

自己評価報告書

平成23年 4月 12日現在

機関番号：13302

研究種目：若手研究（A）

研究期間：2008～2011

課題番号：20680001

研究課題名（和文） 高度な並行・並列組込みソフトウェアの検証法に関する研究

研究課題名（英文） Verification Methods for Highly Parallelized Embedded Software

研究代表者

青木 利晃（AOKI TOSHIAKI）

北陸先端科学技術大学院大学・情報科学研究科・准教授

研究者番号：20313702

研究分野：総合領域

科研費の分科・細目：情報学・ソフトウェア

キーワード：形式検証，モデル検査

1. 研究計画の概要

最近の組込みソフトウェアは、マルチタスクが取り扱い可能なリアルタイムオペレーティングシステムを用いるだけでなく、マルチCPU、マルチOS、マルチコアCPUを用いて高度に並行・並列化されて実装されている。そこで、本研究課題では、このような高度に並行・並列化された組込みソフトウェア、さらには、それらがヘテロに組み合わせられた組込みソフトウェアを対象とした検証法を、モデル検査手法を拡張することにより提案する。

2. 研究の進捗状況

本研究では、まず、1. リアルタイムオペレーティングシステム(RTOS)の検証実験、および、2. マルチコア上で動作するソフトウェアの検証実験を行った。1 では、車載システムのRTOSであるOSEK/VDXを対象とした。これにより、検証には、その外側である環境の取扱いが重要であることが判明した。また、2 では、Playstation 3に搭載されているCellプロセッサで動作するプログラムを対象とした。これにより、ボトルネックとなるバスのスループットなどのパフォーマンスに関する見積りが重要であることが判明した。

そこで、次に、1 に関しては、環境を効率的に取扱い手法、および、ツールを提案した。RTOSは様々な使われ方をするため、それぞれの使われ方に関して検証する必要がある。そこで、昨年度、UMLにより整理して記述し、その記述からモデル検査のための記述を複数自動生成するアルゴリズムを提案した。今年度は、そのアルゴリズムに基づいて、モデル検査用の記述を自動生成するツールのプ

ロトタイプを作成した。2 に関しては、実時間ソフトウェアの設計を対象としたパラメトリック分析手法を提案した。この手法では、動作の実行時間を変数として表現した設計モデルを対象として、デッドラインなどの実時間性を満たす変数に関する条件を求める。今年度は、そのアルゴリズムと停止性、健全性、完全性などの基本的な性質、および、ツールのプロトタイプを作成した。

3. 現在までの達成度

②おおむね順調に進展している。

(理由)

本研究では、高度な並列・並行組込みソフトウェアを対象とした検証法を提案することが目的である。これまでに、その具体的な例として、RTOSとマルチコアCPU上で動作するプログラムを対象として、それらの問題の一部を特定し、具体的な検証法を提案することができた。さらに、ツールの実装に関しても、当初の予定どおり、実装を行うことができた。

4. 今後の研究の推進方策

今後は提案手法の評価を行う。評価のために、車載オペレーティングシステムを対象とした実験とスケジューリングを伴うマルチタスクソフトウェアを対象とした実験を行う。また、これまでの研究により、提案手法を補助する工学的な手法が必要であることが判明している。例えば、環境モデルを整理する手法や検証結果を管理する手法である。これらについても、並行して研究を行っていく。

5. 代表的な研究成果
(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4件)

①Pham Ngoc Hung, Viet Ha Nguyen, Toshiaki Aoki, Takuya Katayama: A Minimized Assumption Generation Method for Component-Based Software Verification, IEICE Transactions Vol.E93-D, No.8, pp.2172-2181, Aug. 2010, 査読あり.

②Pham Ngoc Hung, Toshiaki Aoki, Takuya Katayama: Modular Conformance Testing and Assume-Guarantee Verification for Evolving Component-Based Software, IEICE Transactions Vol.E92-A, No.11, pp.2772-2780, Nov., 2009, 査読あり.

③Hideaki Nishihara, Koichi Shinozaki, Koji Hayamizu, Toshiaki Aoki, Kenji Taguchi, Fumihiro Kumeno:Model checking education for software engineers in Japan, ACM SIGCSE Bulletin, Volume 41 , Issue 2 (June 2009), p.45-50, 2009, 査読あり.

[学会発表] (計19件)

① Kenro Yatake and Toshiaki Aoki: Automatic Generation of Model Checking Scripts based on Environment Modeling, The 17th International SPIN Workshop on Model Checking of Software (SPIN 2010), pp.58-75, Sep. 27, 2010. オランダ

②Chaiwat Sathawornwichit, Toshiaki Aoki and Takuya Katayama: Modeling of Real-Time System Designs for Parametric Analysis, the 16th IEEE International Conference on Embedded and Real-Time Computing Systems and Applications (RTCSA 2010), pp.81-91, Aug. 23, 2010. マカオ

③Pham Ngoc Hung, Toshiaki Aoki and Takuya Katayama: A Minimized Assumption Generation Method for Component-Based Software Verification, In the 6th International Colloquium on Theoretical Aspect of Computing, LNCS 5684, pp.277-291, Springer-Verlag, Aug. 18, 2009. マレーシア

[図書] (計2件)

①青木利晃:組込みソフトウェア開発技術, 9章 組込みソフトウェアの静的検証技術 (pp.271-307), CQ 出版, ISBN 978-4-7898-4548-9, 2011.

②吉岡信和, 青木利晃, 田原康之: SPINによる設計モデル検証, 近代科学社, 226 ページ, 2008.