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　３ 年　 ６ 月　 １ 日現在

機関番号：１３９０１
研究種目：基盤研究(C)（一般）
研究期間：2018～2020
課題番号：１８Ｋ１１１６１

研究課題名（和文）循環証明体系の証明論的分析

研究課題名（英文）Proof theoretic analysis of cyclic proof systems

研究代表者
中澤　巧爾（Nakazawa, Koji）

名古屋大学・情報学研究科・准教授

研究者番号：８０３６２５８１

交付決定額（研究期間全体）：（直接経費）　　3,100,000円

研究成果の概要（和文）：本研究では，帰納的に定義された述語を含む論理式に対する証明体系である循環証明体系に注目し，その基本性質であるカット除去可能性などの証明論的性質を調べた．主な成果は以下のとおりである．(1) プログラム検証に利用されている分離論理において，シンボリックヒープと呼ばれる論理式のクラスに対する循環証明体系ではカット除去ができない例があることを示した．(2) この循環証明体系において，カットをある種の部分論理式にまで制限しても証明能力が真に異なることを示した．(3) 分離論理の基盤論理であるbunched logicに対する循環証明体系でもカット除去ができない例があることを示した．

研究成果の学術的意義や社会的意義
循環証明体系は，帰納的述語を含む論理式の妥当性判定のために有用であり，とくに分離論理の循環証明体系はプログラミング検証の分野への応用が期待される．証明探索においてカット規則を適用するためには発見的な手法が必要である．このため，カット除去定理は証明探索のために期待される性質である．本研究の結果は，完全な証明体系のためにはカット規則が必要であることを示すものであり，証明探索の実現のためにはある種の制限が必要であるという理論的限界を明らかにするものである．

研究成果の概要（英文）：We investigate proof theoretic properties of cyclic proof systems, and we obtain the following results. (1) We show that the cut-elimination fails in the cyclic proof system for the symbolic heap separation logic. (2) We show that the restriction of the cut rule to extended subformulas of the bottom sequent in that system properly changes the provability. (3) We show that the cut-elimination fails in the cyclic proof system for the bunched logic.

研究分野：プログラミング言語理論

キーワード：分離論理　カット除去定理　循環証明

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

ソフトウェアの安全性を保証するための技術の一つであるプログラム解析は，プログラムの性質を静的に分析し，プログラムが目的に応じた良い性質をもつことを実行前に保証するものである．プログラム解析は大きな研究分野として確立し，理論的にも応用的にも多くの成果が得られている．

実際に利用されている基盤ソフトウェアの多くは，C 言語などの比較的低級な言語によって実装されており，これらのプログラムは明示的にヒープメモリ領域の操作を含む．このようなプログラムの検証は，ヒープ内のポインタ構造の自由さ故，非常に難しい問題として古くから取り組まれていたが，近年，Reynolds によって導入された分離論理をもとにしたプログラム論理を用いた手法が注目され，理論，実用ともに大きな成功を収めている．しかし，これまでに主に扱われていたのはその核の部分のみであり，現在もなお，様々な拡張や，さらなる理論的研究が活発に行なわれている．

多くのプログラムは繰返しの構造によって、リストや木などの繰返し構造をもつデータを扱う．このような，ヒープ内のポインタの繰返し構造を論理式で表現するためには，帰納的に定義された述語を用意する必要がある．このため，分離論理の帰納的述語による拡張を考えることは非常に重要である．Brotherston らによる循環証明体系は，このような一般の帰納的述語定義を含む分離論理式 のための証明体系である.彼らは，論理式の自動検証のために証明探索の手法を利用し，（Iosif らによる）モデル理論的手法と比較して高速に検証できるシステムを開発している．

２．研究の目的

本研究では，帰納的述語を含む論理式のための証明体系である循環証明体系の性質を明らかにすることを目的とする．とくに，分離論理を対象とする循環証明体系に注目し，この体系に関して，証明体系の基本的な性質であるカット除去定理を中心に考察する．さらに，それらの知見を分離論理に限らない他の論理に対する循環証明体系に適用し，一般の循環証明体系が持つ証明論的性質を明らかにすることを目的とする．

循環証明体系は，帰納的述語を含む論理式に対する妥当性判定のために有用であると考えられているが，循環証明体系における自動証明探索においてカット規則を適用するためには，カット論理式を発見的に求める必要がある．このため，カット除去定理は理論的な重要性のみならず，自動証明への応用のためにも期待される性質である．

３．研究の方法

本研究では，以下の方法で研究を行なった．

まず，循環証明体系ではカット除去定理が成立しないことが予想されていたため，カット除去定理が成立しないことを，反例を挙げることにより証明する．

この反例を参考にすることにより，適当な制限によってカット除去定理が成立する循環証明体系を構築すること，または，自動証明の妨げにならない程度にカット規則を制限することを目指す．

(1) 帰納的述語を制限することにより，カット除去が可能となる循環証明体系の構築を目指す．具体的には，述語定義節の形や，述語のアリティ（引数の数）を制限した循環証明体系におけるカット除去可能性を調べる．
(2) カット論理式の探索空間を，規則の結論の部分論理式に制限することができれば，自動証明探索の妨げにはならない．このため，カット論理式を（拡張された）部分論理式に制限したカット規則を考え，任意の証明可能な論理式が制限されたカットのみで証明可能（この性質を部分的カット除去定理と呼ぶ）であるかを調べる．

さらに，以上の結果を，分離論理以外の論理に対する循環証明体系に対して考察し，一般の循環証明体系に関する証明論的性質を調べる．具体的には，分離論理の基盤論理である bunched logic の循環証明体系について，カット除去可能性を調べる．

４．研究成果

主な研究成果は以下のとおりである．

(1) 分離論理の循環証明体系においてカット除去定理が不成立であることの証明：分離論理のうち，シンボリックヒープと呼ばれる論理式に対する循環証明体系においてカット除

去定理が成立しないことを証明した．シンボリックヒープは，プログラム検証への応用のためには充分であるとされる論理式のクラスである．本研究では，線型リストの断片を表す述語を 2 つの異なる方法で定義し，それらの間の同値性がカット規則を使わなければ証明できないことを示した．この成果をまとめた論文は，コンピュータソフトウェア誌に掲載された．

(2) 分離論理の循環証明体系におけるカット規則の制限に関する分析：(1)と同様の，シンボリックヒープの循環証明体系において，カット規則を，その結論式の（拡張）部分論理式に制限した体系を考え，制限されたカット規則が通常のカット規則より証明可能性の面で真に弱いことを示した．拡張部分論理式は，通常の部分論理式に加え，帰納的述語の展開を許す，非常に広いクラスであるが，その程度の制限でも証明可能性が真に異なることを明らかにした．この成果をまとめた論文は，国際会議 FLOPS2020 に採択された．

(3) bunched logic の循環証明体系においてカット除去定理が不成立であることの証明：分離論理の基盤論理である bunched logic の循環証明体系において，カット除去定理が成立しないことを証明した．bunched logic は，シンボリックヒープの証明体系に比べて構造規則と呼ばれる推論規則を持ち，このため，シンボリックヒープに対する証明をそのまま適用することはできない．このため本研究では，循環証明の展開による新たな手法を用いて bunched logic の場合のカット除去定理不成立を証明した．

(4) 述語のアリティ制限によるカット除去に関する分析：(3)の証明で与えた反例はアリティ 0 の帰納的述語のみからなるものであり，さらに，この証明はそのまま分離論理の場合に適用可能である．これにより，分離論理と bunched logic においては，帰納的述語のアリティを 0 に制限してもカット除去定理が成立しないことが示された．

５．主な発表論文等

〔雑誌論文〕　計2件（うち査読付論文　2件／うち国際共著　0件／うちオープンアクセス　1件）

１．著者名 KIMURA Daisuke、NAKAZAWA Koji、TERAUCHI Tachio、UNNO Hiroshi	４．巻 37
２．論文標題 Failure of Cut-Elimination in Cyclic Proofs of Separation Logic	５．発行年 2020年
３．雑誌名 コンピュータ ソフトウェア	６．最初と最後の頁 1_39～1_52
掲載論文のDOI（デジタルオブジェクト識別子） 10.11309/jssst.37.1_39	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Tatsuta Makoto、Nakazawa Koji、Kimura Daisuke	４．巻 11893
２．論文標題 Completeness of Cyclic Proofs for Symbolic Heaps with Inductive Definitions	５．発行年 2019年
３．雑誌名 LNCS (APLAS 2019)	６．最初と最後の頁 367～387
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-34175-6_19	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計6件（うち招待講演　1件／うち国際学会　1件）

１．発表者名 早乙女献自，中澤巧爾，木村大輔
２．発表標題 分離論理における記号ヒープのための循環証明体系におけるカットの制限について
３．学会等名 第22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(PPL2020)
４．発表年 2020年

１．発表者名 Daisuke Kimura, Koji Nakazawa, Tachio Terauchi, and Hiroshi Unno
２．発表標題 Failure of cut-elimination in cyclic proofs of separation logic
３．学会等名 第21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 (PPL2019)
４．発表年 2019年

１．発表者名
Koji Nakazawa, Makoto Tatsuta, and Daisuke Kimura

２．発表標題
Spatial factorization in cyclic-proof system for separation logic

３．学会等名
第21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（PPL2019）

４．発表年
2019年

１．発表者名
Koji Nakazawa, Daisuke Kimura, Tachio Terauchi, Hiroshi Unno, and Kenji Saotome

２．発表標題
On cut elimination in cyclic-proof systems

３．学会等名
3rd Workshop on Mathamatical Logic and Its Applications (MLA 2019)（国際学会）

４．発表年
2019年

１．発表者名
中澤巧爾

２．発表標題
プログラムの正しさを証明する---分離論理入門---

３．学会等名
日本数学会2019年度年会（招待講演）

４．発表年
2019年

１．発表者名
早乙女献自，中澤巧爾

２．発表標題
循環証明体系における準カット除去可能性について

３．学会等名
第21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（PPL2019）

４．発表年
2019年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究分担者	木村　大輔 (Kimura Daisuke) (90455197)	東邦大学・理学部・講師 (32661)	

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関