# 安全・高信頼なソフトウェアライブラリ構成法の基礎研究

代表研究者　　浜名 誠　　群馬大学大学院 理工学府 助教

## 1　研究調査の要旨

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、従来よりも厳密にデータの定義ができる依存データ型を用い「安全性保証付きライブラリを統一的に構成する理論」を与える研究である。

## 2　研究成果

### 2.1　目的・意義

本研究は安全なソフトウェアライブラリを構成するための理論を明らかにすることを目的とした。依存型と性質保証の関係解明には、依存型とデータ構造の関係の次の課題を明らかにした。

[I] データ構造と基本操作を、どのように依存型として創出するか
(欲しいデータ構造の仕様から依存型を統一的に合成する方法)

[II] その依存型はどのように論理的に推論できるのか
(依存型を形式的に論じ型検査を行うための等式論理の確立)

本研究が使うアプローチは圏論的代数の枠組みである。これらにより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手法を提供を目指した。

### 2.2　研究方法と結果

課題 [I]**「与えられたデータ構造の依存型としての表現方法と理論の解明」**

依存型とは、値でパラメタ化された型である。代数的に統一的にデータ構造と基本操作を依存型で表す方法と、その理論を次の 3 ステップを経ることにより解明した。

1. パラメ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。これを発展させ、より複雑な木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んだ。アルゴリズムの分野で知られる B 木、AVL 木、赤-黒木、Zipper といった純関数型データ構造とその上の基本操作を依存型の観点から再考察した。

2. 得られた依存型の有効性を確認するために、依存型システム Agda に実装し、基本操作のプログラミングを行った。

3. 実装の知見を一般化し、データ構造と依存型表現の対応関係がどのように捉えられるかを理論的に明らかにした。前項で実装した依存型からは前層の圏上の依存多項式関手をつくり出すことができたので、自由 $\Sigma$ モノイドが構成できた。結果としてデータ構造の圏論的性質を表す構造が構成できた。

課題 [II]**「依存型はどのように論理的に推論できるのか—依存型の等式論理体系の確立」**

依存型の進化を議論するためのフレームワークとして、何と何が等しいのかを論ずるための論理、等式論理が必要である。この体系と意味論を次の 3 ステップを経ることにより解明した。

1. 依存型の圏論的意味論から等式論理の抽出
2. 依存型等式論理の定式化
3. 等式論理の高次元代数によるモデル

## 2.3 研究成果

安全・高信頼なソフトウェアライブラリ構成法可能にさせる多相システムを統一的に扱うための体系である多相性代数理論を構築することに成功した。次の三つの成果を得た。

(1) 様々な多相型体系を包括する、多元的な型宇宙を持つ多相型代数理論を完成させた。

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

(3) 多相型付き λ 計算の停止性証明を代数化し、Reduciblity の概念が、実際は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。

(1) が本研究の主要結果で、型理論 (正しさのための論理的枠組み) と代数 (プログラムの抽象仕様の枠組み) の理論を統合するようなこれまでにない統一理論を構築することができた。特に (3) については、Girad による Reducibility という極めてトリッキーな型付き集合の構成よる証明が、本研究の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を明らかにした興味深い結果といえる。

研究成果について論文を執筆し、Springer-Verlag 社の *Functional and Logic Programming* 誌にて出版した。また本研究のアプローチが評価され、第 16 回横山科学技術賞を受賞した。さらに当分野の基礎的な重要性を持つアラン・チューリングの論文の解説書を翻訳し、本研究の基礎知識を社会に還元した。また国際会議 HOR'12 の議長を務め、査読委員会の設定と論文の選定、および会議の議長とマネージメントを行った。本会議は名古屋での書換え会議の中で最大の動員数を得ることができた。

研究成果について論文を執筆した論文が、理論計算機科学の最難関会議である ACM/IEEE の LICS'13 に受理され、IEEE 社の *Logic in Computer Science* 誌にて出版された。ジェネリックなプログラムを可能にさせる多相データ型は、初め関数型プログラミング言語で取入れられ、その有効性からその後は、オブジェクト指向言語や、並行計算システムなど様々な計算システムへと取入れられてきた。この論文は、これら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性代数理論を理論計算機分野で初めて提案した画期的なものである。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。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。

また関数型プログラミングとプログラム意味論の有力国際会議 MSFP'14 および国内での最大のプログラミング言語研究のワークショップ PPL'14 のプログラム委員を務めた。

さらに 国立情報学研究所にて意味論的関数型プログラミングの研究会の企画と主催、研究発表を行った。本研究会は情報学研究所にて行う関数型プログラミングの研究会としては最大規模の参加者を得ることができた。

## 2.4 成果発表業績

- **出版論文**

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.

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), p.520-529, IEEE Computer Society.

- **受賞**　第 16 回横山科学技術賞,
「依存型による安全で高信頼なソフトウェアの基礎研究」, 2012 年 10 月 26 日
- **著書**

チャールズ・ペゾルド (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.

- **研究会議 議長/プログラム委員長**

国際会議 6th International Workshop on Higher-Order Rewriting (HOR'12), 名古屋大学, 2012 年 6 月 2 日. `http://www.cs.gunma-u.ac.jp/events/hor/`

第 17 回 日本ソフトウェア科学会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) プログラム委員長, 愛媛県松山市道後, `http://www-kb.is.s.u-tokyo.ac.jp/ppl2015/` , 2015.

- **プログラム委員**

· 第 16 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 2014),
日本ソフトウェア科学会プログラミング研究会, プログラム委員.

· The fifth workshop on Mathematically Structured Functional Programming (MSFP 2014),
12 April, 2014, Grenoble, France, affiliated with ETAPS 2014, program committee member.

· 国際会議 2nd International Workshop on Haskell and Rewriting Techniques (HART'14), affiliated with ICFP 2014, program committee member.

- **研究会主催**

· Semantic Methods in Haskell and Functional Programming Seminar,
国立情報学研究所, 2014 年 3 月 13 日.