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

平成　３０　年　　６　月　１１　日現在

機関番号：　３０１０７
研究種目：　若手研究(B)
研究期間：　2016～2017
課題番号：　１６Ｋ１６０３２

研究課題名（和文）帰納的定理証明の自動化に向けた補題生成と推論戦略の改良

研究課題名（英文）Improvement of lemma generation and reasoning strategies for automated inductive theorem proving

研究代表者

佐藤　晴彦（SATO, HARUHIKO）

北海学園大学・工学部・准教授

研究者番号：３０５４３１７８

交付決定額（研究期間全体）：（直接経費）　　1,000,000円

研究成果の概要（和文）：ソフトウェアシステムの性質を数学的な定理として論理的に証明することで極めて高い信頼性・安全性を確保する形式手法において、人手による証明が高コスト及び困難となることが実用上の障害となっている。このため計算機により自動的に定理を証明する、自動証明システムの適用範囲の拡大が重要な課題となっている。本研究では定理証明問題のうち特に自動化が困難であると知られている証明に帰納法を要する種類の定理（帰納的定理）を対象とし、その証明の自動化において重要となる補題の自動生成について新しい手法を提案した。

研究成果の概要（英文）：With the increasing importance of software systems, the need to ensure safety or correctness of them in a rigorous way is growing. Formal verification is a generic name of such a rigorous approach, where the meaning of the description of a system and of the desirable properties for the system are formalized unambiguously and we mathematically prove that the system has the properties under the formalization. For difficult proof tasks, human experts need to make proofs by hand. Since the cost for involving human experts is expensive, the improvement of automated theorem provers is one of the most important subjects for popularization of formal verification. In order to automate the proof of the type of theorems called inductive theorems, which is the class of theorems requiring mathematical (well-founded) induction to prove and hence is known to be hard to automate, in this study we propose new methods for automated lemma generation required for inductive theorem proving.

研究分野：　ソフトウェア科学

キーワード：　定理自動証明

１．研究開始当初の背景

（１）形式手法によるソフトウェア検証

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「無限個の状態」についての性質を示すことが可能となる。これは「任意の入力・環境においてシステムが正しく動作する」ことを証明することが可能となることを意味し、テスト等の従来の手法と比べて極めて厳密かつ強力である。

（２）現状の形式手法の問題点

一般に、形式手法で用いられる論理体系においては機械的な推論のみで証明が完了することは稀であり、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。より具体的には、形式手法における定理証明問題として頻出する帰納的定理と呼ばれる種類の定理を対象とした自動化に取り組む。帰納的定理とは自然数や再帰的データ構造などの特定の無限集合について成り立つ命題であり、ソフトウェアシステムの検証上重要な性質の多くが帰納的定理として表現できるが、その自動証明が特に困難であることが理論的に知られている。

３．研究の方法

本研究では、帰納的定理証明の自動化において重要となる、主定理の直接的な証明が困難な場合に必要となる補助定理（補題）の自動発見について、以下の２つの方法：

（１）主定理の証明が失敗する様子を分析することで有効な補題を導く方法（トップダウン的な手法）

（２）主定理を直接用いず、基本的なものから順に考えうる補題の集合を可能な限り構成する方法（ボトムアップ的な手法）

に基づいて研究を行った。

４．研究成果

（１）　トップダウン的な手法に関する成果

トップダウン的な補題発見手法として、既存の発散鑑定法（引用文献①）に基づいた新しい補題生成手法を提案した。発散鑑定法は様々な問題に対して有効である一方、最終的な補題の生成は観察により導かれた等式を適切に一般化することが必要であり、過度に一般化を行うと誤った補題が生成されてしまうという問題があった。

この問題に対し、発散を構成する等式列における各等式間の差分に含まれる項とそうでない項同士は独立であることが自然であるという考えに基づき、そのような項同士の依存関係を解消するように一般化を行う手法を提案した。

既存の証明問題セットを用いた実験の結果、提案手法は既存の発散鑑定法では証明が失敗する複数の問題について証明が可能となること、また発散鑑定法と相補的に利用することで処理時間の増加を抑えつつ全体的な証明成功率を向上させることが可能であることを示した。

以上の成果をまとめた論文を現在論文誌に投稿中である。

（２）　ボトムアップ的な手法に関する成果

既存のボトムアップ的な補題発見手法（引用文献②③）では帰納法の枠組みとして単純で自動化が容易な構造帰納法が用いられていたが、複雑な再帰的定義に対しては直接的には適用できないため、適用範囲が限定されていることが問題であった。

この問題に対し、構造帰納法の証明能力を超えたより複雑な定理を扱えるようにするため、代わりにより一般的かつ強力な書き換え帰納法を用いる手法を提案した。より具体的には、書き換え帰納法で用いる順序関係の構成において繰り返し必要となる停止性証

明を効率的に行う仕組みの提案や、等式を書き替え規則として扱うための向き付けについて、その探索範囲を削減するための有効な向き付けの特徴付けを行った。基本的なリスト処理関数を対象とした実験により、構造帰納法では直接的な証明が構成できない補題の発見が可能であること、また提案した４種類の向き付け手法を組み合わせることにより、定義が比較的複雑な問題において発見できる補題の数を減少させずに計算時間を４割程度削減できる場合があることを確認した（図１、図２）。この成果について、国際会議で発表を行った。（学会発表①）

またこの実験結果に基づき、既存のボトムアップ的な手法で標準的に用いられている構文的に単純な補題候補から順に証明を試みる方法は有効に働かない場合があることを示し、多くの補題の基礎となる一般性のある補題が構文的に複雑な形を取ることがあるためそのような補題を特定し優先的に証明することの重要性を具体的な事例を通し明らかにした。この成果について、国際会議で発表を行った。（学会発表②）

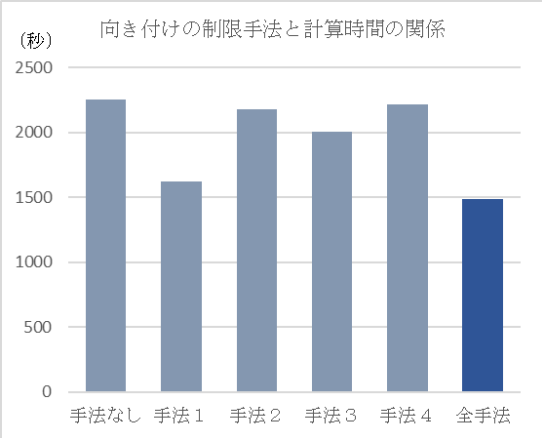

図１：向き付けの制限による計算時間の削減（定義が比較的単純な場合）

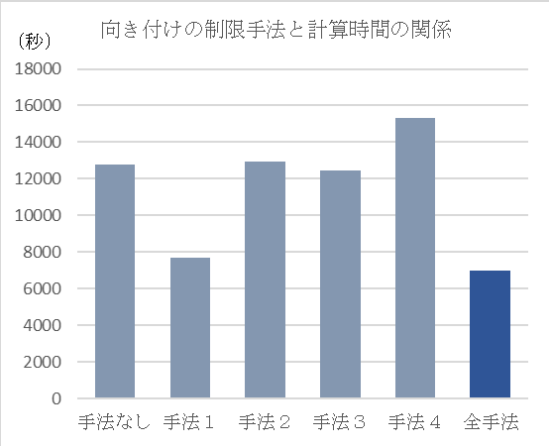

図２：向き付けの制限による計算時間の削減（定義が比較的複雑な場合）

＜引用文献＞

① T. Walsh, “A divergence critic for inductive proof,” Journal of Artificial Intelligence Research, vol. 4, pp. 209-235, 1996.

② M. Johansson, L. Dixon, and A. Bundy, “Conjecture synthesis for inductive theories,” Journal of Automated Reasoning, vol. 47, no. 3, pp. 251-289, 2011.

③ K. Claessen, M. Johansson, D. Ros´en, and N. Smallbone, “Automating inductive proofs using theory exploration,” in Proceedings of the 24th International Conference on Automated Deduction, ser. CADE’13. Berlin, Heidelberg: Springer-Verlag, 2013, pp. 392-406.

５．主な発表論文等

〔雑誌論文〕（計　０件）

〔学会発表〕（計　２件）

① Haruhiko Sato, and Masahito Kurihara, "Discovering Inductive Theorems using Rewriting Induction" Proceedings of 2016 IEEE International Conference on Systems, Man, and Cybernetics, October 9-12, 2016, Hungary, pp. 989-993.

② Haruhiko Sato, and Masahito Kurihara, "On Usefulness of Syntactically Complex Lemmas in Theory Exploration for Inductive Theorems," Lecture Notes in Engineering and Computer Science: Proceedings of The International MultiConference of Engineers and Computer Scientists 2018, March 14-16, 2018, Hong Kong, pp. 489-492.

〔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：なし

６．研究組織

(1)研究代表者

佐藤　晴彦（SATO, Haruhiko）
北海学園大学・工学部電子情報工学科・准教授
研究者番号：30543178