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　３０　年　　４　月　２５　日現在

機関番号：　１３３０１
研究種目：　基盤研究(C)（一般）
研究期間：　2015～2017
課題番号：　１５Ｋ００９３

研究課題名（和文）革新的ソフトウェアモデル検査による組込みアセンブリプログラムの安全性検証

研究課題名（英文）Verifying safety properties of embedded assembly program using innovative software model checking

研究代表者

山根　智（YAMANE, SATOSHI）

金沢大学・電子情報学系・教授

研究者番号：７０２６３５０６

交付決定額（研究期間全体）：（直接経費）　　3,500,000円

研究成果の概要（和文）：研究成果は以下の2つに大別できる．
（1）動的プログラム解析の枝刈りと抽象化，実行時間見積もりによる最小なモデル構築器（アセンブリプログラムから割込み処理が埋め込まれた最小モデルを構築する）を作成した．
（2）抽象化精錬(CEGAR)型ＳＭＴモデル検査手法を開発した．このモデル検査手法はＳＭＴによる述語抽象化、ＳＭＴ有界モデル検査、ＳＭＴによる反例解析器、ＳＭＴソルバによるInterpolationを用いた精錬述語の生成からなる．なお、ＳＭＴソルバとして、種々のInterpolationをサポートしているUppsala大学のPrincessを用いた．

研究成果の概要（英文）：The research outcome can be roughly divided into the following two.
(1) We have developed a minimal model constructor (constructing a minimum model with interrupt processing embedded from the assembly program) by pruning and abstraction of dynamic program analysis and execution time estimation.
(2) SMT model checking method based on Abstraction and Refinement (CEGAR) was developed. This model checking method consists of predicate abstraction by SMT, SMT bounded model check, counter-example analyzer by SMT, and refinement predicate generation using Interpolation by SMT solver. As the SMT solver, Princess of Uppsala University which supports various interpolations was used.

研究分野：　ソフトウェア

キーワード：　ソフトウェアモデル検査　組込みアセンブリプログラム　抽象化精錬　ＳＭＴ　定理証明

１．研究開始当初の背景

トヨタ車プリウスの制御プログラムの不具合などの国際的な問題もあり，**組込みソフトウェアの安全性保証の研究は，最重要な国際的課題**である(毎年開催されるACM EMSOFT 等)．従来の研究は仕様やＣプログラムのモデル検査のみであり，ハードウェアとの相互作用の検証を実現しておらず，安全性保証が不可能である．**本研究の目的は，ハードウェアとの相互作用を検証するために，アセンブリプログラムのモデル検査手法を開発することである**．

申請者は，**時間オートマトンや確率時間オートマトン，ハイブリッドオートマトンのモデル検査(S.Yamane，AMAST Series in Computing 2007)，詳細化検証(山根 他,コンピュータソフトウェア 2008)，抽象化精錬型モデル検査**(山根 他,**電情通学会 CST 研究会優秀論文賞 2008**)を構築してきた．一方，分担者は，**プログラムの安全性保証のためには，プログラム解析手法が有効であることを示している(櫻井 他，情処論文誌 PRO 2012 年論文賞)．申請者らは，大規模化に対応して，ハードウェア依存情報として代表的なビット列演算の効率的な検証のために，アセンブリプログラムのＳＭＴ有界モデル検査手法を構築して，プロトタイプにより有効性を実証している**(山根 他,IEEE GCCE 2014 等)．**しかし，タイマ割込み処理などの検証及び実用レベルの大規模ソフトウェアの検証などの解決すべき重要な問題が多く残されている**．

計画を進めていく上で，申請者は次のような予備的な研究成果を得ている．

① **動的プログラム解析**により，組込みアセンブリプログラムから **I/O 及びタイマの割込み処理を含む，モデルの構築手法**を検討した．このモデルは**枝刈りと抽象化，実行時間の見積もりを動的プログラム解析**に含めており，モデルのサイズを小さくできることを確認している．(山根 他,組込みシンポジウム 2014 等)

② リアルタイムプログラム（変数付き時間オートマトン）の**抽象化精錬（CEGAR (CounterExample-Guided Abstraction Refinement))型モデル検査器**を開発しており，実装及び検証実験を行い，有効性を確認している(山根 他，数理解析研究所講究録 2007)．

２．研究の目的

上記の背景およびこれまでの研究成果をもとに，**本研究は，組込みアセンブリプログラムの安全性検証を実現するために，(1)動的プログラム解析及び，(2)ＳＭＴ有界モデル検査と抽象化精錬検証の融合により，I/O 割込み処理及びタイマ割込み処理を含めた大規模アセンブリプログラムの革新的ソフトウェアモデル検査の理論と技術の開発を行い，(3)その実験的な評価に関する研究を行う**．研究期間内に以下のことを明らかにする．

(1)**動的プログラム解析による枝刈りと抽象化，実行時間の見積もり**により，組込みアセンブリプログラムから**状態爆発の抑制可能な最小モデル**を構築する手法を明らかにする．なお，このモデルはハードウェアとの相互作用を実現している**割込み処理を含む**．

(2)**ビット列の背景理論のＳＭＴ有界モデル検査手法及び抽象化精錬，Resolution 定理，クレイグの補間定理**との融合により，組込みアセンブリプログラムの**抽象化精錬型ＳＭＴモデル検査手法**が実現できることを明らかにする．なお，ＳＭＴとは,背景理論付きSATのことであり，ビット列の背景理論のＳＭＴでは，ビット列演算が効率的に検証できる理論である．

(3)**上記の(1)と(2)からなるアセンブリプログラムの革新的ソフトウェアモデル検査**により，Ｃ言語プログラムでは検証

できない，**スタックオーバーフローや割込み多重化の安全性などの重要なハードウェア依存の検証性質が検証**できることを明らかにする．さらに，**実際に稼働中の大規模組込みアセンブリプログラムの安全性検証**が実現できることを明らかにする．

３．研究の方法

本研究では，アセンブリプログラムの安全性検証のために，**モデル構築器と抽象化精錬(CEGAR)型ＳＭＴモデル検査からなる革新的ソフトウェアモデル検査器**を開発し，実験する．

(1) **動的プログラム解析の枝刈りと抽象化，実行時間見積もりによるモデル構築器**（アセンブリプログラムから割込み処理が埋め込まれた最小モデルを構築する）

(2) **抽象化精錬(CEGAR)型ＳＭＴモデル検査**（大規模プログラムのモデルをモデル検査する）

① **抽象化器**（**抽象化述語**により，抽象モデル及びその精錬モデルを構築する）

② **ＳＭＴ有界モデル検査器**（**ビット列の背景理論を用いたＳＭＴ有界モデル検査器**）

③ **ＳＭＴによる反例解析器**（ＳＭＴソルバで，**反例**が元のモデルに存在するかを判定する）

④ **クレイグの補間定理による精錬器**（偽反例を無くすために，**クレイグの補間定理**を用いて，ＳＭＴソルバで，精錬用述語を発見する）

(3) **大規模組込みアセンブリプログラムがハードウェア依存の検証性質を持たすかどうか**を，ソフトウェアモデル検査器で検証を行う．

４．研究成果

上記の研究目的及び研究方法の（1）と（2）に対応して、研究成果は以下の２つに大別できる．

（1）**動的プログラム解析の枝刈りと抽象化，実行時間見積もりによる最小なモデル構築器**（アセンブリプログラムから割込み処理が埋め込まれた最小モデルを構築する）を作成した．

（2）**抽象化精錬(CEGAR)型ＳＭＴモデル検査手法**を開発した．このモデル検査手法はＳＭＴによる述語抽象化、**ＳＭＴ有界モデル検査、ＳＭＴによる反例解析器、ＳＭＴソルバによる Interpolation を用いた精錬述語の生成からなる．なお、ＳＭＴソルバとして、種々の Interpolation をサポートしている Uppsala 大学の Princess を用いた．**

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１６件）

(1)小田島直樹、福田岳飛、山根智：定理証明器 Princess を用いた組込みアセンブリプログラムのリアルタイム安全性の演繹的検証， MSS2017-84，pp.35-40，2018.
(2)S.Yamane: Invited paper Deductively Verifying Embedded Software in the Era of Artificial Intelligence = Machine Learning + Software Science, IEEE 6th GCCE2017, pp.1-4, 2017.
(3)S.Yamane, R.Konoshita, T.Kato: Model checking of embedded assembly program based on simulation, IEICE Transactions on Information and Systems, Vol.E100-D, No.8, pp.1819-1826, 2017.
(4)山根智：組込みアセンブリプログラムのリアルタイム安全性の演繹的検証 ～ □≦TIME q = □(q∧(time≦TIME)) ～ , MSS2017-12, pp.59-64, 2017.
(5)山根智：組込みアセンブリプログラムのリアルタイム性の検証手法 ～ 組込みプログラムのためのモデル検査と演繹的検証 ～, MSS2016-83, pp.11-16, 2017.
(6)R. Yanase, T. Sakai, M. Sakai, S. Yamane：A Case Study of Formal Approach to Dynamically Reconfigurable Systems by Using Dynamic Linear Hybrid Automata, LNCS 10009, pp.74-89, 2016.
(7)Satoshi Yamane, Tomonori Kato, Ryosuke Konoshita：Simulation and Model checking of embedded assembly program, pp.1-8, ESS2016, 2016.

(8)Y.Ono, K.Sakurai, S.Yamane: LogChamber: Inferring Source Code Locations Corresponding to Mobile Applications Run-time Logs, Journal of Information Processing Vol. 24, No. 4, pp.700-710, 2016.
(9) R.Yanase, M.Sakai, T.Sakai ,S.Yamane : Specification and Verification of Dynamically Reconfigurable Systems using Dynamic Linear Hybrid Automata, Journal of Software Engineering and Applications, Vol.9, No.9, pp.452-478, 2016.
(10) K. Hamaya, S. Yamane: Detecting Bank Conflict of GPU Programs Using Symbolic Execution?Case Study, Journal of Software Engineering and Applications, Vol.10, No.2, pp.159-167, 2016.
(11)柳瀬 龍, 山根 智: 線形ハイブリッドオートマトンの non-Zeno 公平性検証に対する遷移述語抽象化の適用, MSS2015-40, pp.29-33, 2016.
(12)K. Hamaya, S. Yamane: Detecting Bank Conflict of GPU Programs Using Symbolic Execution, pp.1-3, IEEE 5th Global Conference on Consumer Electronics, 2015.
(13) T.Adachi, S.Yamane, K.Sakurai: Distributed CFG-based Symbolic Execution for Assembly Programs , IEEE 4th GCCE, pp.1-5, 2015.
(14) K. Sakurai, H. Masuhara: The omission finder for debugging what-should-have-happened bugs in object-oriented programs, 30th ACM SAC,pp.1962-1969, 2015.
(15) R.Yanase, T.Sakai, M.Sakai, S.Yaname: Formal Verification of Dynamically Reconfigurable Systems , IEEE 4th GCCE, pp.1-5, 2015.
(16)公下亮佑, 山根 智: 記号実行による組込みアセンブリプログラムのソフトウェアモデル検査, MSS2015-15, pp.77-81, 2015.

〔学会発表〕(計 0件)

〔図書〕(計 0件)

〔産業財産権〕

○出願状況(計 0件)

名称：
発明者：
権利者：
種類：
番号：
出願年月日：
国内外の別：

○取得状況(計 0件)

名称：
発明者：
権利者：
種類：
番号：
取得年月日：
国内外の別：

〔その他〕
ホームページ等

６．研究組織
(1)研究代表者
山根智(YAMANE SATOSHI)

研究者番号：70263506

(2)研究分担者
櫻井孝平 (SAKURAI KOUHEI)

研究者番号：80597021

(3)連携研究者
( )

研究者番号：

(4)研究協力者
( )