様式 C-19

科学研究費補助金研究成果報告書

平成２２年　４月　１日現在

研究種目：基盤研究（Ｃ）

研究期間：2007～2009

課題番号：19500025

研究課題名（和文）　述語抽象化検証による大規模組込みシステム向きオブジェクト指向設計自動検証手法

研究課題名（英文）　Automatic verification method for large scale embedded object-oriented design based on predicate abstraction

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

研究成果の概要（和文）：リアルタイムオブジェクト指向言語を開発して、オブジェクトが生成消滅するシステムに対して、構造と時間の抽象化精錬で直接に検証できる、動的リアルタイムＣＥＧＡＲの開発と実装に取り組んだ。その結果、動的リアルタイムＣＥＧＡＲの実現により、オブジェクトの生成消滅といった構造の変化及びリアルタイム性を同時に抽象化精錬して、リアルタイムオブジェクト指向システムの効率的なモデル検査が実現できることを明らかにした。

研究成果の概要（英文）：We have developed real-time object-oriented language and Dynamically Real-Time CEGAR. Dynamically Real-Time CEGAR abstracts and refines both system configurations and real-time properties. It can directly and efficiently verify systems, in which components are generated and eliminated.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2007 年度	900,000	270,000	1,170,000
2008 年度	700,000	210,000	910,000
2009 年度	700,000	210,000	910,000
年度			
年度			
総　計	2,300,000	690,000	2,990,000

研究分野：情報学

科研費の分科・細目：情報学・ソフトウェア

キーワード：組込みシステム、述語抽象化検証、オブジェクト指向

１．研究開始当初の背景

リアルタイム組込みシステムのオブジェクト指向設計検証に関する研究は、最重要な研究分野であり、組込みシステムの生産性と信頼性を飛躍的に向上させる“銀の弾丸”として国際的に期待されている研究分野である。しかし、組込みシステムは、リアルタイムシステムであってタイミング制約が厳しく、多数のオブジェクトが生成消滅しながら並行動作して、しかもシステムが大規模であるために、仕様記述と自動検証が困難である。このために、オブジェクト指向分析設計手法UML（Unified Modeling Language）が標準化されているが、リアルタイム組込みシステムにおいては実用化されていない状況である。

日本では、リアクティブシステムのオブジェクト指向の定理証明やステートチャートのモデル検査の研究のみであり、リアルタイム組込みシステムに対応していない。一方、海外では、組込みシステムのオブジェクト指向設計検証に関する研究は非常に盛んであるが、状態爆発のために、実用レベルのシステムの検証を実現していない。

以上の研究動向の中で、本研究では、オブジェクト指向の観点から、リアルタイム組込みシステムの特徴を独自にとらえたリアルタイムオブジェクト指向言語を開発して、その効率的な検証方式ＣＥＧＡＲを開発する。具体的には、リアルタイムオブジェクト指向組込みシステムの特徴は、オブジェクトの生成消滅、オブジェクトの並列動作、タイミング制約及びオブジェクト内部の状態の複雑性であるとして、これらを記述するリアルタイムオブジェクト指向言語を開発して、これらを抽象化精錬して自動検証を実現する。

２．研究の目的

本研究では、実用レベルのリアルタイム組込みシステムをオブジェクト指向で設計検証することを目的として、以下を研究する。本研究では、リアルタイムオブジェクト指向組込みシステムの特徴は、オブジェクトの生成消滅、オブジェクトの並列動作、タイミング制約及びオブジェクト内部の状態の複雑性であるとして、これらを記述するリアルタイムオブジェクト指向言語を開発して、これらを抽象化精錬して自動検証を実現する。

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を対象として、図１に示すように、段階を踏んで研究を進める。まず、リアルタイムオブジェクト指向言語を開発して、次に、リアルタイムオブジェクトの動的な性質（オブジェクトの生成消滅）を静的な記述にエンコードして既存の検証器で検証して、次に、オブジェクトの構造と時間を抽象化精錬する検証手法を開発して、最後に、動的な構造とリアルタイム性を抽象化精錬する、動的リアルタイムＣＥＧＡＲを開発する。

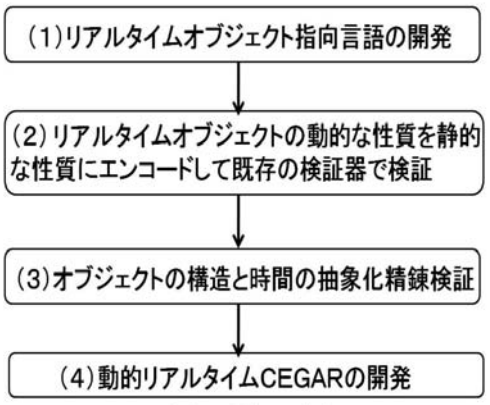

図1　研究の方法

４．研究成果

本研究では、以下の研究成果をあげた。

（１）まず、オブジェクトの生成消滅、リアルタイム性及び動作の構造などを仕様記述できる、リアルタイムオブジェクト指向言語を開発した。

（２）次に、動的再構成可能組込みシステムを対象として、リアルタイムオブジェクトの動的な性質を静的な仕様記述にエンコードすることによって、既存の検証器 HYTECH により検証を実現して、性能などの評価を行った。

（３）次に、リアルタイムオブジェクトの構造と時間の抽象化精錬を行う自動検証方式を開発して、実装とその評価を行った。

（４）最後に、図２に示すように、リアルタイムオブジェクトの生成消滅といった構造とリアルタイム性の抽象化精錬を行う検証方式である、動的リアルタイムＣＥＧＡＲを開発して、実装して評価を行った。

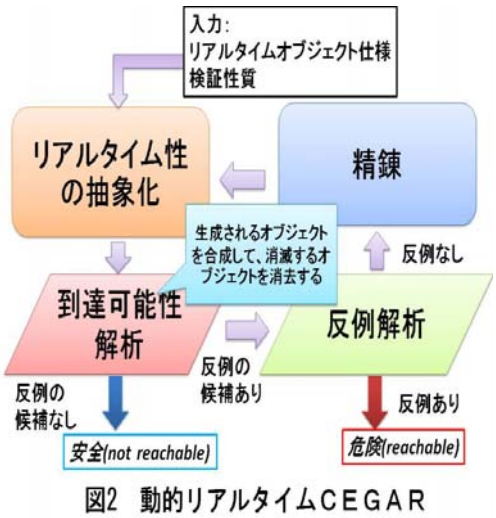

図2　動的リアルタイムＣＥＧＡＲ

以上により、リアルタイム組込みシステムのオブジェクト指向設計の仕様記述言語を開発して、その効率的な検証方式動的リアルタイムＣＥＧＡＲを開発して、その有効性を実証した。

今後、動的ハイブリッドＣＥＧＡＲ及びその分散並列検証器を実現する予定である。

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 11 件）

(1)S.Yamane:"Development Method for Real-Time Software based on Timed Weak Simulation Verification", Embedded Systems: Status and Perspective, pp.1-15, American Scientific publishers, 2010. (in press), 査読有

(2)山根 智:"組込みシステムにおけるハイブリッドオートマトンの形式的手法", 計測と制御, Vol.48 No.11, pp.810-815,2009 , 査読無

(3)山崎真一, 山根 智:"階層構造の抽象化精錬によるステートチャートの自動検証", コンピュータソフトウェア, Vol.26,No.3,pp.155-170, 日本ソフトウェア科学会, 2009 ,査読有

(4)橋爪裕樹, 山根 智:"確率ゾーングラフを用いた確率時間強模倣関係による検証, 電子情報通信学会論文誌, J92-D-I, No.1, pp.25-38,2009 , 査読有

(5)S.Yamane: Special Section on Concurrent/Real-time and Hybrid Systems：Theory and Applications, E91-A, No.11, pp.3206-3206, IEICE TRANSACTIONS on Fundamentals ,2008 , 査読無

(6)山根 智, 小寺広志, 荒井恒夫:" 確率時間オートマトンの確率時間強模倣検証器の開発 ",コンピュータソフトウェア, Vol.25, No.3, pp.148-193, 日本ソフトウェア科学会, 2008, 査読有

(7)山根 智:"リアルタイムシステムの形式的検証",コンピュータソフトウェア, Vol.25 ,No.3, pp.81-87, 日本ソフトウェア科学会,2008 , 査読有

(8)山根 智: "組込みシステムのフォーマルメソッドにおけるハイブリッドシステムの仕様記述と形式的検証",Fundamentals Review, Vol.2, No.1, pp.22-34, 電子情報通信学会, 2008, 査読無

(9)坂倉賢昭, 山根 智;"UML と時間オートマトンを用いたソフトリアルタイムシステムの設計解析手法",情報処理学会論文誌, Vol.48, No9, pp.2410-2421, 2007 , 査読有

(10)S. Yamane:"The automatic verification system for real-time systems using symbolic model-checking", Real-Time Systems: Modeling, Design, and Applications, volume 8 of AMAST Series in Computing , pp.137-152, World Scientific Publishing, 2007, 査読有

(11)S. Yamane:" Theory and practice of probabilistic timed game for Embedded Systems", Embedded Software and Systems , Lecture Notes in Computer Science 4523, pp.109-120,2007 , 査読有

〔学会発表〕（計 13 件）

(1)南翔太、瀧内新悟、瀬古口智、中居佑輝、山根 智: 動的再構成可能プロセッサのモデル化, 仕様記述とモデル検査, 6 回ディペンダブルシステムシンポジウム（DSS2009）, 日本ソフトウェア科学会,pp.102-121,2009 年 12 月 15 日, 大阪大学(大阪府).

(2)山崎真一、酒井誠、山根 智: 階層時間オートマトン群の並列動作の述語抽象化精錬検証手法, 6 回ディペンダブルシステムシンポジウム (DSS2009), 日本ソフトウェア科学会,pp.179-197,2009 年 12 月 15 日, 大阪大学(大阪府).

(3)越田彰太、山根 智: 確率ゲーム理論による組込みシステムのモデル化とモデル検査, 電子情報通信学会信学技報, vol. 109, no. 301, CST2009-24, pp. 35-40, 2009 年 11 月 26 日, 名古屋大学(愛知県).

(4)高橋正樹、森下 篤、山根 智: 確率時間 REGAR による PTCTL のサブクラスのモデル検査, 電子情報通信学会信学技報, vol. 109, no. 301, CST2009-25, pp. 41-46, 2009 年 11 月 26 日, 名古屋大学(愛知県).

(5)森下篤,駒形龍太,山根 智: **招待講演**"確率時間 CEGAR",電子情報通信学会研究報告 CST2009-5,pp.25-30, 査読無,2009 年 11 月 26 日, 名古屋大学(愛知県). **(2008 年度 CST 研究会優秀論文賞)**

(6)山根 智:**招待講演**"組込みシステムの形式的手法", 第 22 回 回路とシステム軽井

沢ワークショップ，査読無，pp.1-6,2009 年 4 月 20 日，軽井沢プリンスホテル(長野県).

(7)林　将志、山根 智: 確率時間ゲーム理論による組込みシステムのモデル化，仕様記述及び検証，数理解析研究所講究録 RIMS Kokyuroku 1649 pp.39-46 2009 年 2 月 1 日,京都大学数理解析研究所(京都府).

(8) 中居佑輝，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、2008-EMB-10,pp.75-82,2008 年 11 月 28 日、キャンパスプラザ京都(京都府).

(9) 安井雅俊，山崎真一，山根　智：並列動作する確率時間システムに対する拡張 CEGAR、2008-EMB-10,pp.83-90,2008 年 11 月 28 日、キャンパスプラザ京都(京都府).

(10)山根　智、瀧内新悟：“制限付きストップウォッチオートマトンと時間オートマトンを用いた，プリエンプティブスケジューリングシステムの UML 分析設計からタスク設計までの設計検証方法論”、電子情報通信学会ソサエティ大会シンポジュム,AS-4-3,pp.1-2,2007 年 9 月 13 日、鳥取大学(鳥取県).

(11)山根　智、瀧内新吾：“組み込システムの UML 分析設計からタスク設計までの設計検証方法論”、情報処理学会研究報告 SE2007，pp.87-94，2007 年 9 月 28 日、キャンパスプラザ京都(京都府).

(12)瀧内新吾、山根　智：“ストップウォッチオートマトンによるプリエンプティブスケジューリングシステムの検証”、システム・情報部門学術講演会、pp.427-432,計測制御学会、2007 年 11 月 27 日、国立オリンピック記念青少年総合センター(東京都).

(13)山根 智:**チュートリアル**“リアルタイムシステムの仕様記述と検証”，組込みシンポジュウム ESS2007，査読無，チュートリアル資料,2007 年 10 月 18 日，日本科学未来館(東京都).

〔図書〕（計１件）

(1)山根 智:**著書**″ハイブリッドオートマトン″,電子情報通信学会ハンドブック／知識ベース,査読無，pp.1-6，オーム社，2010.（電子版公開）

６．研究組織

(1)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