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　元 年　 ６ 月 １７ 日現在

機関番号：１２６０８
研究種目：若手研究(B)
研究期間：2015～2018
課題番号：１５Ｋ１５９６９

研究課題名（和文）非近似的アプローチによるリアクティブシステム仕様の効率的な実現可能性判定法

研究課題名（英文）Efficient realizability verification of reactive system specifications without approximation

研究代表者
島川　昌也（Shimakawa, Masaya）

東京工業大学・情報理工学院・助教

研究者番号：００７４９１６１

交付決定額（研究期間全体）：（直接経費）　　2,900,000円

研究成果の概要（和文）：リアクティブシステム仕様の実現可能性に関する検証は，仕様記述において見過ごされがちな危険な状況に陥る可能性を検出することができるが，一般に煩雑で計算コストの高い処理を伴う．本研究では，リアクティブシステム仕様の実現可能性判定の高速化を目的として，以下の事項に取り組んだ．(1) 部分的にBDDを利用して効率的に実現可能性判定手続きを実装する手法（部分シンボリック技法と呼ぶ）を開発した．この手法の最大の特長は，非近似的な実現可能性判定にも適用できることである．(2) 実現可能性判定を行う際に用いるωオートマトンをon-the-flyに簡約する手法を開発した．

研究成果の学術的意義や社会的意義
本研究の意義は，リアクティブシステム仕様の非近似的な実現可能性判定の効率化に成功した点である．既存研究では，シンボリック技法を適用するために近似的なアプローチがとられていた．本研究では，部分シンボリック技法により非近似的な実現可能性判定手続きを効率的に実装する手法を提案し，実験により，近似的なアプローチに引けを取らない性能がでることを確認した．

研究成果の概要（英文）：Realizability verification of reactive system specifications can detect dangerous situations that may arise that were not expected while drawing up the specifications. However, such verification typically involves complex, intricate analyses. In this research, we aimed at reducing the cost of realizability verification for reactive system specifications, and we worked on the following: (1) We developed an efficient method (called partially symbolic method) for implementing procedures of realizability verification, in which binary decision diagrams (BDDs) are used partially. The greatest feature of this method is that it is applicable to realizability verification without approximation (2) We developed an on-the-fly simplification method for omega-automata which are used in realizability verification.

研究分野：形式手法

キーワード：リアクティブシステム仕様　実現可能性　ω-オートマトン

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９、ＣＫ－１９（共通）

１．研究開始当初の背景

高い安全性が求められるシステムの開発においては，厳密な仕様を形式的に記述し，分析することが有効である．環境からの要求に対して適切なタイミングで応答を返すことが強く求められるリアクティブシステムを対象とした場合は，時間論理でその動作仕様を記述し，実現可能性の検査を行うことで，仕様記述において見過ごされがちな危険な状況に陥る可能性を検出することができる．実現可能性とは，「どのように要求がきても，仕様を満たすように応答を返す実現システムが存在する」という性質である．この性質が満たされることが分かれば，常に仕様を満たすことが保証された実現システム（のモデル）の合成も可能である．

しかしながら，リアクティブシステム仕様の実現可能性判定は，一般に煩雑で計算コストの高い処理を伴う．それゆえ，実現可能性判定を適用できる仕様の規模は限られており，それが実用化への障壁となっている．

このような問題の解決に向けて，判定手続きの実装にシンボリック技法を用いる研究や近似的アプローチによる効率化の研究が進んでいる．シンボリック技法とは，検証手続きにおいて必要となるオートマトンの遷移関係をひとつの命題論理式で表現し，命題論理式を高速に処理することができる BDD (Binary Decision Diagram)や SAT ソルバを用いて判定を行う実装技法である．通常の実現可能性判定においては，ωオートマトン（無限語を扱うオートマトン）の決定化が必要となるが，その手続きは煩雑がゆえ，シンボリック技法が適用できない．そのため，近似的アプローチにより，決定化手続きを単純化したうえでシンボリック技法が用いられる．これらのシンボリック技法や近似的アプローチによる実現可能性判定の効率化に関する研究は，一定の成果が得られており，ツールの開発等も進んでいる．

一方，シンボリック技法以外の実装技法や近似を行わない非近似的アプローチによる実現可能性判定の効率化については，研究がほとんど行われていなかった．ツールも存在していなかった．

２．研究の目的

本研究では，リアクティブシステム仕様の実現可能性判定の高速化を目的とし，シンボリック技法以外の実装技法や，近似を行わない非近似的アプローチによる実現可能性判定の効率化方法を模索する．

我々は，過去に，部分的に BDD を利用する効率化技法：部分シンボリック技法を提案し，他の検証分野で成功している．この技法は適用範囲が広いため，非近似的な実現可能性判定にも適用できる．この部分シンボリック技法による非近似的な実現可能性判定の性能が，シンボリック技法による近似的な実現可能性判定に引けをとらないか調査する．

また，部分シンボリック技法には，上位レイヤでの（実装レベルよりも上位のレベルでの）効率化が施しやすいとう利点がある．通常のシンボリック技法においては，不必要な状態の除去などの他の効率化技法を併用させると，遷移関係の表現が複雑になるため，逆にパフォーマンスが落ちることがある．一方で，本研究で我々が用いる部分シンボリック技法ではそのような問題はおきない．そこで，実現可能性判定を行う際に用いるωオートマトンの簡約手法などについても検討する．

３．研究の方法

(1) 部分的に BDD を利用する部分シンボリック技法により，実現可能性判定手続きを実装する手法を検討する．実現可能性判定は，次の手順で行われる：(i) 仕様から非決定性ωオートマトン（無限長の語を扱うオートマトン）を構成する．(ii) 非決定性ωオートマトンを決定化して，決定性ωオートマトンを構成する．(iii) 決定性ωオートマトンを分析する．(ii)の手続きは，特に煩雑で計算コストの高い処理を伴う．ここでは，この(ii)の処理を部分シンボリック技法を用いて実装する手法を検討する．

(2) (1)で検討した手法を基に実現可能性判定ツールを開発する．そして，既存ツールと比較する．具体的には，シンボリック技法による近似的な実現可能性判定ツールとその判定にかかる時間を比較する．

(3) 実現可能性判定効率化のためのωオートマトン簡約手法について検討する．

４．研究成果

(1) 部分シンボリック技法により実現可能性判定手続きを実装する手法を提案した．判定手続き内のωオートマトンの決定化において，部分シンボリック技法を用いる．提案した手法では，オートマトンの各状態の遷移集合（その状態を起点とする遷移の集合）をひとつの BDD（Multi-terminal BDD という種類の BDD を用いる）で表現し，各状態は明示的に扱う．非近似的な実現可能性判定手続きだけでなく，近似的な実現可能性判定手続きの実装に部分シンボリック技法を適用する手法も与えた．

［学会発表 10 の成果の一部］

(2) 部分シンボリック技法による非近似的実現可能性判定ツール，及び部分シンボリック技法による近似的実現可能性判定ツールを開発した．そして，シンボリック技法による近似的実現可能性判定ツールとそれらの性能を実験により比較した．実験の結果，それぞれの性能は対等であることがわかり，本研究で提案した手法の有効性が確認できた．
［学会発表 10 の成果の一部］

(3) 実現可能性判定効率化のためのωオートマトン簡約手法を提案した．提案した手法では，構成途中に簡約を適用することで扱う状態やエッジを減らし，構成自体のコストも低減させる on-the-fly アプローチをとる．決定性ωオートマトン構成時に，状態にラベルされる情報から決定性ωオートマトンの模倣関係を計算し，それを用いて余分な状態やエッジを除去する．(2) で開発した部分シンボリック技法による実現可能性判定ツールにこの簡約手法を織り込み，実験により，この手法の有効性を確認した．
［学会発表 1 の成果］

(4) 上位レイヤの効率化手法である実現可能性の分割検証法について検討した．分割検証法とは，次のようなものである：(i)分割されたそれぞれの部分仕様において決定性ωオートマトンを構成する．(ii)各部分オートマトンにおいて局所的な情報を捨象する．(iii)各部分オートマトンを統合し，解析する．このような検証では，(ii)において局所的な情報を捨象できるため，一括検証に比べて高速に判定を行える．本研究では，効果的な分割検証を行うための仕様の分割方法を提案した．
［学会発表 7 の成果］

(5) 部分シンボリック技法を用いて，時間論理サブセットよる仕様の実現可能性判定ツールを開発した．構文を制限した時間論理サブセットを対象とした，効率的な実現可能性判定手続きが提案されている．ここでは，そのような時間論理サブセット用実現可能性判定手続きを，(1) と同様，部分シンボリック技法を用いて実装する手法を提案し，ツールを開発した．
［学会発表 8 の成果の一部］

５．主な発表論文等

〔雑誌論文〕（計 1 件）

① Takashi Tomita, Atsushi Ueno, Masaya Shimakawa, Shigeki Hagihara, Naoki Yonezaki, Safraless LTL synthesis considering maximal realizability, 査読有, Acta Informatica, Volume 54, Issue 7, pp. 655 - 692, Nov. 2016. DOI:10.1007/s00236-016-0280-3

〔学会発表〕（計 11 件）

① Masaya Shimakawa, Shigeki Hagihara, Naoki Yonezaki. Towards Improvement of Realizability Checking for Reactive System Specifications by Simplification of Infinite Games, Workshop on Computation: Theory and Practice (WCTP 2018), Sep. 2018.

② Masaya Shimakawa, Shigeki Hagihara, Naoki Yonezaki. Efficiency of the Strong Satisfiability Checking Procedure for Reactive System Specifications, International Conference on Computer, Electronic Engineering and Information Science (CEEIS 2017), Dec. 2017.

③ Masaya Shimakawa, Shigeki Hagihara, Naoki Yonezaki. Towards Improvements of Bounded Realizability Checking, Workshop on Computation: Theory and Practice (WCTP2017), Sep. 2017.

④ Shigeki Hagihara, Masaya Shimakawa, Naoki Yonezaki. Discussion on Verification of Voting Protocols, 17th Philippine Computing Science Congress (PCSC 2017), Proceedings of the 17th Philippine Computing Science Congress, Mar. 2017.

⑤ Shigeki Hagihara, Masahiko Tomoishi, Masaya Shimakawa, Naoki Yonezaki. Combining Unification and Rewriting in Proofs for Modal Logics with First-order Undefinable Frames, 5th International Conference on Computer Science, Electronics Technology and Automation (ICCSETA 2017), Mar. 2017.

⑥ Masaya Shimakawa, Kenji Osari, Shigeki Hagihara, Naoki Yonezaki. Modularization of formal specifications for efficient synthesis of reactive systems, 6th International Conference on Software and Computer Applications (ICSCA 2017), Feb. 2017.

⑦ Shigeki Hagihara, Yoshiharu Fushihara, Masaya Shimakawa, Masahiko Tomoishi, Naoki Yonezaki. Web server access trend analysis based on the Poisson distribution, 6th International Conference on Software and Computer Applications (ICSCA 2017), Feb. 2017.

⑧ Masaya Shimakawa, Yuuji Iwasaki, Shigeki Hagihara, Naoki Yonezaki. Discussion of LTL Subsets for Efficient Verification, Workshop on Computation: Theory and Practice (WCTP2016), pp. 1-14, Sep. 2016.

⑨ Shigeki Hagihara, Atsushi Ueno, Takashi Tomita, Masaya Shimakawa, Naoki Yonezaki. Simple synthesis of reactive systems with tolerance for unexpected environmental behavior, the 4th FME Workshop on Formal Methods in Software Engineering (FormaliSE '16), pp. 15-21, May. 2016.

⑩ Masaya Shimakawa, Shigeki Hagihara, Naoki Yonezaki. Towards Unbounded Realizability Checking, Workshop on Computation: Theory and Practice (WCTP2015), pp. 80-90, Sep. 2015.

⑪ Masaya Shimakawa, Shigeki Hagihara, Naoki Yonezaki. Reducing Bounded Realizability Analysis to Reachability Checking, 9th International Workshop on Reachability Problems (RP 2015), Lecture Notes in Computer Science, Vol. 9328, pp. 140-152, Sep. 2015.

〔図書〕（計 0 件）

〔産業財産権〕
○出願状況（計 0 件）

○取得状況（計 0 件）

〔その他〕
特になし

６．研究組織

(1)研究分担者
なし

(2)研究協力者
なし