

1. 高階代数指向プログラミングによる新しいソフトウェア原理とその実現

九州工業大学 情報工学研究院 情報・通信工学研究系 教授 浜名 誠

概要

情報システムが重要な社会基盤の一つとなるにつれ、ソフトウェアの安全性保証が大きな課題となっている。本研究は関数型プログラミング言語を拡張し、信頼性のあるソフトウェアの基盤技術として新しいプログラミング原理である「高階代数指向プログラミング (HOAP)」の確立とその実装を与える事を目的とする。キーとなるアイデアは、高階代数データ型の高階書換え系による計算原理、および圏論的モデルから導かれる普遍性である。代数系が持っていた本来のポテンシャルを生かした「高階代数データ型プログラミング」の原理を確立する。

背景および目的

情報システムが重要な社会基盤の一つとなるにつれ、ソフトウェアの安全性保証が大きな課題となっている。このために近年、関数の概念を用いてプログラムを構成する関数型プログラミング言語が注目されている。関数型言語は、その数理的性質の良さからソフトウェア科学の分野で理論面、応用面ともに活発に研究されており、近年では産業界レベルにおいても関数型言語の生産性の高さや強力な機能が注目されており、C++ や Java などの主流プログラミング言語、MapReduce などの大規模計算フレームワークにも、関数型プログラミングのアイデアが取り入れられてきている。

本研究は関数型プログラミング言語を拡張し、信頼性のあるソフトウェアの基盤技術として新しいプログラミング原理である「高階代数指向プログラミング (HOAP)」の確立とその実装を与える事を目的とする。

方法

関数型言語において最も有用な機構の一つとして代数データ型があげられる。他言語族では複雑な定義となる線形リストや木構造といった再帰的なデータ構造を、関数型言語では代数データ型を用いることで自然に定義し、パターンマッチの機構により操作できる。これはプログラムを明解にすることで、バグ混入を防ぎ、また数学的なプログラム推論、変換を可能にさせる利点を持つ。

本研究は、高階関数と代数データ型を用いた関数型プログラムを高階書換え系によってモデル化する。これによって計算原理を解明する。また圏論的モデルから導かれる普遍性を用い、代数系が持っていた本来のポテンシャルを生かした高階代数指向プログラミングの原理を確立する。

研究成果

国際会議 SCSS 2024 にて、関数型言語 Haskell のために書換え理論を高階多相型へ拡張し、停止性と合流性検証手法と、書換え規則の正当性検証手法を研究した。これにより、関数型プログラミング言語 Haskell の書換え

規則の正しさを自動的に検証する基礎理論を構築した。この結果を東京大学で開催された第 40 回日本ソフトウェア科学会大会で発表し、日本ソフトウェア科学会大会優秀発表賞を受賞した。

国際会議 FLOPS 2024 で発表した論文では、コンパイラ最適化の妥当性を形式的に検証する際に重要な、評価（実行時）と洗練（コンパイル時）の間の関係を、項書換え理論の枠組みで捉え直し、文脈的改善(Contextual Improvement)を導出する手法を確立した。これは危険対解析手法によるもので、特に高階関数と代数データ型を用いたプログラムに対して既存手法よりも体系的で自動化が容易である。

プログラミング言語の国際論文誌 Science of Computer Programming 誌および国際会議 FLOPS 2020 で発表した論文では、多相型と型推論を書換え系に初めて導入した多相書換え系の理論を構築した。合流性検証のための危険対解析、モジュラ性といった性質の理論的証明をした。これを用いて、計算効果のある関数型言語の基礎体系である 計算的 λ 計算(Computational lambda-calculus)の合流性を初めて証明した。

学術論文誌 Logical Methods in Computer Science 誌で発表した論文では、二階書換えの停止性に関する新しいモジュラーな証明法を確立した。これは意味ラベリング手法を拡張した新規な証明方法によるものである。さらに応用として、代数的効果、エフェクトハンドラ、エフェクト理論を持つ Call-by-Push-Value 計算系の停止性を証明した。これは現実の関数型言語への有用な応用である。

結果とまとめ

本研究では、高階関数、代数データ型、多相型、計算効果を含む関数型プログラムを、書換え理論に基づいて統一的に扱うための基礎理論を構築した。特に、停止性・合流性・書換え規則の正当性・プログラム変換の妥当性を検証するための手法を整備し、Haskell を含む実用的な関数型プログラミング言語への応用可能性を示した。

これらの成果により、高階代数指向プログラミング (HOAP) の中核となる計算原理と検証原理を明確化した。すなわち、代数データ型の構成的な表現力と、高階関数・多相型・計算効果を含む現代的な関数型言語の機能を、書換え系の枠組みで形式的に扱えることを示した点に本研究の意義がある。

今後は、得られた理論をもとに、より実用的な検証ツールやプログラミング言語処理系への実装を進めることで、信頼性の高いソフトウェア開発を支える基盤技術として発展させることが課題である。

(完)

発表論文

- 1) Makoto Hamana. Foundations of Haskell's Rewrite Rules based on Higher-Kinded Polymorphic Rewrite Systems, 10th International Symposium on Symbolic Computation in Software Science (SCSS 2024), Lecture Notes in Computer Science 14991, pp. 79-95, Springer, 2024.
- 2) Koko Muroya, Makoto Hamana. Term Evaluation Systems with Refinements: First-Order, Second-Order, and Contextual Improvement, 17th International Symposium on Functional and Logic Programming (FLOPS 2024), Lecture Notes in Computer Science, pp. 31-61, Springer, 2024.
- 3) Makoto Hamana. Complete Algebraic Semantics for Second-Order Rewriting Systems based on Abstract Syntax with Variable Binding, Mathematical Structures in Computer Science, Cambridge University Press, Volume 32, Special Issue 4: The Power Festschrift, pp. 542--573, 2022.
- 4) Makoto Hamana. Modular Termination for Second-Order Computation Rules and Application to Algebraic Effect Handlers, Logical Methods in Computer Science, Vol. 18, Issue 2, No.8, June 14, 2022.
- 5) Yao Faustin Date, 浜名誠. GSOL: A Confluence Checker for Haskell Rewrite Rules. コンピュータソフトウェア, 39 巻 3 号, pp. 82-87, 岩波書店, 2022.

- 6) Makoto Hamana, Tatsuya Abe, and Kentaro Kikuchi. Polymorphic Computation Systems: Theory and Practice of Confluence with Call-by-value, Science of Computer Programming, Elsevier, Volume 187, 102322, 15 February 2020.