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 １３ 日現在

機関番号：３２６３８
研究種目：若手研究
研究期間：2018～2022
課題番号：１８Ｋ１８０２８

研究課題名（和文）効率的なωオートマトン操作法と非制限的仕様検証への応用

研究課題名（英文）Efficient methods of operating omega-automata and its applications to specification verification

研究代表者
島川　昌也（Shimakawa, Masaya）

拓殖大学・工学部・准教授

研究者番号：００７４９１６１

交付決定額（研究期間全体）：（直接経費）　　3,100,000円

研究成果の概要（和文）：形式仕様検証は人力では見つけにくい欠陥を検出できるが，その計算コストは高い．本研究では，リアクティブシステム仕様の非制限的検証，つまり仕様の構文や検証性質を制限しない検証のコスト削減を目的として，以下に取り組んだ．(1)リアクティブシステム仕様の検証で基盤となるωオートマトンや無限ゲームの効率的な操作手法を提案した．具体的には，無限ゲームの簡約方法や，部分シンボリック技法を用いたωオートマトンや無限ゲームの各種操作の効率的な実装手法を提案した．(2) 提案したωオートマトンや無限ゲームの効率的な操作手法を基に仕様検証器を開発した．

研究成果の学術的意義や社会的意義
形式仕様の自動検証はその有効性は認識されているものの，計算コストの高さからごく小規模な対象にその適用は限られている．特にリアクティブシステム仕様の自動検証では，理論的基盤として用いられるωオートマトンや無限ゲームの処理が煩雑であることから，その問題は顕著である．本研究では，そのような計算コストの問題を緩和させるため，いくつかの効率化手法を提案した．その成果はリアクティブシステム仕様の自動検証のより大規模で実際的な対象への適用に寄与するものと考えている．

研究成果の概要（英文）：Formal specification verification can detect errors that are difficult to find manually. However, its computation cost is high. In this research, we aimed at reducing the cost of verification for reactive system specifications, that does not restrict the syntax of specifications or checking properties, and we worked on the following: (1) We proposed efficient methods for operating ω-automata and infinite games, that are the foundations of verification for reactive system specifications. Specifically, we gave a method for simplifying infinite games, and implementation methods for operating ω-automata and infinite games, using partially symbolic techniques. (2) We developed a verification tool, that is based on the proposed methods.

研究分野：システム検証

キーワード：ωオートマトン　仕様検証

様　式　Ｆ－１９－２

１．研究開始当初の背景

外部とのインタラクションの維持を目的としたリアクティブシステムにおいては，入出力のタイミングが重要であるため，時間の概念を取り扱うことが可能な形式言語で，ふるまいに関する仕様を厳密に記述し，それを検証することが有効である．これにより，人力では見つけにくい欠陥を計算機によって自動で検出できる．

しかしながら，線形時間論理仕様の実現可能性検査をはじめとした，いくつかのリアクティブシステム仕様の検証は，煩雑で計算コストの高い処理を伴う．それらの検証は，システムの無限のふるまいを考慮するため，無限長の語（ω語）や無限サイズの木（ω木）を扱うωオートマトンや無限ゲーム上の問題に帰着されるが，ωオートマトンや無限ゲームの操作手続きの一部は，煩雑で計算コストが高い．

上記問題の解決に向けて，以下のような制限的検証に関する研究が進んでいる．

- 検証する性質の制限（近似的な検証）
- 仕様記述言語の制限

これらのアプローチでは，検証において必要となるωオートマトンや無限ゲームの操作手続きが単純化され，シンボリック技法と呼ばれる効率的な実装手法が適用できる．検証コストは削減されるものの，検証できる性質や仕様は限定的である．

一方，非制限的なアプローチの研究は，ほとんど行われていなかった．理由としては，非制限的検証では，必要となるωオートマトンや無限ゲームの操作手続きが煩雑であるため，シンボリック技法が適用できないことが挙げられる．しかし近年我々は，部分シンボリック技法と呼ぶ実装手法を提案し，他の検証分野で成功している[1]．この実装手法は適用範囲が広いため，複雑なωオートマトンや無限ゲームの操作／仕様の非制限的検証にも適用可能である．これにより，シンボリック技法を用いた制限的手法に引けをとらない性能がでる可能性がある．既に我々は，ω語オートマトンの決定化手続きについては，[2，3]で部分シンボリック技法による効率的な実装を与えている．

２．研究の目的

本研究では，我々の過去の研究成果を踏まえて，リアクティブシステム仕様の非制限的検証の効率を，制限的検証と同等までに押し上げることを目的とする．非制限的検証の効率化が成功すれば，

- 非近似的検証が可能に → 大規模な仕様の正確な検証結果が得られるようになる．
- 制限のない仕様記述言語での検証が可能に → 多様な仕様の検証が可能になる．

これまで効率的な実現方法が知られていなかった非制限的検証の効率化に取り組む点が本研究の最大の特徴である．既存研究では，シンボリック技法を用いるため，制限的なアプローチがとられているが，それは限定的な解決に過ぎない．本研究では，我々が近年提案した部分シンボリック技法を用いて非制限的検証の効率化に取り組み，計算コストの問題の本質的な解決を目指す．

３．研究の方法

リアクティブシステム仕様の非制限的検証の効率化に向けて，以下に取り組む．

3.1.部分シンボリック技法によるωオートマトンや無限ゲームの操作手続きの効率的な実装法

部分シンボリック技法とは，我々が過去に[1,2,3]で提案しているωオートマトンや無限ゲームの操作手続きを効率的に実装する手法のひとつである．通常のシンボリック技法では，オートマトンやゲームグラフ全体をひとつの Binary Decision Diagram (BDD)で表現するのに対して，部分シンボリック技法では，BDD を部分的に利用する．すなわち，オートマトンの一部のみを BDD で表現する．通常のシンボリック技法には，次のような問題がある：

A) 煩雑な手続きへの適用が難しい．
　例えば，ωオートマトンの決定化手続きにおいては一部でツリー構造を必要とするが，それを BDD のみで表現するのは難しい．

B) 他の効率化技法(上位レイヤでの効率化など)を併用しにくい．
　例えば，不要な状態や遷移の除去などの他の効率化技法を併用すると，状態集合や遷移関係の BDD での表現が複雑になるため，逆に効率が悪くなることがある．

一方，部分シンボリック技法は，BDD と相性のよい部分のみで BDD を利用するため，適用可能な範囲が広く，また他の効率化技法との併用が行いやすいという特徴を持つ．

部分シンボリック技法には，オートマトンやゲームのどの部分をどのように BDD で表現するかによって様々なバリエーションが存在しえる．そこで本研究では，部分シンボリック技法の各種バリエーションについて検討し，それらを用いたωオートマトンや無限ゲームの各種操作手続きの実装手法を提案する．(決定化の実装手法については[2，3]で提案済みである．ここではその他の操作・判定を扱う．)

3.2.ωオートマトンや無限ゲームについての上位レイヤでの効率化技法
　上述のとおり，部分シンボリック技法は，上位レイヤの効率化技法との併用も有効である．そこで本研究では，上位レイヤの効率化技法として，オートマトンやゲームの簡約手法についても検討する．

3.3.仕様検証器の開発
　上の成果を組み込んだ仕様検証器を開発する．

４．研究成果
　本研究の成果は以下の通りである．

4.1.部分シンボリック技法によるωオートマトンや無限ゲームの操作手続きの効率的な実装法
　部分シンボリック技法の以下の 2 種のバリエーションで，ωオートマトンや無限ゲームの積集合演算，和集合演算，補集合演算，空判定演算を実装する手法を提案した．
　　① 各状態からの複数の遷移をひとつの BDD で表現するもの
　　(BDD の変種である MtBDD を利用)
　　② 各遷移にラベルされる遷移条件をひとつの BDD で表現するもの
また，実際にそのパフォーマンスを実験により調査した．部分シンボリック技法を用いた実装がナイーブな実装に比べて高速に各種操作を行えることが確認できた．また，対象のオートマトンにおいて非決定的な分岐が少ないとき，バリエーション①はバリエーション②よりも高速であるという傾向があることもわかった．

4.2 ωオートマトンや無限ゲームについての上位レイヤでの効率化技法
　一部の仕様検証においては，仕様から無限ゲーム（ω木オートマトンと同等のものである）を構成してそれを解析する．一般にその無限ゲームのサイズは大きく，検証のコストは高い．その問題を低減するため，以下に取り組んだ．(i)無限ゲームの模倣関係の導入した．この模倣関係は，非決定性状態遷移系（やプロセス代数）の模倣関係の一般化となっている（非決定性オートマトンは非決定的な分岐のみを持つのに対して，無限ゲームはユニバーサルな分岐も持つ）．(ii) その模倣関係をベースに，勝利戦略が存在するかを判定する上で不必要なエッジを無限ゲームから取り除く手法を提案した．(iii) その単純化を仕様から無限ゲームを構成する途中に適用する手法を提案した（無限ゲームを構成される際に各ノードにラベルされる情報から模倣関係を算出できることを利用する）．この手法は，無限ゲームのサイズを小さくするだけでなく，無限ゲームの構成のコストも下げることができる．提案手法のパフォーマンスを実験により調査し，多くの例題でこの手法が有効であることを確認した．

4.3 仕様検証器の開発
　これまでに提案してきたωオートマトンや無限ゲームの操作手続きの実装手法を基盤として，仕様検証器の実装を行った．積合成演算／和集合演算の実装法は部分仕様の統合において活用し，補集合演算や空判定の実装法は，仕様の実現可能性や強充足可能性と呼ばれる性質の判定において活用した．

参考文献

[1] S. Mochizuki, M. Shimakawa, S. Hagihara, N. Yonezaki. Fast Translation from LTL to Büchi Automata via Non-transition-based Automata. International Conference on Formal Engineering Methods, ICFEM 2014, LNCS Vol. 8829, pp. 364-379, Springer, 2014.
[2] M. Shimakawa, S. Hagihara, N. Yonezaki. Towards Unbounded Realizability Checking. Workshop on Computation: Theory and Practice, WCTP 2015, pp.80-90, 2015.
[3] 科研費 若手研究(B), 15K15969, 研究代表者：島川昌也, 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, 2015-04-01～2019-03-31.

５．主な発表論文等

〔雑誌論文〕　計2件（うち査読付論文　2件／うち国際共著　0件／うちオープンアクセス　1件）

１．著者名 Ito Sohei、Osari Kenji、Shimakawa Masaya、Hagihara Shigeki、Yonezaki Naoki	４．巻 bxab116
２．論文標題 Efficient Realizability Checking by Modularization of LTL Specifications	５．発行年 2021年
３．雑誌名 The Computer Journal	６．最初と最後の頁 bxab116
掲載論文のDOI（デジタルオブジェクト識別子） 10.1093/comjnl/bxab116	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 TOMITA Takashi、HAGIHARA Shigeki、SHIMAKAWA Masaya、YONEZAKI Naoki	４．巻 E105.D
２．論文標題 A Characterization on Necessary Conditions of Realizability for Reactive System Specifications	５．発行年 2022年
３．雑誌名 IEICE Transactions on Information and Systems	６．最初と最後の頁 1665～1677
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transinf.2021FOP0005	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 －

〔学会発表〕　計4件（うち招待講演　0件／うち国際学会　4件）

１．発表者名 Masaya Shimakawa, Kentaro Hayashi, Shigeki Hagihara and Naoki Yonezaki
２．発表標題 Towards Interpretation of Abstract Instructions using Declarative Constraints in Temporal Logic
３．学会等名 International Conference on Software and Computer Applications (ICSCA 2020)（国際学会）
４．発表年 2020年

１．発表者名 Masaya Shimakawa, Atsushi Ueno, Shohei Mochizuki, Takashi Tomita, Shigeki Hagihara, Naoki Yonezaki
２．発表標題 Towards Efficient Implementation of Realizability Checking for Reactive System Specifications
３．学会等名 International Conference on Software and Computer Applications (ICSCA 2019)（国際学会）
４．発表年 2019年

１．発表者名 Shigeki Hagihara, Masaya Shimakawa, Naoki Yonezaki
２．発表標題 Verification of Verifiability of Voting Protocols by Strand Space Analysis
３．学会等名 International Conference on Software and Computer Applications (ICSCA 2019)（国際学会）
４．発表年 2019年

１．発表者名 Masaya Shimakawa, Shigeki Hagihara, Naoki Yonezaki
２．発表標題 Towards Improvement of Realizability Checking for Reactive System Specifications by Simplification of Infinite Games
３．学会等名 Workshop on Computation: Theory and Practice (WCTP2018)（国際学会）
４．発表年 2018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

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