様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成２４年　５月２５日現在

機関番号：10101
研究種目：若手研究（Ｂ）
研究期間：2010～2011
課題番号：22700021
研究課題名（和文）　多重化に基づく，等式論理における帰納的定理証明の自動化

研究課題名（英文）　Automation of inductive theorem proving in equational logic with multi-context reasoning

研究代表者
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

研究成果の概要（和文）：ソフトウェアシステムの信頼性を高めるための基礎技術の一つである帰納的定理証明において，その自動化を推進するための効率の良い手続き及び推論戦略について研究した．複数の証明戦略を効率よく並列に実行するため，複数の並列動作に共通する処理を一括で実行する多重化の枠組みを用いた証明手続きを提案した．また証明の自動化において重要となる自動補題生成の実現に向け，正しい補題のみを生成する手法の基礎を構築した．

研究成果の概要（英文）：We have studied on the efficient procedure and reasoning strategy for automating inductive theorem proving, which is an important technique for verifying correctness of software systems. First, we proposed a proof method with multi-context reasoning, which can perform inferences commonly appearing in some different reasoning strategies simultaneously. Second, we proposed a principle for generating correct lemmas which are often required in inductive theorem proving.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2010 年度	500,000	150,000	650,000
2011 年度	500,000	150,000	650,000
2012 年度	0	0	0
2013 年度	0	0	0
2014 年度	0	0	0
総　計	1,000,000	300,000	1,300,000

研究分野：総合・新領域系 ，総合領域
科研費の分科・細目：情報学，ソフトウェア
キーワード：定理自動証明，項書換え系，帰納的定理証明

１．研究開始当初の背景

ソフトウェアシステムは社会の至る所で利用されており，その重要性の高まりと共に大規模化・複雑化が進んできたため，信頼性・安全性の確保が困難となってきている．このため，システムの検証において従来広く用いられてきたシミュレーションやテスト等の手法に代わって，システムが仕様を満たすことを論理的に証明する形式手法が注目されてきている．シミュレーションやテストによる従来の手法では，実際に試験が行なわれたごく限られた場合に対してのみシステムが正しいことが確認されるだけであるが，形式手法では帰納法を始めとした推論手続きによって無限の場合を取り扱えること，すなわち「どのような場合においてもシステムは正しい」ことを証明することが可能である点で，従来の手法と比べて非常に強力である．

しかし，形式手法で用いられる論理体系に

おいては機械的に推論が進められることは稀であり，多くの場合では論理的な推論に習熟した人間の補助が必要となる．このため，現在広く用いられている形式手法に基づくシステムの検証ツールの多くは，機械的に推論が可能な所は自動的に処理が行われ，そのような処理が困難な場合はユーザーに適切な指示を求めるという対話的なシステムとなっている．このような場合にユーザーに要求される補助の多くは，論理に関わる研究者ではない一般の技術者にとっては非常に困難なものであり，これは形式手法が非常に強力でありながらも，システム開発の現場への普及が進んでいない大きな原因の一つである．

２．研究の目的

本研究の目的は，形式手法に基づく検証において人間に要求されている処理をなるべく減らし，ツールが自動的に処理する範囲を広げることで，専門知識を持たない一般の技術者が利用し易いツールを実現することである．

３．研究の方法

これまで研究代表者は，形式手法のうち特に等式で記述される性質についての検証手法（等式論理における推論）に関して，その自動化及び効率化に関する研究を進めてきた．特に，等式論理に基づく推論手続きにおいて最も基本的かつ重要な役割を果たす完備化手続きについて，従来人間の補助を必要としていた処理を自動的に，かつ効率よく行うための拡張（多重完備化手続き）を提案した．この拡張を用いた実験により，人間の直観や洞察を用いなくとも，ある種の機械的な探索によって十分高速に証明を成功させることが可能であることを示した．

一般に，大規模なシステムの検証においては単一の定理証明手法のみでは十分とは言えず，問題の特性に応じて適切な手法を組み合わせて利用する必要がある．本研究者は定理証明手法のうちの一つである完備化手続きについてその自動化を推進してきたが，その過程で解決した課題は多くの定理証明手法に潜在するものであり，我々の知見はそれらにも有効であることが期待できる．

本研究では，完備化手続きと非常に関連の深い手法であり，現実的なシステムの検証において極めて重要となる帰納法を用いた証明の自動化・効率化に取り組む．帰納法は再帰処理，繰り返し処理，無限データ構造といった，プログラムに普遍的な要素の検証において必須である一方，自動証明が極めて難しく，最先端の検証ツールにおいても帰納法を用いた証明では適切な補題の導入や推論戦略の制御といった高度な補助が必要となっている．よって，専門知識を持たない技術者にとって帰納法を用いた検証は依然として敷居が高いものとなっている．

本研究では，等式論理における帰納法を用いた代表的な証明原理である書き換え帰納法について，その自動化及び効率化に取り組む．書き換え帰納法は，完備化手続きを応用した帰納的定理証明手法として広く研究されてきた潜在帰納法を一般化したものであり，推論の本質的な構造は完備化手続きと非常に類似している．このため，我々が提案した完備化手続きの効率の良い自動化手法が，書き換え帰納法に対しても同様に適用可能である．この手法の導入を主軸に置き，

(A) 多重化に基づく強力な書き換え帰納法手続きの実現

(B) 適切な推論戦略の自動選択

(C) 多重化における既存の自動補題生成手法の導入

(D) 正しい補題の自動生成

の４点の課題について研究を進める．

４．研究成果

（１） 課題ごとの研究成果

上に挙げた４点の研究課題それぞれについての成果は次の通りである．

(A) 多重化に基づく強力な書き換え帰納法手続きの提案

書き換え帰納法における重要なパラメータである簡約順序について，それについての制約を保持し潜在的な多数の簡約順序を並列的に取り扱えるように多重化し，自動証明可能な範囲を広げた手続きを提案した．また，本質的に等価な制約や推論上有用でない制約を自動検出することで考慮すべき制約を削減し高速化するための原理を提案した．

(B) 適切な推論戦略の自動選択の実現に向けた，基礎理論の構築と実験

帰納的定理の証明を成功させるには，書き換え規則の適用順序の選択や適切な補題の追加といった非決定的な推論が重要であり，探索範囲を現実的なサイズに制限するには適切な推論戦略を設定する必要がある．本研究では多数の例に対する実験を通して書き換え規則の適切な適用順序を検討した．また決定可能な帰納的定理のクラスに関する既存の研究成果に基づき，正当性の検証が容易かつ有用性の高い補題の特徴付けを行った．

(C) 多重化に基づく書き換え帰納法手続きへの自動補題生成手法の導入

証明の自動化においては適切な補題の追加が極めて重要である．書き換え帰納法における有効性が確かめられている自動補題生成手続きの一つに発散鑑定法に基づく一般化が知られている．前年度に提案した多重化に基づく書き換え帰納法手続きにこの発散鑑定法に基づく一般化手続きを導入し，その有効性を調べた．実験により，多重化による帰納法の枠組みの探索と補題生成の組み合わせにより自動証明が容易となる例が発見された．

(D) 健全な等式変換に関する理論の構築と，そのための正規形集合の認識手続きの実現

補題生成手法の一つである発散鑑定法は等式の一般化を基礎としているが，それにより補題の正しさが失われる可能性がある．正しさを保存する健全な一般化を実現するため，等式中のある部分が取り得る計算結果全体を表す正規形集合の同一性に基づく健全な一般化の理論を構築した．またその同一性判定手続きを実現するため，正規形集合を認識する木オートマトンを構成し，木オートマトンの同一性判定手続きに帰着させる手続きを提案した．

（2） 得られた成果の位置付けとインパクト

書き換え帰納法を用いた帰納的定理の証明において，本研究成果に類するような広範囲の自動化を進めている研究は他に例がない．本研究によって，関数型・論理型プログラムといった等式に基づくシステムの検証がより敷居の低いものとなることが期待される．また，プログラムの等価性に基づく効率の良いシステムの自動生成・変換といった，帰納的定理証明を基盤とする様々な応用においても，同様の自動化による利便性の向上が期待できる．

（3）今後の展望

より強力かつ効率の良い手続きの実現に向け，今後取り組むべき課題としては以下の２点が挙げられる．

① 特定の公理系に特化した，強力かつ効率の良い手続きの実現

近年，これまで書き換え帰納法が取り扱えなかった難しい定理の証明を可能とする，推論規則の拡張に関する研究が進められている．これらの新しい推論手続きは順序付けが出来ない等式を一般的に取り扱えるため非常に強力であるが，可能となる推論の幅が非常に広く，適切な自動化が困難であると思われる点が多い．

この問題に対し，順序付けが出来ない等式のうち，頻繁に用いられる等式群に特化することで，効率のよい自動化された手続きが実現できるものと考えられる．

② 書き換え帰納法手続きにおける停止性検証の効率化

停止性に関する研究の歴史は長く，その中で数多くの停止性自動検証器が継続的に開発されてきている．これに伴い，停止性検証器をより発展的なシステムの検証・解析・合成ツールの構成要素として用いる試みが広く行われており，書き換え帰納法の自動化においても停止性検証器は重要な役割を果たす．しかし，現時点で存在する停止性検証器の多くは検証能力の向上に主眼を置いており，検証に要する時間が膨大となる傾向にあり，他の検証器から繰り返し利用される場合に適したものとなっていない．

書き換え帰納法手続きにおける停止性検証では，停止性が示されている書き換え規則の集合に，新たな規則を追加して得られる集合の停止性を改めて示すという形の処理が繰り返し行われる．この性質を利用し，書き換え帰納法手続きに適した効率の改善が可能であると考えられる．

５．主な発表論文等

〔雑誌論文〕（計１件）

① Haruhiko Sato, Masahito Kurihara, Multi-context rewriting induction with termination checkers, IEICE Transactions on Information and Systems, E93-D, 942-952, 2010, 査読有

〔学会発表〕（計３件）

① Haruhiko Sato, Recognition of Normal Forms for Sound Generalization, 35th TRS meeting, 2011, 査読無し
② 佐藤 晴彦, 書き換え帰納法における文脈探索の有効性について, 情報処理学会 第 84 回プログラミング研究発表会, 2011, 査読なし
③ Sarah Winkler, Haruhiko Sato, Aart Middeldorp, Masahito Kurihara, Optimizing mkbTT (System Description), 21st International Conference on

Rewriting Techniques and Applications, 2010, 査読有

〔図書〕（計０件）

〔産業財産権〕
○出願状況（計０件）

○取得状況（計０件）

〔その他〕
ホームページ等

６．研究組織
(1)研究代表者
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

(2)研究分担者
なし

(3)連携研究者
なし