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 ２０ 日現在

機関番号：６２６１５
研究種目：基盤研究(B)（一般）
研究期間：2018～2020
課題番号：１８Ｈ０３２２６

研究課題名（和文）分離論理を用いたソフトウェア検証システム

研究課題名（英文）Software verification system by separation logic

研究代表者
龍田　真（Tatsuta, Makoto）

国立情報学研究所・情報学プリンシプル研究系・教授

研究者番号：８０２１６９９４

交付決定額（研究期間全体）：（直接経費）　　13,000,000円

研究成果の概要（和文）：本研究の目的は，オハーン理論を発展させることにより高精度なソフトウェア検証を可能にする新理論を構築することであった．研究成果は，オハーン理論に一般帰納的述語，配列，算術を追加した論理体系を定義し，その論理体系に対して，定理証明，両仮説形成，記号計算のループインバリアント生成の三つを計算する効率よいアルゴリズムを与え，それらのアルゴリズムの正しさおよび決定可能性を数学的に証明し，またそれらのアルゴリズムの効率を実装実験により証拠付けた．この実装システムを用いていくつかのプログラムの安全性を検証した．

研究成果の学術的意義や社会的意義
オハーン理論は分離論理を用いたメモリ安全性の自動検証理論として理論的にも実用的にも成功したが、一方でそれは精度が不十分であった．本研究は，オハーン理論をより高精度な自動検証ができるように発展させた理論が何であるか明らかにでき、学術的意義が高い．
航空機，銀行オンラインシステムなど，ソフトウェアは社会的に重要な役割を担っている．一方では，ソフトウェアは今だに人手で生産されている．このため，高信頼ソフトウェアの生産は大問題である．本研究は，ソフトウェア検証の理論を発展させることにより，これらの問題の解決をすすめることができ、社会的意義が大きい．

研究成果の概要（英文）：The purpose of this research is to deepen O'Hearn's theory to establish new theory for more precise software verification. The results of this research is to define a logical system which is obtained by adding general inductive definitions, arrays, and arithmetic to O'Hearn's theory, and present efficient algorithm for theorem proving, biabduction, and loop invariant generation for the logical system, prove the correctness and the decidability of these algorithms, and showed evidence for efficiency of these algorithms by implementation and experiments. By this implementation, we proved the safety of several programs.

研究分野：理論計算機科学

キーワード：ソフトウェア検証　ソフトウェア解析　分離論理　メモリ安全性

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

ソフトウェア検証理論は，ソフトウェア検証という目的自体の困難性，使われる理論の数学的複雑性により，学術的に挑戦価値のある研究課題である．その中でソフトウェアのメモリ安全性を自動検証する理論は近年よい理論的方向が発見され，特に研究価値がある．

ソフトウェアの自動検証は，ソフトウェア解析が必要であり，その理論は抽象解釈による．抽象解釈とは，プログラムの扱う値を抽象化した抽象値から成る集合である抽象領域を構成し，この抽象領域上でプログラムを仮想的に実行し，ループ部分はワイドニングという近似方法を構成することにより必ずループの計算を終了させ，プログラムの返す抽象値によりそのプログラムの性質を解析するソフトウェア解析の方法である．抽象解釈は Cousot により提案され現在もソフトウェア解析の中心的理論として活発に研究されている．

ホーア理論は，ソフトウェア検証の重要な基本理論である．仕様記述のために論理式を用い，式{A}P{B}により，論理式 A が成り立つときプログラム P を実行してそれが停止したとき論理式 B が成り立つことを表す．ホーア論理は，プログラムの部分ごとに性質が記述できるためモジュラー性があり，また仕様記述言語が論理式であるため条件やアノテーションが書きやすい．これらの利点は抽象解釈には一般にはないものである．

抽象値として論理式をとることにより，抽象解釈においても，性質の記述を論理式で行い，またモジュラー性が可能になる．これは{¥bf 記号実行}とよばれる．記号実行は主としてテストデータ生成に用いられ活発に研究されているが，ソフトウェア解析としても有望な理論である．

分離論理は，比較的新しい論理であり，2002 年に Reynolds により提案され，一階述語論理を分離連言を追加することにより拡張してこれを仕様記述に用い，ポインタ操作を含む逐次的命令型プログラムをホーア論理の方法により検証する理論である．分離論理の長所は，表現力が高いため仕様記述が簡潔になり，また十分強力な決定可能なフラグメントが構成できること，フレーム規則が成り立ちこれによりポインタプログラムに対してもソフトウェア検証がモジュラー性をもつことである．

近年，記号実行の一つとして，オハーンらにより分離論理におけるフラグメントである記号ヒープを抽象値とする抽象解釈が提案され，メモリ安全性の自動検証理論として理論的にも実用的にも成功している．これを{¥bf オハーン理論}とよぶ．オハーン理論は，精度が不十分であり，有名なバグでも発見することができない場合があった．

２．研究の目的

ソフトウェア検証理論として近年よい理論(オハーン理論)が提案され理論的にも実用的にも成功しているが，精度がまだ不十分である．本研究の大目的は，オハーン理論を発展させることにより高精度なソフトウェア検証を可能にする新理論を構築することである．本研究の目的は，オハーン理論に一般帰納的述語，配列，算術を追加した論理体系を定義し，その論理体系に対して，定理証明，両仮説形成，記号計算のループインバリアント生成の三つを計算する効率よいアルゴリズムを与え，それらのアルゴリズムの正しさおよび決定可能性を数学的に証明し，またそれらのアルゴリズムの効率を実装実験により証拠付けることである．

３．研究の方法

本研究の方法は，一般的帰納的述語に対して循環証明を，配列および算術に対してプレスバーガー算術への翻訳を，ループインバリアント生成アルゴリズムに対してゲージ領域などの既知の最新の抽象領域の組み合わせを，それぞれアイデアとして研究を進める．この実装システムを用いてさまざまなソフトウェアの C コードのメモリー安全性を検証する．より具体的には，オハーン理論に一般帰納的述語，配列，算術を追加した論理体系を定義し，その論理体系に対して，定理証明，両仮説形成，記号計算のループインバリアント生成の三つを計算する効率よいアルゴリズムを与え，それらのアルゴリズムの正しさおよび決定可能性を数学的に証明し，またそれらのアルゴリズムの効率を実装実験により証拠付ける研究方法を進めた．

４．研究成果

(1) C プログラムの関数ポインタ除去

ヌルポインター参照やメモリリークがないことを保証するメモリ安全性の検証は、システムソフトウェアに実用的に重要である。オハーンのグループは、メモリ安全性の解析/検証の新しい方法として、分離論理とバイアブダクションを用いるモジュラーな抽象解釈を提案した。この方法を実現するために、モジュラーな抽象解釈を行う前にコールグラフを構成する必要がある。こ

の論文は、この方法により、メモリ安全性の解析/検証 C プログラミング言語で書かれたシステムソフトウェアに対して行うことを目的とし、最初のステップとしてこの論文は、コールグラフを構成するために関数ポインタ呼出を除去する関数ポインタ除去器を与えた。このツールは SVF をポインタ解釈に用いる。まず、Clang 構文解析器により C プログラムが LLVM プログラムに翻訳され、次に SVF が LLVM プログラムを解析する。この論文で与えられるツールは、C プログラム中の関数ポインタ呼出と LLVM プログラム中の関数ポインタ呼出の対応関係を発見し、C プログラムを同じ機能であり関数ポインタ呼出のない C プログラムに変換するこの関数ポインタ除去器を gzip, git, OpenSSL に適用した実験結果が与えられ、これらの実験結果は、このツールが解析/検証の目的に関して十分効率的で正確であることを示した。

(2) 配列のある記号ヒープのエンテイルメントの決定可能性

この論文は、プレスバーガー算術と配列のある分離論理における記号ヒープのエンテイルメント妥当性判定問題決定可能性に関する２つの結果を与えた。第一の結果は、配列と存在限量子のある体系に関するものである。決定手続きの正当性が、後件の配列の大きさが存在束縛されていないという条件の下で証明された。この条件は、ブラザーストンが 2017 年に提案した条件異なり、２つの条件は独立である。主なアイデアは、記号ヒープのエンテイルメントからプレスバーガー算術への新しい翻訳である。第二の結果は、配列とリストの両者のある体系に対する決定可能性である。鍵となるアイデアは、バーディンらが 2005 年に提案したアンロールコラプス技法を、配列、算術、両結合リストに拡張したことである、

(3) 配列とリストのある分離論理に対する両仮説形成

この論文は、配列とリストをもつ分離論理の記号ヒープに対する両仮説形成問題解くアルゴリズムを与える。この論理は、ポインタ操作プログラムのプログラム検証のためのホーア流論理の性質記述言語である。両仮説形成問題は与えられた仮定と結論から仮定に対する追加の仮説と結論に対する追加の仮説で、エンテイルメントが真となるようなものを発見することを求める。両仮説形成は分離論理によるモジュラー解析および自動検証必要不可欠である。なぜなら、それは、関数呼び出し側の条件と呼び出された関数の事前条件がマッチすることを保証するするからである。この論文は両仮説形成アルゴリズムの正当性を証明した。このアルゴリズムに基づいた両仮説形成器が、本研究の自動プログラム検証器の一部として実装され、小さい入力に対する両仮説形成器の実験結果も示され、これはこのアルゴリズムが有用であることを示している。

(4) 直観主義ポデルスキーリバルチェンコ定理と直感主義帰納的定義と直観主義循環証明の同等性

循環証明体系は、帰納的および余帰納的定義を表現する別の方法と、効率的証明探索を与える。ポデルスキーリバルチェンコ停止性定理はプログラム停止性解析に重要である。この論文は、最初に、ハイティンク代数 HA において帰納法に対するクリーニブラウアー定理と帰納法に対するポデルスキーリバルチェンコ定理が証明可能であることを、証明する。次に、この定理を用いて、この論文は、直観主義循環証明体系の証明可能性とマルティンレーフ帰納的定義の直観主義体系の証明可能性に対して、両体系が HA を含むとき、それらの同等性を証明する。

(5) 分離論理に対する循環証明体系における空間的因子分解

一般帰納的述語のある分離論理におけるエンテイルメント判定に対する新しい証明体系を提案した。提案された体系は展開-マッチ-除去の証明戦略を伴う循環証明体系に基づく。この戦略における困難のひとつは、展開すべき述語を発見することである。この問題を解決するために、因子規則と呼ばれる新しい推論規則を導入した。この推論規則は、空間論理式における帰納的述語の因子分解を可能にし、また、展開-マッチ-除去の証明戦略により展開すべき述語を発見することを可能にした。帰納的述語を線形に制限すれば、この証明体系は完全で決定可能である。この証明探索手継ぐ気のプロトタイプ実装による実験結果も示した。この体系は、カット論理式や補題を発見するヒューリスティック機構の助力なしに、ある困難な例を証明できた。

(6) 分離論理によるポインタプログラム検証の完全性と表現性

ポインタプログラム検証のためのレイノルズの分離論理体系を研究した。この論文はその完全性定理を証明し、また、各プログラムおよび各事後条件の最弱事前条件があるアサーションにより表現できるという表現性定理を証明した。この論文は、次の新しいセルを表現する述語を導入し、完全性と健全性を、決定可能的意味論の下で、拡張した体系に対して証明した。

(7) 帰納的定義のある記号ヒープに対する循環証明の完全性

分離論理は、ソフトウェア検証において理論的にも実用的にも成功している。記号ヒープに対する決定手続きは、重要な問題のひとつである。この論文は、錐帰納的定義と呼ばれる帰納的定義の一般形をもつ記号ヒープに対する循環証明体系を提案し、また、その健全性と完全性を証明した。錐帰納的定義は有界木幅帰納的定義に、存在限量子に対する制限を課したものであるが、それらはまだ広いクラス再帰的データ構造を含む。完全性は、証明探索アルゴリズムを用いて証明され、またそれは錐帰納的定義をもつ記号ヒープのエンテイルメントに多雨する決定手続きを与える。このアルゴリズムは時間計算量は、非決定可能二重指数である。このアルゴリズムに対するプロトタイプシステムが実装され、実験結果も与えられている。

５．主な発表論文等

〔雑誌論文〕　計9件（うち査読付論文　9件／うち国際共著　2件／うちオープンアクセス　1件）

１．著者名 Daisuke Kimura, Makoto Tatsuta	４．巻 17
２．論文標題 Decidability for Entailments of Symbolic Heaps with Arrays	５．発行年 2021年
３．雑誌名 Logical Methods in Computer Science	６．最初と最後の頁 1--33
掲載論文のDOI（デジタルオブジェクト識別子） 10.23638/LMCS-17(2:15)2021	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 Daisuke Kimura, Mahmudul Faisal Al Ameen, Makoto Tatsuta, and Koji Nakazawa	４．巻 13008
２．論文標題 Function Pointer Eliminator for C Programs	５．発行年 2021年
３．雑誌名 Lecture Notes in Computer Science	６．最初と最後の頁 23--37
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-89051-3_2	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, Makoto Tatsuta, Mahmudul Faisal Al Ameen, Koji Nakazawa, and Mirai Ikebuchi	４．巻 1
２．論文標題 Biabduction for Separation Logic with Arrays and Lists	５．発行年 2022年
３．雑誌名 Proceedings of the 24st JSSST Workshop on Programming and Programming Languages (PPL2021)	６．最初と最後の頁 1--16
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 Stefano Berardi and Makoto Tatsuta	４．巻 11202
２．論文標題 Intuitionistic Podelski-Rybalchenko Theorem and Equivalence between Inductive Definitions and Cyclic Proofs	５．発行年 2018年
３．雑誌名 LNCS	６．最初と最後の頁 13--33
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-030-00389-0_3	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 該当する

1．著者名 Koji Nakazawa, Makoto Tatsuta, Daisuke Kimura, and Mitsuru Yamamura	4．巻 1
2．論文標題 Spatial Factorization in Cyclic-Proof System for Separation Logic	5．発行年 2019年
3．雑誌名 Proceedings of the 21st JSSST Workshop on Programming and Programming Languages (PPL2019)	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） 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 Makoto Tatsuta, Wei-Ngan Chin, and Mahmudul Faisal Al Ameen	4．巻 267
2．論文標題 Completeness and Expressiveness of Pointer Program Verification by Separation Logic	5．発行年 2019年
3．雑誌名 Information and Computation	6．最初と最後の頁 1--27
掲載論文のDOI（デジタルオブジェクト識別子） 10.1016/j.ic.2019.03.002	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 該当する

1．著者名 Koji Nakazawa, Makoto Tatsuta, Daisuke Kimura, and Mitsuru Yamamura	4．巻 37 (1)
2．論文標題 Spatial Factorization in Cyclic-Proof System for Separation Logic	5．発行年 2020年
3．雑誌名 Computer Software	6．最初と最後の頁 125--144
掲載論文のDOI（デジタルオブジェクト識別子） 10.11309/jssst.37.1_125	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 Koji Nakazawa, Makoto Tatsuta, Daisuke Kimura, and Mitsuru Yamamura	4．巻 -
2．論文標題 Cyclic Theorem Prover for Separation Logic by Magic Wand	5．発行年 2018年
3．雑誌名 Proceedings of 1st Workshop on Automated Deduction for Separation Logics (ADSL 2018)	6．最初と最後の頁 1--19
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 Makoto Tatsuta, Koji Nakazawa, and Daisuke Kimura	４．巻 11893
２．論文標題 Completeness of Cyclic Proofs for Symbolic Heaps with Inductive Definitions	５．発行年 2019年
３．雑誌名 Lecture Notes in Computer Science	６．最初と最後の頁 367--387
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_19	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6件（うち招待講演　0件／うち国際学会　3件）

１．発表者名 益岡幸弘，龍田真
２．発表標題 帰納的定義付き一階述語論理の循環証明体系におけるカット除去
３．学会等名 記号論理学と情報科学研究集会(SLACS 2021)
４．発表年 2021年

１．発表者名 Makoto Tatsuta
２．発表標題 Brotherston's Conjecture: Equivalence of Inductive Definitions and Cyclic Proofs
３．学会等名 九州大学 論理と計算セミナー
４．発表年 2022年

１．発表者名 Makoto Tatsuta
２．発表標題 Completeness of Cyclic Proofs for Symbolic Heaps with Cone Inductive Definitions
３．学会等名 Third Workshop on Mathematical Logic and its Applications (MLA 2019)（国際学会）
４．発表年 2019年

１．発表者名
Makoto Tatsuta

２．発表標題
Different provability between Martin-Lof's inductive definitions and cyclic proofs

３．学会等名
Mathematical Logic and Constructivity (MLOC 2019)（国際学会）

４．発表年
2019年

１．発表者名
龍田 真

２．発表標題
マルティンレーフの帰納的定義と循環証明体系の同等性

３．学会等名
第54回MLG数理論理学研究集会

４．発表年
2019年

１．発表者名
Yukihiro Masuoka and Makoto Tatsuta

２．発表標題
Cut-elimination in cyclic proof system for first-order logic

３．学会等名
Fourth Workshop on Mathematical Logic and its Applications (MLA 2021)（国際学会）

４．発表年
2021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
研究協力者	ベラルディ　ステファノ (Berardi Stefano)		

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
研究協力者	チン　ウェイガン (Chin Wei-Ngan)		
連携研究者	中澤　巧爾 (Nakazawa Koji) (80362581)	名古屋大学・情報科学研究科・准教授 (13901)	
連携研究者	木村　大輔 (Kimura Daisuke) (90455197)	東邦大学・理学部・准教授 (32661)	

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			
イタリア	トリノ大学			
シンガポール	シンガポール大学			