデータ構造に関する帰納法により証明されることが多い。従って、このような性質(帰納的定理)の自動検証はソフトウェア検証に極めて有効であると考えられる。書き換えシステムに基づく帰納的定理の自動証明は等式論理を基礎とする系の仕様やプログラムの検証の基礎となっている。書き換えシステムに基づく帰納定理の自動証明において、申請者らは自動証明法の原理を整理・拡張するとともに、自動証明システムの補助機能である補題生成法の拡張を行った。また、これらの成果に基づいて、書き換え帰納法に基づく帰納的定理の自動証明システムの実装を行った。このシステムは同じ原理を基盤に持つ帰納的定理の自動証明システムとして代表的な SPIKE システムト較べても基本的な性能については同等以上の証明能力を有するまでになっている。これらの成果の実験を通じて、これ以上の証明能力の向上のためには、補題発見法の高度化が必須であると考えた。

２．研究の目的

書き換え帰納法では、証明すべき等式と仮定の集合の対に対して推論規則を繰り返し適用する。このとき、推論規則の適用が無限に繰り返される場合には帰納的定理であるかどうかを判定できない。しかしながら、証明すべき等式集合に適当な等式を補題として追加することにより証明が成功することがある。従来の書き換え帰納法に基づく帰納的定理の自動証明システムを考察した結果、補題の生成がたびたび証明の成功に鍵になるにもかかわらず、従来、補題生成に大きな計算リソースが割りあてられていないことが、適用性が限られる大きな要因になっている。また、帰納定理自動証明において、従来主に知られている補題候補の発見法は 2 種類のみであり、補題を効率的に決定する手法も確立されていない。このため、補題の生成技術がより強力な帰納定理自動証明を実現する上でのボトルネックとなっていると考えられた。そこで、書き換えシステムに基づく帰納定理の自動証明において、証明技術の向上に資する補題生成法についてその高度化を試みることを目指した。

３．研究の方法

補題生成手法の考案および考案した補題生成手法の実験評価および改良に取り組む。提案した補題生成手法を組み入れた補題の探索戦略の定式化および効率的な探索戦略、定理自動証明システムの高度化に取り組む。また、書き換え帰納法とは異なる証明手法である潜在帰納法や明示的帰納法に基づく自動証明システムへの補題生成手法の応用についても検討を進める。特に、補題生成手法の考案については、以下の複数の着想点から新しい原理にもとづく補題生成法について検討する：(1) 発散を生じる等式からの補題生成、(2) 公理の等価性に基づく補題生成、(3) パターンに基づく補題生成、(4) 決定可能性理論を利用した補題生成。

４．研究成果

(1) 正則項の効率的な単一化手続き

発散を生じる等式から得られる正則項の繰り返しは発散鑑定法による補題生成の基礎となっている。項の繰り返しから得られる無限項は正則項とよばれ、計算に現われるさまざまなループ構造を表現するのに適している。有理項の効率的な単一化手続きを見い出し、それを用いて無限項書き換えシステムの性質を反証する手法を考案した。

(2) 交換律や結合律をもつ項書き換えシステムの合流性

交換律や結合律は等式システムの性質として非常に重要であるが、書き換え帰納法で扱うのが困難な性質として知られている。交換律や結合律など停止しない書き換え規則をもつ項書き換えシステムの合流性の自動証明法を与えた。合流性は潜在帰納法の基礎となる性質であり、本手法は、書き換え帰納法で扱うのが困難である交換律や結合律といった性質を潜在帰納法で扱うために重要と考えられる。

(3) 正則項書き換えシステムにおける決定可能性

発散から生じる等式からの補題発見への応用を目指して、正則項書き換えの基礎理論の構築を行った。従来、直交システムに限定されていた正則項書き換えシステムを一般化した体系を提案し、特にオートマトン理論を用いて書き換えステップや正規性の決定可能性を明らかにした。また、直交システムの実効合流性を示した。

(4) 半単一化問題の形式推論体系の提案

項の繰り返しの検出は単一化をより一般化した半単一化によっても検出することが出来る。半単一化問題は、一般的には決定不能であることが知られているが、一様な半単一化問題については、 効率的な解法が知られている。一方で、単一化問題について知られているような 形式推論体系にもとづく解法については、厳密な解法や停止性の証明が従来与えられていない。そこで、一様な半単一化問題についての形式推論体系にもとづく解法を与え、どのような証明戦略のもとで停止性が保証されるか検討を行なった。また、半単一化を用いた
発散パターン抽出の可能性について検討を行った。

(5) 決定手続きを利用した補題生成

書き換え帰納法に基づく帰納的定理の決定手続きについて、その基本原理を整理する

とともにその適用条件を明らかにした。特に、従来提案されていた条件を組み合わせた、より柔軟な条件においても帰納的定理が決定可能となることを示した。また、書き換え帰納法において有効な補題決定手続きについて、従来とは異なる始代数を用いるアプローチに基づき、いくつかの理論について、書き換え帰納法等の帰納法を用いない決定手続きを考案した。その正当性を証
明するとともに、実験システムを開発し、その有効性を検証した。

(6) パターンに基づく補題生成

プログラムの効率化のための変換パターンの逆変換が補題生成に利用できるという観察に基づき、自動証明のための類似の変換として提案されていた文脈移動法と文脈分割法について、書き換え帰納法に基づく帰納的定理証明において用いるための必要条件について検討した。また、これらを組み合わせた実験システムを構築し、末尾再帰プログラムにおいてプログラムの形から文脈移動法と文脈分割法を適用するための補題を抽出するとともに、補題の検証と末尾再帰プログラムにおける帰納的定理証明の組み合わせの有効性を検証した。

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 16 件）

① Takahito Aoto,
Disproving confluence of term rewriting systems by interpretation and ordering,
In Proceedings of the 9th International Symposium on Frontiers of Combining Systems (FroCoS 2013), Nancy, France, September 2013, pp.311-326, Lecture Notes in Artificial Intelligence, Vol.8152, Springer-Verlag. 査読有,
http://link.springer.com/chapter/10.1007%2F978-3-642-40885-4_22

② 鈴木翼, 青戸等人, 外山芳人,
永続性に基づく項書き換えシステムの合流性証明法,コンピュータソフトウェア, Vol.30, No.3, pp.148-162, 2013. 査読有

③ Takahito Aoto and Munehiro Iwami,
Termination of rule-based calculi for uniform semi-unification, In Proceedings of the 7th International Conference on Language and Automata Theory and Applications (LATA 2013), Bilbao, Spain, April 2013, pp.56-67, Lecture Notes in Computer Science, Vol.7810, Springer-Verlag. 査読有,
http://link.springer.com/chapter/10.1007%2F978-3-642-37064-9_7

④ 的場正樹, 青戸等人, 外山芳人,
片側減少ダイアグラム法による項書き換えシステムの可換性証明法,コンピュータソフトウェア, Vol.30, No.1, pp.187-202, 2013. 査読有

⑤ 高橋翔大, 青戸等人, 外山芳人,
ボトムアップ書き換えに基づく最内書き換え到達可能性判定,第 15 回プログラミングおよびプログラミング言語ワークショップ論文集, 2013. 査読有

⑥ 中嶋辰成, 青戸等人, 外山芳人,
書き換え帰納法に基づく帰納的定理の決定可能性,第 15 回プログラミングおよびプログラミング言語ワークショップ論文集, 2013. 査読有

⑦ Takahito Aoto and Jeroen Ketema,
Rational term rewriting revisited: decidability and confluence,
In Proceedings of the 6th International Conference on Graph Transformation (ICGT 2012), Bremen, Germany, September 2012, pp.172-186, Lecture Notes in Computer Science, Vol.7562, Springer-Verlag. 査読有,
http://link.springer.com/chapter/10.1007%2F978-3-642-33654-6_12

⑧ Takahito Aoto and Yoshihito Toyama,
A reduction-preserving completion for proving confluence of non-terminating term rewriting systems
Logical Methods in Computer Science, Vol.8, No.1:31, pp.1-29, 2012. 査読有,
http://www.lmcs-online.org/ojs/viewarticle.php?id=1099&layout=abstract

⑨ 岩見宗弘, 青戸等人,
無限項書き換えシステムにおける強頭部正規化可能性および一般生成性の自動反証,コンピュータソフトウェア, Vol.29, No.1, pp.211-239, 2012. 査読有

⑩ 磯部耕己, 青戸等人, 外山芳人,
多項式サイズ正規形を保証する項書き換えシステムの経路順序,
コンピュータソフトウェア, Vol.29, No.1, pp.176-190, 2012. 査読有

⑪ 的場正樹, 青戸等人, 外山芳人
片側減少ダイアグラム法による項書き換えシステムの可換性証明法, 第 14 回プログラミングおよびプログラミング言語ワークショップ論文集, pp.168-182, 2012. 査読有

⑫ 鈴木翼, 青戸等人, 外山芳人
永続性にもとづく項書き換えシステムの合流性証明,第 14 回プログラミングおよびプロ

グラミング言語ワークショップ論文集，pp.153-167，2012．査読有

⑬ Takahito Aoto，Toshiyuki Yamada and Yuki Chiba，
Natural inductive theorems for higher-order rewriting，In Proceedings of the 22nd International Conference on Rewriting Techniques and Applications (RTA 2011)，Novi Sad，Serbia，May/June 2011，pp.107-121，Leibniz International Proceedings in Informatics，Vol.10，Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik．査読有，http://drops.dagstuhl.de/opus/volltexte/2011/3111/

⑭ Takahito Aoto and Yoshihito Toyama，
Reduction-preserving completion for proving confluence of non-terminating term rewriting systems In Proceedings of the 22nd International Conference on Rewriting Techniques and Applications (RTA 2011)，Novi Sad，Serbia，May/June 2011，pp.91-106，Leibniz International Proceedings in Informatics，Vol.10，Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik．査読有，http://drops.dagstuhl.de/opus/volltexte/2011/3110/

⑮ 磯部耕己，青戸等人，外山芳人，
多項式サイズ正規形を保証する項書き換えシステムの経路順序,第13回プログラミングおよびプログラミング言語ワークショップ論文集，pp.99-113，2011．査読有

⑯ 村井正勝，青戸等人，外山芳人，
基底項書き換え系の多項式時間合流性判定法の改良,第13回プログラミングおよびプログラミング言語ワークショップ論文集，pp.84-98，2011．査読有

〔学会発表〕（計11件）
① 佐藤洸一，菊池健太郎，青戸等人，外山芳人，
自動検証のためのプログラム変換,日本ソフトウェア科学会第 30 回大会，PPL5-5，2013.9.13,東京

② 四方駿作，青戸等人，外山芳人，
閉包操作に基づく項書き換えシステムの到達可能性判定,日本ソフトウェア科学会第30回大会，PPL5-4，2013.9.13,東京

③ 内田和真，青戸等人，外山芳人，
永続性と減少ダイアグラム法に基づく合流性証明法，日本ソフトウェア科学会第 30 回大会，PPL4-1，2013.9.13,東京

④ Takahito Aoto，
Disproving confluence of term rewriting systems by interpretation and ordering (extended abstract),In Proceedings of the 2nd International Workshop on Confluence (IWC 2013)，Eindhoven，The Netherlands，June 28 ，2013，pp.5-9.

⑤ 椛澤涼，青戸等人，外山芳人，
木オートマトンに基づく項書き換えシステムの逆計算，日本ソフトウェア科学会第 29 回大会，3B-4，2012.8.22 ，東京

⑥ 高橋翔大，青戸等人，外山芳人，
ボトムアップ書き換えに基づく到達可能性の判定法，日本ソフトウェア科学会第 29 回大会，3B-3，2012.8.22 ，東京

⑦ 中嶋辰成，青戸等人，外山芳人，
書き換え帰納法に基づく帰納的定理の決定手続き，日本ソフトウェア科学会第 29 回大会，3B-2，2012.8.22 ，東京

⑧ Yuki Chiba and Takahito Aoto，
Transformations by templates for simply-typed term rewriting，In Proceedings of the 6th International Workshop on Higher-Order Rewriting (HOR 2012)，Nagoya，Japan，June 2．2012，pp.3-8.

⑨ 岩見宗弘，青戸等人，
無限項書き換えシステムにおける性質に関する考察，「代数と言語のアルゴリズムと計算理論」研究集会報告集，数理解析研究所講究録，Vol.1769，pp.153-157，京都大学数理解析研究所，2011.4.26

⑩ 的場正樹，青戸等人，外山芳人，
減少ダイアグラム法による項書き換えシステムの可換性証明法 ，日本ソフトウェア科学会第 28 回大会，1A-3，2011.9.27 ，那覇

⑪ 鈴木翼，青戸等人，外山芳人，
永続性にもとづく項書き換えシステムの合流性証明 ，日本ソフトウェア科学会第 28 回大会，1A-2，2011.9.27 ，那覇

〔図書〕（計0件）

〔産業財産権〕
○出願状況（計0件）

名称：
発明者：
権利者：
種類：
番号：
出願年月日：
国内外の別：

○取得状況（計０件）

名称：
発明者：
権利者：
種類：
番号：
取得年月日：
国内外の別：

〔その他〕
ホームページ等
http://www.nue.riec.tohoku.ac.jp/index-j.html

６．研究組織
(1)研究代表者
青戸　等人（AOTO TAKAHITO）
東北大学・電気通信研究所・准教授
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