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

平成　２９　年　　６　月　１３　日現在

機関番号：　６２６１５
研究種目：　基盤研究(C)（一般）
研究期間：　2015～2016
課題番号：　１５Ｋ００００２７

研究課題名（和文）分離論理を用いたソフトウェア検証の基礎理論

研究課題名（英文）Theory of software verification 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）　　3,600,000円

研究成果の概要（和文）：(1) 単項帰納的定義と暗黙存在のある分離論理のエンテイルメントの決定可能 性を証明した。この体系は、有界木幅分離論理 SLRDbtw から、暗黙存在変数を追加し、帰納的定義を単項に制限することにより得られる。(2) 単項帰納的定義をもつ記号ヒープのエンテイルメント判定器を実装した。効率的実装のためのアイデアとして、木のノード間の同値関係に関する最適化を説明した。(3) 相互再帰手続きをもつポインタープログラムにホーア論理と分離論理の拡張した体系の完全性を証明した。(4) プレスバーガー算術と帰納的定義をもつ分離論理における記号ヒープの充足可能性問題を解いた。

研究成果の概要（英文）：(1) We proved the decidability of entailments in separation logic with monadic inductive definitions and implicit existentials. This system is obtained from the bounded-treewidth separation logic SLRDbtw by adding implicit existential variables and restricting inductive definitions to monadic ones. (2) We implemented an entailment checker for the logical system of symbolic heaps with monadic inductive definitions. We proposed optimization of equivalence relation on tree nodes. for efficient implementation. (3) We proved the completeness of an extension of Hoare's logic and separation logic for pointer programs with mutual recursive procedures. (4) For the satisfiability problem of symbolic heaps in separation logic with Presburger arithmetic and inductive definitions. we first proved the system without any restrictions is undecidable. Secondly we proposed some syntactic restrictions and we proved the decidability by presenting a decision procedure.

研究分野：　理論計算機科学および数理論理学

キーワード：　分離論理　ソフトウェア検証　記号ヒープ　帰納的定義

１．研究開始当初の背景

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。特に、メモリーエラー(バッファオーバーフロー、未割当メモリへのアクセス、メモリーリーク)は、航空機コントローラの不具合、サーバーの脆弱性などを実際に引き起こした。メモリーエラーが起きないことの保証は、安全を守るために必要不可欠である。

メモリーエラーは、現在、抽象解釈(パリ高等師範学校の Astree など)、動的テストケース生成(マイクロソフトの SAGE など)、モデル検査、自動定理証明(INRIA の Coq,ロンドン大学の smallfoot など)の方法で検証されている。それぞれの方法は長所短所をもち、主な問題点は、抽象解釈は多くの誤警告が出ること、動的テストケース生成は適用対象がアセンブラ言語が中心であること、モデル検査は探索空間が爆発すること、自動定理証明では自動化できず対話的入力が必要であること、である。

分離論理は、2002 年に提案された新しい論理であり、現在のメモリ状況を記述するプリミティブと、メモリを分割して性質を証明する結合子(分離連言)を持つ。性質記述言語を一階述語論理から分離論理に拡張することにより、ホーア論理によってポインタやメモリを扱う C プログラムの性質が検証できる.

分離論理を用いてメモリーエラーがないことを検証する研究は有望である。ホーア論理でソフトウェアの全機能を検証することは、決定不可能であるが、メモリーエラーに限定すれば決定可能である部分体系を作ることができるからである。決定可能な部分体系に対しては、自動定理証明の方法が対話的入力なしに全自動で適用できる。これは自動定理証明による検証方法の問題点を解決している。

分離論理の決定可能な部分論理体系として記号ヒープ体系が 2004 年に O'Hearn らにより提案された. 記号ヒープ体系は、P and S の形の論理式だけに限定する。ここで、P は変数間の等式、不等式の連言であり、S は、空メモリ、１個のセルからなるメモリ、帰納的定義述語で記述されるメモリ、を分離連言で結合した式である。

記号ヒープ体系におけるメモリの抽象化の中心は、帰納的定義述語である。帰納的定義述語は、例えばリストセグメントや木を表す述語であり、用途に応じて追加して検証に用いる。例えば リストセグメント Lseg(x,y) を追加し、現在のメモリが x から始まる重複のないリストであり、最後のセルはメモリ外のアドレス y を指す、ということを記述する。同時に、Lseg がこの意味をもっていることを表現するため、Lseg に関する推論規則を追加する。今のところ、この推論規則は、Lseg などのデータ構造ごとに、数学的な技巧をこらして、完全かつ決定可能であるように追加する。しかし, 一般的帰納的定義は、決定可能性を保つために、追加することはできていない。この記号ヒープ体系は、そのエンテイルメント P1 and S1 |- P2 and S2 の真偽が決定可能であることが知られている。この論理体系に基づいた検証システムは, 数万行のソフトウェアを検証し、理論上も実用上も成功した。

帰納的定義述語は、リスト、木などの再帰的データ構造を記述するために必要不可欠である。それらの再帰的データ構造に関する性質を示すには、それぞれのデータ構造に関する帰納法が必要である。例えば、リストに関する性質は、リスト帰納法により証明される。一般的帰納的定義は、帰納的定義述語とその帰納法を、一般的な形で与える。リストなどの個々のデータ構造の帰納的定義とその帰納法は、一般的帰納的定義の具体化により得られる。

記号ヒープ体系を特定のデータ構造を記述する帰納的定義述語に拡張する場合に、エンテイルメントの真偽が決定可能であるかはそのデータ構造ごとに未知であった。もし、一般的帰納的定義が決定可能性を保って追加できれば、使いたい新しいデータ構造に対して、その帰納的定義と帰納法は一般的帰納的定義の具体化により得られ、データ構造ごとに数学的技巧をこらして推論規則を用意する必要がなくなり、検証の自動化が大いに前進する。

一般的帰納的定義を追加しても、エンテイルメントの真偽が決定可能であるかは未知であったが、2013 年よりブレークスルーをもたらすであろう研究結果が出始めた。2014 年に Kanoovich らは、一般的帰納的定義を追加すると、エンテイルメントの真偽は決定不可能であることを証明した。Brotherston らは 2014 年に、一般的帰納的定義を追加しても、エンテイルメントの片側である P and S に対しては その充足可能性が決定可能であることを証明した。Iosif らは 2013 年に、一般的帰納的定義に制限条件を加え、メモリの表すグラフの treewidth が有界であるように限定することにより、エンテイルメントの真偽が決定可能であることを証明した。

現在の問題点は、一般的帰納的定義をプログラム検証に用いるためには、そのエンテイルメントが決定可能であることが必要であるがそれには制限条件が必須であること、また、Iosif らの制限条件では、よく使用される基本的なデータ構造であるポインターのリストセグメントなどを使うことができないことである。

２．研究の目的

本研究では、研究期間内に、一般的帰納的

定義の条件で次の(1)(2)を満たすものを発見し、その性質を証明する。
(1) 記号ヒープ体系にその条件下の一般的帰納的定義を追加しても、エンテイルメントの真偽が決定可能である,
(2) リストセグメントなどのよく使用される基本的なデータ構造が記述できる.
また、発見した条件を用いてヒープ記号体系と一般的帰納的定義に基づく C プログラムの検証体系を計算機上に実現し、ベンチマークを走らせることにより、その理論の有効性を確かめる。
本研究の研究成果の意義は、理論上も実用上も大きい。理論的には、分離論理にどのような形で決定可能性を保って一般的帰納的定義を追加することができるか、その場合の決定手続きはどのような形になるのか、が判明し、数理論理学および理論計算機科学に大きな知見をもたらす。また、実用上は、現在プログラム検証における有望な方法のひとつであるメモリーエラーを自動定理証明により検証する方法に対して、リストセグメントのようなよく使われる基本的なデータ構造を扱うプログラムを全てカバーし、それらのプログラムを全自動で検証できる方法をはじめて与える。

３．研究の方法

(1) Iosif らの証明の条件を吟味し、その条件を緩めて、リストセグメントを扱えるようにする。
Iosif らの論文では、一般的帰納的定義の制限条件として、progress, connectivity, establishment の３つの条件を課している。progress は、帰納的定義の各規則が、ちょうどひとつのメモリーセルを割り当てることを要求する。establishment は, 存在限量された変数が帰納的定義を展開していくとメモリーセルに割り当てられることを要求する。この３つの条件により、帰納的定義述語の展開木と帰納的定義述語が記述するヒープのなすグラフが同型になる。この論文は、この状況下で帰納的定義述語を単項二階論理に翻訳することにより、帰納的定義述語が成り立つことを、対応するヒープのグラフ構造の単項二階論理における判定手続きを用いることにより、判定している。一方で、progress と establishment の２つの条件は、リストセグメントの帰納的定義を排除している。
本研究のアイデアのひとつは、展開木とヒープのなすグラフが葉を除いて同型となるように、この 2 条件を弱めることにある。progress を、述語を再帰的に呼び出していない規則ではセルを割り当てなくてもよい、という弱い条件に置き換えることができると予想する。establishment もこれに合わせて弱めることができると予想する。この弱い条件では、展開木の葉は、対応するヒープのグラフでは葉であるかまたは対応するノードがない、という状況になる。この場合にも単項二階論理への翻訳が帰納的定義述語の判定手続きを与える、と予想する。以上の予想を、Iosif らの論文の証明を吟味することにより、証明する。これが証明できれば、リストセグメントが表現できる一般的帰納的定義であって、エンテイルメントが決定可能である論理体系を発見できたことになる。

(2) 単項二階論理への翻訳の方法と、変数同値類の方法の両者を合わせて、新しい条件を発見する。
Brotherston の論文では、変数の同値類を考えることにより、モデルの探索空間を狭めて、決定可能性を証明した。Iosif らの論文では、記号ヒープ体系の論理式を単項二階論理へ翻訳することにより、決定可能性を証明した。２つのアイデアを合わせ、記号ヒープ体系を変数の同値類を考慮しながら単項二階論理へ翻訳することにより、新しい決定可能性条件を発見する。

(3) 上で得られた条件を用いて、エンテイルメントの決定手続き、検証システムの決定手続きを設計する。
上の(1)または(2)で得られた条件を元に、論理体系におけるエンテイルメントの決定手続きを構成し、決定可能性を証明する。また、これを用いて、記号ヒープと一般的帰納的定義を用いた C プログラムの検証システムの決定手続きを構成する。
検証システムの決定手続きは、O'Hearn らの 2005 年の論文を拡張することにより行う。

(4) 構成した検証システムの決定手続き(または半決定手続き)を、パソコン上に実装する。
実装は、得られた決定手続き(または半決定手続き)を用いて、O'Hearn らの 2004 年および 2005 年の論文をはじめとする分離論理の検証システムの実装の論文のアイデアを参考にして、検証システムのプロトタイプを作成する。

(5) 実装した検証システムに，ベンチマークなどを走らせ実験する。理論の有効性を実証する。

４．研究成果

(1) 単項帰納的定義と暗黙存在をもつ分離論理

単項帰納的定義と暗黙存在のある分離論理のエンテイルメントの決定可能性を証明した。この体系は、Iosif et al が 2013 年に提案した有界木幅分離論理 SLRDbtw から、暗黙存在変数を追加し、帰納的定義を単項に制限することにより得られる。提案した体系

は、決定可能であり、さらに、ポインターリストのようなポインターをデータとする一般的再帰的データ構造を扱うことができる。鍵となるアイデアは、局所アドレスまたは無限遠を表すあるアドレスを暗黙存在変数に割り当てることにより、この変換により得られる定義節は SLRDbtw の確立条件を満たすことを用いて、問題を SDRDbtw の決定可能性に帰着することである。暗黙存在を SLRDbtw に追加すると、エンテイルメントが決定不可能性になることも証明した。このことは暗黙存在が決定可能性を左右することを示している。

(2) 単項帰納的定義をもつ記号ヒープの単項二階論理への翻訳

単項帰納的定義をもつ記号ヒープのエンテイルメント判定器の実装を論じた。エンテイルメントが決定可能であり、また、この体系は一般的帰納亭定義と暗黙存在をもつため、この論理体系は実装に値する。実装は、この体系を単項二階論理に翻訳し、得られる MSO 論理式をデンマークで開発された既存の決定可能手続きである MONA を用いて判定する方法で実現した。翻訳の同等性定理を論じた。また、木のノード間の同値関係に関する最適化など、効率的実装のためのいくつかのアイデアを説明した。

(3) 再帰手続きをもつ分離論理の完全性

相互再帰手続きをもつポインタープログラムにホーア論理と分離論理の拡張した体系の完全性を証明した。また、アサーション言語の表現性も証明した。２つの新しい推論規則を導入し、分離論理では不健全である公理と冗長な推移論規則を除去することにより、新しい体系を構築し、これを用いて完全性を証明した。このため、与えられた状態の完全な情報を記述する新しい式を導入し、事前条件として用いた。また、アボートのない実行に対する必要十分条件を与える事前条件を定義した。これにより最強事後条件が利用できるようになった。

(4) 帰納的定義とプレスバーガー算術をもつ分離論理の決定手続き

プレスバーガー算術と帰納的定義をもつ分離論理における記号ヒープの充足可能性問題を解いた。まず、制限条件のない体系に対して、その問題が決定不可能であることを証明した。次に、構文的制限を、決定可能性のために提案した。この制限条件は、帰納的定義をもつプレスバーガー算術の新しい体系を考察することにより得られた。算術のこの部分体系では、全ての帰納的定義述語は、最終的周期的集合を表現し、このため除去することができる。提案する体系は、ソートされたリストや AVL 木といったかなり複雑な述語の算術部分の充足可能性を扱うことができ、この体系は十分に一般的である。最後に、制限された帰納的定義と算術をもつ記号ヒープに対する決定手続きを与えることにより、決定可能性を証明した。

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 4 件）

[1] Makoto Tatsuta, Quang Loc Le, and Wei-Ngan Chin, Decision Procedure for Separation Logic with Inductive Definitions and Presburger Arithmetic, In: Proceedings of the 14th Asian Symposium on Programming Languages and Systems (APLAS 2016), Lecture Notes in Computer Science 10017 (2016) 1--21, 査読有, DOI: 10.1007/978-3-319-47958-3_22.

[2] Mahmudul Faisal Al Ameen and Makoto Tatsuta, Completeness for Recursive Procedures in Separation Logic, Theoretical Computer Science 631 (2016) 73- - 96, 査読有, doi: 10.1016/j.tcs.2016.04.004

[3] Makoto Tatsuta and Daisuke Kimura, Translation of Symbolic Heaps with Monadic Inductive Definitions into Monadic Second-Order Logic, In: Proceedings of the 18th JSSST Workshop on Programming and Programming Languages (PPL2016), 15 pages, 2016, 査読有.

[4] Makoto Tatsuta and Daisuke Kimura, Separation Logic with Monadic Inductive Definitions and Implicit Existentials, In: Proceedings of the 13th Asian Symposium on Programming Languages and Systems (APLAS 2015), Lecture Notes in Computer Science 9458 (2015) 69--89, 査読有, DOI: 10.1007/978-3-319-26529-2_5.

〔学会発表〕（計 3 件）

[1] Daisuke Kimura, Decidability of Entailments in Separation Logic with Arrays, Workshop on Mathematical Logic and its Application, 2016.9.16--17, 京都大学 (京都府京都市).

[2] Makoto Tatsuta, Decidable subsystem of Presburger Arithmetic with Inductive Definitions and Application to Symbolic Heaps, International Workshop on

Mathematics for Computation (M4C), May 8--13, 2016, Niederalteich (Germany).

[3] Makoto Tatsuta, Decidability and Undecidability in Symbolic-Heap System with Inductive Definitions, In: Proceedings of Continuity, Computability, Constructivity: From Logic to Algorithms (CCC2015) (2015), 2015.9.16, Kochel (Germany).

６．研究組織

(1)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

(2)連携研究者
木村大輔 (KIMURA, Daisuke)
東邦大学・理学部情報科学科・講師
研究者番号: 90455197