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　 ６ 月　 ３ 日現在

機関番号：１３３０２
研究種目：挑戦的萌芽研究
研究期間：2013～2015
課題番号：２５５４０００３

研究課題名（和文）形式証明の理論依存性解析とその計算可能証明発見への応用

研究課題名（英文）Dependecy analysis on formal proofs and its applications on discovery of computational proofs

研究代表者
小川　瑞史（Ogawa, Mizuhito）

北陸先端科学技術大学院大学・情報科学研究科・教授

研究者番号：４０３６２０２４

交付決定額（研究期間全体）：（直接経費）　　2,900,000円

研究成果の概要（和文）：古典的存在証明からの計算的意味の抽出について、未解決問題を含む決定問題の難問に対する証明構造のケーススタディを行った。「右線形かつ強無曖昧な項書換え系は合流性を持つ」(RTA open problem 58)は、可算選択公理を用いた停止順序の存在は証明できるが、具体的な順序の構成が困難なため未解決問題である。順序の構成条件の精査と、有限リダクショングラフによる構成的証明に基づき、二つの異なる新たな部分クラスに対し、肯定的結果を得た。また、最近、散見される決定問題の難問に対する二つのyes/noをそれぞれ決定する準アルゴリズムを並行させる証明手法について、一般化の考察を進めた。

研究成果の概要（英文）：The extraction of computational content from classical existence proof has been investigated by case study on difficult problems. One is an open problem in rewriting "a right-linear and strongly nonoverlapping term rewriting system is confluent" (RTA open problem 58). If confluent, the existence of a termination ordering is proved by the countable choice axiom. However, due to the difficulty of actual construction of the termination ordering, it remains still open. We showed positive answers to two new subclasses; one by investigating possible termination ordering structures, and another by a new method based on the finiteness of a reduction graph.
As an alternative to the extraction of computational content, we investigate recent decidability proofs consisting of two semi-algorithms, of which one tries to say "yes", and another tries to say "no". They work concurrently, and the result will be eventually found by either of them. Their generalization has been observed.

研究分野：形式手法

キーワード：形式証明　計算的意味　項書換え系　合流性　構成的証明

１．研究開始当初の背景

数理論理には古典的論理と構成的論理の二つの流れがあり、通常、数学者は前者を証明に用い、後者は証明と計算の対応から 20 世紀初頭に生まれた。数学者には、一般に背理法を用いた証明が短くエレガントという価値観がある。しかし背理法は、ときとして存在証明できるが、その具体的なインスタンスは計算不能という状況を生む。たとえば、直交項書換え系の最適書換えは存在するが、どのリデックスの書換えが最適書換えとなるか（最適戦略）は計算不能であることが知られている。また Graph Minor 定理により、広範なグラフ問題について $O(n^2)$アルゴリズムの存在を証明できるが、そのようなアルゴリズムはしばしばまだ知られていない。

本研究提案は、提案者の過去の Higman 補題に基づく時間概念を含むデータベース質問処理の線形時間アルゴリズムの計算可能証明に基づく導出（存在は証明されていたが、構成が知られていず、本提案者が Higman の補題の証明構造を精査することで導出法を示した。M.Ogawa, *A Linear Time Algorithm for Monadic Querying of Indefinite Data over Linearly Ordered Domains, Information and Computation* 186(2), pp.236-259, 2003）を実例として踏まえ、古典的証明から計算可能証明へ変換可能となる条件の探求をめざす。そのための証明解析の支援系として定理証明系 Isabelle/HOL 上での形式証明と、古典的推論の利用を自動検出する理論依存性解析ツールの実装をめざす。

当初のアイデアは、古典的証明を計算的意味（手続き）をもつ部分と、手続きの停止性証明の部分に分けて、前者の抽出を試みるものである。古典的証明と構成的証明の差は、たとえば排中律、背理法、選択公理などである。このうち、選択公理はしばしば Zorn の補題の形（古典的には等価）として停止性証明に用いられる。しかし、論理体系として計算的意味を含む証明の部分と、停止性証明の部分の二つを区別するのは困難であり、Higman の補題と Lovasz の補題を対象にしたケーススタディを想定した。特に、ケーススタディにおける証明構造を機械的に扱えるようにするため、定理証明系 Isabelle/HOL 上での形式証明およびその証明木上の操作ツールの実装を想定した。

２．研究の目的

アルゴリズムの存在証明が古典的論理によりなされても、アルゴリズムの構成が容易でない問題を対象として、古典的証明からの計算的意味の抽出を目的とする。

その際、計算的意味の抽出が可能なクラスを明確化するため、ノントリビアルな定理の証明を用いたアルゴリズムの存在証明を実例とし、証明構造の精査のケーススタディを行う。その際、証明構造を機械的に扱えるようにするため、定理証明系 Isabelle/HOL 上での形式証明およびその証明木上の操作ツールの実装をめざす。

当初のアイデアは、古典的証明を計算的意味（手続き）をもつ部分と、しばしば Zorn の補題を用いた手続きの停止性の証明の部分に分けて、前者の抽出を試みるものである。論理体系として上記二つを区別する困難は予想されていたが、手続き的切り分けの一般化すら、予想以上に困難であった。また証明解析ツールの実装も、定理証明系 Isabelle/HOL の実装の内部の詳細に立ち入る必要があるなどの予想以上の工学的困難が山積した。

そのため、その別アプローチとして、yes/no をそれぞれ判定する二つの準アルゴリズム（停止性が保証されない手続き）を並行して実行する決定性問題の証明手法について、その証明構造と一般化もあわせて考察する。

３．研究の方法

当初のアイデアは、古典的証明を計算的意味（手続き）をもつ部分と、しばしば Zorn の補題を用いた手続きの停止性の証明の部分に分けて、前者の抽出を試みるものであった。これは構成的証明が、手続きの停止性まで構成的証明を要求し、Zorn の補題（古典的には選択公理と等価）を用いている場合、容易ではないと予想されたためである。しかし、論理体系として上記二つを区別するのは困難であり、そのため Higman の補題や Lovasz の補題などのケーススタディを進めることを当初の方針とした。特に、証明構造を機械的に扱えるようにするため、定理証明系 Isabelle/HOL 上での形式証明およびその証明木上の操作ツールの実装をめざした。（学生雇用 1 名）

しかしながら、定理証明系の習得は容易ではなく、また証明木を取り出す実装は非標準な使い方のため、定理証明系内部の実装の詳細を調査する必要があり、進捗が遅れた。そのためツール実装は延期し、項書換え系の未解決問題、および近年、いくつかの決定性問題に対する yes/no をそれぞれ判定する二つの準アルゴリズム（停止性が保証されない手続き）を並行する手法などについて、証明手法の構造を理論的に明らかにすることを先行した。

対象とした項書換え系の未解決問題は、「右線形かつ強無曖昧な項書換え系は合流性を持つ」(RTA open problem 58)、および近年、決定性証明の難問に対し、yes/no をそれぞれ判定する二つの準アルゴリズム（停止性が保証されない手続き）を並行して実行する手法である。

これらに対する基本的な研究の方法は、前者については、主にリダクショングラフの健全な操作法の精査と、リダクショングラフの有限性を保つための不変条件の発見である。

後者については、３つの実例

(a) ペトリネットの到達可能性
J.Leroux. *Vector addition system reachability problem: A short self-contained proof,* 第38回ACMプログラミング言語の原理国際会議 (POPL), pp.307-316, 2011
(b) Normed BPAのbranching bisimulation
Y.Fu. *Checking equality and regularity for normed BPA with silent moves,* 第40回オートマトン、言語とプログラミング国際コロキウム (ICALP), Springer-Verlag LNCS 7966, pp.238-249, 2013
(c) 決定性トップダウン木-文字列変換器の等価性
H.Seidl, S.Maneth, G.Kemper. *Equivalence of deterministic top-down tree-to-string transducers is decidable,* 第56回 IEEE 計算機科学の基礎国際会議 (FOCS), pp.943-962, 2015.
の精査による証明構造の一般化であり、やはり適切な不変条件の発見がキーとなっている。

４．研究成果

対象とした項書換え系の未解決問題は、「右線形かつ強無曖昧な項書換え系は合流性を持つ」(RTA open problem 58)である。合流性の標準的証明法は、書換え列のピーク除去の際、減少するwell-foundedな順序の発見である。Vincent van Oostromが提案したdecreasing diagramでは、合流性が成り立つ場合、必ずそのような順序が存在することは証明できる（可算選択公理を利用）が、順序の構成は容易ではない。これに対し、従来手法の順序設計の拡張に基づく部分的解決（学会発表(2)）および、新たなリダクショングラフの提案に基づく構成的証明手法による部分的解決（学会発表(3,4)）を得た。特に後者のリダクショングラフは、合流性を考える際、始状態となる書換え列が与えられたとき、その合流性をもつ部分列から帰納的に合流可能な書換え関係のグラフの拡大を図る。この際、必要となる書換え関係は局所的であり、有限グラフの範囲で構成可能である点が証明のポイントである。その結果、「弱浅かつ強無曖昧な項書換え系は合流性を持つ」を示した。

もう一つの対象とした問題は、近年、いくつかの未解決問題および複雑な決定性証明の簡単化として、yes/noをそれぞれ判定する二つの準アルゴリズム（停止性が保証されない手続き）を並行して実行する手法が提案されている。この例は、
(a) ペトリネットの到達可能性 (2011年)
(b) normed BPAのbranching bisimulation（2013年）
(c) 決定性トップダウン木-文字列変換器の等価性（2015年）
などである。これらは、noの場合には不変式が存在することを証明した上、yes判定の準アルゴリズムは比較的単純な探索によるyesの証拠の探索、no判定の準アルゴリズムは不変式の探索と設定する。

たとえば、(a) ペトリネットの到達可能性では、始点から終点が到達可能な場合には、順次、遷移列を網羅的に探索することで実際の到達可能な遷移列が構成される。始点から終点が到達不能な場合は、プレスバーガー算術式が不変式として存在し、始点から到達可能な状態集合と、終点に到達可能な状態集合を分割可能なことが証明される。そのため到達不能な場合は、プレスバーガー算術式を網羅的に探索することで、具体的な分割法が示される。

また、別の例として、(c) 決定性トップダウン木-文字列変換器の等価性判定の場合は、等価でない場合は異なる結果を返す入力の網羅的探索に帰着する。等価な場合には、等価性を表現する再帰関係を満たす多項式環のイデアルで極大なものの存在が証明でき、不変式の候補として、そのようなイデアルを網羅的に探索に帰着する。特に、多項式環のイデアルは有限生成なので、イデアルは枚挙可能であり、準アルゴリズムが構成される。

これらの例は、古典的証明の計算的意味とその停止性証明の切り分けと異なり、不変式の（古典的）存在証明による異なるアプローチの可能性を見せている（学会発表(1)）。

本研究提案では、当初計画と異なる方向に進展しているが、本研究予算終了後も上記の二つの準アルゴリズムによる手法、さらに延期していた定理証明系 Isabelle/HOL による Lovasz の補題の形式証明（Higman の補題については連携研究者の C.Sternagel らが Open induction 形式証明ライブラリを用いて形式証明を行った）などを継続する予定である。

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 0 件）

〔学会発表〕（計 4 件）

(1) Mizuhito Ogawa. Decidability by two semi-algorithms. 第5回証明・計算・計算量国際ワークショップ（2016年5月5日、ミュンヘン大学、ミュンヘン、ドイツ）（査読なし、口頭発表）
(2) Jiaxiang Liu, Jean-Pierre Jouannaud, Mizuhito Ogawa. Confluence of Layered Rewrite Systems. 第24回計算機科学論理国際会議（CSL2015），（2015年9月9日、ベルリン工科大学、ベルリン、ドイツ）LIPICS Vol.41, pp.423-440.（査読有）
(3) Masahiko Sakai, Michio Oyamaguchi, Mizuhito Ogawa. Non-E-Overlapping, Weakly Shallow, and Non-Collapsing TRSs are Confluent. 第25回自動推論国際会議

(CADE-25), （2015 年 8 月 4 日、ベルリン自由大学、ベルリン、ドイツ）Springer-Verlag LNAI 9195, pp.111-126.（査読有）
（4）Masahiko Sakai, Michio Oyamaguchi, Mizuhito Ogawa. Non-E-Overlapping and Weakly Shallow TRSs are Confluent. 第 3 回合流性国際ワークショップ（IWC2014）.（2014 年 7 月 13 日、ウィーン工科大学、ウィーン、オーストリア）（査読なし、口頭発表）

〔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
定理証明系 Isabelle/HOL 形式証明アーカイブ Open Induction
http://www.isa-afp.org/devel-entries/Open_Induction.shtml

６．研究組織
(1)研究代表者　小川 瑞史（OGAWA MIZUHITO）
　北陸先端科学技術大学院大学 情報科学研究科・教授
　研究者番号：40362024

(2)研究分担者
（　　）
　研究者番号：

(3)連携研究者
（　　）
　研究者番号：

(4) 研 究 協 力 者　Christian Sternagel (Christian Sternagel)
　インスブルック大学・ポスドク