

科学研究費助成事業 研究成果報告書

平成 28 年 6 月 6 日現在

機関番号：12301

研究種目：挑戦的萌芽研究

研究期間：2013～2015

課題番号：25540002

研究課題名(和文) Haskell コアの意味論 - 先端的ソフトウェア検証基盤へ向けて

研究課題名(英文) Semantics of Core Haskell -- Towards Foundations of Verification of Advanced Functional Programs

研究代表者

浜名 誠 (Makoto, Hamana)

群馬大学・その他部局等・助教

研究者番号：90334135

交付決定額(研究期間全体)：(直接経費) 2,900,000円

研究成果の概要(和文)：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。

高い信頼性を持つソフトウェア構築のための基盤として、プログラミング言語の数学的モデルと基礎理論が必要である。このために本研究は、Haskell言語のコア言語の数学的モデルの探求を通じ、関数型プログラム検証に役立つプログラム理論を構築した。

研究成果の概要(英文)：In order to establish dependable software systems, we need to establish mathematical models and their theories. We develop various theories of functional programming through exploring mathematical models of Haskell's core language.

研究分野：ソフトウェア科学

キーワード：プログラム理論 圏論 関数プログラム 情報学基礎 Haskell

1. 研究開始当初の背景

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。高い信頼性を持つソフトウェア構築のための基盤として、プログラム言語の数学的モデルの基礎理論が必要である。このために本研究は、関数型プログラミング言語の国際標準の一つである Haskell 言語のコア言語の数学的モデルの探求を通し、Haskell プログラム検証に役立つ幅広いプログラム理論の構築、およびチュートリアルなどを通して、それらの理論を広く分かりやすく伝える事を目指した。

2. 研究の目的

申請者はこれまで、関数型言語の意味論を様々な側面から明らかにしてきた (高階書換え系 [05'06'07'09]、項グラフ構造 [06'09'10]、多相型 [11]、GADT [11]、副作用 [12] のモデル)。これらは数学的構造である前層上の代数構造を、様々な角度から適用して別個の対象をモデル化できることを示したものである。この一連の研究から得られた統一的な代数的視点を以て、Haskell 言語のコア言語の数学的モデル化について多角的に取り組む。

3. 研究の方法

プログラム理論で培われてきた以下の様々な意味論の側面を Haskell のコア言語に対して数学的モデルを詳しく調べる事を行った。

- (i) 操作的— 高階書換え系、グラフ計算系による定式化
- (ii) 代数的— 関数型プログラムの等式推論の枠組みと、代数的エフェクトの理論
- (iii) 型理論的— Haskell におけるデータのモデル化を指向

4. 研究成果

(I) コア Haskell の操作的意味論へのアプローチとして以下の三つの成果を得た。

- (1) 高階関数のモデルである遺伝単調高階関数類がモノイドを成すことを明らかにした。これを元にした二階項書換え系の代数的停止性証明へと応用した。

(2) 多相型付き 計算の停止性証明を代数化し、Reducibility の概念が、多相代数理論のモデルの一つである事を明らかにできた。Girard による Reducibility という極めてトリッキーな型付き集合の構成による証明が、多相代数理論のモデルの一例になることを明らかにし、これまで知られていなかった Reducibility 証明の本質とその代数的な性質のよさを初めて明らかにした興味深い結果といえる。Haskell プログラムの停止性推論に有効である。

(3) seq コンビネータのある Haskell コア言語を考察し、それを Moggi の計算モナドメタ言語に共有付き let 文を追加したものへの変換方法を考案した。ここでの等式推論体系は、seq による値呼びも加味した必要呼び計算をモデル化するものとなった。

(II) コア Haskell の代数理論へのアプローチとして以下の二つの成果を得た。

(1) seq 機構の公理化の研究。Haskell には正格評価を導入する seq 演算子が存在するため、その代数理論は単純な call-by-name の理論ではない。評価順序を公理化するための複数の方策を検討し、seq の case 文による表現が適切であることが分かった。GHC の中間言語において取られているアプローチを調べ、それとマッチする方法でもある。

(2) 再帰メカニズムの代数的公理化

再帰演算子の定式化のために、Conway 演算子と commutative identity という特殊な公理を用い、イテレーション理論として定式化する事でドメイン理論のような順序構造を必要としない、純粋な代数理論として再帰演算子を公理化可能である事がわかった。

また共同研究者の勝股は、Haskell の副作用のモデルとして使われるモナドと代数理論、エフェクトについてのチュートリアルを第 17 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 (PPL'15) にてを行い、発表賞を受賞した。

(III) コア Haskell のデータのモデル化に向けて型理論的アプローチにより以下の果を得た。

安全性保証付きデータ構造の理論の適用範囲をさらに進化させ、半構造データおよび根付きグラフに対する帰納データ構造の解明と代数化の論文の発表を行った。これにより半構造データおよび根付きグラフという複雑なデータ構造へ応用を広げることができた。

また 2013 年に発表した多相代数理論と関係が深い書換え系についてのチュートリアルを第 18 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 (PPL'16) にてを行い、発表賞を受賞した。

これらにより、信頼性のあるソフトウェアの理論的基礎としての依存型を用いた安全性保証付きデータ構造の理論の幅広い基礎の提供と、チュートリアルを通して関連コミュニティに貢献ができたと考えられる。

5. 主な発表論文等

[雑誌論文](計 6 件)

- [1] M. Hamana. Strongly Normalising Cyclic Data Computation by Iteration Categories of Second-Order Algebraic Theories, *Formal Structures for Computation and Deduction*, LIPIcs, 2016, 査読有.
- [2] S. Fujii, S. Katsumata, P. Mellies. Towards a Formal Theory of Graded Monads *Foundations of Software Science and Computation Structures (FoSSaCS 2016)*, LNCS 9634 2016, pp. 513-530, 査読有.
- [3] M. Hamana. Iteration Algebras for UnQL Graphs and Completeness for Bisimulation, *Fixed Points in Computer Science*, Electronic Proceedings in Theoretical Computer Science 191, pp.75-89, 2015, 査読有.
- [4] S. Katsumata, T. Sato. Codensity Liftings of Monads *Algebra and Coalgebra in Computer Science (CALCO 2015)*, LIPIcs 35, 2015, pp. 156-170, 査読有.
- [5] S. Katsumata. Parametric Effect Monads and Semantics of Effect Systems *Proc. of ACM Symposium on Principles of Programming Languages*, POPL 2014, 2014, pp. 633-645 査読有.
- [6] M. Fiore and M. Hamana. Multiversal Polymorphic Algebraic Theories: Syntax, Semantics, Translations, and Equational Logic, *Proc. of Twenty-Eighth Annual ACM/IEEE Symposium on Logic in Computer Science (LICS 2013)*, pp. 520-529, IEEE Computer Society, 2013, 査読有.

[学会発表](計 15 件)

- [1] 浜名誠. プログラミング言語研究のための (高階) 項書換え系入門, チュートリアル, 第 18 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 (PPL'16), 岡山県玉野市, 2016 年 3 月 8 日, 発表賞受賞.
- [2] 勝股 審也. モナド、代数理論と計算効果第 17 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 (PPL'15), 道後プリンスホテル, 2015 年 3 月 4 日, 発表賞受賞.
- [3] M. Hamana. Algebraic Semantics of Higher-order Abstract Syntax and Second-order Rewriting, International Summer School on Rewriting (ISR 2015), Leipzig, Germany, 10-14 August, 2015.
- [4] M. Hamana. Iteration Algebras for UnQL Graphs and Completeness for Bisimulation, The 10th International Workshop on Fixed Points in Computer Science (FICS'15), Technische Universitat Berlin, Germany. 11 September, 2015.
- [5] M. Hamana. Iteration Algebras for UnQL Graphs and Completeness for Bisimulation, Internal seminar, FireEye, Dresden, Germany, 15 September, 2015.
- [6] 浜名誠. Iteration Algebras for UnQL Graphs and Completeness for Bisimulation, 通研・共同プロジェクト「メタプログラムに

- に対する論理的アプローチ (3)」, 東北大学 電気通信研究所, 2015 年 9 月 28 日.
- [7] 浜名誠. A Sound and Complete Equational Axiomatisation of Cyclic Semi-structured Data, 通研・共同プロジェクト「メタプログラムに対する論理的アプローチ (2)」, 東北大学 電気通信研究所, 2015 年 2 月 24 日.
- [8] 浜名誠. Polymorphic Algebraic Theories and Logical Predicates, Semantic Methods in Haskell and Functional Programming Seminar, 国立情報学研究所, 2014 年 3 月 13 日.
- [9] 浜名誠. Multiversal Polymorphic Algebraic Theories, NII Shonan Meeting on Coinduction for Computation Structures and Programming Languages, 湘南国際村, 2013 年 10 月 8 日.
- [10] 浜名誠. On Multiversal Polymorphic Algebraic Theories, 通研・共同プロジェクト「メタプログラムに対する論理的アプローチ (1)」, 東北大学 電気通信研究所, 2013 年 12 月 18 日.
- [11] M. Hamana. Multiversal Polymorphic Algebraic Theories: Syntax, Semantics, Translations, and Equational Logic, Twenty-Eighth Annual ACM/IEEE Symposium on Logic in Computer Science (LICS'13), Tulane University, New Orleans, USA, 26 June, 2013.
- [12] M. Hamana. Multiversal Polymorphic Algebraic Theories, Category Theory Conference (CT'13), Macquarie University, Sydney, Australia, 11 July, 2013.
- [13] M. Hamana. Multiversal Polymorphic Algebraic Theories, General Algebra and Its Applications (GAIA'13), La Trobe University, Melbourne, 16 July, 2013.
- [14] 浜名誠. 多元宇宙多相型代数理論, 日本ソフトウェア科学会第 30 回大会, 9 月 11 日, 2013.
- [15] 浜名誠. Polymorphic Abstract Syntax via Grothendieck Construction, 15th JSSST Workshop on Programming and Programming Languages (PPL'13), 会津若松, 2013.
- [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] (計 2 件)
- 受賞
- 浜名誠. 第 18 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 PPL2016 発表賞
「プログラミング言語研究のための (高階) 項書換え系入門」
- 勝股審也. 第 17 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 PPL2015 発表賞
「モナド、代数理論と計算効果」
- ホームページ
<http://www.cs.gunma-u.ac.jp/~hamana/>
- ## 6. 研究組織
- (1) 研究代表者
- 浜名誠 (HAMANA MAKOTO)
群馬大学・大学院理工学府・助教
研究者番号: 90334135
- (2) 研究分担者
- 勝股審也 (SHINYA KATSUMATA)
京都大学・数理解析研究所・助教
研究者番号: 30378963