様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成 ２７ 年　 ６ 月　 ９ 日現在

機関番号：１３３０１
研究種目：基盤研究(C)
研究期間：2012～2014
課題番号：２４５０００３４

研究課題名（和文）動的ハイブリッドオートマトンによる動的再構成可能組込みシステムの高度な設計検証

研究課題名（英文）Advanced methods of design and verification for dynamically reconfigurable embedded systems

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）　　3,800,000円

研究成果の概要（和文）：動的再構成可能組込みシステムは，ソフトウェア(汎用CPU)とハードウェア(動的再構成可能プロセッサ(DRP))が協調して，低消費電力で多様な機能を実現する革新的なアーキテクチャであり，複雑な構成と動作を有している．
本研究では，①動的ハイブリッドオートマトンの開発，②その抽象化精錬検証の開発により，コタスクの生成消滅，周波数の動的変化，状態の階層並列性などを扱える設計検証を実現して，動的再構成可能組込みシステムの高度な設計検証技術を確立して，その有効性を実証する．

研究成果の概要（英文）：A system which can changes its configuration during operations is called Dynamically Reconfigurable System. In a Dynamically reconfigurable system, software (CPU) and hardware (DRP(Dynamically Reconfigurable Processor)) behaves cooeratively.
In this study, we develop dynamic hybrid automata, and CEGAR(CounterExample-Guided Abstraction Refinement) based model checking. Also we develop our model checker based on our proposed methods, and show them effective.

研究分野：形式的手法

キーワード：組込みシステム　ハイブリッドオートマトン　モデル検査　抽象化精錬　仕様記述　形式的検証　動的再構成可能システム　CEGAR

１．研究開始当初の背景

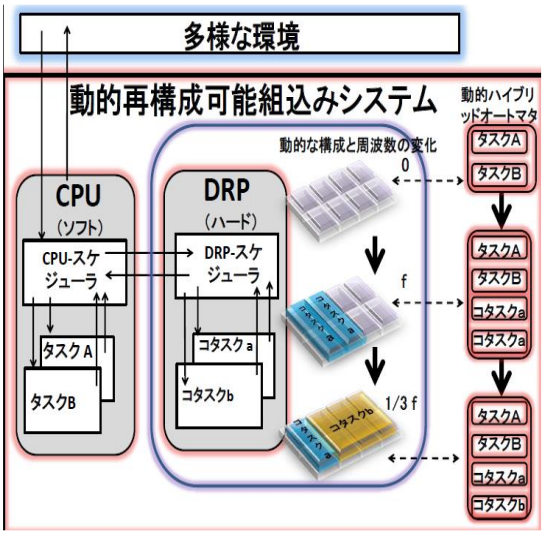
動的再構成可能組込みシステムは，稼働中に，汎用マイコンが動的再構成可能プロセッサの構成を変更して，低消費電力で多様な機能を容易に実現するシステムであるが，システムの構成変化や動作が複雑であり，動的構成の変化や周波数の変化などを設計検証技術で保証することが必須である．申請者は，世界に先駆けて，ハイブリッドオートマトンを用いて，動的再構成可能組込みシステムを対象として，ソフトウェア記述(汎用 CPU)とハードウェア(DRP)記述を協調させたシステム仕様記述と検証を行っている（南，山根，他　コンピュータソフトウェア 2011）．ここで，動的再構成可能組込みシステムにおいて，周波数の変化やプリエンプティブ性などの仕様記述と検証のため，ハイブリッドオートマトンが必須であることを実証した．しかし，動的再構成を直接的に仕様記述でき，CPU-DRP のデータ転送及び状態の階層並列性の仕様記述も可能な動的オートマトンの開発及びその効率的な検証手法の開発などの検討課題も多い．

本研究では，まず，動的ハイブリッドオートマトンを開発して，次に，動的ハイブリッドオートマトンを用いて，ソフトウェア(汎用 CPU)記述とハードウェア記述(DRP)の協調システムとして仕様記述を行い，次に，その動的な抽象化精錬のモデル検査を開発して，最後に，現実のシステムの仕様記述と検証を行って，提案手法の有効性を実証した．

２．研究の目的

上記の背景及び研究成果をもとに，図のようなソフトウェア(CPU)とハードウェア(DRP)との協調システムの観点から，動的再構成可能組込みシステムの高度な設計検証手法を構築する．

ここで，CPU は CPU スケジューラとタスクからなるリアルタイムシステムである．一方，動的再構成可能プロセッサは DRP スケジューラやコタスク(MPEG,JPEG 等の処理)などからなり，並列動作するコタスクの数が動的に変化して，そのコタスクの構成に依存して周波数が動的に変化する動的ハイブリッドオートマタの並列システムである．



研究期間内に，以下のことを明らかにする．

(1) コタスクの生成消滅やキュー，CPU-DRP 間データ転送，状態の階層並列性（ステートチャート）を表現できる動的ハイブリッドオートマトンの構文と意味を明らかにする．

(2)動的ハイブリッドオートマトタの並列システムにより，動的再構成，つまりソフトウェア(CPU)とハードウェア(DRP)との協調システムがシステム仕様記述できることを明らかにする．

(3) 並列動作やハイブリッド性，データなどによる検証時の状態爆発を抑制することが重要である．そこで，CEGAR(CounterExample Guided Abstraction Refinement)と on-the-fly の考えを融合して，システムの動的な構成の変化に応じて，ハイブリッド性やデータを抽象化して，その抽象モデルを精錬して検証する，動的ハイブリッドオー

トマタに対応した動的ハイブリッドCEGAR を開発して，実用レベルのシステム検証できることを明らかにする．

３．研究の方法

本研究では，動的再構成可能組込みシステムの高度な設計検証手法を構築するために，以下を行う．

(1) 仕様記述言語として，動的ハイブリッドオートマトンを開発して，事例のシステム仕様記述を行う．

(2) 検証手法として，CEGAR と on-the-fly を融合して，動的な構成の変化に対応して，ハイブリッド性やデータを抽象化精錬する動的ハイブリッドCEGAR 検証手法を開発し，実装する．

(3) ターゲットシステムを対象として実証実験と評価を行う．

なお，申請者は既存のハイブリッドオートマトンを用いて，動的再構成可能組込みシステムの設計検証を実現しており，研究成果（南，山根他，コンピュータソフトウェア 2011）を出しており，本研究では，これを拡張して高度な設計検証手法を構築する．

４．研究成果

上記の研究目的および方法の(1)，(2)，(3)に対応し，研究成果は以下の２つに大別される．

(1) 仕様記述言語の動的ハイブリッドオートマトンの開発：

コタスクの生成消滅やキュー，CPU-DRP 間データ転送，状態の階層並列性，周波数の動的変化を仕様記述するために，以下のように既存のハイブリッドオートマトンの構文を拡張して，動的ハイブリッドオートマトンの構文を定義する．

① CSP や CCS などのプロセス代数の生成消滅演算子により，コタスクの生成消滅を表現する
② P.Godefroid らの Queue-content Decision Diagram (QDD)により，キューを表現する
③ ステートチャートの階層並列性記述手法を導入する

また，動的ハイブリッドオートマトンの意味は操作的意味論に基づいて帰納的に定義する．

(2) CEGAR と on-the-fly の融合による検証：

並列動作とハイブリッド性による検証時の状態爆発を抑制するために，動的な構成変化毎に，ハイブリッド性とデータを抽象化精錬する動的ハイブリッド CEGAR (CounterExample Guided Abstraction Refinement)の手法を開発する．さらに，背景理論付き SMT ソルバを用いて，動的ハイブリッド CEGAR の実装を行った．SMT ソルバでは，実数の背景理論を用いて，一階述語論理の限定記号消去および反例解析における精錬述語の抽出を行った．

これにより，ハイブリッド性やリアルタイム性などを持つ安全性や活性などの複雑な性質を効率的に検証可能となった．

(3)実証実験と評価：

我々が以前行った動的再構成可能組込みシステムのシステム仕様記述例（南，山根，他　コンピュータソフトウェア 2011）をもとに，仕様記述したもので実証実験を行った．従来手法に比較して，大規模なシステムの検証を実現した．

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) 公下亮佑，山根智，櫻井孝平：“組込みアセンブリプログラムのモデル構築によるモデル検査”，査読有，pp.1-10，組込みシステムシンポジウム，情報処理学会，東京都渋谷区，2014.

(2) 小橋潤平，山根智，竹下淳：“組込みアセンブリプログラム解析によるＳＭＴモデル検査”，査読有，pp.1-6，組込みシステムシンポジウム，情報処理学会，東京都渋谷区，2014.

(3) S. Yamane T. Shimizu：”Development of Probabilistic Timed CEGAR”，The 2014 International Conference on Systems and Informatics (ICSAI 2014)，査読有，pp.1-10，IEEE，中国，2014.

(4) J.Kobashi,S.Yamane,A.Takeshita：”Development of SMT-Based Bounded Model Checker for Embedded Assembly Program”，IEEE 3rd Global Conference on Consumer Electronics，査読有，pp.1-3，IEEE,千葉県千葉市，2014.

(5) R.Konoshita,K.Sakurai,S.Yamane：”Model Generation by the Exhaustive Search for Embedded Assembly Programs and Application to Model Checking”，IEEE 3rd Global Conference on Consumer Electronics，査読有，pp.1-4，IEEE,千葉県千葉市，2014.

(6) 中川洋介，櫻井孝平，清水裕亮，山根智：“AspectJ を用いた Fault-Injection による Hadoop MapReduce の耐故障処理に関する性能評価”,情報処理学会論文誌コンピューティングシステム（ACS），査読

有,7(1),pp.35-45, 情報処理学会,2014.

(7) 山田 英史, 中居 祐輝, 山根 智:“動的再構成可能システムの仕様記述言語の提案およびその検証実験”, 情報処理学会論文誌 プログラミング (PRO), 査読有,6(3),pp.1-19, 情報処理学,2013.

(8) Ryo Yanase, T. Sakai, M. Sakai, S. Yamane:”Development of Model Checker of Dynamic Linear Hybrid Automata”,IEEE 37th COMPSAC ,査読有,pp.1-2, 京都府京都市, 2013.

(9) 清水裕亮,櫻井孝平,山根 智:“Hanoi: 複数レイヤーのトレースログを用いた Hadoop のパフォーマンス解析”, 第 25 回 コンピュータシステム・シンポジウム (ComSys 2013),査読有,pp.54-63,情報処理学会,東京都江東区, 2013.

(10)竹下淳, 小橋潤平, 山根 智:“組込みアセンブラの SMT 検証の理論と実験”, 組込みシステムシンポジウム 2012 (ESS2012),査読有, pp.197-202 ,情報処理学会, 東京都渋谷区, 2012.

(11)清水隆也, 森下篤, 山根 智:“確率時間 CEGAR の開発とその実証実験”, 情報処理学会論文誌 プログラミング (PRO), 査読有,5(2),pp.43-66,2012.

(12)畠中克也, 山根 智:“確率線形ハイブリッドオートマトンの到達可能性検証”, 情報処理学会論文誌, 査読有,53(12),pp.2671-2681, 情報処理学会, 2012.

(13)R.Yanase,S.Minami,S.Yamane: ”Hybrid Automata Theoretic Specification and Verification of CPU-DRP Embedded Systems”, Bulletin of Networking, Computing, Systems, and Software, 査読無, 1(1), pp.16-20,2012.

(14)Y.Shimizu,K.Sakurai,S.Yamane: ”Trace-mining Profile for Large-Scale Distributed Framework Hadoop”,The 18th IEEE Pacific Rim International Symposium on Dependable Computing (PRDC 2012) in the Fast Abstracts track,査読有,pp.1-2,IEEE, 新潟県新潟市, 2012.

(15)R.Yanase, T.Sakai, M.Sakai, S.Yamane :”A New Approach to Specify and Verify Embedded Systems consisting of CPU and DRP”, The 18th IEEE Pacific Rim International Symposium on Dependable Computing (PRDC 2012) in the Fast Abstracts track, 査読有,pp.1-2,IEEE, 新潟県新潟市,2012.

(16) 清水 裕亮,櫻井 孝平,山根 智:“トレースを用いた大規模分散基盤 Hadoop 向けのプロファイル手法の提案”,第 24 回 コンピュータシステム・シンポジウム (ComSys 2012),査読有,pp.70-78,情報処理学会,東京都文京区, 2012.

〔学会発表〕(計 6件)

(1)冨坂征平, 柳瀬龍, 櫻井孝平, 山根智:“線形ハイブリッドオートマタの CEGAR を適用した SMT ベースモデル検査”, IEICE Technical Report, 114(493), pp.47-52, 電子情報通信学会, 石川県金沢市, 2015.

(2)小橋潤平, 竹下淳, 山根智, 櫻井孝平:”割込み遷移削減手法を導入した組込みアセンブリコード向け SMT ベースモデル検査器の開発”, IEICE Technical Report, 114(493), pp.53-56, 電子情報通信学会, 石川県金沢市, 2015.

(3)加藤友紀, 公下亮佑, 櫻井孝平, 山根智:“組込みアセンブリプログラムからのモデル抽出による記号モデル検査”, IEICE Technical Report, 114(493), pp.65-70, 電子情報通信学会, 石川県金沢市, 2015.

(4)冨坂征平, 柳瀬龍, 小野祐貴, 山根智:“組込みシステムを対象とした線形ハイブリッドオートマトンのモデル検査器の開発と検証”,情報処理学会論文誌プログラミング (PRO) ,7(1),pp.33-33,情報処理学会, 福岡県小倉市, 2014.

(5)山根 智, 酒井 誠:“動的組込みシステムの仕様記述言語の開発”, 信学技報, 査読無, vol.113, no.279, MSS2013-37, pp.23-28, 電子情報通信学会, 岩手県花巻市, 2013.

(6)柳瀬龍, 酒井辰典, 酒井誠, 山根 智:”動的再構成可能組込みシステムのモデル化と仕様記述”,, 査読無, pp.1-4, 第 10 回 ディペンダブルシステムワークショップ (DSW 2012), 日本ソフトウェア科学会,兵庫県神戸市, 2012.

６．研究組織

(1)研究代表者

山根 智 (YAMANE SATOSHI)

金沢大学理工研究域電子情報学系・教授

研究者番号：70263506