

機関番号：11301

研究種目：基盤研究 (C)

研究期間：2008～2010

課題番号：20500002

研究課題名 (和文) リップリング法と書き換え帰納法を融合した定理自動証明法の研究

研究課題名 (英文) Combining Rippling and Rewriting Induction for Inductive Theorem Proving

研究代表者

青戸 等人 (AOTO TAKAHITO)

東北大学・電気通信研究所・准教授

研究者番号：00293390

研究成果の概要 (和文)：

プログラムの性質や仕様を記述する帰納的定理の自動証明法として項書き換えシステムに基づく暗黙的帰納法に着目し、その高度化を図った。主な研究成果としては、書き換え帰納法における順序付け不能な等式の取り扱いを改良するとともに、改良書き換え帰納法に基づく定理自動証明システムを構築した。また、帰納的定理自動証明で重要な補題自動生成法については、健全一般化法の一般化を行った。また、反証機能付き書き換え帰納法に対応する健全発散鑑定法を考案し、さらに、異なる複数の補題を独立に導入する書き換え帰納法フレームワークを考案した。複数の自動補題生成法を効率的に適用する戦略を構築した。また、反証機能付き書き換え帰納法の適用可能性に必要な合流性についてその証明法の理論を拡張するとともに、自動証明システムの構築を行った。

研究成果の概要 (英文)：

Our focus in this project is inductive theorem proving based on term rewriting systems. We are, in particular, interested in rewriting induction methods. We extended rewriting induction to enhance provability of non-orientable conjectures, and we implemented an inductive theorem prover based on our extension. Lemma discovery is an important aspect of inductive theorem proving and we generalized a sound generalization technique and gave sound divergence critic, which are useful when the rewriting induction is equipped with the disproving mechanism. We propose rewriting induction framework to incorporate different lemma generation methods. We also investigate automated confluence proving, as it is a necessary property to extend rewriting induction with the disproving mechanism. We gave new techniques to prove confluence and implemented a confluence prover.

交付決定額

(金額単位：円)

| | 直接経費 | 間接経費 | 合計 |
|--------|-----------|---------|-----------|
| 2008年度 | 1,000,000 | 300,000 | 1,300,000 |
| 2009年度 | 1,000,000 | 300,000 | 1,300,000 |
| 2010年度 | 1,100,000 | 330,000 | 1,430,000 |
| 年度 | | | |
| 年度 | | | |
| 総計 | 3,100,000 | 930,000 | 4,030,000 |

研究分野：総合領域

科研費の分科・細目：情報学・情報学基礎

キーワード：定理自動証明、書き換えシステム、リップリング、書き換え帰納法、潜在帰納法、健全一般化法、発散鑑定法、合流性

1. 研究開始当初の背景

形式手法に基づくソフトウェアの検証法は活発に研究されている。プログラムのさまざまな性質はデータ構造に関する帰納法により証明されることが多い。従って、このような性質(帰納的定理)の高度な自動証明法はソフトウェア検証に極めて有効であると考えられる。等式による証明・計算モデルとして、書き換えシステムが知られており、書き換えシステムに基づく帰納的定理自動証明法の研究が行われている。特に、いくつかの明示的帰納法に基づく帰納的定理自動システムは成功を納めている。一方、複雑な帰納法が必要な高度な証明にも対応可能な方法として暗黙的帰納法が知られており、さまざまな理論的な研究が行われている。しかしながら、暗黙的帰納法に基づく帰納的定理自動システムは証明能力は一般にはあまり高くない。申請者の先行研究で、抽象等価性理論に基づく暗黙的帰納法構築や書き換え帰納法の拡張を行っていた。これらの先行研究に基づき、明示的帰納法で採用されているリップリング法などのヒューリスティクスと書き換え帰納法を融合することにより、より高度な帰納的定理自動証明機構の構築が可能ではないかと予想した。

2. 研究の目的

本研究の目的は帰納的定理の自動証明法として項書き換えシステムに基づく暗黙的帰納法に着目し、その高度化を図ることである。このため明示的帰納法の強力なヒューリスティクスであるリップリング法と申請者らの考案した抽象等価性理論に基づく書き換え帰納法の枠組みを融合し、より高度な帰納的定理自動証明機構を構築するとともに、両

者の特徴を生かした新しい自動証明法の提案を目指す。

3. 研究の方法

理論的な枠組みの構築およびそれに基づく帰納的定理証明システムの構築実験を通じた評価を行うために、調査・解析、理論の構築、実験システムの構築、実験システムの高度化および応用へと順次移行しつつ、理論と実験の両面から手法の妥当性や有効性を検討した。具体的には、以下の3フェーズを並行して進めた。

- (1) 暗黙帰納法へのリップリング法の導入
- (2) 自動補題発見法の高度化
- (3) 帰納的定理自動証明の実験システムの構築とその高度化

4. 研究成果

- (1) 順序付け不能な等式の取り扱える書き換え帰納法

先行研究で提案していた順序付け不能な等式の取り扱える書き換え帰納法の枠組みを改良するとともに、その改良書き換え帰納法に基づく帰納的定理自動証明の実験システムを構築した。この理論は書き換え帰納法に基づく帰納的定理自動証明システムとして有名なSPIKEにも影響を与え、SPIKEの拡張が提案されることになった。

- (2) 健全一般化法の一般化

補題自動生成法は帰納的定理自動証明に極めて重要な役割を果たす。健全な補題の生成は、帰納的定理自動証明において複雑な戦略を必要としない安全な補題生成法であり、反証機能付き書き換え帰納法でも利用可能な

補題生成法である。従来提案されていた健全一般化法が間違いを起こす場合があることを突き止めるとともに、従来法を修正・拡張する健全一般化法を考案した。

(3) 健全発散鑑定法の考案

発散鑑定法はある種の発散系列が観測される場合に有効な補題を構成することの出来る補題生成法であるが、健全な補題が生成されるとは限らない。そこで生成される補題の健全性が保証される健全発散鑑定法を考案した。

(4) 書き換え帰納法フレームワークの考案

複数の自動補題生成法を効率的に適用する戦略として、異なる複数の補題を独立に導入する書き換え帰納法フレームワークを考案した。そして、このフレームワークに基づき、先行して提案した自動補題生成法を取り入れた、帰納的定理自動証明システムの構築を行った。

(5) 合流性証明

反証機能付き書き換え帰納法の適用可能性に必要な合流性についてその証明法の理論を拡張するとともに、自動証明システムの構築を行った。

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 9 件)

1. Yuki Chiba, Takahito Aoto and Yoshihito Toyama, Program transformation templates for tupling based on term rewriting, IEICE Transactions on Information

and Systems, Review existence , Vol.E93-D, No.5, pp.963-973, 2010.

2. Takahito Aoto and Toshiyuki Yamada, Argument filterings and usable rules for simply typed dependency pairs, In Proceedings of the 7th International Symposium on Frontiers of Combining Systems (FroCoS 2009), Trento, Italy, Review existence , LNAI 5749, pp.117-132, 2009.
3. Takahito Aoto, Junichi Yoshida and Yoshihito Toyama, Proving confluence of term rewriting systems automatically, In Proceedings of the 20th International Conference on Rewriting Techniques and Applications (RTA 2009), Brasília, Brazil, Review existence , LNCS 5595, pp.93-102, 2009.
4. 吉田順一, 青戸等人, 外山 芳人, 項書き換えシステムの合流性自動判定, コンピュータソフトウェア, 査読有, Vol.26, No.2, pp.76-92, 2009.
5. 寫津聡志, 青戸等人, 外山 芳人, 反証機能付き書き換え帰納法のための補題自動生成法, コンピュータソフトウェア, 査読有, Vol.26,

- No.2, pp.41-55, 2009.
6. Takahito Aoto,
Sound lemma generation for
proving inductive validity of
equations, In Proceedings of the
28th International Conference
on Foundations of Software
Technology and Theoretical
Computer Science (FSTTCS
2008), Bangalore, India,
Dagstuhl Seminar Proceedings,
Review existence , Vol.08004,
pp.13-24, 2008.
 7. Jean-Pierre Jouannaud and
Yoshihito Toyama, Modular
Church-Rosser Modulo: The
Complete Picture, International
Journal of Software and
Informatics, Review existence ,
Vol.2, No.1, pp.61-75, 2008.
 8. Yoshihito Toyama,
Termination proof of
S-expression rewriting systems
with recursive path relations, In
Proceedings of the 19th
International Conference on
Rewriting Techniques and
Applications (RTA 2008),
Hagenberg, Austria, Review
existence , LNCS 5117,
pp.381-391, 2008.
 9. Takahito Aoto, Designing a
rewriting induction prover with
an increased capability of
non-orientable theorems, In
Proceedings of
Austrian-Japanese Workshop on
Symbolic Computation in
Software Science (SCSS 2008),
Hagenberg, Austria, Review
existence , pp.1-15, 2008.
- [学会発表] (計 12 件)
1. 磯部耕己, 青戸等人, 外山芳人,
多項式サイズ正規形を保証する項
書き換えシステムの経路順序, 第
13 回プログラミングおよびプロ
グラミング言語ワークショップ,
2011 年 3 月 9~11 日, 北海道札幌
市
 2. 村井正勝, 青戸等人, 外山芳人,
基底項書き換え系の多項式時間合
流性判定法の改良, 第 13 回プロ
グラミングおよびプログラミング言
語ワークショップ, 2011 年 3 月 9
~11 日, 北海道札幌市
 3. 的場正樹, 青戸等人, 外山芳人,
SMT ソルバを用いた項書き換え
システムの合流性自動判定, 電気
関係学会東北支部連合大会, 平成
22 年 8 月 26~27 日, 青森県八戸市
 4. 鈴木翼, 青戸等人, 外山芳人,
文脈移動法による項書き換えシ
ステムの変換, 電気関係学会東北支
部連合大会, 平成 22 年 8 月 26~
27 日, 青森県八戸市
 5. 道又淳一, 青戸等人, 外山芳人,
拡大手法に基づく項書き換え系の
合流性自動証明,
第 12 回プログラミングおよびプ
ログラミング言語ワークショップ,

2010年3月3～5日,香川県琴平町

6. 岩見宗弘, 青戸等人, 無限項書き換えシステムにおける強頭部正規化可能性の反証手続き, 第12回プログラミングおよびプログラミング言語ワークショップ 2010年3月3～5日,香川県琴平町
7. 村井正勝, 青戸等人, 外山芳人, 基底項書き換え系の合流性自動判定, 第8回情報科学技術フォーラム(FIT2009), 2009年9月2～4日,宮城県仙台市
8. 磯部耕己, 青戸等人, 外山芳人, S式書き換えシステムの停止性を保証するカー化について, 第8回情報科学技術フォーラム(FIT2009), 2009年9月2～4日,宮城県仙台市
9. 道又淳一, 青戸等人, 外山芳人, 多重 Knuth-Bendix 完備化における危険対除去手法の導入, 第8回情報科学技術フォーラム(FIT2009), 2009年9月2～4日,宮城県仙台市
10. 磯部耕己, 青戸等人, 外山芳人, S式書き換え系の停止性を保証するカー化について, 第11回プログラミングおよびプログラミング言語ワークショップ, 2009年3月9～11日,岐阜県高山市
11. 道又淳一, 青戸等人, 外山芳人, 多重 Knuth-Bendix 完備化における効率化手法の導入, 第11回プロ

グラミングおよびプログラミング言語ワークショップ, 2009年3月9～11日,岐阜県高山市

12. 村井正勝, 青戸等人, 外山芳人, 基底項書き換え系の合流性判定手続きの効率化, 第11回プログラミングおよびプログラミング言語ワークショップ, 2009年3月9～11日,岐阜県高山市

[図書] (計 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

<http://www.nue.riec.tohoku.ac.jp/index-j.html>

6. 研究組織
(1) 研究代表者
青戸 等人 (AOTO TAKAHITO)
東北大学・電気通信研究所・准教授
研究者番号: 00293390

(2) 研究分担者
外山 芳人 (TOYAMA YOSHIHITO)
東北大学・電気通信研究所・教授
研究者番号: 00251968