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 ２０ 日現在

機関番号：１０１０１
研究種目：基盤研究(C)（一般）
研究期間：2013～2015
課題番号：２５３３００７４

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証明とその応用

研究課題名（英文）Inductive theorem proving and its application 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）　　3,900,000円

研究成果の概要（和文）：　並列計算機上で多重文脈型推論基盤システムを開発し，停止性検証，完備化，帰納的定理証明を効率良く実行するシステムを開発した。代数的ソフトウェアの正しさの検証に関わる標準的なベンチマーク問題について，従前よりも文脈を適切に探索して推論に成功することと，従前のシステムでは解けなかった問題が，補助定理を自動生成することで解けることを確認した。
　探索に関わる人工知能技術とヒューリスティクスを組み合わせることによって，本システムの重要部分である停止性自動検証の並列計算機上での実装技術を開発し，効率を向上させた。また，プログラミング言語SCALAのもつ遅延評価機構を用いて，システムの実行効率を改善した。

研究成果の概要（英文）：Multi-context reasoning systems which execute termination verification, completion, and inductive theorem proving efficiently on parallel computers have been developed. Based on standard benchmark problems on the verification of correctness of algebraic software, it has been verified that the systems succeeded in the reasoning by finding more appropriate contexts than the previous systems and, by automatically generating useful lemmas, could solve the problems which had been unsolved before. By combining heuristics and artificial intelligence technology on searching, implementation techniques of automated termination verification on parallel computers have been developed. By using the lazy evaluation mechanism of the programming language SCALA, the efficiency of the execution of the systems has been improved.

研究分野：ソフトウェア

キーワード：項書換え系　帰納的定理自動証明　多重文脈推論　代数的ソフトウェア　代数的仕様記述　システム形式検証

１．研究開始当初の背景

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適切に（しばしば，トリッキーに）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し，その解決を図るための普遍性の高い技術について研究を行うべきである。

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となる。

このような問題を解決するために，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ような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」の推論システムと呼んでいる。

具体的には，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きている。主として完備化と呼ばれる推論システムを扱い，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構造を「文脈」としてモデル化している。

(1) アイデアの原型は 1999 年に J. of Automated Reasoning に公表した本研究代表者の論文に見られる。ここでは s, t を項，L1, L2, L3 を文脈の集合とするとき，ノードと呼ばれるデータ構造<s：t, L1,L2,L3 >を導入し，L1(L2)に属する文脈の下では書換え規則 s→t (t →s)が，L3 に属する文脈の下では等式 s＝t がデータベース中に存在すると解釈し，文脈集合の和・差・積などのメタ操作をベースレベル推論と組み合わせることで，ノード集合に対する推論システムを構築している。

(2) 2004 年には人工知能学会論文誌において最初の飛躍的成果を公表した。そこでは文脈の集合を f>g 等の原始命題を組み合わせた 1 つの論理関数として表現し，それを二分決定グラフ（BDD）によりコンパクトに実装した。さらに，2006 年の電子情報通信学会論文誌においては，適用可能な停止性のクラスを広げて文脈の数が指数関数的に 10～50 倍に増加しているのに対し，実行時間は 1%程度しか増加しないことを実証した。

(3) 2009 年の新たな飛躍的成果（電子情報通信学会英文論文誌）においては，文脈を動的に生成・更新できるようにシステムを拡張し，任意の停止性証明器を動的に起動して，等式の向き付け方向（左から右，その逆，又はその両方）を文脈として動的に追加することにより，システムの機能と性能を格段に向上させた。実際，世界最高水準の停止性証明器開発技術をもつインスブルック大学のチームと共同で実装したシステムは，この分野で最も権威ある国際会議の１つ(IJCAR)において「システム開発論文」に採択され，口頭発表とデモンストレーションを行った。

(4) 2012 年にはこの技術をさらに最適化して包括的に議論した論文を J. of Automated Reasoning に公表した。また，多重文脈型推論処理ができない「任意の停止性証明器を用いて多数の停止性証明を行う」というボトルネック部分を，マルチコア CPU を用いて並列実装し，実行速度を 10 倍以上に向上させた。

(5)この完備化の枠組みは，帰納的定理の自動証明にも応用することができる。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。

(6)2010 年に，研究代表者らは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 35 題を現実的な時間内で解くこと

ができた研究成果は電子情報通信学会論文賞を受賞した。

(7)その後，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（補題）と呼ばれる仮説の生成能力が欠けている点にあることがわかった。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，主定理の証明のために用いるものである。そこで本研究では，補助定理の自動生成技術を多重文脈型推論システムに組み込むことにより，帰納的定理の自動証明能力を格段に強化したいと考えるに至った。

２．研究の目的

(1) 文脈（計算開始から現時点までに行った選択の列）が互いに類似した非決定性並行プロセス間には，多くの場合，同一の計算・推論の処理が多数共通に存在する。本研究は，それらを共通に処理することによってシステム性能を飛躍的に高めることを狙った「多重文脈型推論」の基盤を開発するという全体構想の中で，補助定理を自動生成して帰納的定理の自動証明を行う多重文脈型推論システムを開発すること，及びそれを代数的ソフトウェアの正しさの検証に応用してその可用性を高めることを目的とする。

(2) 具体的には，ソフトウェア工学と人工知能の境界領域内の「項書換え系」として知られる代数的ソフトウェアに関する研究分野を中心として，等式や書換え規則に関わる推論（停止性検証，完備化，定理証明等）を取り扱うシステムの研究開発を進める。様々な人工知能技術とヒューリスティックスを使い，基礎から実装そして応用へつなげることを目的とする。

３．研究の方法

(1) 初年度には，主として基礎技術の調査とシステムの計画に係る研究を推進する。すなわち，項書換え系分野における補助定理の生成や帰納的定理の証明・発見の基礎技術の調査を行い，それらの技術から，本研究の目的に適したものを取捨選択し，システムを計画する。

(2) 続く２つの年度では，実装のプラットフォームとして，本研究経費の設備備品費で購入する 64 コアの並列計算機システムを用いることとし，前年度のシステム計画に基づいて，システムの設計・実装に関して研究を進める。システムが正しく帰納的定理証明を実行することを確認すると共に，予備的な評価を実施し，ここまでの中間成果を学会等において発表し，広くコメントや助言を求めるようにする。また，関連の国際会議などで発表される最新の技術動向を調査することなどを含めて検討する。

(3)最終的に，開発したシステムの性能評価を行い，必要に応じて設計・実装の改善を行う。また，応用分野であるプログラム検証の分野について調査を行い，その分野特有の問題群を用いて，開発したシステムの可用性の評価を行い，必要に応じて設計・実装の改善を行う。そして本研究の成果を総括し，今後の課題を明らかにする。

なお，連携研究者の佐藤晴彦は，主として，協力研究者（大学院生）とともに，システムの計画・設計・実装に係る連携研究を行う。

４．研究成果

(1) 並列計算機システムの上で，関数型オブジェクト指向プログラミング言語 SCALA を用い，多重文脈型推論基盤システムを再実装し，その上で停止性検証，完備化，帰納的定理証明を効率良く実行するシステムを開発した。システムはこれまで C 言語（歴史はあるが複雑なプログラムを書きづらい言語）で実装していたため，本研究で必要な高度で複雑なシステム開発が困難であったが，SCALA で実装したことにより，関数型言語とオブジェクト指向言語の特徴を活用して，短期間で所定の開発を行うことができた。

(2) 代数的ソフトウェアの正しさの検証に関わる標準的なベンチマーク問題に本システムを適用し，所定の制限時間内に，従前よりも文脈を適切に探索して推論に成功することを確認した。後述するように，従前のシステムでは解けなかった問題が，本システムでは補助定理を自動生成することに解けている。

(3) 探索に関わる人工知能技術とヒューリスティクスを組み合わせることによって，本システムの重要部分である停止性自動検証の並列計算機上での実装技術を開発し，効率を向上させた。また SCALA のもつ遅延評価機構を用いることにより，現時点での計算結果が将来参照されるかどうか不明な計算を実際に必要になるまで遅延させるような実装が容易に可能となり，その結果システムの実行効率が改善された。

(4) 開発したシステムを評価した結果の概要を表１に示す。ここでは６題の問題について，３つのシステムによる実行時間を示している。単位は秒であり，所定の時間（60 秒）で解が得られなかった場合は，fail と記している。従前のシステム（mrit）では fail であった問題が，本研究で開発した補助定理を自動生成するシステム mrit+で解けている。また mrit+の実装を SCALA の遅延評価機構を利用して改善した lz-itp では，さらに実行時間が短くなっている。

表１　ベンチマークテストの結果概要

problem	mrit	mrit+（本研究）	lz-itp（本研究）
1	fail	0.62	0.60
2	fail	0.97	0.93
3	12.95	12.80	12.38
4	fail	18.09	17.74
5	fail	1.08	1.05
6	fail	1.05	1.02

fail > 60

(5) 本システムの開発に関わる研究活動から派生した知見として，与えられたオブジェクト指向プログラムをテストしたい状況において，条件判定式に記述された変数制約を満たすオブジェクトの状態（ターゲット）が複数個ある場合でも，プログラムの実行がそれらの状態を満たすようになるための入力（テストケース）を自動的に生成する方法として，動的記号実行に基づくメソッド実行列（これを実行すると判定条件を満たす）の自動生成法を考案した。これは今後の別研究課題となり得るものである。

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３件）

① ChengCheng Ji, Haruhiko Sato, Masahito Kurihara, Lazy Evaluation Schemes for Efficient Implementation of Multi-Context Algebraic Completion System, IAENG International Journal of Computer Science, 査読有, Vol. 42, No. 3, 2015, pp. 282-287

② Hiroki Takamatsu, Haruhiko Sato, Satoshi Oyama, Masahito Kurihara, Automated Test Generation for Object-Oriented Programs with Multiple Targets, IAENG International Journal of Computer Science, 査読有, Vol. 41, No. 3, 2014, pp. 198-203

③ Rui Ding, Haruhiko Sato, Masahito Kurihara, Parallelization of Termination Checkers for Algebraic Software, Transactions on Machine Learning and Artificial Intelligence, 査読有, Vol. 2, No. 4, 2014, pp. 102-114

〔学会発表〕（計８件）

① ChengCheng Ji, Haruhiko Sato, Masahito Kurihara, A New Implementation of Multi-Context Algebraic Inductive Theorem Prover, World Congress on Engineering and Computer Scientists 2015, 23 October 2015, Berkeley (USA)

② ChengCheng Ji, Haruhiko Sato, Masahito Kurihara, An Efficient Implementation of Multi-Context Algebraic Reasoning System with Lazy Evaluation, International MultiConference of Engineers and Computer Scientists 2015, 18 March 2015, Hong Kong (China)

③ Hiroki Takamatsu, Haruhiko Sato, Satoshi Oyama, Masahito Kurihara, Method Sequence Generation for Multiple Object States using Dynamic Symbolic Execution, 2014 IEEE International Conference on Systems, Man, and Cybernetics, 6 October 2014, San Diego (USA)

④ Haruhiko Sato, Masahito Kurihara, Recognition of Normal Forms with Tree Automata for Inductive Theorem Proving, Science and Information Conference 2013, 7 October 2013, London (UK)

６．研究組織

(1)研究代表者

栗原　正仁（KURIHARA, Masahito）
北海道大学・大学院情報科学研究科・教授
研究者番号：５０１３３７０７

(2)研究分担者
なし

(3)連携研究者

佐藤　晴彦（SATO, Haruhiko）
北海道大学・大学院情報科学研究科・助教
研究者番号：３０５４３１７８

(4)研究協力者

季　承成（JI, ChengCheng）
高松　宏樹（TAKAMATSU, Hiroki）
丁　睿（DING, Rui）