様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成 24 年 4 月 16 日現在

機関番号：13903
研究種目：基盤研究(C)
研究期間：2009 ～ 2011
課題番号：21500136
研究課題名（和文）　セキュアシステム構築のための計算論理的基盤技術の研究

研究課題名（英文）Study on Computational Logic-based Methodologies for Building Secure Systems

研究代表者
世木 博久（SEKI HIROHISA）
名古屋工業大学・大学院工学研究科・教授
研究者番号：90242908

研究成果の概要（和文）：本研究はシステムやソフトウェアを対象にして，その設計や開発の正当性，妥当性の形式的検証を可能とする計算論理的基盤技術の確立を目的とする．そのための計算論理に基づく方法として，論理プログラムによって対象システムの記述し，プログラム変換技術を用いてその性質を検証するという方法論をとる.次のような3つの研究成果を得た．(1) 層状論理プログラムに対する変換において，従来の負の展開規則の条件が誤っていること反例を挙げて示し，これを解決するための新しい負の展開規則を与えた．(2) 拡張された負の展開規則を与え，その結果プログラム変換による検証法の適用可能性を拡大させた．(3) 余論理プログラム(co-logic programs)に対するプログラム変換規則を与えた．従来知られている検証方法より簡明な検証ができることを示した．

研究成果の概要（英文）：The overall objective of this research project is to construct a computational-logic based methodology for the verification of complex software systems using the transformational verification method; we use logic programs to represent a given system and a correctness property we want to prove, and then apply to a logic program encoding the system and the property to be verified, a sequence of transformations that preserve the validity of that property. We have obtained the following three main results:
(1) We have shown that negative unfolding for locally stratified programs proposed in the literature is not always correct, and proposed a new negative unfolding rule which guarantees the preservation of the meaning of a given program. (2) We have proposed an extended framework for unfold/fold transformation of stratified programs, including, among others, an extended negative unfolding. It makes the application conditions of the rule more general, thereby making the transformational verification method more applicable. (3) We have proposed a new framework for unfold/fold transformation of co-logic programs, and proved that our transformation system preserves the intended semantics of co-logic programs. We have shown by some examples that our transformational verification method can be used for verifying some properties of Büchi automata in a succinct way.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2009 年度	1,000,000	300,000	1,300,000
2010 年度	1,100,000	330,000	1,430,000
2011 年度	1,100,000	330,000	1,430,000
年度			
年度			
総　計	3,200,000	960,000	4,160,000

研究分野： 総合領域
科研費の分科・細目： 情報学・知能情報学
キーワード： 計算論理，推論アルゴリズム，システム検証，プログラム変換

１．研究開始当初の背景

ソフトウェアはますます複雑化・高度化する様々なシステムを制御し運用するための社会基盤として広く利用されており，その安全性や信頼性を保証することは喫緊の課題となっている．ソフトウェアの妥当性確認(バリデーション)やテストという伝統的な方法では，誤りやバグを発見することはできるが，正当性を保証することはできない．従って，安全性や信頼性の向上のためには，その正当性を形式的に検証することを可能にする形式的手法に基づいたソフトウェア設計の方法論を構築することが必要となる．また，対象として，安全性が社会的にも経済的にもとりわけ重要なミッション・クリティカルなシステムであるリアクティブ・システム (reactive systems) を扱うことができるような検証の枠組が必要とされている．

従来のシステム検証の方式としては，Clarke らによるモデル検査 (model checking) とその拡張が代表的である．この方法の課題として，(i) 主に有限状態システムが対象で，本研究が対象とする無限状態システムの扱いは未だ限定的で十分に研究されていないこと，(ii) 安全性(safety)や活性(liveness)などの振舞い仕様を時相論理式(CTL や LTL など)で表現した性質が検証の対象のため，表現が本質的に命題論理式に制限されており，システムの構造的性質などの自然な表現が難しいことがある．

また，計算論理の分野でも論理プログラムを用いた検証方法が研究されてきた．例えば，Jaffar らによる時間オートマトンに対する制約論理プログラム(CLP)による方法では，振舞い仕様と構造的性質を検証の対象とし，特別な帰納法(coinduction)スキーマを用いて検証を行う．また，論理プログラムの変換を用いた検証方式では，特別な帰納法スキーマを必要としない利点があるものの，リアクティブ・システムのような動作が無限に継続するようなシステムは扱われてこなかった．

我々は先行研究で，局所層状論理プログラムに対するプログラム変換の新しい枠組みを提案している．本研究ではそれに基づき，リアクティブ・システムを対象として通常の有限項のみならず無限項を操作するプログラム変換技術を用いて検証を行うアプローチをとる．このような方法はそれ自体が新しい研究課題であり，世界的にも事例がほとんどない．

また，この方法は特別な帰納法スキーマを用いない点で Jaffar らの方法より単純で，従って実応用への有効性を持つ．実際的なシステム検証に用いるためには，この端緒となる研究結果を基にして無限項を扱う論理プログラム変換の方法論を確立し，実応用のための課題を明らかにすることが必要となる．

２．研究の目的

本研究では、複雑化・高度化するシステムやソフトウェアを対象にして、その安全性や信頼性の向上を目指し，設計・開発の正当性・妥当性の形式的検証を可能とする計算論理的基盤技術の確立を目的とする．ソフトウェアの正当性を検証する形式的手法として，本研究では，正当性の証明との親和性に優れている点で計算論理に基づく方法がとりわけ適当で有効であると考えて，その分野で蓄積されている研究成果を可能な限り利用する．本研究の特徴は，計算論理に基づく技術として，論理プログラムに対するプログラム変換による検証技術を中核に用いる点にある．

本研究の提案者は，先行研究で局所層状論理プログラムに対するプログラムの等価変換の枠組みを提案している．この枠組みを基にしてプログラムの性質の検証に利用するアプローチをとる．これにより，従来のように検証のための特別な帰納法に関する推論スキーマを用意することなく，それ同等な推論をプログラム変換規則の適用によって実現する．本研究では，システムの諸性質を検証するために必要となるプログラム変換の理論的枠組みについてさらに深化させて，実際的な問題に適用するための課題を明らかにすることを目的とする．

３．研究の方法

プログラム変換による検証では，次のような方法で対象とするシステムの性質の検証を行う．対象システムとその証明すべき性質が与えられると，最初に，そのシステムの動作を表現する論理プログラムを構成する．また，証明すべき性質はまず１階述語論理式で表現し，次にそれを論理プログラムの節の形式に等価変換する．このようにして得られた

論理プログラムに対して，プログラムの意味を保存する変換規則を繰り返し適用して，最終的に証明すべき性質を表す論理式の真理値が容易に分かる形式の論理式を導出するように変換を行う．

このようなプログラム変換による方法でシステムの検証を行うためには，その基本となるプログラム変換の理論的基盤を構築すること，変換規則をシステム検証に有効に適用するための方法論を確立すること，そしてその有効性をソフトウェア・システムの検証において確認することが必要となる．本研究では，特に以下の四つのタスクに焦点を当てて研究を行った．

(1) システムの仕様とその性質を記述する論理体系の設計: 対象とするシステムを記述する論理プログラムとして，どのようなクラスの表現を考慮する必要があるか，様々な問題を対象として検討する．また，無限に継続するリアクティブ・システムの仕様や性質を記述するために，有限項のみならず無限項を扱う余論理プログラム (co-logic programs) に基づく仕様記述方式が妥当か，どの程度の表現力があるかを明らかにする．

(2) 論理プログラムに対するプログラム変換規則の設計: 検証方式の中心課題はプログラム変換におけるプログラムの意味の保存である．従来の代表的なプログラム検証の研究では，極小モデルの意味を保存する枠組みを考え，帰納法として通常の帰納法(induction)スキーマを用いている場合が多い．しかるに，システムの諸性質の検証という目的では，余帰納法(coinduction)を用いることが妥当な場合がある．本研究では，帰納法と余帰納法について，同じように適用できる検証方法を検討する．

そのために，まず初めに先行研究で得られた極小モデル(解集合)を保存するプログラム変換の枠組みを利用して，システムの正当性などの様々な性質を検証する方法を中心に推論方式を設計し，検証に必要な変換規則の定式化を進める．また，本検証方式と，帰納法の推論スキーマを陽に用いる従来方式との検証能力の比較についても解析する．

次に，システムの様々な性質を検証するために必要な変換規則の見直しを進めて，これまでの研究の知見を基に従来のプログラム変換の枠組みを拡張し，余論理プログラム(co-logic programs)に対する新しいプログラム変換規則とそれを用いた検証方式を定式化することを目指して検討を行う．また，この方法による検証と従来の方式に基づいた帰納法による推論能力の比較についても解析する．

(3) システム検証のための変換技法の検討: 対象システムの諸性質の検証を可能な限り自動的に行う検証システムの実現に向けて，(2)で検討したプログラム変換規則を適切な順序で適用するための適用戦略の設計を並行して行う．このためには，応用領域からの具体例について，実際に変換の実行過程のパターンを蓄積して(カタログ化)，そこから一般的な適用戦略を獲得する方式をとる． 適用可能な変換ルールが複数ある場合は，非決定的にルールを選択して推論を行うが，このようなルール選択よる探索空間の制御を適切に行わないと、現実的な時間で検証できないことが想定される．これは定理証明の分野と共通する課題なので，検証の対象とするプログラムのクラスを限定するなど，扱う問題のクラスを検討する．

(4) 変換による検証システム実現のための検討: この検証分野の従来研究で扱われているベンチマーク問題を中心にして，変換によるシステム検証例を蓄積する．リアクティブ･システムの代表的な性質である安全性(safety)と活性(liveness)について，その表現と検証するための変換戦略について，幅広く例題を調査し，提案手法の適用可能性を検討する．また，本手法をプログラミング言語(Prolog/Java など)でPC上に実装する場合の課題についても検討する．従来のソフトウェア資産(Pettorossi らによるMAPシステムなど)や知見を可能な限り再利用することを考慮して，検証システムの実装について検討を行う．従来研究でベンチマークとして使われているプログラムを使用し動作確認し，推論能力や計算量等を比較する．

４．研究成果

本研究の主な成果として次の三点があげられる:

(1) 局所層状論理プログラムに対する新しいプログラム変換の枠組みの提案: 我々は先行研究で局所層状論理プログラムに対するプログラムの等価変換の枠組みを提案している．この枠組みを基にして，それをシステムの性質を検証に利用するための拡張を行い，以下のような結果を示した：

① 負リテラルに対する展開規則の新しい適用条件を提案した．層状論理プログラムに対するプログラム変換に関して，負の展開規則を含む従来のPettorossiらの変換システムに誤りがあること反例を挙げて示し，この問題を解決するための新しい負の展開規則を与え，その正当性を示した．

② 新しいゴール置換規則を与え，その正当性を証明した．これは従来提案されている規

則よりも一般的な形で与えられていて，その結果，新しい負の展開規則を特別な場合として含んでいる．
③ 提案したプログラム変換に基づく証明システムが，Jaffar らによって提案されている余帰納法(双対帰納法，coinduction)による証明システムと同等以上の推論能力を持つことを証明した．この目的のために，ゴール置換規則を拡張して“健全な(sound)”ゴール置換規則を導入した．これにより，検証のための特別な帰納法の推論スキーマを用いることなく，畳み込み及びゴールの置換えなどのプログラム変換規則の適用によって Jaffar らの証明系と同等の帰納的推論が実現できることが分かった．

(2) 局所層状論理プログラムに対する変換規則の拡張とその応用：(1)の層状論理プログラムに対する等価変換の枠組みは，従来研究にある問題点を解消するとともに枠組みの拡張を行ったものであるが，この拡張された枠組みでも検証できないような問題が存在している．この課題に対応するために，システム検証のためのプログラム変換の枠組みの拡張を引き続き行い，以下のような結果を示した：

① 負リテラルに対する展開規則の拡張を提案した．従来研究では扱えないような場合でも適用可能な形式を与え，それを含んだ変換の枠組みの正当性を示した．
② 更に上記のプログラム変換システムに新たに 2 つの変換規則，すなわち，斉時畳込み(simultaneous folding)，負リテラルの畳込み(negative folding)を導入し，その場合でも正当性が保たれることを証明した．
③ 提案したプログラム変換に基づく証明システムが，従来研究でのプログラム変換によるプログラムの性質の証明方法と比較して，より単純で従って自動化しやすく，しかも直観的に分かりやすい方法で検証が実現できることを例により示した．

(3) 余論理プログラムに対する新しいプログラム変換の枠組みの提案：Gupta らによる余論理プログラム(co-logic programs) に対するプログラム変換規則を与えた．

① 従来の論理プログラムに対するプログラム変換規則をそのまま余論理プログラムの場合に適用すると，プログラムの意味が正しく保存されないことを示し，新しい適用条件を明らかにした．
② 通常のプログラム変換規則である定義の導入，展開，畳込みの 3 規則に加えて，余論理プログラム向きに設計したゴール置換規則を導入し，その正当性を証明した．
③ 提案したプログラム変換に基づく証明システムと，従来研究でのプログラム変換による検証方法との比較を行った．従来の Pettorossi らによる層状論理プログラムを用いる方法は検証対象の記述が長く複雑になり，その結果検証にもまた複雑な推論を必要とした．これに対して，余論理プログラムに対するプログラム変換規則を定式化することでより簡明な検証が可能になることを示した．

余論理プログラムでは無限項を自然に扱うことができるので，リアクティブ・システムを対象としてその性質を検証することが可能となった．このように，プログラム変換技術を用いたリアクティブ･システムの検証方法の確立へ向けて基礎となる知見を得ることができた点で意義がある．

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 5 件）

① H. Seki, “Proving Properties of Co-logic Programs by Unfold/Fold Transformations”, Logic-Based Program Synthesis and Transformation, 21st Int'l. Symp., LOPSTR2011, Revised Selected Papers, Lecture Notes in Computer Science, Springer-Verlag, LNCS 7225, pp. 205-220, 2012 (印刷中), 査読有.
② H. Seki, “On Inductive Proofs by Extended Unfold/fold Transformation Rules”, Logic-Based Program Synthesis and Transformation, 20th Int'l. Symp., LOPSTR2010, Revised Selected Papers, Lecture Notes in Computer Science, Springer-Verlag, LNCS 6564, pp. 117-132, 2011, 査読有.
③ H. Seki, “On Inductive and Coinductive Proofs via Unfold/fold Transformations”, Logic-Based Program Synthesis and Transformation, 19th Int'l. Symp., LOPSTR2009, Revised Selected Papers, Lecture Notes in Computer Science, Springer-Verlag, LNCS 6037, pp. 82-96, 2010, 査読有.
④ H. Seki, “On Negative Unfolding in the Answer Set Semantics”, Logic-Based Program Synthesis and Transformation, 18th Int'l. Symp., LOPSTR2008, Revised Selected Papers, Lecture Notes in Computer Science, Springer-Verlag, LNCS 5438, pp. 168-184, 2009, 査読有.

〔学会発表〕（計 5 件）

① H. Seki, “Proving Properties of

Co-logic Programs by Unfold/fold Transformations”, Pre-Proc. of 21st Int'l. Symp. on Logic-Based Program Synthesis and Transformation (LOPSTR2011), Univ. of Southern Denmark, pp. 112-126, 2011年7月19日.

② H. Seki, “On Inductive Proofs by Extended Unfold/fold Transformation Rules”, Proc. of the 20th Int'l. Symp. on Logic-Based Program Synthesis and Transformation (LOPSTR2010), RISC-Linz, Report Series No. 10-14, pp. 194-208, 2010年7月25日.

③ H. Seki, “On Inductive and Coinductive Proofs via Unfold/fold Transformations”, Pre-Proc. of 19th Int'l. Symp. on Logic-Based Program Synthesis and Transformation (LOPSTR2009), Univ. of Coimbra, pp. 1-15, 2009年9月10日.

〔その他〕
ホームページ等

６．研究組織

(1)研究代表者

世木 博久（SEKI HIROHISA）
名古屋工業大学・大学院工学研究科・教授
研究者番号：90242908

(2)研究分担者

（　　）

研究者番号：

(3)連携研究者

（　　）

研究者番号：