Title	正当性自動保証機能を備えた高階プログラム自動変換技術
Author(s)	千葉，勇輝
Citation	科学研究費助成事業研究成果報告書: 1-5
Issue Date	2015-06-05
Type	Research Paper
Text version	publisher
URL	http://hdl.handle.net/10119/12818
Rights	
Description	研究種目：若手研究(B)，研究期間：2011～2014，課題番号：23700034，研究者番号：10509756，研究分野：項書き換え

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 ２７ 年　 ６ 月　 ５ 日現在

機関番号：１３３０２
研究種目：若手研究(B)
研究期間：2011～2014
課題番号：２３７０００３４

研究課題名（和文）正当性自動保証機能を備えた高階プログラム自動変換技術

研究課題名（英文）A Framework of Program Transformation by Templates with Automated Verification of the Correctness

研究代表者
千葉　勇輝（Chiba, Yuki）

北陸先端科学技術大学院大学・情報科学研究科・助教

研究者番号：１０５０９７５６

交付決定額（研究期間全体）：（直接経費）　　2,000,000円

研究成果の概要（和文）：項書き換えに基づくパターンによるプログラム変換の枠組みを拡張し，高階関数を直接取り扱うことが出来るプログラム変換枠組みの構築を目指した．理論的計算モデルとして，単純型付項書き換えシステム(Simply Typed Term Rewriting System, STTRS)を採用した．プログラム変換の正当性を検証するための手続きとしてSTTRS等価変換手続きを提案し，その理論的正しさを証明した．
STTRSの枠組みで変換パターンを作成するために，STTRSパターンの概念を提案した．また，STTRSパターンによるプログラム変換を実現するために，STTRSパターンマッチングアルゴリズムを提案した．

研究成果の概要（英文）：We construct a framework of program transformation by templates which can directly deal with higher order functions by extending the framework based on first order term rewriting. Simply typed term rewriting systems (STTRS, for short) are adopted as a computational model in our framework. In order to verify the correctness of transformation in our framework, we propose an equivalent transformation of STTRSs and give sufficient condition for guaranteeing the correctness of transformation based on the equivalent transformation.
We introduce the notion of STTRS patterns for creating transformation templates in our framework. STTRS pattern matching algorithm is proposed to analyze how to apply templates for transforming STTRSs.

研究分野：項書き換え

キーワード：プログラム変換　単純型付項書き換えシステム　パターンマッチング

１．研究開始当初の背景

プログラム自動変換を応用することにより，ソフトウェア開発を効率的に進めることが出来る．プログラム自動変換は，入力プログラムの構造を解析し，適用可能な規則を同定し，その規則を適用することで実現される．変換パターンの概念を導入することで，プログラム自動変換技術は下記の通り一般化することができる(図１).

(1) 変換規則を定義し, 変換パターン(図 1 右側)を与える.

(2) 入力されたプログラム(R)と入力パターン(P)のマッチングを行なう.

(3) 2 で得られたマッチング(φ)を出力パターン(P')に適用する.

(4) 変換後のプログラム(R')を出力する.

図 1: パターンによるプログラム変換

プログラム変換において，プログラム変換の正当性が保証されること，すなわち，入力プログラムと出力プログラムの等価性が保たれること(R=R')は，信頼性の高いプログラム変換を実現するために必要である

Huet と Lang はラムダ計算の枠組みで変換パターンを用いたプログラム変換を形式化し，表示的意味論に基づく変換の正当性を保証する手法を提案した．彼らの手法では，データ構造の帰納的な性質を仮定し，プログラム変換の正当性を保証している．そのため，実際のプログラム変換の正当性を確認するためには，それら仮定された帰納的性質を，各変換毎に，ユーザが帰納法を用いて証明しなくてはならない. また, Huet と Lang 以降，パターンによるプログラム変換の研究では，マッチングに重点が置かれ変換の正当性に関する議論はほとんど行われてこなかった．

そこで，我々は項書き換えを理論的基礎とするパターンによるプログラム変換の枠組みを提案した．項書き換えの基づく定理自動証明手法を応用することにより，変換の正当性を自動的に検証することが可能となった．さらに，その枠組みに基づき，パターンによるプログラム変換システム RAPT (Rewriting-based Automated Program Transformation system) を実装した．

我々の枠組みは，変換の正当性の自動検証を可能にしたものの，1 階の項書き換えを理論的基礎としていたため，関数型プログラムで広く用いられている高階関数を直接取り扱うことが困難であった．そのため，実際広く用いられているプログラムを変換する技術としては不十分であった．

２．研究の目的

高階関数を直接取り扱うことが可能な書き換えシステムとして，単純型付き項書き換えシステム(Simply Typed Term Rewriting System，以下 STTRS)が知られている．本研究の目的は，我々が提案したパターンによるプログラム変換の枠組みを STTRS を用いて拡張し，変換の正当性自動検証可能な高階プログラム自動変換の枠組みを構築することである．そのために，下記の実現を目指す．

(1) 変換の正当性を示すために, STTRS の等価性を検証するアルゴリズムの提案.

(2) 変換パターンの概念を構築.

(3) 1 に基づき, 変換の正当性を検証する手法の提案.

(4) 本研究の枠組みを実装し，プログラム自動変換システムを構築.

(5) 変換パターンを収集.

３．研究の方法

STTRS の概念を適用し，応募者によるパタ

ーンによるプログラム変換の枠組みを拡張する．また，変換の正当性自動検証可能な高階プログラム自動変換技術を提案する．変換の正当性を議論するために，STTRS の等価性を検証するアルゴリズムを構築する．STTRS を用いた変換パターンの概念を定義し，パターンによるプログラム変換の枠組みを構築する．さらに，変換の正当性を検証する手法を構築し，枠組みの実装を行う．実装されたシステムを用いた実験を通して変換パターンを収集し，変換パターンのデータベースの作成を行う．

４．研究成果

(1) プログラム変換の正当性判定

本研究の枠組みにおいてプログラム変換の正当性は STTRS の等価性によって定義される．STTRS の等価性を検証するための手続きとして，STTRS 等価変換を提案した．STTRS 等価変換の理論的正しさの証明過程において，1 階の項書き換えシステムでは自明に成立する新規導入関数の除去が STTRS の枠組みでは自明に成立しないことを明らかになった．Aoto らによって提案された高階十分完全性の概念と，相対停止性を利用することにより，STTRS の枠組みで新規導入関数の除去を示すことができた．STTRS 等価変換において，新規導入関数の除去が示されたので STTRS 等価変換の理論的正しさが証明された．

(2) STTRS パターンマッチング

STTRS にパターン変数を組み込んだ STTRS パターンの概念を導入し，STTRS パターンと STTRS のパターンマッチングアルゴリズムを提案した．STTRS パターンマッチングアルゴリズムを利用することにより，STTRS 変換パターンの適用箇所を明らかにし，STTRS に基づくプログラム変換の実現が可能となる．

(3) 条件付き項書き換えシステムによるプログラム変換

組化変換は余分な再帰呼出しの回数を減らすことにより，プログラムの効率の改善を目指す手法である．条件付き項書き変えシステムを導入することにより，効率的な組化変換を書き換えの枠組みで実現することが可能となる．項書き換えシステムの等価変換を拡張し，条件付き項書き換えシステムの等価変換を提案した．条件付き項書き換えシステムの等価変換により，組化変換の正当性を検証することが出来る．

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 6 件）

1. Dieu-Huong Vu, Yuki Chiba, Kenro Yatake, and Toshiaki Aoki,
Checking the Conformance of a Promela Design to Its Formal Specification in Event-B,
In Proceedings of the third International Workshop on Formal Techniques for Safety-Critical Systems (FTSCS), pp.203-218, 2014.（査読有り）

2. Haitao Zhang, Toshiaki Aoki, and Yuki Chiba,
A Spin-based Approach for Checking OSEK/VDX Applications,
In Proceedings of the third International Workshop on Formal Techniques for Safety-Critical Systems (FTSCS), pp.187-202, 2014.（査読有り）

3. Haitao Zhang, Toshiaki Aoki, Hsin-Hung Lin, Min Zhang, Yuki Chiba and Kenro Yatake,
SMT-based Bounded Model Checking for OSEK/VDX Applications,
In Proceedings of the 20th Asia-Pacific Software Engineering Conference (APSEC

2013), IEEE, vol.1, pp.307-314, 2013.（査読有り）
4. Daniel Gaina, Zhang Min, Yuki Chiba and Yasuhito Arimoto,
Constructor-based Inductive Theorem Prover,
In Proceedings of the 5th Conference on Algebra and Coalgebra in Computer Science (CALCO 2013), Warsaw, Poland, Lecture Notes in Computer Science, Springer-Verlag, Vol.8089, pp.328-333, 2013.（査読有り）
5. Yuki Chiba and Takahito Aoto,
Transformations by Templates for Simply-Typed Term Rewriting,
In Proceedings of the 6th International Workshop on Higher-Order Rewriting (HOR 2012), Nagoya, Japan, June 2012, pp.3-8, 2012.（査読有り）
6. Takahito Aoto, Toshiyuki Yamada and Yuki Chiba,
Natural Inductive Theorems for Higher-Order Rewriting,
In Proceedings of the 22nd International Conference on Rewriting Techniques and Applications (RTA 2011), Novi Sad, Serbia, May/June 2011, pp.107-121, Leibniz International Proceedings in Informatics, Vol.10, Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik.（査読有り）

〔学会発表〕（計２件）
1. 青木 利晃，千葉 勇輝，松原 正裕，西昌能，成沢 文雄，
ISO26262 における安全仕様のゴール木を用いた浅い形式化，
第21回 ソフトウェア工学の基礎ワークショップ（FOSE 2014），ポスターセッション，2014年12月12日 鹿児島県霧島市.
2. Yuki Chiba,
Verifying the Correctness of Tupling Transformations based on Conditional Rewriting,
First International Workshop on Rewriting Techniques for Program Transformations and Evaluation (WPTE 2014), 13 July 2014, Vienna, Austria.

〔図書〕（計１件）
1. Manfred Schmidt-Schauß, Masahiko Sakai, David Sabel, Yuki Chiba:
First International Workshop on Rewriting Techniques for Program Transformations and Evaluation, WPTE 2014, July 13, 2014, Vienna, Austria. OASICS 40, Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik 2014, ISBN 978-3-939897-70-5 74 pages.

〔産業財産権〕
○出願状況（計１件）

名称　：要求仕様の記述と検証のためのシステム
発明者：青木利晃 千葉勇輝 松原正裕 松原満 成沢文雄 西昌能
権利者：日立製作所
種類　：特許
出願番号：特願 2014-174730
出願年月日：2014/08/29
国内外の別：国内

○取得状況（計０件）

名称：
発明者：
権利者：
種類：
番号：

出願年月日：
取得年月日：
国内外の別：

〔その他〕
ホームページ等
http://www.jaist.ac.jp/~chiba/index-ja.html

６．研究組織
(1)研究代表者
千葉 勇輝 (Yuki Chiba)
北陸先端科学技術大学院大学・情報科学研究科･助教
研究者番号：10509756

(2)研究分担者
(　　)

研究者番号：

(3)連携研究者
(　　)

研究者番号：