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　　２　日現在

機関番号：　１３９０１
研究種目：　基盤研究(B)（一般）
研究期間：　2013～2016
課題番号：　２５２８００２３

研究課題名（和文）高レベル言語で記述されたリアクティブシステムに対する実時間性質の検証

研究課題名（英文）Verification of real-time reactive systems in high-level programming languages

研究代表者
結縁　祥治（Yuen, Shoji）

名古屋大学・情報科学研究科・教授

研究者番号：７０２３０６１２

交付決定額（研究期間全体）：（直接経費）　　12,900,000円

研究成果の概要（和文）：本研究では、再帰呼び出しや割り込みなどの手続き呼び出しを持つ高レベル言語で記述された実時間プログラムの振舞いをモデル化するNested Timed Automaton(以下NeTA)を提案し、到達可能性が決定可能であることを示し、安全性検証が可能であることを示した。NeTAは、時間オートマトンをスタックアルファベットに持つプッシュダウンシステムである。さらに、時間オートマトンがスタック上にあるときにクロックを凍結する機構を導入しても、一定の条件のもとで到達可能性が保存することを示した。さらに、効率的なゾーン構成による検証手法について検討した。

研究成果の概要（英文）：This study presents a safety verification of real-time programs described by a high level programming language with syntax such as recursive calls and interrupt handlings. We proposed a new behavioral model called 'Nested Timed Automata', NeTA for short. The state reachability of NeTA is shown to be decidable. This shows the safety verification is possible. NeTA is a pushdown system whose stack alphabets are timed automata. We also introduced the clock freezing for clocks of timed automata while it is on the stack. It is shown that the reachability is kept decidable under a certain condition. We investigated an efficient Zone-constrcution method to improve the efficiency.

研究分野：　並行計算モデル

キーワード：　実時間システム　到達可能性解析　プッシュダウンシステム　クロック凍結

１．研究開始当初の背景

組み込みデバイスコントローラなどに代表されるように、現代社会におけるリアクティブシステムの重要性は計り知れない。また、近年、ソフトウェアシステムの安全性は社会的に大きな問題として取り沙汰され、ソフトウェア検証が非常に高い関心を集めている。特に、外部環境に対応し連動的に動作するリアクティブシステムにおいては、「定められた時間内にあるイベントが必ず起こる」等の実時間性質（real-time property）の検証が極めて重要な課題である。従来、リアクティブシステムはマシン言語など低レベルなプログラミング言語で記述される場合が多かった。しかし、近年では、安全性およびプログラミング簡易性の向上を目指し、より高度なオブジェクト指向言語や関数型言語の導入が推進しており、高い関心を集めている。再帰関数、再帰データ構造、高階関数、オブジェクト、割り込みハンドラなど高度な機能を含むプログラミング言語（以降、本申請書では、「高レベル言語機能」および「高レベル言語」と呼ぶ）に対してのプログラム検証は、有限状態 automaton を検証対象モデルとする古典的なモデル検査などの検証手法では難しい。しかし、近年、「ソフトウェアモデル検査」とひと括りで呼ばれることが一般的となった、モデル検査の技術と抽象実行などのプログラム解析の技術を融合した新たなソフトウェア検証手法の登場により、多くの高レベル言語において、安全性（safety property）（「イベントがプログラム実行中に起こらない」）や活性（liveness property）（「イベントがいずれ起こる」）などの時間の制約を伴わない性質については検証が現実的となった[1]。対して、現在、実時間性質を扱えるプログラム検証手法は、timed automaton [2] としてモデル化されたシステムに対するモデル検査など、低レベル言語を対象としたものに限られる。Timed automaton は、有限状態 automaton に「クロック変数」と呼ばれる時間の経過と共に値が増加する変数を加えた計算モデルであり、ハードウェアや低レベル言語で記述されたリアクティブシステムの検証には有効な枠組みである。しかし、有限状態 automaton が高レベル言語で記述されたプログラムの検証に不十分であると同様に、timed automaton は高レベル言語にて記述されたリアクティブシステムの検証には不十分である。

２．研究の目的

高レベル言語で記述されたリアクティブシステムに対しての実時間性質検証の手法を確立する。その手段は、近年のソフトウェアモデル検査技術と従来の低レベル言語に対するリアクティブシステム検証技術の融合である。本課題の前身となる応募者の過去研究での貢献は、実時間性質検証のための新しい計算モデルの提案とそれに対する到達可能性判定など基礎的検証問題の計算可能性について議論した、主に理論的なものであり、実際の高レベル言語で記述されたリアクティブシステム検証への実用にはほど遠い。そこで、本課題の主要目標として以下を設定した。

(1) 従来の理論的枠組みをベースに、近年の DPTDA（dense-timed pushdown automaton）[3] についての研究結果なども取り入れ、（一階の）再帰関数や割り込みハンドラを扱うリアクティブシステムの検証アルゴリズムを構築する。
(2) HORS（higher-order recursion scheme）モデル検査を目的として、高レベル言語のためのソフトウェアモデル検査の技術を取り入れ、(1)の成果を高階関数、再帰データ構造、オブジェクトなどを扱うさらに高レベルなリアクティブシステムの検証に拡張する。
(3) 検証ツールを作成し、C 言語で記述された再帰関数や割り込みハンドラを含んだリアクティブシステムおよび、リアクティブシステムのための高レベル言語である FRP で記述されたプログラムに対して検証実験を行う。

３．研究の方法

(1) 時間 PDA モデル検査:
一階の再帰関数および割り込みハンドラを含むリアクティブシステムの検証を実現である。PDA（pushdown automaton）とは、有限状態 automaton と無限長のスタックを組み合わせた計算モデルである。ソフトウェアモデル検査において、PDA は再帰関数や
割り込みハンドラの表現などに用いられる。直感的には、無限長のスタックを用い、関数呼び出し際のコールスタックや割り込み際のタスクスタックを正確に表現する。ここでスタック要素は自体は有限であるため、述語抽象[3] などの技術を用い、スタック要素で表現されるデータの抽象化を行う。PDA に対するモデル検査は safety 性質および liveness 性質など時間の概念を伴わない性質において決定可能であり、効率の良いアルゴリズムも存在する。

(2) HORS の応用：
時間の概念を含まない性質を対象とする場合、高階関数など高レベル言語機能を扱えるソフトウェアモデル検査は、HORS（higher-order recursion scheme）と呼ばえる、直感的にはスタック自体をスタック要素とする「高階の PDA」をベースの検証対象計算モデルとした手法を応用しする。実時間性質においては、一階の場合と同じく、高階ソフトウェアに対する実用的な検証は実現されていない。高階ソフトウェアモデル検査の技術と、クロック変数を加えた（一階の）PDA に対する検証のノウハウを組み合わせ、高レベル言語に対して有効な実時間性質検証の手法を確立する。

また、リアクティブシステムのための高レベル言語 FRP を対象とする検証ツールを作成し検証実験を行う。
（３）検証ツールの設計：
PDA の到達可能性検証は一般に高い計算複雑さを持つ。同様のモデルを用いる限り、複雑さを下げることは難しいため、本質的に効率的な検証アルゴリズムを得ることは不可能である。実時間性をもつプログラムには高い信頼性が求められるため、高い計算複雑さを持つ場合でも、一定のコストをかけて検証をすることも必要である。検証に対して、効率を向上させる技法、例えば、ゾーン構成などに基づいた検証手法を提案し、実装を試みる。

４．研究成果
(1) 時間 PDA によるモデル検査
時間モデル検査については、Nested Timed Automaton(NeTA)を新たに提案し、NeTA に対して状態到達可能性が決定可能である結果を得た。NeTA は、従来研究で提案されている DTPDA を拡張したモデルであり、高レベル言語で記述された実時間プログラムの振舞いを精度よくモデル化する。NeTA の振舞いは拡張された形の DTPDA に変換することができ、拡張された DTPDA の到達可能性が決定可能であることから、NeTA のエラー到達性が決定可能であるとが示される。このことは、高レベル言語による記述において、クロックを導入してもエラー到達性が基本的には検証可能であることを示している。ここでは、既存研究の Abudulla らの DTPDA[ ]のモデルにスタックに格納されたクロックと push 動作時、pop 動作時にスタック上に格納されるクロックとの値の受け渡しが可能なように拡張している。このような拡張を行ってもと到達可能性は保存される。
　さらに実時間プログラムにおいてスタック上に格納されている間はクロックの値を進めないモデルについて検討した[業績　]。時間を含めたモデルにおいてクロックを進めない（凍結する）動作は、クロックの進行において本質的な難しさを導入することになり、一般にはスタックを持たない場合においても、線形ハイブリッドシステムと同等の能力をもつことが知られている。ハイブリッドシステムにおいては状態到達可能性は決定不能である[]。NeTA にクロック凍結を導入したモデル NeTA-F においては、スタックに格納されることがなく、凍結されないクロック（グローバルクロックと呼ぶ）の数が１つであれば、到達可能性が決定可能であることを示した。グローバルクロックが複数の場合は、２カウンターマシンの振舞いがエンコード可能なので、到達可能性は決定不能となる。グローバルクロックは実際のプログラムにおいては、システムクロックであるとすると大きな制限とはならない。
(2) HORS モデル検査：
従来研究に引き続き高階関数プログラムの停止性について研究を進めるとともに、関数型言語におけるハイブリッドシステムの検証手法について、研究を行った。ここでは、無限小定数による検証手法[4]に対して限量子除去による具体的な検証手続きを提案した。さらに、ハイブリッドシステムを記述する FRP である Haskell/Yampa の振舞いのモデル化について検討し、差分的に実行するための意味論を与えた。
(3) 検証ツールの設計：
業績で得られた NeTA の振舞いをそのまま検証ツールとして実現すると状態爆発が発生することが予想される。このため、検証ツールではより効率的な検証手法が必要である。時間オートマトンの場合を参考にして、Zone 構成によって時間経過による離散化領域数の増大を避ける手法を研究した。DTPDA に対する Zone 構成をもとにして、クロック凍結機構を持つ NeTA および DTPDA に対するゾーン構成を研究した。研究期間内には極めて初期的な予備実験しかできなかったが、ゾーン構成においても５，６個程度以上のクロックを導入すると検証時間が爆発的に増大することがわかった。実用的な検証ツールのためにはプッシュダウンシステムの到達可能性手法を利用する必要がある。

○引用文献
[1] N. R. Krishnaswami and N. Benton. Ultrametric Semantics of Reactive Programs. In Proc of LICS 2011.
[2] R. Alur and D. L. Dill. A Theory of Timed Automata. Theoretical Computer Science 126(2) 1994.
[3] P. A. Abdulla, M. F. Atig, and J. Stenman. Dense-Timed Pushdown Automata. In Proc of LICS 2012.
[4] K. Suenaga, I. Hasuo: Exercises in Nonstandard Static Analysis of Hybrid Systems. CAV 2012: 462-478

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　12　件）
① Guoqiang Li, Xiaojuan Cai, Mizuhito Ogawa, Shoji Yuen: Nested Timed Automata, FORMATS2013, Lecture Notes in Computer Science 8053, pp168-182, 2013
② Iain Phillips, Irek Ulidowski, Shoji Yuen: Modelling of Bonding with Processes and Events, RC2013, Lecture Notes in Computer Science 7948, pp

③ 岩塚卓弥、寺内多智弘、結縁祥治：無限小定数と限量子除去法によるハイブリッドシステムの検証に向けて、情報処理学会論文誌PRO, Vol6(3), 2013, pp.20-32

④ Takuya Kuwahara, Tachio Terauchi, Hiroshi Unno, Naoki Kobayashi: Automatic Termination Verification for Higher-Order Functional Programs, ESOP2014, Lecture Notes in Computer Science 8410, 2014, pp392-411

⑤ Eric Koskinen, Tachio Terauchi: Local temporal reasoning, CSL-LICS 14, 2014, pp. 59:1-59:10

⑥ Irek Ulidowski, Iain Phillips, Shoji Yuen: Concurrency and reversibility, RC2014, Lecture Notes in Computer Science 8507, 2014, pp.1-14

⑦ Yunqing Wen, Guoqiang Li, Shoji Yuen: An Over Approximation Forward Analysis for Nested Timed Automata, SOFL+MSVL2014, Lecture Notes in Computer Science 8979, 2015, pp.62-81

⑧ Guoqiang Li, Mizuhito Ogawa, Shoji Yuen: Nested Timed Automata with frozen clocks, FORMATS2015, Lecture Notes in Computer Science 9218, 2015, pp.189-205

⑨ Yunqing Wen, Guoqiang Li, Shoji Yuen: On reachability analysis of Updatable Timed Automata with One Updatable Clock, SOFL+MSVL2015, Lecture Notes in Computer Science 9559, 2016, pp.147-161

⑩ Tachio Terauchi: Explaing the Effectiveness of Small Refinement Heuristics in Program Verificaiton with CEGAR, SAS2015, Lecture Notes in Computer Science, 9291, 2015, pp.128-144

⑪ Akihiro Murase, Tachio Terauchi, Naoki Kobayashi, Ryosuke Sato, Hiroshi Unno: Temporal Verification of Higher-order Functional Programs, POPL2016, 2016, pp.57-68

⑫ Arthur Blot, Masaki Yamamoto, Tachio Terauchi: Compositional Synthesis of Leakage Resilient Programs, Lecture Notes in Comuter Science 10204, 2017, pp.277-297

〔学会発表〕（計 7 件）

① 黒板亮太、結縁祥治：時間制約による Alloy 記述の拡張、電子情報通信学会ソフトウエアサイエンス 信学技法 113-448, pp.1-6, 2014

① 平岡祥、結縁祥治：クロック凍結機構をもつ稠密プッシュダウンオートマトンのゾーン構成による検証、電子情報通信学会ソフトウエアサイエンス 信学技法 116-277, pp.43-48, 2016

② 市橋友樹、結縁祥治：Yampa プログラム実行のための振舞いモデル、電子情報通信学会ソフトウェアサイエンス 信学技報 SS 116-127, pp.99-104, 2016

② 平岡祥、結縁祥治：クロック凍結機構をもつ稠密プッシュダウンオートマトンのゾーン構成による検証、電子情報通信学会ソフトウエアサイエンス 信学技法 116-277, pp.43-48, 2017

③ 稲垣貴大、結縁祥治：Android アプリケーションの並行実行における予期しない消費電力増加の検出、電子情報通信学会ソフトウエアサイエンス 信学技法 116-277, pp.85-90, 2017

④ Keigo Imai, Shoji Yuen and Nobuko Yoshida: Session Typed Programming with Poles and Lenses, Dagstuhl seminar 17501, 2017

⑤ Shoji Yuen: Towards the zone based reachability analysis of dense timed pushdown automata with frozen clocks, 46th TRS meeting, 2017

〔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〕
ホームページ等

６．研究組織
(1)研究代表者
結縁祥治（YUEN, Shoji）
名古屋大学大学院情報科学研究科・教授
研究者番号：70230612

(2)研究分担者
寺内多智弘　（TERAUCHI, Tachio）
北陸先端科学技術大学院大学先端科学技術研究科・教授
研究者番号： 70447150

(3)連携研究者
(該当なし)
(4)研究協力者
李国強（LI, Guoqiang　　）
上海交通大学・ソフトウェア学院・准教授

今井敬語（IMAI, Keigo ）
有限会社：IT プラニング、
現在：岐阜大学・工学部・助教

ウリドフスキー　イレック(Ulidowski Irek)
レスター大学・情報学部・准教授