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　６ 年　 ６ 月 １４ 日現在

機関番号：１３３０１
研究種目：基盤研究(C)（一般）
研究期間：2021～2023
課題番号：２１Ｋ１１８２４

研究課題名（和文）割込みを持つ組込みアセンブリプログラムのリアルタイム性のソフトウェアモデル検査

研究課題名（英文）Software model checking for real-time properties of embedded assembply program with interruptions

研究代表者
山根　智（Yamane, Satoshi）

金沢大学・電子情報通信学系・教授

研究者番号：７０２６３５０６

交付決定額（研究期間全体）：（直接経費）　　3,000,000円

研究成果の概要（和文）：割込みを持つ組込みアセンブリプログラムのリアルタイム性のソフトウェアモデル検査の理論と実装の研究を対象とし、SMTソルバーを用いて、抽象化精錬によるソフトウェアモデル検査の実現と評価の研究を行った。具体的にはイベント割込みとタイマ割込みの両方を扱い、それらの割込み処理の削減の理論、実装、評価及び、抽象化精錬によるソフトウェアモデル検査の理論、実装、評価を行った。まず、イベント割込みを対象とし、模倣関係による削減の理論、実装、評価を行い、ソフトウェアモデル検査を実現した。次に、時間割込みを対象とし、時間模倣関係による時間割込み処理の削減の理論、実装、評価を行い、ソフトウェアモデル検査を実現した。

研究成果の学術的意義や社会的意義
（１）学術的意義：ハードウェアとの相互作用及びタイミング制約に関する組込みソフトウェア検証は最重要な未解決問題であり，割込み処理を持つ組込みソフトウェアのリアルタイム性の検証を実現するソフトウェアモデル検査が必須である．「割込み処理を持つ組込みソフトウェアのリアルタイム性検証」という学術的「問い」は，(a)割込み処理をアセンブリプログラムに埋め込んで，(b)タイマ割込み処理などの組込みソフトウェアの特性を表す形式的意味モデルへ変換を行い，(c)ソフトウェアモデル検査技術の確立である．
（２）社会的意義：自動運転などの組込みソフトウェア安全性保証の研究は，社会的に最重要な国際的課題である．

研究成果の概要（英文）：Theoretical and implementation studies of software model checking of real-time performance of embedded assembly programs with interrupts were conducted using the SMT solver, and the realization and evaluation of software model checking by abstraction refinement were studied. Specifically, both event interrupts and time interrupts were treated, and the theory, implementation, and evaluation of reduction of their interrupt processing, as well as the theory, implementation, and evaluation of software model checking by abstraction refinement were conducted.
First, we addressed event interrupts, and conducted the theory, implementation, and evaluation of reduction by imitation relations to realize software model checking.
Second, for time interrupt, the theory, implementation, and evaluation of reduction of time interrupt processing by the time imitation relation were conducted, and software model checking was realized.

研究分野：コンピュータソフトウェア

キーワード：組込みソフトウェア　割込み処理　アセンブリプログラム　ソフトウェアモデル検査　抽象化精錬　SMTソルバー　双模倣関係

様式　Ｃ－１９，Ｆ－１９－１，Ｚ－１９（共通）

１．研究開始当初の背景

組込みプログラムの不具合の解消及び，自動運転の大規模ソフトウェアの安全性確保などの課題もあり，組込みソフトウェア安全性保証の研究は，社会的かつ科学技術上の最重要な国際的課題である(毎年開催ACM EMSOFT等)．従来の研究は仕様やＣプログラムの検証であり，組込みソフトウェアのハードウェアとの相互作用，割込み処理やタイミング制約の検証が不十分である．申請者はハードウェアとの相互作用及びリアルタイム性を組込んだモデルの構築手法を開発して，アセンブリプログラムのソフトウェアモデル検査において先導的な研究を展開している(山根,Electronics 2020，IEICE 2020)．本研究では，割込み処理とリアルタイム性を効率的に検証するために，プログラム動作に影響する割込み処理のみを埋め込んだアセンブリプログラムを，時間Kripke構造(アセンブリ命令の実行時間付き状態遷移システム)に変換して，ソフトウェアモデル検査手法を開発する．

ハードウェアとの相互作用及びタイミング制約に関する組込みソフトウェア検証は最重要な未解決問題であり，これを解決するためには，割込み処理を持つ組込みソフトウェアのリアルタイム性の検証を実現するソフトウェアモデル検査が必須である．一方，ハードウェアとの相互作用は組込みＣプログラム言語とアセンブリ言語で記述されており（B.Schlich，ACM TECS 2010)，プログラムの実行時間に関わるタイミング制約はＣプログラムよりもアセンブリプログラムを対象とするほうが正確に検証できる(山根，IEICE 2017)ので，Ｃプログラムよりもアセンブリプログラムを検証するほうが適切である．以上より，「割込み処理を持つ組込みソフトウェアのリアルタイム性検証」という本研究課題の核心をなす学術的「問い」は，プログラム解析により，(a)プログラム動作に影響する割込み処理のみをアセンブリプログラムに埋め込んで，(b)タイミング制約やタイマ割込み処理などの組込みソフトウェアの特性を表す形式的意味モデル(時間Kripke 構造)へ変換を行い，(c)ソフトウェアモデル検査技術(SMT 定理証明による抽象化,抽象モデル検査，反例解析，Interpolation，精錬化)の確立である．

２．研究の目的

本研究では，タイミング制約が厳しく，割込み処理を持つ組込みソフトウェアのリアルタイム性のソフトウェアモデル検査の開発を目的とする．割込み処理を埋め込んだアセンブリプログラムを対象に，定理証明技術を用いて， SMT 述語抽象化，SMT 抽象モデル検査，SMT 反例解析，SMT Interpolation，SMT 述語精錬化により，モデル検査技術を開発し，組込みアセンブリプログラムのタイマ割込みなどのリアルタイム安全性検証を目的とする．

３．研究の方法

本研究では，申請者らのこれまでの研究成果をもとに，割込み処理を持つ組込みアセンブリ

プログラムのリアルタイム安全性検証を実現するために，以下を研究する．
(1) プログラム解析を用いて，割込み処理を埋め込んだアセンブリプログラムのタイミング制約及びタイマ割込みなどの形式的意味を時間Kripke 構造により定義する．
(2) 時間Kripke 構造のSMT 述語抽象化，SMT 抽象モデル検査，SMT 反例解析，SMT Interpolation，SMT 述語精錬化により，アセンブリプログラムのリアルタイム性のソフトウェアモデル検査の理論の開発を行い，その実験的な評価に関する研究を行う．

以下の分担（代表者 山根がモデル検査の理論実装，分担者 櫻井がプログラム解析，大学院生が実装）で，研究期間内に下記のことを明らかにする．
(1) 時間Kripke 構造により，割込み処理を埋め込んだアセンブリプログラムのタイミング制約及びタイマ割込みなどを形式的意味定義（担当：山根，櫻井）：
① アセンブリプログラムのタイミング制約及びタイマ割込みなどの形式的意味を時間Kripke 構造で表現する．
② プログラム解析により，プログラム動作に影響する割込み処理のみを埋め込んだアセンブリプログラムを時間Kripke 構造に変換し，さらに検証性質をリアルタイム時相論理で仕様記述する．
③現実の組込みアセンブリプログラムの意味及びその検証性質が時間Kripke 構造及びリアルタイム時相論理で表現できることを，理論的及び実験的に明らかにする．
(2)アセンブリプログラムのソフトウェアモデル検査（担当：山根,櫻井,大学院生３名）：
① アセンブリプログラムのソフトウェアモデル検査を開発する．
② アセンブリプログラムをSMT 述語抽象化して，時間Kripke 構造の抽象化を行い，抽象化精錬によるソフトウェアモデル検査を行う．
③ 抽象時間Kripke 構造のSMT 抽象モデル検査，SMT 反例解析，SMT Interpolation，SMT 述語精錬化により，組込みアセンブリプログラムのリアルタイム性の抽象化精錬のソフトウェアモデル検査を開発する．大学院生３名と共同で，プロトタイプを実装して，組込みソフトウェアのリアルタイム性の検証が行えることを明らかにする．

４．研究成果

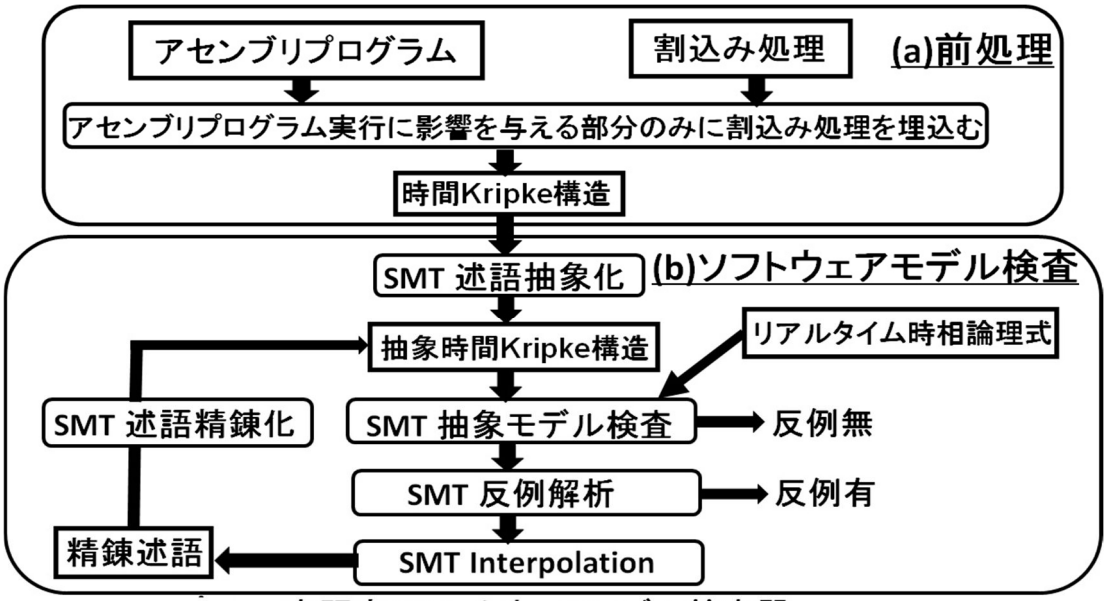
前節の各項目に沿って，研究成果を述べる．

(1) 時間 Kripke 構造により，割込み処理を埋め込んだアセンブリプログラムのタイミング制約及びタイマ割込みなどを形式的意味定義：
①イベント割込みとタイマ割込みを対象として，割込みプログラムを割込み呼び出しプログラムに埋め込む．埋め込むときに，割込み呼び出しプログラムの処理に影響を与えない割込みプログラムを埋め込まないようにして，割込み処理を削減する．なお，その理論的な正当性は時間双模倣理論により保証した．この削減手法により，時間 Kripke 構造の状態数が60%～90%削減できた．

②割込みプログラムを埋め込んだ割込み呼び出しプログラムを時間 Kripke 構造に変換して，ソフトウェアモデル検査の入力とする．

(2)アセンブリプログラムのソフトウェアモデル検査：

以下の図のように，(a)時間 Kripke 構造を(b)ソフトウェアモデル検査に入力して，SMT ソルバーを用いて抽象化精錬のモデル検査を行う．ソフトウェアモデル検査器では，術語抽象化と述語試練，Interpolation による精錬術後の生成を行い，抽象化と精錬のモデル検査を行う．現在，ソフトウェアモデル検査のプロトタイプの実装は完了して，事例により評価を行っている．



本研究のソフトウェアモデル検査器

(3)まとめと今後の課題：

本研究により，割込みを持つ組込みアセンブリプログラムを対象として，SMT ソルバーを用いた抽象化精錬によるソフトウェアモデル検査器を実現した．これにより，ハードウェアに依存したプログラムの論理とタイミング制約の正当性を検証できたことを実証した．しかし，ソフトウェアモデル検査器は現状ではプロトタイプであり，規模の大きな実例の検証にはいたっていない．今後の課題としては，ソフトウェアモデル検査器の完成などがあげられる．

５．主な発表論文等

〔雑誌論文〕　計3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 小柴真之介、山根智	４．巻 SE-213
２．論文標題 有界モデル検査を用いたリアルタイムOSカーネルのタスク管理モジュールの形式的検証	５．発行年 2023年
３．雑誌名 情報処理学会ソフトウェア工学研究会	６．最初と最後の頁 1-8
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
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 Taro Kiriyama, Yajun Wu, Satoshi Yamane	４．巻 10
２．論文標題 Reduction of Timer Interrupts for Embedded Assembly Programs Based on Reduction of Interrupt Handler Executions	５．発行年 2021年
３．雑誌名 2021 IEEE 10th Global Conference on Consumer Electronics (GCCE)	６．最初と最後の頁 464-466
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/GCCE53005.2021.9622013	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 Satoshi Yamane , Taro Kriyama , Yajun Wu	４．巻 13
２．論文標題 An Efficient Reduction of Timer Interrupts for Model Checking of Embedded Assembly Programs	５．発行年 2024年
３．雑誌名 Electronics	６．最初と最後の頁 1-12
掲載論文のDOI（デジタルオブジェクト識別子） 10.3390/electronics13020463	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0件

〔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
研究分担者	櫻井　孝平 (Sakurai Kohei) (80597021)	金沢大学・電子情報通信学系・助教 (13301)	

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