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　２ 年　 ６ 月 ３０ 日現在

機関番号：１２１０２
研究種目：若手研究(A)
研究期間：2016～2019
課題番号：１６Ｈ０５８５６

研究課題名（和文）高レベル言語で記述されたソフトウェアの時相的・関係的仕様の検証

研究課題名（英文）Temporal and Relational Verification of High-Level Programs

研究代表者
海野　広志（Unno, Hiroshi）

筑波大学・システム情報系・准教授

研究者番号：８０５６９５７５

交付決定額（研究期間全体）：（直接経費）　　11,270,000円

研究成果の概要（和文）：本研究では、ソフトウェアの信頼性向上を目的とし、これまで研究代表者らが提案してきたリファインメント型システムやホーン節制約解消法といった高レベル言語のための検証理論とそれに基づく全自動検証ツールRCamlを発展させ、高レベルプログラムの関係的・時相的仕様検証を実現した。特に、関係的仕様検証が可能な（余）帰納的定理証明に基づくホーン節制約解消法および時相的仕様検証が可能な不動点論理制約解消法を世界で初めて実現した。

研究成果の学術的意義や社会的意義
本研究で提案した高レベルプログラムの時相的・関係的検証のためのリファインメント型システム、不動点論理、動的論理といった検証理論・手法は、既存手法が扱えなかった高階関数や代数データ型といった発展的な言語機能を扱うことを可能とした。また、本研究では、提案した検証理論に基づき、高階関数型言語 OCaml のための検証ツール RCaml、不動点論理制約解消ツール MuVal、述語制約解消ツール PCSat の開発も行っており、今後これらのツールを実際のソフトウェア開発現場で実用可能なレベルまで発展させれば、ソフトウェアの信頼性向上に大きく貢献することが期待される。

研究成果の概要（英文）：In this research, we have extended verification methods and tools based on refinement types and constrained Horn clauses to enable relational and temporal verification of high-level programs. For relational verification, we have proposed Horn constraint solving methods based on (co-)inductive theorem proving. We have also presented methods for solving first-order fixpoint logic constraints to enable temporal verification.

研究分野：プログラム検証

キーワード：プログラム検証　プログラミング言語　関係的仕様　時相的仕様　依存リファインメント型　ホーン節制約解消　不動点論理　帰納的定理証明

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

計算機システムが、交通・金融・医療・電力等の重要な社会基盤をはじめ、経済活動や日常生活にも深く関わっている今日、その信頼性の確保は喫緊の社会的課題である。そのための技術として、ソフトウェアがその仕様を満たしていることをプログラム理論・形式言語理論・アルゴリズム論に基づき数学的に証明もしくは反証することが可能な形式検証法が学術界・産業界双方から注目されている。実際に、世界中の研究グループやMicrosoft、Facebook といった世界的企業によって様々な検証ツールが開発・公開されているが、それらの多くは、C 言語といった低レベル言語で記述された低レベルプログラムを対象としていたり、高レベルの言語機能が使われていた場合には低精度もしくは半自動の検証しかできなかったり、オブジェクト指向・関数型といった高レベル言語で記述された高レベルプログラムの全自動・高精度検証の実現には理論・実践の両面で多くの課題を残していた。

研究代表者らはリファインメント型やホーン節制約解消法といった高レベル言語のための形式検証理論で世界をリードする研究を行ってきており、実践面でも関数型言語 OCaml や XML 処理言語といった高レベル言語のための全自動・高精度形式検証ツールを世界に先駆けて実現している。その中でも特に本研究に関係するのは、リファインメント型システムを用いた、高階関数型言語のための検証理論と、それに基づいて開発された OCaml 言語のための全自動・高精度形式検証ツール RCaml である。ここでリファインメント型システムとは、高レベルプログラムの詳細な仕様を型として記述し、プログラムが実際にその仕様を満たすことを形式的に検証することが可能なプログラム論理であり、より低レベルな言語のためのプログラム論理として有名なホーア論理の高レベル言語版といえる。OCaml 言語の従来の型システムでは、整数の加算を行う関数に対して、「整数を 2 つ受け取って 1 つ返す」という仕様を表す型「$\mathrm{int} \to \mathrm{int} \to \mathrm{int}$」を記述・検証（型検査）することしかできないが、リファインメント型システムでは、「$(x : \mathrm{int}) \to (y : \mathrm{int}) \to \{z : \mathrm{int} \mid z = x + y\}$」のように、「整数 x, y を受け取ってそれらの和と等しい整数 z を返す」といったより詳細な仕様を述語論理式を用いて記述・検証（型検査）可能である。そのようなリファインメント型検査法としては、述語論理式の妥当性判定に SMT ソルバを用いたものが提案されていたが、研究代表者らはそのさらに先を行き、検証に伴うユーザ負担を劇的に軽減した全自動型推論法を世界で初めて実現し、前述の型検査・推論ツール RCaml を世界に先駆けて開発した。技術的には、型推論問題を述語変数上のホーン節集合として表された制約系の解消問題に帰着・解消している。このようにプログラム検証問題をホーン節制約解消問題に帰着するアプローチは、近年システム検証分野で盛んに研究されており、研究代表者らの研究はその先駆けである。

２．研究の目的

本研究では、研究代表者がこれまでに研究・開発を行ってきた高レベル言語のための検証理論であるリファインメント型システムおよびホーン節制約解消法、関数型言語 OCaml のための全自動・高精度検証ツールである RCaml を発展させ、実用上重要であるにも関わらず既存手法では十分に扱えなかった言語機能（(余）帰納的データ構造・リンクデータ構造）および仕様（時相的仕様・関係的仕様）の全自動・高精度検証法の確立を目指した。

３．研究の方法

研究目的で掲げた、検証対象とする (1) 言語機能の拡張と (2) 仕様の拡張の両方を並行して進めた。各拡張について、理論構築を行った後、実装と評価を行った。

1. リファインメント型システムおよびホーン節制約解消法それぞれを（余）帰納的データ構造、リンク

データ構造といった発展的なデータ構造に対応させる。さらに、それらを用いて検証対象とする各言語機能をエンコードする方法について研究する。

2. リファインメント型システムおよびホーン節制約解消法それぞれを時相的仕様検証が可能なように拡張する。さらに関係的仕様検証のための拡張も行い、時相的かつ関係的仕様の検証も実現する。

４．研究成果

本研究では、高レベルプログラムの関係的・時相的仕様検証の実現のために、(1) 安全性仕様の検証に限定されていたリファインメント型システムを停止性・非停止性・非安全性検証および時相的仕様検証が可能なように拡張し（それぞれ POPL18 と LICS18 に論文採択）、(2)while プログラムの時相的仕様記述に限定されていた動的論理を高階関数型プログラムの仕様記述が可能なように拡張した（CAV18 に論文採択）。さらに、安全性仕様検証に限定されていたホーン節制約解消法を拡張し、(3) 関係的仕様検証が可能な（余）帰納的定理証明に基づく制約解消法を提案し（CAV17 に論文採択）、(4) 時相的仕様検証問題を表現できるようにホーン節制約を一般化した不動点論理制約を（LICS18 論文で）提案、その制約解消法として解のテンプレートに基づく手法（論文投稿中）、述語抽象および確率推論に基づく手法（AAAI20 に論文採択）、決定木学習に基づく手法（論文投稿中）を実現した。また、提案した検証理論に基づき、高階関数型言語 OCaml のための検証ツール RCaml、不動点論理制約解消ツール MuVal、述語制約解消ツール PCSat の開発も行った。

上記の国際会議 CAV はシステム検証分野のトップ会議であり、POPL はプログラミング言語分野のトップ会議である。また、LICS は理論計算機科学分野のトップ会議であり、AAAI は人工知能分野のトップ会議である。このように、本研究の成果は複数分野のトップ会議に論文採択され、研究代表者の海野がホーン節制約解消に関する国際ワークショップである HCVS'18 の招待講演を依頼されるなど、国際的に高い評価を得ている。さらに、HCVS'19 併設の CHC 競技会に提案手法を実装したツールである PCSat を提出し、関連ツールとの比較評価を行うなど、理論面だけでなく実装・評価においても大きな成果が得られている。

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　1件／うちオープンアクセス　5件）

１．著者名 Yuki Satake, Hiroshi Unno, Hinata Yanagi	４．巻 34
２．論文標題 Probabilistic Inference for Predicate Constraint Satisfaction	５．発行年 2020年
３．雑誌名 Proceedings of AAAI 2020	６．最初と最後の頁 1644-1651
掲載論文のDOI（デジタルオブジェクト識別子） 10.1609/aaai.v34i02.5526	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 Naoki Kobayashi, Takeshi Nishikawa, Atsushi Igarashi, Hiroshi Unno	４．巻 11822
２．論文標題 Temporal Verification of Programs via First-Order Fixpoint Logic	５．発行年 2019年
３．雑誌名 Proceedings of SAS 2019, LNCS	６．最初と最後の頁 413-436
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-32304-2_20	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 Daisuke Kimura, Koji Nakazawa, Tachio Terauchi, Hiroshi Unno	４．巻 37
２．論文標題 Failure of Cut-Elimination in Cyclic Proofs of Separation Logic	５．発行年 2020年
３．雑誌名 コンピュータ ソフトウェア	６．最初と最後の頁 1_39-1_52
掲載論文のDOI（デジタルオブジェクト識別子） 10.11309/jssst.37.1_39	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 Hiroshi Unno, Yuki Satake, Tachio Terauchi	４．巻 2 Issue POPL
２．論文標題 Relatively Complete Refinement Type System for Verification of Higher-Order Non-deterministic Programs	５．発行年 2017年
３．雑誌名 Proceedings of the ACM on Programming Languages	６．最初と最後の頁 12:1-12:29
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/3158100	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 Satake Yuki, Hiroshi Unno	4．巻 10981
2．論文標題 Propositional Dynamic Logic for Higher-Order Functional Programs	5．発行年 2018年
3．雑誌名 Proceedings of CAV 2018, LNCS	6．最初と最後の頁 105-123
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-96145-3_6	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 Yoji Nanjo, Hiroshi Unno, Eric Koskinen, Tachio Terauchi	4．巻 なし
2．論文標題 A Fixpoint Logic and Dependent Effects for Temporal Property Verification	5．発行年 2018年
3．雑誌名 Proceedings of LICS 2018	6．最初と最後の頁 759-768
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/3209108.3209204	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 該当する

1．著者名 Hiroshi Unno, Sho Torii, Hiroki Sakamoto	4．巻 10427
2．論文標題 Automating Induction for Solving Horn Clauses	5．発行年 2017年
3．雑誌名 Proceedings of CAV 2017, LNCS	6．最初と最後の頁 571-591
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-63390-9_30	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19件（うち招待講演　1件／うち国際学会　8件）

1．発表者名 Yuki Satake, Hiroshi Unno, Hinata Yanagi
2．発表標題 Probabilistic Inference for Predicate Constraint Satisfaction
3．学会等名 The 34th AAAI Conference on Artificial Intelligence（国際学会）
4．発表年 2020年

１．発表者名
Naoki Kobayashi, Takeshi Nishikawa, Atsushi Igarashi, Hiroshi Unno

２．発表標題
Temporal Verification of Programs via First-Order Fixpoint Logic

３．学会等名
The 26th International Static Analysis Symposium (SAS 2019)（国際学会）

４．発表年
2019年

１．発表者名
Hiroshi Unno

２．発表標題
Horn Clauses and Beyond for Relational and Temporal Program Verification

３．学会等名
The 5th Workshop on Horn Clauses for Verification and Synthesis (HCVS'18)（招待講演）（国際学会）

４．発表年
2018年

１．発表者名
南條 陽史, 海野 広志

２．発表標題
一階不動点論理の循環証明体系とプログラム検証への応用

３．学会等名
日本ソフトウェア科学会第35回大会

４．発表年
2018年

１．発表者名
柳 日向, 海野 広志

２．発表標題
Belief Propagation for Predicate Satisfiability Checking（ポスター発表）

３．学会等名
第21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

４．発表年
2019年

１．発表者名
Yuki Satake, Hiroshi Unno

２．発表標題
Propositional Dynamic Logic for Higher-Order Functional Programs

３．学会等名
第21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

４．発表年
2019年

１．発表者名
Yoji Nanjo, Hiroshi Unno, Eric Koskinen, Tachio Terauchi

２．発表標題
A Fixpoint Logic and Dependent Effects for Temporal Property Verification

３．学会等名
第21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

４．発表年
2019年

１．発表者名
Daisuke Kimura, Koji Nakazawa, Tachio Terauchi, Hiroshi Unno

２．発表標題
Failure of Cut-Elimination in Cyclic Proofs of Separation Logic

３．学会等名
第21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

４．発表年
2019年

１．発表者名
Daisuke Kimura, Koji Nakazawa, Tachio Terauchi, Hiroshi Unno

２．発表標題
On Cut-elimination in Cycle Proof Systems（ポスター発表）

３．学会等名
The 16th Asian Symposium on Programming Languages and Systems (APLAS'18)（国際学会）

４．発表年
2018年

１．発表者名
Daisuke Kimura, Koji Nakazawa, Tachio Terauchi, Hiroshi Unno

２．発表標題
On Cut-elimination in Cycle Proof Systems

３．学会等名
The 4th Workshop on New Ideas and Emerging Results (NIER'18)（国際学会）

４．発表年
2018年

１．発表者名
中尾 收, 佐竹 佑規, 海野 広志

２．発表標題
関係的仕様からの関数型プログラム合成

３．学会等名
日本ソフトウェア科学会第34回大会

４．発表年
2017年

１．発表者名
四宮 誠一, 海野 広志

２．発表標題
余帰納法に基づく定理証明の自動化

３．学会等名
日本ソフトウェア科学会第34回大会

４．発表年
2017年

１．発表者名
Yoji Nanjo, Hiroshi Unno, Eric Koskinen, Tachio Terauchi

２．発表標題
Dependent Temporal Effects and Fixpoint Logic for Verification

３．学会等名
第20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（PPL2018）

４．発表年
2018年

１．発表者名
Hiroshi Unno, Yuki Satake, Tachio Terauchi

２．発表標題
Relatively Complete Refinement Type System for Verification of Higher-Order Non-deterministic Programs

３．学会等名
ACM Symposium on Principles of Programming Languages（国際学会）

４．発表年
2018年

１．発表者名
Yuki Satake, Hiroshi Unno

２．発表標題
Propositional Dynamic Logic for Higher-Order Functional Programs

３．学会等名
International Conference on Computer Aided Verification（国際学会）

４．発表年
2018年

１．発表者名
Yoji Nanjo, Hiroshi Unno, Eric Koskinen, Tachio Terauchi

２．発表標題
A Fixpoint Logic and Dependent Effects for Temporal Property Verification

３．学会等名
ACM/IEEE Symposium on Logic in Computer Science（国際学会）

４．発表年
2018年

１．発表者名
佐竹 佑規，海野 広志

２．発表標題
Temporal Dependent Contracts for Higher-Order Functions

３．学会等名
日本ソフトウェア科学会第33回大会

４．発表年
2016年

１．発表者名
Yuki Satake, Hiroshi Unno

２．発表標題
Temporal Logics for Higher-Order Functional Programs based on Trace Semantics（ポスター発表）

３．学会等名
第19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（PPL2017）

４．発表年
2017年

１．発表者名
Hiroki Sakamoto, Sho Torii, Shu Nakao, Hiroshi Unno

２．発表標題
A Horn Constraint Solver based on Inductive Theorem Proving（ポスター発表）

３．学会等名
第19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（PPL2017）

４．発表年
2017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