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 ２８ 年　 ６ 月　 ６ 日現在

機関番号：１２３０１
研究種目：基盤研究(B)（一般）
研究期間：2012～2015
課題番号：２４３００００１

研究課題名（和文）依存型理論による安全性保証付きデータ構造の創出・推論・進化

研究課題名（英文）Foundations of Dependable Datatypes by Dependent Types

研究代表者
浜名　誠（Makoto, Hamana）

群馬大学・大学院理工学府・助教

研究者番号：９０３３４１３５

交付決定額（研究期間全体）：（直接経費）　　4,900,000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。本研究は、信頼性のあるソフトウェアの理論的基礎を確立するために、安全性が保証されたプログラムを構成するための理論を与える事を目的とした。このために従来よりも厳密にデータの定義ができる依存データ型(dependent types)の代数的モデルを明らかにし、その応用を与えた。

研究成果の概要（英文）：In order to establish fundamentals of dependable software systems, we aim to establish theories of dependable software. We develop foundations and applications of dependent types by clarifying algebraic models of types and equational theories of dependent types.

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　多相型　代数理論

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。本研究は、信頼性のあるソフトウェアの理論的基礎を確立するために、安全性が保証されたプログラムを構成する理論を与える事を目的とした。本課題の特徴は、従来よりも厳密にデータの定義ができる依存データ型 (dependent types) と代数的手法を用いる事である。

2. 研究の目的

本研究は安全なデータ構造を構成する理論を明らかにすることを目的とする。依存型と性質保証の関係解明には、まず依存型の数学的構造 (モデル) を知る必要があるが、申請者の既存研究で依存多項式関手で表現可能であると分かっている。本提案は、依存型とデータ構造の関係の基盤研究として、圏論的代数の枠組みを使い、データ構造上の基本操作の安全性を事前に保証する枠組みを与え、依存型を用いた信頼性のあるソフトウェア構築の基礎を提供する事を目的とした。

3. 研究の方法

本研究は、データ構造における不変条件を依存型におけるパラメタとして表現し、安全性の保証があるデータ構造の表現の研究を行い、依存型のプログラムの停止性保証技法を探求する。また関数型言語において依存型を用い、ディペンダビリティの保証されたデータ構造を表現する方法を解明する。加えてその上の基本操作のプログラムの安全性保証技術の確立を目指した。

さらにデータ構造における本質的な不変条件を依存型におけるパラメタとして表現する方法と理論を段階的に解明する方針を取った。

4. 研究成果

(I) データ構造中のループ要素を特徴付ける研究を行った。Haskell 言語は再帰的定義により循環データ構造を定義することができる。さらに、言語要素アローを用いるとループを含む計算の新しいプログラミングができる。循環データ構造とループの計算というこれら一見異なるプログラム要素には実際は共通の原理があることを明らかにした。これはトレース付きフレイド圏を用いるもので、圏論的解釈を異なる実例に対して用いると、循環データ構造やループのある計算の様々なパターンを統一的に導出できることが分かった。この結果は国際会議 11th International Symposium on Functional and Logic Programming で発表し、Springer-Verlag から出版された。

またこれらの成果により、第 16 回群馬大学 横山科学技術賞を「依存型による安全で高信頼なソフトウェアの基礎研究」にて受賞した。

(II) 依存型を形式的に論じるためのモデルの等式論理の確立を行った。結果、様々な多相システムを統一的に扱うための体系である多相型代数理論を構築することに成功した。一般化依存多項式を用いることで、任意のシグネチャによる多相型構文と項中の型の代入を厳密にモデル化することができた。そして代数的モデルを持つ論理体系を圏論的考察から導出し、その正当性を証明した。特に多相型の型宇宙は Σ モノイドであることを明らかにし、これにより複数の型宇宙の間の変換を議論することが可能となった。これにより既存の種々の型理論とモデルを統一、単純化し、その本質を明確化する理論となった。また、この体系が確かに様々な実際例を統一的に扱うことができることを実際に例示することにより示した。

この結果は、理論計算機科学のトップ国際会議 ACM/IEEE Logic in Computer Science (LICS'13) で発表し、IEEE Press から出版された。

(III) 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構築ができた。

5. 主な発表論文等

[雑誌論文](計 4 件)

[1] M. Hamana. Strongly Normalising Cyclic Data Computation by Iteration Categories of Second-Order Algebraic Theories, *Formal Structures for Computation and Deduction*, LIPIcs, to appear, 2016, 査読有.

[2] M. Hamana. Iteration Algebras for UnQL Graphs and Completeness for Bisimulation, *Proc. of The 10th International Workshop on Fixed Points in Computer Science* (FICS'15), Electronic Proceedings in Theoretical Computer Science 191, pp.75-89, 2015, 査読有.

[3] 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.

[4] M. Hamana. Correct Looping Arrows from Cyclic Terms: Traced Categorical Interpretation in Haskell, *Functional and Logic Programming*, Lecture Notes in Computer Science 7294, p.136-150, Springe-Verlagr, 2012, 査読有.

[学会発表](計 16 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] 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.

[3] 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.

[4] M. Hamana. Iteration Algebras for UnQL Graphs and Completeness for Bisimulation, Internal seminar, FireEye, Dresden, Germany, 15 September, 2015.

[5] 浜名誠. Iteration Algebras for UnQL Graphs and Completeness for Bisimulation, 通研・共同プロジェクト「メタプログラムに対する論理学的アプローチ (3)」, 東北大学 電気通信研究所, 2015 年 9 月 28 日.

[6] 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学的アプローチ (2)」, 東北大学 電気通信研究所, 2015 年 2 月 24 日.

[7] 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.

[8] 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学的アプローチ (1)」, 東北大学 電気通信研究所, 2013 年 12 月 18 日.

[9] 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.

[10] M. Hamana. Multiversal Polymorphic Algebraic Theories, Category Theory Conference (CT'13), Macquarie University, Sydney, Australia, 11 July, 2013.

[11] M. Hamana. Multiversal Polymorphic Algebraic Theories, General Algebra and Its Applications (GAIA'13), La Trobe University, Melbourne, 16 July, 2013.

[12] 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 2013.

[13] M. Hamana. Polymorphic Abstract Syntax via Grothendieck Construction, 15th JSSST Workshop on Programming and Programming Languages (PPL'13), 会津若松, 2013.

[14] M. Hamana. Constructing Correct Looping Arrows from Cyclic Terms: Traced Categorical Interpretation in Haskell, Symposium on Symbolic Computation and Software Science, 筑波大学, 6 月 3 日, 2012.

[15] M. Hamana. Correct Looping Arrows from Cyclic Terms: Traced Categorica l Interpretation in Haskell, 11th International Symposium on Functional and Logic Programming (FLOPS'12), 神戸大学, 5 月 23 日, 2012.

[16] M. Hamana. Constructing Correct Looping Arrows from Cyclic Terms: Traced Categorical Interpretation in Haskell, 14th JSSST Workshop on Programming and Programming Languages (PPL'12), 南紀白浜, 3 月 8 日, 2012.

[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]

○受賞
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」

○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