

平成 23 年 5 月 31 日現在

研究種目：基盤研究(B)  
 研究期間：2007 ～ 2009  
 課題番号：19300007  
 研究課題名(和文) 計算と論理の融合によるバグのないソフトウェア構築環境に関する研究  
 研究課題名(英文) Software development environment based on integration of computation and logic  
 研究代表者  
 佐藤 雅彦 (SATO MASAHIKO)  
 京都大学・大学院情報学研究科・教授  
 研究者番号：20027387

研究成果の概要(和文):本研究では,安全なソフトウェアを効率的に開発できる環境の構築を目指し,その理論的基盤を与えるロジカル・フレームワークとして,計算概念と論理体系を統一的に扱える自然枠組 (Natural Framework, NF) の構築とその実装を目的とし,主に次のような成果を得た. (1) メタ変数の理論を形式化した. (2) 自然枠組において計算体系とその理論を統一的に扱うための形式的言語体系をメタ変数の理論をもとに構築した. (3) 自然枠組の実装のためのプログラミング言語の設計を行った.

研究成果の概要(英文): This project proposes the Natural Framework (NF) as a theoretical foundation of software development environments. NF is a logical framework in which we can describe both calculus systems and logical systems, and hence we can uniformly discuss reliability of both software and meta theories for software. In this project, in order to realize NF, (1) a formal theory of meta variables has been proposed, (2) a syntactic theory for NF has been proposed, and (3) a programming language to implement NF has been designed.

交付決定額

(金額単位:円)

	直接経費	間接経費	合計
2007年度	3,800,000	1,140,000	4,940,000
2008年度	3,500,000	1,050,000	4,550,000
2009年度	3,200,000	960,000	4,160,000
年度			
年度			
総計	10,500,000	3,150,000	13,650,000

研究分野:総合領域

科研費の分科・細目:情報学・ソフトウェア

キーワード:自然枠組,ソフトウェア開発,ソフトウェア検証,メタ言語,式の理論

## 1.研究開始当初の背景

近年,ソフトウェアの品質に対する要求はますます高まっているが,実際のソフトウェア開発においては,ソフトウェア構築環境とは別に検証システムを用意する必要があったり,検証システム自体の正しさを保証する議論は手書きの非形式な証明に頼っているなど,未だ安全性・効率性の面で不十分な点が多い.

このような状況を改善するため,ソフトウェアの正しさを厳密に検証する理論と技術,および,その理論そのものの安全性を保証するためのメタ理論が必要である.さらに,バグのないソフトウェアの構築のために,これらの技術をとりこんだソフトウェア構築環境を実現することが必要である.

## 2.研究の目的

本研究では,論理学の手法を用いて形式的体系の性質を記述・検証するための言語体系であるロジカル・フレームワーク (論理枠組) を基礎としたソフトウェア構築環境を実現することを目的とする.とくに,ソフトウェア自身だけではなく,ソフトウェアの性質を記述するための理論をも含めた階層をまるごと対象とする議論が可能であるような言語体系を構築するために,メタ変数の概念の形式化を行い,それを用いて計算と論理を融合したロジカル・フレームワークの理論を構築・実装することを目的とする.

より具体的には以下のとおりである.

(1) ソフトウェア自身だけでなく,そのソフトウェアに関するメタな議論のための論理的体系をも形式的に記述するために,通常非形式的に扱われるメタ変数を形式的な概念として取り扱うための理論を構築する.

(2) ロジカル・フレームワークの基盤となる形式言語体系として,メタ変数の理論を元に,ソフトウェアを対象とする計算体系と,その理論である論理体系の両方を統一的に記述できるような共通の言語を開発する.

(3) ロジカル・フレームワーク実装用プログラム言語を設計・実装する.

(4) 以上の理論的・技術的研究を総合し,ロジカル・フレームワークを基礎としたソフトウェア構築環境を実装する.この環境では,ソフトウェア開発と同じ枠組で論理体系を表現できるため,ソフトウェア検証や証明支援技術をとりこみ,バグのないソフトウェアを効率良く開発できる環境を実現する.

## 3.研究の方法

以下の計画に沿って研究を行なった.

(1) 我々が既に提案していたロジカル・

フレームワークである自然枠組 (Natural Framework, NF) をもとに, 計算と論理が自然に融合するように拡張を行なう。プログラムとその安全性を検証する論理とを同じ枠組で記述し議論できるようにするために, メタ変数の概念に関する理論的研究を行ない, 得られた知見を自然枠組に反映させる。

(2) 自然枠組の実装に適したプログラム言語を設計し実装する。このプログラム言語を利用して自然枠組を実装し, 証明検査のインターフェイスや半自動化などの機能を設計し実装する。その上で, これらの枠組を利用したソフトウェア構築のための環境を設計し, 実装する。

#### 4. 研究成果

本研究では以下の成果を得た。

(1) メタ変数の概念を形式的に扱うための理論的研究を行なった。本研究で提案する自然枠組においては, プログラムなどの対象と, それらをメタな立場から議論するためのメタ言語を同一の枠組で扱う必要がある。このようなメタ言語中で用いられる引用において重要な役割を果たすメタ変数の概念を形式的に扱うために, 階層的な対象を記述するための形式的体系を提案し, その性質を調べた。

(2) 目標とする自然枠組を記述する言語は必然的に形式的な言語になるが, その形式的言語(対象言語)を人間が理解するためには, 最終的には自然言語をメタ言語として用いる必要がある。通常は, この対象言語とメタ言語は異なる言語であるとされている。しかし, この見方とは対照的な, 対象言語をメタ言語の

部分言語とみなす見方が可能であることを提案し, その有用性を指摘した。

(3) フレームワークの基礎となる式の理論を与えるために, 抽象操作について考察し, これを実現する新しい手法を提案した。数学を形式的に記述するときに変数による抽象操作は必須となる基本的な操作である。本研究では, この抽象操作と, その逆操作である具体化を実現する具体的な新しい方法を提案した。これは, 本研究で提案する自然枠組の式の理論における抽象操作の理論的基盤を与えることが期待されるが, 本手法自体はより一般の形式的言語における抽象操作を表現できるものである。

(4) 以上の理論的考察をふまえ, 設計した自然枠組の実装に向けて, プログラミング言語の設計を行なった。この言語の中核部分で必要となる数学的な対象は, それぞれ, ある基本的な「概念」を満足するものとして特徴づけられ, そのため, 抽象化の操作を必要としない帰納的な記号操作でこれらの数学的対象が構成できることを示した。

#### 5. 主な発表論文等

(研究代表者, 研究分担者及び連携研究者には下線)

[雑誌論文](計 6件)

[1] Takeshi Tsukada and Atsushi Igarashi, A logical foundation for environment classifiers, Proceedings of the 9th International Conference on Typed Lambda-Calculi and Applications

(TLCA '09), LNCS 5608, 341-355, 2009, 査読有.

[2] Masahiko Sato, Takafumi Sakurai, Yuki-yoshi Kameyama and Atsushi Igarashi, Calculi of Meta-variables, Frontiers of Computer Science in China 2(1):12-21, 2008, 査読有.

[3] 佐藤雅彦, フレーゲの計算機科学への影響, 分析哲学の誕生 (日本科学哲学会編, 勁草書房), 127-141, 2008, 査読無.

[4] Masahiko Sato, A Framework for Checking Proofs Naturally, Journal of Intelligent Information Systems 31:111-125, 2008, 査読有.

[5] Masahiko Sato, External and Internal Syntax of the Lambda-Calculus, The Austrian-Japanese Workshop on Symbolic Computation in Software Science (SCSS 2008), 176-195, 2008, 査読有.

[6] Atsushi Igarashi and Masashi Iwaki, Deriving compilers and virtual machines for a multi-level language, Asian Symposium on Programming Languages and Systems (APLAS 2007), 206-221, 2007, 査読有.

[学会発表](計 3 件)

[7] Takeshi Tsukada and Atsushi Igarashi, A logical foundation for environment classifiers, Proceedings of

the 9th International Conference on Typed Lambda-Calculi and Applications (TLCA '09), LNCS 5608, 341-355, 2009, 査読有. [1] と同内容.

[8] Masahiko Sato, External and Internal Syntax of the Lambda-Calculus, The Austrian-Japanese Workshop on Symbolic Computation in Software Science (SCSS 2008), 176-195, 2008, 査読有. [5] と同内容.

[9] Atsushi Igarashi and Masashi Iwaki, Deriving compilers and virtual machines for a multi-level language, Asian Symposium on Programming Languages and Systems (APLAS 2007), 206-221, 2007, 査読有. [6] と同内容.

[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]

ホームページ等

## 6. 研究組織

(1) 研究代表者

佐藤 雅彦 (SATO MASAHIKO)

京都大学・大学院情報学研究科・教授

研究者番号: 20027387

(2) 研究分担者

五十嵐 淳( IGARASHI ATSUSHI )  
京都大学・大学院情報学研究科・准教授  
研究者番号: 40323456

中澤 巧爾( NAKAZAWA KOJI )  
京都大学・大学院情報学研究科・助教  
研究者番号: 80362581

山本 章博( YAMAMOTO AKIHIRO )  
京都大学・大学院情報学研究科・教授  
研究者番号: 30230535

湯浅 太一( YUASA TAIICHI )  
京都大学・大学院情報学研究科・教授  
研究者番号: 60158326

(3) 連携研究者