

発表概要

# 書き換え帰納法における文脈探索の有効性について

佐藤 晴彦<sup>1,a)</sup> 栗原 正仁<sup>1</sup>

2011年6月15日発表

帰納的定理とは、自然数やリストといった帰納的に定義されるデータ構造上で成り立つ命題であり、システムの正当性や安全性といった性質の検証において、帰納的定理の証明は重要となる。等式論理における帰納的定理の証明原理の1つに、Reddyによって提案された書き換え帰納法がある。書き換え帰納法に基づく証明を成功させるには、等式の向き付けや書き換え規則の適用といった非決定性を持つ推論において適切なものを選択し、帰納法の仮定や補題からなる文脈を適切に構成することが重要となるが、適切な文脈を得るための一般的な戦略を事前に定めておくことは容易ではない。本発表では、書き換え帰納法に基づく証明を網羅的な探索に基づいて自動化することを目的とし、書き換え帰納法に基づく複数の証明手続きを効率よく並列実行する多重文脈書き換え帰納法 (MRIIt) を提案する。提案する手続きでは書き換え帰納法に基づく複数の証明手続きの並列実行を仮想的にシミュレートし、項の書き換えや等式の展開などの基本的な推論を複数の手続きの間で共有することで効率化を図る。また、手続きは項書き換え系の停止性自動証明器を利用することで、帰納法に必要な項の順序関係が存在することを保証しながら、潜在的な順序の下で可能となる推論を幅広く試みる。また、手続きが有効ないくつかの例を示し、有効性を検討する。

## Effectiveness of Context-search in Rewriting Induction

HARUHIKO SATO<sup>1,a)</sup> MASAHITO KURIHARA<sup>1</sup>

Presented: June 15, 2011

Inductive theorem is a proposition which is defined on the data structure defined inductively, such as natural numbers and lists. Inductive theorem proving plays an important role in the field of formal verification of systems. The rewriting induction (RI) is a method for inductive theorem proving proposed by Reddy. In order to obtain successful proofs, it is very important to construct appropriate contexts, consisting inductive hypotheses and lemmas, in orientation of each equation and applying rewrite rules. However, it is not easy to specify general strategy for constructing appropriate contexts. In this talk, in order to automate proof search in RI by exhaustive search, we propose a new procedure, called multi-context rewriting induction, which executes several instances of the rewriting induction procedure efficiently in parallel. This procedure efficiently simulates parallel execution of rewriting induction procedures in a single process by sharing basic inferences such as reduction and expansion among simulated instances. This procedure uses automated termination checker of term rewriting systems for ensuring existence of reduction order. Finally, we show some examples for which the new procedure works effectively.

<sup>1</sup> 北海道大学大学院情報科学研究科  
Graduate School of Information Science and Technology,  
Hokkaido University, Sapporo, Hokkaido 060-0814, Japan

<sup>a)</sup> haru@complex.eng.hokudai.ac.jp