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 １７ 日現在

機関番号：１０１０１
研究種目：基盤研究(C)（一般）
研究期間：2016～2018
課題番号：１６Ｋ００００９０

研究課題名（和文）代数的ソフトウェア向き多重文脈型推論基盤システムによる帰納的定理の発見と証明

研究課題名（英文）Discovery and proof of inductive theorems with multi-context reasoning systems for algebraic software

研究代表者

栗原　正仁（Kurihara, Masahito）

北海道大学・情報科学研究科・教授

研究者番号：５０１３３７０７

交付決定額（研究期間全体）：（直接経費）　　3,700,000円

研究成果の概要（和文）：本研究は，多重文脈型推論システムと呼ばれる新しい考え方のシステム構造を用いて，計算機科学および計算機工学において重要な役割を果たす帰納的定理と呼ばれる種類の数学的定理の発見や証明を自動的かつ効率的に行う技術を開発することを全体構想とし，その目的を達成するため，主定理を証明する際に必要となる補助定理を自動的に生成するためのトップダウン的及びボトムアップ的な新しい方法に基づいて総合的に検討を行い，システムの開発を行うとともに，応用として想定されるソフトウェア工学における代数的ソフトウェアの正しさの検証の分野において適用可能であることを実証的に確認したものである。

研究成果の学術的意義や社会的意義
ソフトウェア工学の理論的基礎分野では，作成したソフトウェアの正しさを機械的に確認する技術が重要視されている。そのため代数的にソフトウェアの仕様を記述して実装する技術が考案されており，そこではソフトウェアの正しさを数学的な帰納的定理の証明に帰着させ，それを計算機により自動的に証明するアプローチを採っている。本研究成果はそのような技術開発に対して有益な知見を提供する点に学術的意義があるとともに，最終的にはソフトウェアの正しさの保証を通じて，安心・安全な情報社会の実現に寄与し得る点に社会的意義が認められる。

研究成果の概要（英文）：This research project uses new ideas of system structure called the multi-context reasoning system to apply them to the grand plan to develop technologies for automatic, efficient discovery and proof of a kind of mathematical theorems called inductive theorems, which play important roles in computer science and technology. To attain this purpose, we have developed software systems with new top-down and bottom-up methods for automatic generation of lemmas required in the proof of the main theorems. In addition, we have empirically shown the applicability of this technology in the field of the verification of correctness of algebraic software in software engineering.

研究分野：ソフトウェア科学

キーワード：帰納的定理　定理自動証明　定理自動発見　補題生成　多重文脈型推論　代数的ソフトウェア　項書換え系

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９、ＣＫ－１９（共通）

１．研究開始当初の背景

(1) 非決定的な計算プロセスにおいて，計算開始時点及びそれ以降に遭遇する一連の非決定的選択点で行った選択の列を，そのプロセスの文脈と呼ぶ。正しい選択を行って非決定的な計算を成功に導くことは一般には容易ではないが，多くの研究者は，何らかのパラメータや戦略を事前に多大な手作業による試行錯誤やトリッキーな方法により設定することによって，プロセスから非決定性の多くを排除し，計算を「成功」に導いている。しかし，その「成功」の陰には，多くの「不適切な設定」と「失敗」の累積があることを我々は真摯に認識すべき状況であった。

(2) 単純な計算システムにおいては，１つの文脈において失敗すれば，計算を後戻りさせて他の文脈を試みさせればよい。しかし，複雑なシステムは，多くの場合，半アルゴリズムとなっていて，必ずしも成功にも失敗にも至らず，停止しないで限りなく計算を続行するため，そもそも後戻りができない。したがって，プロセスの分岐による並行計算（又はそれを模擬する逐次計算）が必要とされるが，素朴な実装を行えば，多くの場合，プロセスの数が指数関数的に膨大となり，現実的なシステムを構築することは困難であった。

(3) 本研究代表者はこれまで，その研究の全体構想の中で，類似した文脈をもつプロセス間には，通常，同一の計算・推論の処理が多数共通に存在するという経験的な知見に基づき，それら多数の計算・推論を，１つのプロセス内でまとめて行う推論システムを開発してきた。そのようなシステムでは，平均的な計算量が指数オーダであるにしても，指数関数の基数を小さくして，より大きなサイズの問題まで現実的に扱うことができる。１つのプロセス内で多くの並行プロセスの推論を効率良く模擬実行するこのようなシステムを，多重文脈型推論システムと呼ぶ。

(4) 上記のような問題意識と技術基盤のもと，本研究代表者は，代数的な基盤の上に構築されたソフトウェアに関する計算・推論の分野（項書換え系）に焦点をしぼり，関数記号と変数を用いて構成される項の対「項＝項」である等式や，それを左から右（又はその逆）の方向に向き付けた「項→項」の形をした書換え規則に関わる推論（停止性検証，完備化，定理証明等）を取り扱う多重文脈型推論システムの研究開発を進めていた。たとえば，完備化の推論では，等式を向き付けて停止性が保証される書換え規則を生成する際に，左辺と右辺の項の大小比較に用いる半順序関係を文脈としてモデル化していた。

２．研究の目的

(1) 本研究は，多重文脈型推論システムを用いて，帰納的定理の発見や証明を自動的かつ効率的に行う技術を開発することを全体構想としている。帰納的定理とは，自然数や構造データ等の集合及びそれに関連する演算（モデル）に関して成り立つ言明で，通常は数学的帰納法またはその拡張を用いて証明される。ソフトウェアの分野では再帰や反復と直接関係する重要な研究対象であり，応用の１つとして，わかりやすいが効率の悪いプログラムと，効率は良いがわかりにくいプログラムの両者が，互いに等価であることを帰納的定理として証明して，プログラムの正しさを検証するものがある。この構想のもとで，本研究課題では，特に補助定理（補題）の自動生成をできるだけ効果的に行うことをその目的としている。実際，本研究代表者は，2010 年に公表した論文（電子情報通信学会論文賞受賞）において，多重文脈型推論を帰納的定理証明に応用し，標準問題 69 題のうち 36 題を現実的な時間内で解けることを報告したが，一方，このシステムで解けない 33 題の問題について分析を進めた結果，その限界の原因はシステムに補助定理の生成能力が欠けている点にあることがわかったためである。補助定理は，主定理を証明するために必要な補助的な言明であり，発見的に仮説として生成し，それを証明した上で，主定理の証明で用いられる。

(2) 本研究課題のもう１つの目的はその応用可能性の検証である。項書換え系の理論と技術は，計算機プログラムを代数的に記述するためのプログラミング言語およびプログラミング支援システムの基礎となっている。そのため，上記目的で開発した技術がそのような応用分野において，特に代数的ソフトウェアの正しさの検証に適用可能かどうかを検証することを目的としている。たとえば，上述したように，わかりやすいが効率の悪い代数的プログラムと，効率は良いがわかりにくい代数的プログラムの両者が，互いに等価であることを帰納的定理として証明して，プログラムの正しさを検証するものがその一例である。

３．研究の方法

(1) 本研究の目的を達成するため，補助定理自動生成のための各種方法（トップダウン的な方法，ボトムアップ的な方法）の要素技術の状況を踏まえた上で，多重文脈型推論システム内で総合化して帰納的定理の自動証明システムを設計・実装するほか，応用分野であるプログラム検証の分野に特有の調査研究を踏まえて評価・改善を行うことが欠かせない。そこで本研究では，およそこの順次性に基づいて，要素技術の調査とシステムの計画，システムの設計・実装，及び応用分野の調査とシステムの評価・改善，の 3 ステップに基づく研究の方法を採った。補

助定理の仮説生成方法は種々提案されているが，大きく分類すると，トップダウン的な方法とボトムアップ的な方法に分けられる。本研究は，その両方について総合的に検討を行う方法を採った。

(2) トップダウン的な方法は，主定理を構文的に拡張したり論理的に分析したりして，補助定理となりそうな仮説を生成するもので，あくまでも証明したい主定理に基礎を置く点でゴール指向である。この方法はさらに健全な方法か否かで２つに分類できる。健全な仮説生成法は，主定理が実際に定理であるならば証明可能である（正しい）仮説のみを生成する手法である。証明可能な仮説を生成するので，システムの実行時負荷を軽減するが，その反面，仮説生成能力に限界がある。一方，健全ではない仮説生成法は，「いちかばちか」で正しさの保証はないが有用な仮説を生成しようとする方法である。証明不可能な仮説を生成するので，システムに大きな実行時負荷を与えるが，その反面，仮説生成能力に優れている。本研究はこれまで証明できなかった問題の証明に成功することを目的としているので，後者のアプローチを採った。

(3) ボトムアップ的な方法は，主定理とは無関係に，事前に公理として与えられた理論体系（背景知識）で成り立つ様々な定理を自動生成しようとする。生成された定理のうち有用そうなものをデータベースに登録しておけば，その一部を補助定理として主定理を証明できるかもしれないという立場をとる。ある種の伝統的な論理体系では，完全性をもつ推論規則を公理につぎつぎと適用していけばすべての定理を生成できることがあるが，帰納的定理証明の分野ではそのようなことはできず，「定理自動発見」とも呼ばれるほどに発見的な方法がとられる。この方法は，システムに極めて大きな実行時負荷を与えるが，仮説生成能力が極めて高く，計算機の CPU 速度の向上と記憶容量の拡大にも支えられ，ここ 10 年くらいの間に立ち上がった後，急速に発展してきているが，まだまだ課題も多い。本研究では，これまで十分に調査してこなかったこの新しい技術についても調査を行い，その特徴を整理し，書換え帰納法と呼ばれる既存方法との組み合わせに基づく新しい方法について検討を行うこととした。

４．研究成果

(1) トップダウン的な方法については，既存の発散鑑定法を拡張した新しい補助定理自動生成方法 Peripheral Sculpture を提案した。この方法は，推論によって等式の無限列と思われるものが生成されたとき，その列を構成する隣接する等式の差分を分析し，そこから周辺部(peripheral part)と静穏部(calm part)と呼ばれる部分を抽出し，前者に現れる変数名を新しい名前に一般化することによって補助定理の仮説を生成する。この方法を既存の方法 Joining と組み合わせることにより，前述したこれまで解けなかった 33 題の問題のうち新たに 18 題を自動的に解くことができた。

(2) 上で述べた成果の裏には，さらに今回開発した多重文脈型推論システムの存在がある。本研究では，そのアイデアを学術的に明確に示すため，それを Multi-context Postulate と名付けた推論規則として論理学的に厳密に提示し，それに基づいてシステムを実装した。この推論規則の基本的な考え方は，補助定理の候補となる仮説が複数個（n 個）生成されたとき，システムは n+1 個のプロセスに分岐し，そのうち n 個のプロセスはそれぞれ１個の仮説を採用して推論を進め，残りの１個のプロセスはどの仮説も採用せずにこれまでの推論を進めることにある。前半の各１個のみ採用するプロセスは，健全でない仮説生成法が生成する多数の仮説のうちとりあえず１つだけを採用することにより，計算効率の悪化を最小に留めている。また後半の１つも採用しないプロセスは，健全でない仮説生成法が生成する誤った仮説の採用を防ぐ役割をもっている。多重文脈型推論システムでは，プロセスの数がこのように n+1 倍になっても，計算時間の増大は一般にそれよりはるかに小さく抑えられる傾向があり，効率良く推論が行われる。特に，注目すべき点は，(1)で述べた２つの方法（Peripheral Sculpture と Joining）を組み合わせても，計算時間は前者のみで実行した時間＋後者のみで実行した時間よりも少なくて済むことがある点であり，これも多重文脈型推論システムから得られる利点の一つである。

(3) 開発した技術が代数的ソフトウェアの正しさの検証の分野において適用可能であることを実験によって確認した。具体的には，(1)で述べた 33 題の問題にはすでにそのような分野を想定したものが含まれているほか，それとは別にその分野に含まれる問題群についても実験を行い，適切に効率良く問題が解かれることを確認した。これらの研究成果は電子情報通信学会の英文論文誌（2019 年 2 月）において公表した。

(4) 上記の研究成果はさらに一般的に議論することができる。そこで，本研究及びそれに関連する一連の研究の成果を，より一般的でわかりやすい言葉を用いて総括し，国際会議（WCECS 2018）において発表を行うことにより，この分野の研究者にアイデアの原理やその意義等について広く啓発を行った。特に，(2)で述べた Multi-context Postulate は，本研究で示した枠組みの特殊形として理解できる。このような特殊形は他にも有用そうな種々のものが考えられ，今後の検討の方向性として参考になる。

(5) ボトムアップ的な方法については，書換え帰納法とボトムアップ手法の組合せにより，補助定理自動生成方法をより効果的にする方法を考案した。この方法は優れた既存方法のうちの一つである HipSpec に対して幾つかの工夫を施したものである。第一の工夫は，生成される仮説集合の大きさを抑制するために，ある仮説が等式の単純化(simplify)のために適用可能なときに，その仮説をその場で動的に証明し，証明された場合には，それを直ちに補助定理として採用する点にある。第二の工夫は，多くの仮説は他の仮説の特殊形になっていることから，そのような冗長な仮説を検出して除去する点にある。第三の工夫は，等式（l=r）を向き付ける方向が２つ（l→r，r→l）あるために生成される仮説の数が増えることを抑制するために，向き付けを制限する４つの条件として，①定義記号の減少性，②定義記号下の構成子記号の減少性，③定義記号の抑制的分配性，及び④右結合優先性を導入し，これらのいずれかを満たすときにのみ l→r への向き付けを許す点にある。これらの成果は国際会議（SMC 2016）において公表した。

(6) さらにボトムアップ的な方法の今後の方向性に関する議論として，構文的に複雑で通常はその生成を抑制したいと考えられる仮説であっても，それを採用して補助定理とすることによって，主定理を効果的に証明できる複数の事例を示し，それらへの対応策を今後の課題として提示した。これまでの技術は論理式（等式）の複雑性を構文的な観点から定義し，複雑な等式の生成を抑制するヒューリスティックスを採ることにより，現実的な時間で推論に成功してきているが，本研究では，そのアプローチではうまくいかない重要な事例を示しており，今後の研究課題とその解決の方向性を示唆している。この成果については国際会議（IMECS 2018）において公表した。

５．主な発表論文等

〔雑誌論文〕（計１件）

① Chengcheng Ji, Masahito Kurihara, Haruhiko Sato, Multi-context automated lemma generation for term rewriting induction with divergence detection, IEICE Transactions on Information and Systems, 査読有, Vol. E102-D, No. 2, 2019, pp. 223－238
DOI: https://doi.org/10.1587/transinf.2017EDP7368

〔学会発表〕（計３件）

① Masahito Kurihara, Haruhiko Sato, ChengCheng Ji, Automated proof and discovery of inductive theorems with rewriting induction over multi-context reasoning systems: state-of-the-art technologies and perspectives, World Congress on Engineering and Computer Science 2018 (WCECS 2018), 2018
② Haruhiko Sato, Masahito Kurihara, On usefulness of syntactically complex lemmas in theory exploration for inductive theorems, International MultiConference of Engineers and Computer Scientists 2018 (IMECS 2018), 2018
③ Haruhiko Sato, Masahito Kurihara, Discovering inductive theorems using rewriting induction, 2016 IEEE International Conference on Systems, Man, and Cybernetics (SMC 2016), 2016

〔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：
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：

国内外の別：

〔その他〕
ホームページ等
http://kussharo.complex.ist.hokudai.ac.jp

６．研究組織
(1)研究分担者
研究分担者氏名：

ローマ字氏名：

所属研究機関名：

部局名：

職名：
研究者番号（8 桁）：

(2)研究協力者
研究協力者氏名：佐藤 晴彦
ローマ字氏名：Haruhiko Sato