様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　元 年　 ５ 月 ２７ 日現在

機関番号：１１３０１
研究種目：基盤研究(C)（一般）
研究期間：2016～2018
課題番号：１６Ｋ００００９１

研究課題名（和文）文脈移動変換と高階書き換え理論に基づくプログラム検証法の研究

研究課題名（英文）Program Verification Methods based on Context-Moving Transformation and Higher-Order Rewriting Theory

研究代表者

菊池　健太郎（KIKUCHI, Kentaro）

東北大学・電気通信研究所・助教

研究者番号：４０３９６５２８

交付決定額（研究期間全体）：（直接経費）　　2,700,000円

研究成果の概要（和文）：書き換えシステムに基づく新しいプログラム検証手法を開発することを目的として研究を進めた。研究成果の概要は以下の通りである。
(1) 束縛変数を伴う書き換えシステムに対して、名目書き換えシステムと関連する体系における合流性の判定条件についての成果が得られた。また、高階の書き換え体系に対する合流性・停止性の自動判定システムの開発に参加し、国際競技会において良い成績を収めた。
(2) 文脈移動変換と関連する帰納的定理証明の手法に対して、十分完全性を持たない書き換えシステムにおける潜在帰納法についての考察から、無限リストのような計算が停止しない式を含むプログラムに適用可能な新しい検証手法を開発した。

研究成果の学術的意義や社会的意義
束縛変数を伴う書き換えシステムに対する合流性や停止性についての研究及びその成果は、従来の第一階項書き換えシステムに基づく帰納的定理証明手法である潜在帰納法および書き換え帰納法を、高階項に対する書き換えシステムに基づく手法へ拡張するにあたって重要になると考えられる。また、十分完全性を持たない書き換えシステムにおける潜在帰納法についての研究及びその成果は、入力によって計算が停止しない様々なプログラムに対する検証手法を開発するにあたって重要になると考えられる。これらの成果を利用したプログラム及びプログラミング言語に対する検証手法は、ソフトウェアの信頼性を向上させる技術として役立つことが期待できる。

研究成果の概要（英文）：We conducted research to develop new methods for program verification based on rewriting techniques. The main results of this research are summarised as follows:
(1) Concerning rewriting systems with variable binding, we obtained several new conditions on confluence of nominal rewriting systems and other related systems. Also, we have taken part in the development of automated confluence and termination provers for versions of higher-order rewriting systems, and achieved excellent results in international competitions.
(2) Through observations on inductionless induction methods in rewriting systems without the sufficient completeness property, we developed a new verification method that is applicable to programs including those expressions which induce non-terminating computation such as infinite lists.

研究分野：プログラム理論

キーワード：書き換えシステム　プログラム検証

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９、ＣＫ－１９（共通）

１．研究開始当初の背景

近年のセキュリティへの関心や深刻なシステムトラブルの頻繁な発生により、ソフトウェアの信頼性を向上させる技術や手法の重要性が認識されてきている。そのような技術や手法のうち、ソフトウェアが満たすべき性質を数学的に証明することによりその信頼性を保証しようとする形式手法の考え方は、徐々に普及している。本研究では、プログラムが満たすべき性質を数学的に証明することによってプログラムの正しさを保証することを目指すプログラム検証法を取り扱う。具体的には、関数型言語で書かれたプログラムの性質を、既存の証明支援系や代数仕様言語で記述した上で、帰納法を用いてその性質を証明する場合と類似の問題を取り上げる。

２．研究の目的

本研究では、定理自動証明や代数的仕様記述の分野で用いられてきた書き換えシステムに基づく検証手法を、プログラムおよびプログラミング言語の性質を証明するために適した方向へ拡張し、ソフトウェアの信頼性を向上させる技術として役立てることを目的としている。具体的には､文脈を操作するプログラム変換を利用した末尾再帰プログラムの性質の検証､および、束縛変数の利用を可能とした高階書き換えシステムに基づく検証、という二方向で従来の手法を拡張するための理論的基礎を構築する。また、拡張した手法を実際のプログラム例に適用することにより、その有効性を明らかにする。

３．研究の方法

本研究では、プログラムおよびプログラミング言語の性質の検証において困難をもたらすと考えられている(a)帰納法による証明における適切な補題の生成と(b)束縛変数を伴うシステムの性質の証明という二つの課題を、書き換えシステムに基づく手法を用いることで解決することを目指す。具体的には、以下のような方法で研究を進める。

(a)の課題に対しては､書き換えシステムにおける暗黙的帰納法による証明と文脈移動変換とを組み合わせ、プログラムの性質の検証の自動化により適した理論を構築する。研究代表者らが先行研究において取り扱った手法では、どのような評価戦略でも停止する性質(停止性)と、基底項が常に値まで評価される性質(十分完全性)を持つプログラムに対してのみ有効であったため、言語の操作的意味による違いは現れなかった。しかし、停止性や十分完全性を持たないプログラムに対しては、評価戦略や実行時エラーの有無が、変換の正当性に影響を与えるということが明らかになっている。本研究では、停止性や十分完全性を持たないプログラムに対する変換の正当性を定式化し、その条件を判定する手続きを、書き換え帰納法あるいは潜在帰納法を変更・拡張することによって与えることに取り組む。

(b)の課題に対しては､研究代表者らによる先行研究で得られている名目書き換えシステムに関する成果を発展させ、暗黙的帰納法に基づく検証のための理論的基礎を構築する。そのためには、危険対や合流性・停止性といった性質を解析する技術を発達させる必要がある。本研究では、名目書き換えシステムや関連する高階の書き換え体系についての先行研究の成果を整理・発展させて、必要となる理論の構築に取り組む。

４．研究成果

(1) 名目書き換えシステムについて研究代表者らの先行研究で得られていた合流性の判定基準を、危険対が存在する場合を含むクラスに対する基準に拡張した。具体的には、左線形項書き換えシステムに対する並列閉包定理とその一般化による合流条件を、左線形名目書き換えシステムに対する合流条件に拡張した。この条件は、α安定性を持たない名目書き換えシステムに対しても有効であるため、従来の束縛変数を伴う高階書き換えの枠組みでは取り扱えない例に対しても適用可能である。この拡張された判定基準を合流性自動判定システムに実装し、様々な具体例による合流性判定の実験を行うことにより、その有効性を確認した。また、この合流性自動判定システムにおいて危険対生成と交差性判定の際に使用されている同変名目単一化の手続きを、推論規則の形で整理した。これらの理論的洞察と実証実験において得られた合流性や危険対に関する知見は、従来の書き換えシステムに基づく定理証明手法である完備化や帰納的定理証明手法である書き換え帰納法および潜在帰納法を、束縛変数を伴う書き換えシステムに基づく手法へ拡張するにあたって重要になると考えられる。

(2) 一方、名目書き換えシステムのようにα同値性を明示的に扱うことはせず、α同値な項を同一視するような書き換えシステムの枠組みとその記述形式を提案し、分離並列簡約との強可換性を用いた合流条件を与えることを試みた。しかしながら、そのような枠組みにおいては書き換えシステムのクラスの条件を書き下すことが困難であることが分かり、合流条件の厳密な議論のためには名目書き換えシステムの枠組みのほうが優れているという知見が得られた。この経験から、実際に束縛変数を伴うシステムを記述するためには、型

付きラムダ項等を用いてαβη同値な項を同一視するような高階項による表現を利用することも有用であるという考えに至り、研究期間の最終年度には、群馬大学の浜名誠氏によって提案された高階の書き換え体系に対する合流性・停止性の自動判定システムである SOL システムの開発に携わった。SOL システムは、当該年度に開催された国際合流性競技会および国際停止性競技会の高階部門において、最も多くの自動証明数を獲得することができた。この開発を通じて得られた合流性や停止性に関する知見は、従来の第一階項書き換えシステムに基づく帰納的定理証明手法である潜在帰納法および書き換え帰納法を、高階関数や多相型を持つ高階項に対する書き換えシステムに基づく手法へ拡張するにあたって重要になると考えられる。

(3) プログラムを表す書き換えシステムの変換の一つである文脈移動変換においては、変換の正当性を保証するために文脈交換律などの特殊な等式が元の書き換えシステムの帰納的定理であることを証明する必要がある。研究代表者らの先行研究では、停止性や十分完全性を持たない書き換えシステムの変換の例について正当性を示しているが、その考え方を一般的な等式の帰納的定理の証明においても適用できないか検討した。帰納的定理の証明手法である潜在帰納法では、合流性と十分完全性が条件として必要であると考えられているが、本研究の検討の結果、十分完全性については全ての項に対してではなく証明すべき等式の両辺の項に対してのみ要求すればよいということが明らかになった。この知見を利用して拡張された潜在帰納法に基づく新しいプログラム検証手法を提案した。その有効性を確認するため、無限リストのような計算が停止しない式を部分的に含むプログラム例に適用する調査を行った。この調査では、遅延評価の関数型言語とプログラム変換に精通している芝浦工業大学の篠埜功氏と共同で作業を進めた。また、提案する検証手法を適用する際に必要となる「項に対する十分完全性」を判定する手続きの構築に研究分担者とともに取り組み、第一階項書き換えシステムの場合を対象として判定のための導出システムを考案した。

５．主な発表論文等

〔雑誌論文〕（計５件）

① Makoto Hamana and Kentaro Kikuchi, The System SOL version 2018, Proceedings of the 7th International Workshop on Confluence (IWC 2018), 70-70, 2018. 査読無
http://project-coco.uibk.ac.at/2018/papers/sol.pdf

② Kentaro Kikuchi, Takahito Aoto and Yoshihito Toyama, Parallel Closure Theorem for Left-Linear Nominal Rewriting Systems, Proceedings of the 11th International Symposium on Frontiers of Combining Systems (FroCoS 2017), LNAI 10483, 115-131, 2017. 査読有
DOI:10.1007/978-3-319-66167-4_7

③ Kentaro Kikuchi, Confluence by Strong Commutation with Disjoint Parallel Reduction, Preproceedings of the 4th International Workshop on Rewriting Techniques for Program Transformations and Evaluation (WPTE 2017), 2017. 査読有
https://www.cs.ox.ac.uk/conferences/fscd2017/preproceedings_unprotected/WPTE_Kikuchi.pdf

④ Takahito Aoto and Kentaro Kikuchi, Nominal Confluence Tool, Proceedings of the 8th International Joint Conference on Automated Reasoning (IJCAR 2016), LNAI 9706, 173-182, 2016. 査読有
DOI:10.1007/978-3-319-40229-1_12

⑤ Takahito Aoto and Kentaro Kikuchi, A Rule-Based Procedure for Equivariant Nominal Unification, Proceedings of the 8th International Workshop on Higher-Order Rewriting (HOR 2016), 2016. 査読有

〔学会発表〕（計２件）

① 菊池健太郎，篠埜功，無限のデータを含む等式に対する帰納的定理証明，日本ソフトウェア科学会第 35 回大会，2018 年.

② 伊藤佑太，菊池健太郎，外山芳人，完備化手続きにおける関数記号導入の戦略，平成 28 年度 電気関係学会東北支部連合大会，2016 年.

６．研究組織

(1)研究分担者

研究分担者氏名：青戸　等人

ローマ字氏名：(AOTO, Takahito)

所属研究機関名：新潟大学

部局名：自然科学系
職名：教授
研究者番号（8 桁）：00293390