様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　５ 年　 ６ 月　 ４ 日現在

機関番号：１４３０１
研究種目：基盤研究(B)（一般）
研究期間：2017～2020
課題番号：１７Ｈ０１７２４

研究課題名（和文）クラス理論に基づく自己拡張可能なソフトウェア検証体系の深化

研究課題名（英文）Deepening of a self-extendable software verification system based on class theory

研究代表者
佐藤　雅彦（Sato, Masahiko）

京都大学・情報学研究科・名誉教授

研究者番号：２００２７３８７

交付決定額（研究期間全体）：（直接経費）　　14,000,000円

研究成果の概要（和文）：ソフトウェアの安全性を検証するための理論として,論理学の手法を用いて形式的体系の性質の記述及び検証を数学的に厳密な方法で行う言語体系である論理枠組が提案されている.本研究では,従来の論理枠組は型理論の上に構築されているのに対してクラス理論の上に構築することを実現した.
ここでのクラス理論は本研究で新しく提案した理論であり,型理論にない柔軟性があり,さらにクラス全体のクラスを矛盾なく扱えるという特徴がある.この特徴のため,論理枠組の中で,枠組自身に言及し,その構造を解析することができた.とくに重要な成果として,変数の束縛機構を分析し,λ計算とコンビネータ論理の同値性を示すことができた.

研究成果の学術的意義や社会的意義
社会基盤としての計算機の重要性の増加により,ソフトウェアの安全性など,ソフトウェの品質に対する要求はますます高まっている.
本研究は,バグのないソフトウェアを構築するためのクラス理論に基づく理論的基盤を与え,さらにそれを用いて(ユーザによる自己拡張を許す)自然枠組(Natural Framework)とよばれるソフトウェア実行および検証環境を提供するものであり，大いに学術的意義，社会的意義がある.

研究成果の概要（英文）：In order to verify the safety of software, the concept of Logical Framework is proposed. A logical framework can be used to internally realize formal systems and prove their properties in a rigorous manner. In contrast to the fact that most logical frameworks are based on type theory, we realized our logical framework based on class theory.
We proposed the new class theory in this research. The class theory is more flexible than type theories and enjoys the property that it can deal with the class of all classes in a consistent way. Due to this property, our logical framework can refer to the framework itself and can analyze its structure by itself. We analyzed the mechanism of variable binding in the lambda calculus, and could show the equivalence of lambda-calculus and combinatory logic.

研究分野：ソフトウェアの基礎理論

キーワード：クラス理論　型理論　証明検証　ソフトウェアの安全性

1. 研究開始当初の背景

(1) ソフトウェアの安全性を検証するための理論として, 論理学の手法を用いて形式的体系の性質の記述及び検証を数学的に厳密な方法で行なう言語体系であるロジカル・フレームワーク (論理枠組) が提案されてきていた. 形式的な計算体系であるプログラミング言語をロジカル・フレームワーク上で記述することにより, ソフトウェアに求められる仕様を正確に記述し, 与えられたソフトウェアがその仕様を満足することを厳密に検証することが可能となる. さらにロジカル・フレームワークを計算機上に実装することができれば, これらの記述・検証の機械的に正確な検査が可能となり, ソフトウェアの品質面, 安全面の信頼性が高まることが期待された.

(2) このことから, ソフトウェアの安全性を保証するためには, ① 形式的体系 (ここではプログラミング言語, およびソフトウェア) を正確に記述するためのロジカル・フレームワークの理論研究, および, ② ロジカル・フレームワーク上に記述された推論過程が正しいかどうかを機械的・形式的に検査する技術の研究といった, 理論的基盤を与えることが重要である. さらに, バグのないソフトウェアを効率良く開発するためには, これらの理論的基盤をとりこんだソフトウェア構築環境を実現することが非常に重要である. ここで注意すべきは, ソフトウェア理論自体の正しさをロジカル・フレームワークの上で議論するためには, 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必要がある, という点である. 以上の目的の実現のためには, 計算の概念を利用したより自然な形での証明の構築を可能とする計算と論理を融合し, 自己拡張可能なロジカル・フレームワークを設計する必要があった.

2. 研究の目的

(1) 近年のインターネット/計算機の爆発的な普及, それに伴う社会基盤としての計算機の重要性の増加により, ソフトウェアの安全性など, 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. しかし, 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しなければならないなど, 安全性の面で充分とは言えず, 実際, バグを含んだソフトウェアが重要な箇所で利用され, 重大な障害が発生している例も多い.

(2) 本研究は, この要求に応えるため, バグのないソフトウェアを構築するためのクラス理論に基づく理論的基盤を与え, さらにそれを用いて (ユーザによる自己拡張を許す) 自然枠組 (Natural Framework) とよばれるソフトウェア実行環境およびソフトウェア検証環境を同時に提供するシステムを計算機上に実現することを目的とした.

3. 研究の方法

(1) 基礎理論研究. 本研究で構築するシステムがメタレベルと対象レベルをシステム自身で記述, 操作でき, さらに自己拡張可能になるようにするために必要な概念であるクラス理論, 自然枠組およびメタ変数を中心にした理論研究を行った. 本研究で提案したクラス理論は, 既存のロジカル・フレームワークの多くがその基礎としている型理論の弱点を取り除き, さらにより単純な構成原理のもとに, 自己拡張可能性等の, 型理論にない柔軟性を持つように設計することを考えた. とくに次のことに着目して研究を進めた. 型理論においては, 一旦理論が固定されると, その型理論でユーザが新しく構築できる型は, その理論で許されるスキーマにあてはまるものに限定される. このため, ユーザが本当にほしい型を自然に実現することはできず, 既存の型を組合せることで不自然な形で実現することになり, ユーザによる自己拡張の自由はない. 提案したクラス理論では, ユーザがほしい対象のクラスを, そのクラスの対象が満足すべき「性質」から直接, ユーザ自身が構築できる仕組みを提供することができた.

(2) システム実装. 自然枠組システム実装のために用いる言語として, 自然枠組記述言語自身を用いる予定であるので, 研究の前半ではこの言語の実装を行い, 後半ではこの言語を用いて自然枠組システムの実装を行っ

た. 実装にあたっては Scheme の処理系のひとつである Racket を用いた.

4. 研究成果

(1) メタ変数の概念の形式化. メタ変数に関する理論的な考察を行なった. 非形式的には既に幅広く用いられているメタ変数の概念を, 理論的に考察し, できる限りその意味を正確に反映する形で形式化した. 本研究では, 今回提案するクラス理論の手法を用いて, メタ変数を扱うための形式的計算体系を構成する方法をとったが, この際, メタ変数の概念を, 既存の様々な計算体系に付加することができるような形で定式化できる方法で構成した. この手法の正しさと, 汎用性を確認するため, 型なし λ 計算や単純型付 λ 計算などにこの方法を適用してメタ変数の概念を追加し, この体系に関して, 合流性や停止性などの期待される性質を証明することができた.

(2) 変数束縛を持つデータ構造に関する研究. プログラムにおけるパラメータを持つ手続き, 全称化 (「すべての〜について」) を伴なう論理式といった概念を扱うためには, 変数束縛のある構造を対象として議論を行なう必要がある. しかし, このような構造に対しては, 素朴な帰納法による証明技法は正しくないことが知られている. そのため, 変数束縛を持つデータ構造に関する性質を証明するための技法を, クラス理論の立場から研究し, 自然枠組上の証明検査に適用した. この成果は, 本研究代表者が変数束縛機構に関して共同研究を行っているミュンヘン大学の Helmut Schwichtenberg 教授との共同研究によるものである.

(3) λ 計算とコンビネータ論理との関係について. λ 計算とコンビネータ論理の両方を代数的に再構築し, これら両者が代数的に同型であることを residual の理論を用いて示した.

５．主な発表論文等

〔雑誌論文〕　計7件（うち査読付論文　7件／うち国際共著　0件／うちオープンアクセス　1件）

１．著者名 佐藤雅彦	４．巻 53
２．論文標題 証明支援系と型理論	５．発行年 2020年
３．雑誌名 科学哲学	６．最初と最後の頁 3-23
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Sato Yuhi、Kameyama Yukiyoshi、Watanabe Takahisa	４．巻 -
２．論文標題 Module generation without regret	５．発行年 2020年
３．雑誌名 Proceedings of the 2020 ACM SIGPLAN Workshop on Partial Evaluation and Program Manipulation (PEPM '20)	６．最初と最後の頁 1-13
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/3372884.3373160	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Kawata Akira、Igarashi Atsushi	４．巻 -
２．論文標題 A Dependently Typed Multi-stage Calculus	５．発行年 2019年
３．雑誌名 Asian Symposium on Programming Languages and Systems (APLAS2019)	６．最初と最後の頁 53～72
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-34175-6_4	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Taro Sekiyama, Atsushi Igarashi	４．巻 LNCS 11423
２．論文標題 Handling Polymorphic Algebraic Effects	５．発行年 2019年
３．雑誌名 Proceedings of European Symposium on Programming (ESOP 2019)	６．最初と最後の頁 1-28
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-17184-1_13	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

１．著者名 Junpei Oishi and Yukiyoshi Kameyama	４．巻 無
２．論文標題 Staging with control: type-safe multi-stage programming with control	５．発行年 2017年
３．雑誌名 Proceedings of the 16th {ACM} {SIGPLAN} International Conference on Generative Programming: Concepts and Experiences (GPCE 2017)	６．最初と最後の頁 29--40
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/3136040.3136049	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Takahisa Watanabe and Yukiyoshi Kameyama	４．巻 無
２．論文標題 Program generation for ML modules (short paper)	５．発行年 2018年
３．雑誌名 Proceedings of the ACM SIGPLAN Workshop on Partial Evaluation and Program Manipulation (PEPM'08)	６．最初と最後の頁 60-66
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/3162072	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Hirofumi Nakamura, Kensuke Kojima, Kohei Suenaga, Atsushi Igarashi	４．巻 無
２．論文標題 A Nonstandard Functional Programming Language	５．発行年 2017年
３．雑誌名 Proceedings of 15th Asian Symposium on Programming Languages and Systems (APLAS 2017)	６．最初と最後の頁 514-533
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-71237-6_25	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計8件（うち招待講演　1件／うち国際学会　5件）

１．発表者名 Satoru Kawahara, Yukiyoshi Kameyama
２．発表標題 One-shot Algebraic Effects as Coroutines
３．学会等名 The 21st International Symposium on Trends in Functional（国際学会）
４．発表年 2020年

１．発表者名
Akira Kawata, Atsushi Igarashi

２．発表標題
A Dependently Typed Multi-Stage Calculus

３．学会等名
Asian Symposium on Programming Languages and Systems (APLAS2019)（国際学会）

４．発表年
2019年

１．発表者名
勝田峻太朗, 五十嵐淳

２．発表標題
依存型を備えた多段階計算の同値型による拡張

３．学会等名
第22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（PPL2020）

４．発表年
2020年

１．発表者名
Masahiko Sato

２．発表標題
Reflections on the eta-rule of the lambda-calculus

３．学会等名
Oberseminar, Ludwig Maximillian University of Munich（招待講演）（国際学会）

４．発表年
2019年

１．発表者名
Taro Sekiyama, Atsushi Igarashi

２．発表標題
Handling Polymorphic Algebraic Effects

３．学会等名
European Symposium on Programming (ESOP2019)（国際学会）

４．発表年
2019年

１．発表者名
Yukiyoshi Kameyama

２．発表標題
A Lightweight Approach to Module Generation

３．学会等名
IFIP Working Group 2.11, 18th meeting (Kyoto, Jpaan)（国際学会）

４．発表年
2018年

１．発表者名
Masahiko Sato

２．発表標題
A common notation system for both lambda calculus and combinatory logic

３．学会等名
Oberseminar Mathematische Logik, (LMU Munich, Mathematisces Institut)

４．発表年
2017年

１．発表者名
Masahiko Sato

２．発表標題
A common notation system for the lambda calculus and combinatory logic

３．学会等名
Second Workshop on Mathematical Logic and its Applications

４．発表年
2018年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究分担者	桜井　貴文 (Sakurai Takafumi) (60183373)	千葉大学・大学院理学研究院・教授 (12501)	

6．研究組織（つづき）

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究分担者	亀山　幸義 (Kameyama Yukiyoshi) (10195000)	筑波大学・システム情報系・教授 (12102)	
研究分担者	五十嵐　淳 (Igarashi Atsushi) (40323456)	京都大学・情報学研究科・教授 (14301)	

7．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

8．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関