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　１３　日現在

機関番号：　１３９０１
研究種目：　挑戦的萌芽研究
研究期間：　2014～2016
課題番号：　２６５４００２６

研究課題名（和文）コード証明に基づく実時間システムの検証

研究課題名（英文）Verification of real-time systems based on proving codes

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）　　2,600,000円

研究成果の概要（和文）：本研究では、実時間性を持つ並行プログラムに対する証明に基づいた検証技法を与える。以下の３つの観点から研究を実施した。(1) コード証明：オープンソースのToppers RTOSの最小モデルであるSSPカーネルのソースコードに対して分離論理によるコードの証明を行った。ビットマップによる優先度フラグの操作が正しく行われることを示した。(2)実時間プログラムの実行モデルとなるNested Timed Automataのエラー到達可能性検査技法を研究した。(3) 関数型言語のDSLであるYampaに対して離散的に実行する場合の動作意味を与えた。

研究成果の概要（英文）：We studied verification techniques for real-time concurrent programs. We investigated following topics: (1) Low-leve code proof for RTOS: We gave a proof for priority flag operation for an open-source RTOS kernel, Toppers/SSP, (2) Reachability analysis for Nested Timed Automata: We gave an approximation and an extension. and (3) we gave an operational semantics of Haskell/Yampa on discrete timed runtime environment to show a faulty behavior of hybrid system programs.

研究分野：　並行計算

キーワード：　実時間性　ソフトウェア検証　並行プログラム

１．研究開始当初の背景

組込みシステムにおけるソフトウェアには高い信頼性と実時間性が求められる。システムの性質からコード規模は小規模であっても、実時間性確保のための割り込みやマルチタスクといった複雑な制御が要求される。人命に関わるようなシステムの制御においては、いかなる状況においてもエラーの発生には大きなリスクを伴うため、プログラム検証の技術の具体的な応用技術の開発が望まれる。

２．研究の目的

本研究では、実時間性が重要な性質である組込みシステムなどの実行基盤として用いられる実時間オペレーティングシスム(RTOS)上で構成される実時間システムが実時間性を含めて正しく振舞うことを検証する手法を確立することを目的とした。オープンソースの RTOS である ToppersOS[1]のプログラムコードに対して証明を行い、実時間性解析のためのタスク実行モデルに対応づける。要求される性質が保証された実行基盤の正しさの上で構成されるソフトウェアシステムの実時間性を検証して、テストを超える実時間ソフトウァの信頼性を獲得すること目標とする。さらに、コード証明に基づいた新たなな RTOS の実装技術の確立を目指す。

３．研究の方法

具体的な実時間コードをもとに、コードの証明とエラー到達可能性の観点でプログラムコードの正しさを証明する。研究は研究の目的としてあげた ToopersOS コードに加えてコード実行の基盤となる時間 PDA のエラー到達可能性に関する研究、および、さらに高度な実時間性を記述する関数型言語として Haskell/Yampa のモデル化に取り組んだ。これらの実時間性をもつコードの実行には、関数による機能に加えてメモリや実行順などを保証することが必要になる。

ToppersOS のコード証明においては、分離論理に基づいて ToppersAPI が仕様として提供している性質が実際に証明を与えることを試みた。このうち、タスクの優先度フラグの振舞いなど実時間性に影響を与える部分について証明を試みた。

プログラム実行の実時間性をさらに正確にモデル化するために時間プッシュダウンシステムの振舞いの検証手法について検討した。実時間を扱うことの可能な実行もでるである Nested Timed Automata[2]の到達可能性とそのための検証手法を研究した。

プッシュダウンを持つ実時間プログラムの抽象的な体系としてプロセス計算 CCS を拡張した HCCS[3]の意味論を検討する。HCCS は Milner の CCS に連続遷移を導入した体系であり、プッシュダウンシステムを記述可能性であるが、プッシュダウンの記述例が与えられていないため、その実行意味について検討する。

実時間の振舞い記述するプログラミング言語として、関数型言語 Haskell の領域埋め込み言語である Yampa の振舞いモデルについて検討した。実行基盤としてはより抽象的なレベルで実行されるため、抽象的な概念のもとに実時間プログラムを記述できるが、その振舞いには検証が必要である。

４．研究成果

研究は３つの観点で進めた。

4-1. Toppers カーネルに対するコード証明：ToppersOS のコード証明については、Toppers/SSP という最も小規模な OS カーネルコードに対して証明を与えた。ここでは、実時間性はビットマップに対する優先度フラグの振舞いによって確保されている。分離論理に対してビットマップ操作を表す述語を組み込んで人手によって証明を与え、コードが正しく動作することを保証した。Toppers/SSP では、制御タスクの数があらかじめ決まっており、今回は３レベルのタスクに対して証明を行った。[学会発表④]

ここでは、以下の２つの性質が成立することを示した。

(1) タスクはすべて実行される
(2) タスクは優先度フラグに従って、順番に実行される

証明においてキーになったのは、Hoare 論理におけるループの選択である。今回は、優先度ビットマップにおいて、上記の性質を直接的に表す不変式を導き、証明を構成した。ToppersOS は多くの実装がなされており、十分なテストが実施されているため、バグの存在は確認できなかった。しかし、証明を与えることでテストデータによらないコード信頼性が確保されたと言える。

さらに、Toppers/FMP においてタスクマイグレーションを行う API に対して証明を試みた。ここでは、結果として証明に失敗した。これは、タスク API の仕様単位と排他制御がずれていることによることがわかった。ただし、この点については、ToppersOS 製作者への聞き取りから振舞い上は問題ないが、コードとして独立した証明は与えにくいということがわかった。当初の予想とは異なる結果となり、証明する性質と実際のコードにはギャップが存在することがわかった。

4.2 Nested Timed Automaton 検証の効率化

Nested Timed Automaton(以下 NeTA)に対しては、到達可能性の検証の近似手法とクロック更新機構の拡張を行い、より正確なモデル化が可能となった。NeTA をまず pushdown system と見なして検証し、さらに各要素となっている Timed Automaton で到達可能性をチェックする。この手法は効率的でことが示

されるが、必ずしも精度が十分とは言えないため、応用が限定される[雑誌論文①]。さらに、ゾーン構成手法を NeTA の基本モデルである DTPDA-F に適用し、ツール設計の基本モデルを構築した　[学会発表⑨、⑩]。

4-3 HCCS によるハイブリッド PDA の記述

プロセス計算の枠組みにおいて時間を扱う体系は多数存在するが、連続変数を導入した体系は限定される。このうち HCCS と呼ばれる拡張について検討した。特に再帰構造を持つ記述について検討し、記述を試みた。再帰構造を持つオートマトン[4]との対応について検討した。[学会発表⑥,⑦]

4-4 Haskell/Yampa の離散意味論

Haskell/Yampa の検証については、Haskell/Yampa で記述される実時間システムが連続的な時間意味を持つハイブリッドシステムとしては正しくても、実際に離散的に実行される場合には様々な問題を起こすことがわかっている。このことをモデル化するために「差分オートマトン」を提案した。連続的に実行されるべき意味路をもつプログラムが離散的に実行される場合に、プログラムが本来持つ性質が保たれな場合があることを示す形式モデルである。連続的な時間上で意味が定義されている場合でも実際は離散的な時間でプログラムは実行される。このとき、離散時間によるサンプリング実行では、必ずしも連続的な条件どおりに条件文が成立しないので、サンプリングのタイミングによって実行が異なる場合がある。このような状況を差分オートマトンはモデル化した。ここで、連続時間は微小時間ごとにのみ実行されのので、微小時間を dt で表し、サンプリングが適切でない場合、予定通りの性質が保てない場合が存在する。差分オートマトンは微笑時間を dt として抽象化し、予期しない振舞いのモデル化を行った[学会発表⑧]。

引用文献：

[1] Toppers プロジェクト：http://toppers.jp
[2] Guoqiang Li, Mizuhito Ogawa, Shoji Yuen: “Nested Timed Automata”, FORMSTS2013, LNCS 8053, pp.168-182,2013
[3] S.Schneider, U.Nestmann: Rigorous Discretization of Hybrid Systems Using Process Calculi. FORMATS 2011: 301-316
[4]S.N.Krishna, L.Manasa,L.Trivedi: What’s decidable about recursive hybrid automata, HSCC15, 2015, pp31-40.

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　2　件）

① Yunqiang Wen, Guoqiang Li and Shoji Yuen: On Reachability of Updatable Timed Automata with One Updatable Clock, Lecture Notes in Computer Science 9559, pp.147-161, 2016
② Yunqing Wen, ,Gquqiang.Li and Shoji Yuen: An Over-Approximation Forward Analysis for Nested Timed Automata, Lecture Notes in Computer Science 8979, pp.62-80, 2015

〔学会発表〕（計　12　件）

① Keigo Imai, Shoji Yuen and Nobuko Yoshida: Session Typed Programming with Poles and Lenses, Dagstuhl seminar 17501, 2017
② Shoji Yuen: Towards the zone based reachability analysis of dense timed pushdown automata with frozen clocks, 46th TRS meeting, 2017
③ 川北悠人、結縁祥治：ハイブリッドシステムに対する CCS の拡張について、電子情報通信学会ソフトウェアサイエンス信学技報 SS 115-420, pp.129-134, 2016
④ 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
⑤ 平岡祥、結縁祥治：クロック凍結機構を持つ稠密時間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ェアサイエンス　信学技報 SS 116-277, pp.43-48, 2016
⑥ 平岡祥、結縁祥治：クロック凍結機構を持つ稠密時間プッシュダウンオートマトンの記号実行、電子情報通信学会ソフトウェアサイエンス　信学技報 SS 116-512, pp.1-6, 2016
⑦ 廣田樹、結縁祥治、東道徹也：部分観測における MaxSAT ソルバを用いたスーパーバイザ合成手法、電子情報通信学会ソフトウェアサイエンス　信学技報 SS 114-510, pp.31-36, 2015
⑧ 荒川洸、結縁祥治：Toppers/SSP カーネルのタスク制御に対する低レベルコード証明、電子情報通信学会ソフトウェアサイエンス　信学技報 SS 114-271, pp.31-36, 2015
⑨ 川北悠人、結縁祥治：ハイブリッドプロセス計算を用いたスーパーバイザ合成について、電子情報通信学会ソフトウェアサイエンス　信学技報 SS 115-20, pp.7-10, 2015
⑩ 川北悠人、結縁祥治：HCCS による再帰的ハイブリッドシステムの記述、電子情報通信学会ソフトウェアサイエンス　信学技報 SS 115-248, pp.7-12, 2015
⑪ 結縁祥治、亀井達郎：値付きタスクオートマトンに基づくコストを意識した実時間タスクスケジューリング、電子情報通信学会ソフトウェアサイエンス　信学技

報 SS 114-127, pp.37-42, 2014
⑫ 荒川洸、結縁祥治：UPPAAL を用いた LEGO Mindstorm EV3 制御プログラムの合成、電子情報通信学会ソフトウェアサイエンス　信学技報 SS 114-271, pp.41-46, 2014

〔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

(3) 研究分担者
(該当なし)

(3)連携研究者
（該当なし）

研究者番号：

(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