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 ２８ 年　 ５ 月 １９ 日現在

機関番号：１１３０１
研究種目：基盤研究(C)（一般）
研究期間：2013～2015
課題番号：２５３３０００４

研究課題名（和文）合流性に基づくプログラム自動検証法の研究

研究課題名（英文）Research on automated program verification based on confluence

研究代表者
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

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理論は定理自動証明や計算モデルで広く利用されている。近年、項書き換えシステムの合流性自動証明システムがいくつか開発されているが、合流性自動証明システムの応用についてはほとんど研究されていない。本研究では、項書き換えシステムの合流性自動証明システムに基づくプログラム自動検証法を研究する。研究成果としては、永続性と型情報に基づく合流性判定、プログラム変換に基づく定理自動証明、名目書き換えシステムの合流性条件、木オートマトン完備化の停止条件、基底合流性の自動判定、整礎順序をもつモノイド上の抽象リダクションシステムなどがある。

研究成果の概要（英文）：The theory of term rewriting systems is widely used in the fields of automated theorem provings and computation models. Although several automated confluence provers of term rewriting systems have been developed recently, little work is reported on applications of them. This research aims to develop automated program verification methods based on automated confluence provers for term rewriting systems. Concrete results include confluence proving based on persistency and type information, automated inductive theorem proving based on program transformations, sufficient criteria for confluent nominal rewriting systems, a sufficient condition for termination of the tree automata completion, automated ground confluence proving, abstract reduction systems on ordered monoid.

研究分野：情報学

キーワード：項書き換えシステム　合流性　定理自動証明　自動検証

1. 研究開始当初の背景

項書き換えシステムの合流性の理論研究は、危険対解析に基づく合流条件の研究(Knuth-Bendix 1977, Huet 1980)を出発点として、多くの理論的成果が蓄積されてきた。しかし、これらの理論的成果に基づいた合流性自動判定システムの開発は、プログラム自動検証や定理自動証明への応用が期待されているにもかかわらず、その自動化の困難さからほとんど着手されていなかった。

申請者らは、世界初の合流性自動判定システム ACP を開発し、多くの例題の合流･非合流性の自動判定に成功した。さらに、この先行研究によって、モジュラ分解による分割統治法、減少ダイアグラム法、リダクション保存完備化法などの手法を組み合わせることで、強力な合流性自動判定が実現可能であることが明らかになった。

申請者らの ACP の成功がひとつの契機となって、現在いくつかの研究グループによる合流性自動判定システムの開発が進められている。また、合流性に関する国際ワークショップ(IWC 2012)では合流性自動判定システムの第1回コンペティションも開催され、ACP はこのコンペティションで優勝している。このように、合流性自動判定システムの本格的な開発は現在始まったところであり、それを利用したプログラム自動検証技術への期待は高い。

2. 研究の目的

本研究の目的は、項書き換えシステムの合流性自動判定に基づく新しいプログラム検証法を創出し、その理論的基礎を確立することである。さらに、申請者らが開発を進めている合流性自動判定システム ACP にその成果を反映させ、実験を通して合流性に基づく検証技術の有効性を明らかにする。本研究の具体的な課題は以下のとおりである。

(1)潜在帰納法と書き換え帰納法を融合することによって、合流性自動判定システムの利用を前提とした新しい帰納的定理自動証明法の基礎理論を構築し、プログラム検証のための基盤技術を確立する。

(2) プログラムの型情報やプログラム間の相互作用情報を、項書き換えシステムの永続性や可換性と対応させることで、プログラム検証に適した合流性判定法を開発する。

(3) 上記の成果に基づいて合流性自動判定システム ACP の開発を進め、ACP を利用したプログラム自動検証法の有効性を実験を通して明らかにする。

本研究によって、強力なプログラム検証手法の開発に成功すれば、プログラム自動検証や定理自動証明などの応用分野において、合流性自動判定に基づく新しい自動検証･証明技術の創出が期待できる。さらに、本研究が契機となって合流性自動判定システムの有効性が明らかになれば、これらの応用分野への波及効果だけではなく、項書き換えシステムの基礎理論に関しても大きな発展が予想される。

3. 研究の方法

本研究の目的は、項書き換えシステムの合流性自動判定システムに基づくプログラム検証法を提案し、その理論的基礎を確立するとともに、強力な自動検証システムを開発することである。このため、研究は以下の4フェーズを部分的に並行して進め、理論と実験の両面から自動判定法の有効性を明らかにする。

(i) 合流性自動判定システムに基づく帰納的定理証明法の構築

(ii) 型情報や相互作用情報を利用した合流性判定法の検討

(iii) 合流性に基づく検証システムの設計と実装

(iv)　実験システム上での実験と評価

なお、本研究を着実に進めるためには、先行研究で試作した合流性自動判定システム ACP の理論的成果と基盤技術を有効に活用して行くことが不可欠である。このため、全体の研究期間を3年間とし、平成25年度は先行研究の成果を新しい枠組みの中に整理統合する形で基礎理論の構築を進め、先行研究との連続性を確保す

る。平成26年度・27年度では、これらの研究成果を反映させることによって ACP を拡張し、新しいプログラム検証システムの実現を目指す。

4. 研究成果

(1) 項書き換えシステムの合流性自動判定システムの実装と改良を進めた。項書き換えシステムの永続性と型情報を利用した新しい合流性自動判定法を提案し、従来は困難であった減少ダイアグラム法による合流性判定が、非線型項書き換えシステムに対しても有効となることを明らかにした。さらに、さまざまな文献から抽出した例題をもちいて合流性自動判定の実験を行い、本判定システムの有効性を示した。

(2) 自動検証のためのプログラム変換法である文脈移動法と文脈分割法は、末尾再帰プログラムを自動検証に適した単純再帰プログラムへと変換する。この手法が、項書き換えシステムにおいても有効であるであることを理論的に明らかにした。さらに、帰納的定理の自動証明に対して文脈移動法と文脈分割法による自動変換が有効であることを実験をとおして示した。

(3) 高階プログラム自動検証の基礎理論の構築を目指し、束縛変数をもつ書き換えが可能である名目書き換えシステムの新しい形式化を行い、合流性を保証するための十分条件を危険対解析に基づいて明らかにするとともに、合流性自動判定システムの実装と実験を行った。

(4) 項書き換えシステムの到達可能性は合流性の解析や正規化戦略の解析などで重要であり、木オートマトンの完備化は到達可能性を解析するために広く用いられている手法である。書き換え規則間の左辺と右辺の重なりを解析することで、非左右重なり項書き換えシステムに対する完備化手続きが停止するための十分条件を与えた。この十分条件をみたす項書き換えシステムのクラスの到達可能性問題は決定可能である。

(5) 項書き換えシステムの基底合流性を、帰納的定理の自動証明法である書き換え帰納法に基づいて自動判定する新しい手法を提案するとともに、基底合流性自動判定システムを実装し、実験を通してその有効性を示した。

(6) 整礎順序をもつモノイド上での抽象リダクションシステムの理論を構築し、この理論が項書き換えシステムやラムダ計算などの正規化戦略の解析に極めて有効であることを明らかにした。

(7) 合流性に関する国際ワークショップ IWC における合流性自動判定システムのコンペティション(Coco 2013, 2014, 2015)において、本研究で開発を進めた ACP は第1位の成績で優勝した。

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 10 件)

[1] Takaki Suzuki, Kentaro Kikuchi, Takahito Aoto , 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, EPiC Series in Computing, Vol.39, pp.156-168, 2016 ,査読有

[2] Koichi Sato, Kentaro Kikuchi, Takahito Aoto , 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, Lecture Notes in Computer Science, Vol.9527, pp.331-345, 2015 ,査読有

[3] Takaki Suzuki, Kentaro Kikuchi, Takahito Aoto , 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, Leibniz International Proceedings in Informatics, Vol.36, pp.301-317, 2015 ,査読有

[4] 佐藤洸一, 菊池健太郎, 青戸等人, 外山芳人,
項書き換えシステムの変換を利用した帰納的定理自動証明, コンピュータソフトウェア, Vol.32, No.1, pp.179-193, 2015 ,査読有

[5] Takahito Aoto , Yoshihito Toyama ,

Kazumasa Uchida,
Proving confluence of term rewriting systems via persistency and decreasing diagrams, In Proceedings of Joint 25th International Conference on Rewriting Techniques and Applications and 12th International Conference on Typed Lambda Calculi and Applications (RTA-TLCA 2014), Vienna, Austria, LNCS 8560, pp.46-60, 2014 ,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, コンピュータソフトウェア, Vol.31, No.3, pp.294-306, 2014 ,査読有
〔7〕高橋翔大, 青戸等人, 外山芳人,
ボトムアップ最内項書き換えシステムの最内到達可能性, コンピュータソフトウェア, Vol.31, No.1, pp.75-89, 2014 ,査読有
〔8〕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, LNAI 8152, pp.311-326, 2013 ,査読有
〔9〕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, コンピュータソフトウェア, Vol.30, No.3, pp.148-162, 2013 ,査読有
〔10〕Takahito Aoto , 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, LNCS 7810, pp.56-67, 2013 ,査読有

〔学会発表〕(計 2 件)
〔1〕Takahito Aoto , Sorin Stratulat,
Decision procedures for proving inductive theorems without induction, 16th International Symposium on Principles and Practice of Declarative Programming (PPDP 2014), Canterbury, UK, September 8-10 , 2014 ,査読有
〔2〕Takahito Aoto,
Disproving confluence of term rewriting systems by interpretation and ordering (extended abstract), the 2nd International Workshop on Confluence (IWC 2013), Eindhoven, The Netherlands, 2013.6.28 ,査読有

〔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
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

(2)研究分担者
青戸 等人 (AOTO TAKAHITO)
新潟大学・自然科学系・教授
研究者番号: 00293390

(3)連携研究者
( )

研究者番号: