様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２８　年　　６　月　　６　日現在

機関番号：　１３９０３
研究種目：　基盤研究(C)（一般）
研究期間：　2012～2015
課題番号：　２４５００１７１

研究課題名（和文）無限項を扱うプログラム変換を用いたソフトウェア検証方法の研究

研究課題名（英文）Study on Software Verification Methods Using Program Transformation Handling Infinite Terms

研究代表者

世木　博久（Seki, Hirohisa）

名古屋工業大学・工学（系）研究科（研究院）・教授

研究者番号：９０２４２９０８

交付決定額（研究期間全体）：（直接経費）　　3,700,000円

研究成果の概要（和文）：本研究は，リアクティブ・システム等のソフトウェアの正当性を形式的に検証するための方法論の構築を目的とする．そのために，計算論理に基づく形式手法である論理プログラムに対するプログラム推論を用いるアプローチを採用し，次のような3つの主な研究成果を得た．(1) 余論理プログラムに対するプログラム推論とそれを用いた仕様の検証法を示した．(2) その結果を拡張し，ソフトウェアの正当性検証問題であるCTL時間論理式に対するモデル検査を実現できることを示した．　(3) 検証に必要となるプログラムの仕様を効率的に発見するための基礎となるパターン・マイニング方法を示した．

研究成果の概要（英文）：The overall objective of this research is to develop a computational-logic based methodology for verifying software such as reactive systems using transformational verification methods; we use logic programs to represent a given system and reason about its properties. We have obtained the following three main results:
(1) We have proposed a reasoning method for co-logic programs. We have shown by some examples that it can be used for verifying some given specifications in a succinct way. (2) We have proposed an extended framework for co-logic programs, and shown that it is applicable to the model checking problem for CTL temporal logic formulas. (3) We have proposed a new method for pattern mining which will become a basis for specification discovery.

研究分野：　知能情報学

キーワード：　探索・論理・推論アルゴリズム　計算論理　プログラム推論

１．研究開始当初の背景

ソフトウェアは日常生活のあらゆる面で広く利用されている．また，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いるソフトウェアは，欠陥があると人命や経済損失に関わるような大惨事を引き起こす場合がある．このように社会基盤として広く利用されているソフトウェアの信頼性を保証することは極めて重要な課題となっている．

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，正当性を確実に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手法(formal methods)に基づいたソフトウェア設計の方法論が必要となる． 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要求されるミッション・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) の振舞いを取り扱え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代表的な手法としては，Clarke らによるモデル検査 (model checking) とその拡張がある．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一般化 (generic, パラメータ化)された性質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いない．

我々は先行研究で，無限項を扱う確定余論理プログラム(co-logic programs) [Gupta et al. 07]に対するプログラム変換の新しい枠組みを提案した[Seki 11]．本研究では，リアクティブ・システムを対象として，無限項を操作するプログラム推論技術を用いてソフトウェアの検証を行うアプローチをとるが，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，このアプローチは Jaffar らの方法のように特別な帰納法スキーマを用いる必要がない点でより単純化されている．実際的なシステム検証に用いるためには，この研究結果を基にして無限項を扱う論理プログラム推論の方法論を確立し，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

本研究の目的は、システムやソフトウェアの安全性や信頼性を保証するために，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に基づく基盤技術の確立である．本研究では，ソフトウェアの正当性を検証する形式手法として，計算論理に基づく方法が有効であるという前提のもとで，こ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．その中でも，論理プログラムに対するプログラム推論を用いた検証技術を中核に用いる点が本研究の特徴である．

本研究の提案者は，先行研究で無限項を扱う確定余論理プログラムの等価変換の枠組みを提案した．本研究では，この変換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ことを目指す．従来研究のように特別な帰納法の推論スキーマを用いることなく，プログラム推論規則の適用によって帰納法を用いる推論を実現する．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推論の理論的枠組みについてさらに深化させて，実応用のための課題を明確にすることを目的とする．

３．研究の方法

本研究のアプローチであるプログラム推論に基づくシステム検証では，次のような方法によって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，まずそのシステムの動作を論理プログラムで記述する．また，証明すべき性質は１階述語論理式，あるいは時制論理式を用いて表現する．１階述語論理式で記述された場合は，それを論理プログラムの節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

味を保存する推論規則を繰り返し適用して，その結果，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推論を行う．

このようなプログラム推論に基づく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推論の枠組みを構築すること，プログラム推論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．そのために本研究では，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: 対象システムを記述するために論理プログラムを用いるアプローチをとる．その際に，対象記述に必要となる論理式のクラスについて，様々な問題を採り上げて検討する．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，無限項を扱う余論理プログラムを用いた記述方式の妥当性やその表現方式の拡張について検討する．

(2) 論理プログラムに対するプログラム推論方式の設計: 本研究における検証方式では，論理プログラムに対するプログラム推論技術を中核として用いる．その際に，通常の帰納法と余帰納法(co-induction) の両方について，それを用いた検証法の実現方法について検討する．

そのために，先行研究で提案した余論理プログラムに対するプログラム推論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ためのプログラム推論方式の設計を進める．また，本研究で提案する検証方式と，従来の帰納法の推論スキーマを陽に用いる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機能の検討を進めて，余論理プログラムに対する構文上の制限を拡張した新しい拡張プログラム(ホーンμ-プログラムなど)とそれに対する推論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との比較についても調べる．

(3) プログラム推論による検証システム実現のための検討: (2)で検討したプログラム推論を用いた検証システムの実現に向けて，推論規則の適用戦略についての設計を並行して行う．検証の対象とするプログラムのクラスの制限等の対象問題のクラスを検討する．

また，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，プログラム推論によるシステム検証例を蓄積する．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．従来の当該分野におけるソフトウェア資産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，検証能力や計算量等を比較する．

(4) 仕様マイニングのためのパターン発見方式の検討: 検証するプログラムの性質（仕様）をプログラムの実行からマイニングにより発見する方法を検討する．仕様マイニングの基礎となるパターンマイニング・アルゴリズムについて詳細検討をすすめ，そのアルゴリズムを実装して動特性の解析を行う．

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) 余論理プログラムに対するプログラム変換の枠組みの拡張: 先行研究で，Gupta らによる余論理プログラムに対するプログラム変換規則を提案した．

① この枠組みを拡張し，否定を含む余論理プログラムにも適用可能な変換規則を与えた．この方法は，否定除去という従来のプログラム変換技法を利用したものであるが，余論理プログラムにおいてはより弱い条件の下で適用可能であることを示した．
② 提案した否定除去を用いた変換規則と，従来の負リテラルに対する展開規則との比較を行った．その結果，提案方法を用いた変換により，従来の枠組みでは扱えないような変換が可能になることを示した．
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．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がより広いクラスに対して適用できることを例により示した．この結果，従来方法と比較して，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可能になることを示した．

(2) 余論理プログラムを用いたCTL 時間論理式に対するモデル検査の枠組みの提案: 先行研究で余論理プログラムに対するプログラム推論の枠組みを提案した．この枠組みを基にして，その余論理プログラムをモデル検査問題に適用する方法を検討し，以下のような結果を示した：

① CTL 時間論理式に対する分岐時間モデル

検査を扱うために，余論理プログラムが持つ「層状化制限」制約を緩和して「局所層状化制限」という条件を与え，その意味論について考察した．
② CTL 式を扱う弱交替オートマタを余論理プログラムで自然に表現でき，その結果 Kupferman らのオートマタ理論に基づく最も効率のよい方法と同等な計算を行うことを示した．
③層状化制限を満たさない余論理プログラムプログラムを扱うために，Charatonik らのホーンμ-計算が利用できることに注目し，余論理プログラムの推論方法を自然に拡張して，ホーンμ-計算のための証明法に利用できることを示した．

(3) 仕様マイニングのためのパターン発見方式の検討: 仕様マイニングの基礎となるパターンマイニング・アルゴリズムについて検討をすすめ，そのアルゴリズムを実装して動特性の解析を行い，以下のような結果を示した：

① ソフトウェア検証のためには，プログラムが満たすべき性質(仕様)が与えられていなければならないが，これを事前に正確に与えることは一般に難しい．この問題のために，プログラムの実行トレースに良く出現するパターンを発見する仕様マイニングを利用することを検討した．先行研究でパターン・マイニングのためのアルゴリズムを提案しているが，その効率的な実装方法を与えた．
② パターン発見処理の効率化の方法として，分散マイニングに着目し，その際に必要となるパターン集合のマージ・アルゴリズムを示した．
③ マージ・アルゴリズムの効率的な実装のために，パターン集合の持つ性質に着目した効率化手法を提案し，その効果をいくつかの実験により示した．

余論理プログラムの持つ無限項を簡潔に取り扱えるという性質を利用して，リアクティブ・システムを対象とした検証方式を提案した．それにより，プログラム推論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４件）

① Y. Kamiya, H. Seki, “Distributed Mining of Closed Patterns from Multi-Relational Data”, Journal of Advanced Computational Intelligence and Intelligent Informatics, Vol.19 No.6, pp. 804-809, 2015, 査読有.
② H. Seki, “Extending Co-logic Programs for Branching-Time Model Checking”, Logic-Based Program Synthesis and Transformation, 23rd Int'l. Symp., LOPSTR2013, Revised Selected Papers, Lecture Notes in Computer Science, Springer-Verlag, LNCS 8901, pp. 127-144, 2014, 査読有.
③ H. Seki, “Proving Properties of Co-logic Programs with Negation by Program Transformations”, Logic-Based Program Synthesis and Transformation, 22nd Int'l. Symp., LOPSTR2012, Revised Selected Papers, Lecture Notes in Computer Science, Springer-Verlag, LNCS 7844, pp. 213-227, 2013, 査読有.
④ 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, 査読有.

〔学会発表〕（計６件）

① H. Seki, Y. Kamiya, “Merging Closed Pattern Sets in Distributed Multi-Relational Data”, 11th Int'l. Conf. on Concept Lattices and Their Applications (CLA 2014), Kosice (Slovakia), 2014 年 10 月 10 日.
② Y. Kamiya, H. Seki, “Towards Efficient Closed Pattern Mining from Distributed Multi-Relational Data”, Joint 7th Int'l. Conf. on Soft Computing and Intelligent Systems and 15th Int'l Symp. on Advanced Intelligent Systems (SCIS&ISIS 2014), 九州大学（福岡県・北九州市）, 2014 年 12 月 5 日.
③ H. Seki, “Extending Co-logic Programs for Branching-Time Model Checking”, 23rd Int'l. Symp. on Logic-Based Program Synthesis and Transformation (LOPSTR2013), Madrid (Spain), 2013 年 9 月 18 日.
④ H. Seki, “Proving Properties of Co-logic Programs with Negation by Program Transformations”, 22nd Int'l. Symp. on Logic-Based Program Synthesis and Transformation (LOPSTR2012), Leuven (Belguim), 2012 年 9 月 18 日.

⑤ H. Seki, S. Tanimoto, “Distributed Closed Pattern Mining in Multi-Relational Data based on Iceberg Query Lattices: Some Preliminary Results”, 11th Int’l. Conf. on Concept Lattices and Their Applications (CLA 2014), Fuengirola (Spain), 2012年10月13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：