

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成25年 5 月 15 日現在

機関番号：12301

研究種目：若手研究（B）

研究期間：2010～2011

課題番号：22700004

研究課題名（和文） ディペンデント型によるディペンダビリティ保証付きデータ構造の理論

研究課題名（英文） Dependable Data Structures by Dependent Types

研究代表者

浜名 誠 (HAMANA MAKOTO)

群馬大学・大学院工学研究科・助教

研究者番号：90334135

研究成果の概要（和文）：

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、依存データ型(ディペンデント型)と呼ばれる従来よりも厳密にデータの定義ができるデータ型を用い、信頼性のあるデータ構造とその理論を与えた。

研究成果の概要（英文）：

Dependent types are data types which ensure more precise properties of data than ordinary data types. Using dependent types, we develop a theory and applications of dependable data structures, aiming to establish foundations of reliable computer softwares.

交付決定額

(金額単位：円)

	直接経費	間接経費	合計
2010年度	1,600,000	480,000	2,080,000
2011年度	1,400,000	420,000	1,820,000
年度			
年度			
年度			
総計	3,000,000	900,000	3,900,000

研究分野：プログラム理論

科研費の分科・細目：情報学・情報学基礎

キーワード：データ構造、情報基礎、自動定理証明、関数プログラム

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、ソフトウェアのディペンダビリティの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、依存データ型 (ディペンデント型) と呼ばれる従来よりも厳密にデータの定義ができるデータ型を用い、信頼性のあるデータ構造とその理論を与えることを目的とした。

2. 研究の目的

研究代表者は 2009 年、共有や巡回を含む木構造を再帰データ型として厳密に表現する手法を発見した。特筆すべきことは「そこで使われるポインタが不正な領域を指し示すことは絶対にない」と保証することに成功した点である。一般化代数データ型というパラメータを持つデータ型を用いたこの研究で明らかになったことは「型のパラメータ」という要素がデータの安全性を保証するために効果的であるという事実である。この結果は本研究の目的達成のための重要な足掛かりとなった。

本研究はこれを発展させ、型理論で知られるより強力なデータ型である依存型 (ディペンデント型, dependent type) を用い、関数型言語におけるデータ構造とそれ上の基本操作の安全性を事前に保証する方法を解明した。先のパラメータによる性質の保証のアイデアを、より強力な依存型における依存性を用いることで広範囲なデータ構造の安全性保証へ拡張した。次を目的とした。

- 依存型を用いた安全性の保証があるデータ構造の表現と理論を解明する。

これにより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。

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ータとして表現し、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の確立を行うことを目指した。

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ータとして表現する方法と理論を次の 3 ステップを経ることにより解明した。

[I] 依存型とは、値でパラメタ化された型である。例えば「長さ n のベクトルの型」といった型を依存型では表すことができる。このときのパラメータ整数 n をデータが持つ不変条件として捉えることができる。申請者の先行研究により、パラメータをデータの形状と取ると、形状の情報を不変条件に用いるデータ構造を厳密に表すことができることが分かっている。これを発展させ、より複雑な構造のバリエーションを依存型で表現する方法の解明に取り組む。

[II] 得られた依存型を依存型システム Agda(Chalmers 大/産総研) に実装し基本操作のプログラミングを行う。

[III] 実装の知見を元に、最重要課題である「データ構造の安全性を表す不変条件と依存型の関係がどのように捉えられるか」を理論的に明らかにする。Martin-Löf 型理論の圏論的意味論と依存型理論の意味論の先行研究を参考にし、圏論を用いた依存型理論の代数的意味論を構築する。ここでキーとなるアイデアは、適切な前層の圏を設定することで、不変条件が圏のインデックスとして代数的に捉えることができるはずという観察、および「集合の圏」と「前層の圏」の間の随伴である。これまでの研究から、単純なデータ構造の表現の関手代数によるモデルを発展させた依存型表現の代数モデルが、随伴を用いて表現可能であると予想できるため、これによる圏論的代数の構成を行う。

4. 研究成果

(I) 依存型による安全性の保証があるデータ構造の表現と理論の解明を行った。まず、循環共有ポインタを持つ木構造のデータに対して安全な依存型の表現方法を明かにした。ここでの安全性とは、未確定領域を指すポインタがデータ構造上にないことを保証したものである。これを依存型プログラミング言語 Agda を用いて実装し、その有効性を示した。さらにこれを理論的に、ポインタ集合と文脈上の前層の圏における始代数として特徴づけすることに成功した。この結果、学術論文誌 Logical Methods in Computer Science にて出版された。

次に、より複雑なデータ構造として、束縛を持

つ抽象構文構造を考察した。多相型のシステムをモデル化するために、単純型付き抽象構文のための始代数の構成法を繰返し適用することを行った。すなわち、まず多相型の型構造へこの構成を適用し、次に項の構造へ適用した。この構成の中で、グロタンディーク構成を用いることで適切な多相型の文脈のための圏を構成できることを明らかにした。

この前層上の始代数は、多項式関手によって与えられるが、これを依存型の表現とも見なせるため、ここから実際に Agda 上の依存型を導出し、実装してその有効性を確かめた。

この結果は 14th International Conference on Foundations of Software Science and Computation Structures で発表し、論文は Springer-Verlag から出版された。

この二つの結果により、依存型によるデータ構造の表現の基礎理論として、前層上の圏中の始代数が適切であることが明らかになった。

(II) 依存型が帰納的に定義される帰納族とよばれる依存データ型の理論の解明を行った。依存性がない場合の帰納型は、集合上の関手として特徴付けできることが知られているが、帰納族については、個別の場合ごとにアドホックに対処されてきた。これに対し、Gambino と Hyland による依存多項式を用いることにより、すべての帰納族が一般的に依存多項式で表すことができることを初めて明らかにした。加えて Haskell の一般化代数データ型も同様に依存多項式で表すことができることも初めて明らかにした。

そしてこの一般理論をデータ上のディペンダビリティを保証したプログラミングへ応用した。これは帰納族に対するジェネリックな Zipper データ構造を導出することに成功したものである。

この結果は、依存型によるプログラミング技術と理論についての最新結果を議論する国際ワークショップである Shonan Workshop on Dependently Typed Programming 及び Shonan Workshop on Agda Meeting の共通開催日にて発表し、結果を多くの専門家に周知させることができた。本研究成果の洗練された定式化には関連研究者から好評価を得た。そして論文発表として 7th ACM SIGPLAN Workshop on Generic Programming で発表し、論文は ACM Press より出版された。

これにより、依存型によるデータ構造の表現の基礎理論として、依存多項式が有効であることを明らかにすることができた。

5. 主な発表論文等

[雑誌論文](計 5 件)

- [1] [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, Springer-Verlag, 2012, 査読有.
- [2] [Makoto Hamana](#), and Marcelo Fiore. A Foundation for GADTs and Inductive Families: Dependent Polynomial Functor Approach, *Proc. of 7th ACM SIGPLAN International Workshop on Generic Programming*, p.59-70, ACM Press, 2011, 査読有.
- [3] [M. Hamana](#). Polymorphic Abstract Syntax via Grothendieck Construction. *Foundations of Software Science and Computation Structures*, Lecture Notes in Computer Science 6604, p.381-395, Springer-Verlag, 2011, 査読有.
- [4] [M. Hamana](#). Initial Algebra Semantics for Cyclic Sharing Tree Structures. *Logical Methods in Computer Science*, Volume 6, Issue (3:15), p.1-23, 2010, 査読有.
- [5] [M. Hamana](#). Semantic Labelling for Proving Termination of Combinatory Reduction Systems, *Functional and Constraint Logic Programming*, Lecture Notes in Computer Science 5979, p.62-78, Springer-Verlag, 2010, 査読有.

[学会発表](計 8 件)

- [1] 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.

- [2] Correct Looping Arrows from Cyclic Terms: Traced Categorical Interpretation in Haskell, 11th International Symposium on Functional and Logic Programming (FLOPS'12), 神戸大学, 5月23日, 2012.
- [3] 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.
- [4] A Foundation for GADTs and Inductive Families: Dependent Polynomial Functor Approach, ACM SIGPLAN International Workshop on Generic Programming (WGP'11), National Institute of Informatics, 2011.
- [5] Dependent Polynomial Functors for Inductive Families, Shonan Meeting on Dependently Typed Programming and Agda Implementors, 湘南国際村, 2011年09月14日.
- [6] Polymorphic Abstract Syntax via Grothendieck Construction. 14th International Conference on Foundations of Software Science and Computation Structures, Saarbruecken, 2011.
- [7] Representing Polymorphic Higher-Order Abstract Syntax in Agda and Presheaves, 6th Theorem Proving and Provers Meeting (TPP'10), 名古屋大学, 11月25日, 2010.
- [8] Dependent Polymorphism, 日本ソフトウェア科学会第27回大会, 9 2010.

[図書](計1件)

- [1] チャールズ・ベゾルド (著), 井田哲雄, 鈴木大郎, 奥居哲, 浜名誠, 山田俊行 (訳)
チューリングを読む — コンピュータサイエンスの金字塔を楽しもう, 612 頁,
ISBN4822283720, 日経 BP 社, 2012.

[産業財産権]

○出願状況 (計0件)

○取得状況 (計0件)

[その他]

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・大学院理工学研究院・助教

研究者番号: 90334135