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　　３　日現在

機関番号：　１２６０８
研究種目：　基盤研究(C)
研究期間：　2012～2014
課題番号：　２４５０００３２

研究課題名（和文）形式手法による欠陥のある現実規模の組み込みシステム仕様からの修正情報抽出

研究課題名（英文）Extracting information for correction of flaws from embedded system specification of practical scale by formal method

研究代表者

萩原　茂樹（Hagihara, Shigeki）

東京工業大学・情報理工学（系）研究科・助教

研究者番号：７０３３４５４７

交付決定額（研究期間全体）：（直接経費）　　3,600,000円

研究成果の概要（和文）：組み込みシステムの仕様を記述する際、一度に誤りなく記述するのは困難であるため、誤りのある仕様から修正に有益な情報を得たい。本研究では、誤りのある仕様から、その原因と箇所を表す情報を計算する方法を形式手法により構成した。その計算手法では、仕様を満たす振る舞いを表すωオートマトンにおいてグラフ操作を行なうことで欠陥原因と箇所の情報の計算する。ωオートマトンを簡便に簡約する新しい技術を構成し、解析を効率化しただけでなく、計算する修正情報の形に工夫を加え、現実規模の仕様に適用可能とした。本手法の正当性を証明し、計算量を特定した。さらに、本手法をツールとして実装した。

研究成果の概要（英文）：For developing safety-critical embedded systems, verifying specification is expected to reduce the development costs of embedded systems. If a specification has flaws, we must correct the specification. It is desirable to obtain the cause and the location of flaws in the specifications. In this research, we proposed methods for obtaining the cause and the location and of flaws. In our methods, we manipulate omega-automata representing the specification to compute such information. We developed new reduction techniques for automata, and make such information computable for specifications of embedded systems at non-trivial scales. We proved correctness of our methods and clarified the time complexity of our methods. We also implemented our methods and got the tools.

研究分野：　形式手法

キーワード：　形式手法　組み込みシステム仕様　修正情報抽出　時間論理　オートマトン　極小充足不能集合

１．研究開始当初の背景

組み込みシステムは、センサー等を通じた環境からの要求に対して、適切なタイミングで応答を返すオープンなシステムである。これらの中には、原子力発電所の制御システム、航空管制システム、あるいは自動車の制動システムなど安全性が強く求められるシステムが少なくない。組み込みシステムを設計する際、どのようにシステムが動作すべきかを分析し、システム仕様を記述する。その際、条件分岐が不十分である等、仕様自体に欠陥があると、その仕様に沿って作成されたシステムにも欠陥を伴ってしまう。厳密に欠陥がないことを保証した仕様を得ることは非常に重要である。

組み込みシステムは、オープンシステムであるため、その仕様に求められることは、単に矛盾がないことだけではない。「環境がどのような要求をどのような順序で生起しても、仕様を満たすように応答できる実現プログラムが存在する」という性質（実現可能性）が不可欠である。もし仕様が実現可能でなければ、仕様を修正する必要がある。ところが、現実規模の組み込みシステム仕様では、どこをどのように修正すべきかが全く明らかでないため、仕様の欠陥の原因や箇所を表す情報を抽出できれば、その欠陥仕様を修正する大きな助けとなる。

２．研究の目的

本研究では、形式手法を用いて、時間論理で記述された組み込みシステム仕様から、修正に有益な情報として、以下の情報(A),(B)の抽出手法を構成することを目的とする。

(A)誤り原因を表す情報： 環境の振る舞いは制御できないにもかかわらず、実現不能の仕様は環境の振る舞いに対して暗黙の前提条件をつけてしまう。その前提条件は仕様の欠陥原因を暗示するため、この前提条件を直感的に理解しやすい表現で抽出する。

(B)誤り箇所を表す情報： 時間論理で制約的に記述された仕様が実現不能ならば、ある部分仕様で実現不能である。仕様を実現可能にするためには、その部分の制約を緩めるように修正する必要がある。この実現不能となる極小範囲を特定する手法の研究を行う。

３．研究の方法

(1) 現実規模の組み込みシステム仕様から誤り原因を表す情報((A)の情報)を抽出する手法を構成する研究については、これまで我々が構成・プロトタイプ実装していた情報抽出手法を、抽出情報の単純化により、現実規模の仕様を適用可能になるように、変更・拡張する。情報を単純化する際、情報が有意な範囲で抽出する情報を単純化するよう留意する。

(2) 誤り箇所を表す情報((B)の情報)を抽出する手法については、実現不能な仕様に対する無限長語オートマトンから得られる証拠から、その証拠が生成された仕様の範囲を特定することで、誤り箇所を抽出するという方針で構成する。

(3) これら２種類の欠陥情報を抽出する手法において共通に、無限長語オートマトン（ここでは、Büchi オートマトン）を取り扱う。このオートマトンのサイズが巨大なものとなるため、その取扱いがボトルネックとなる。このため、無限長語オートマトンのサイズ縮小手法を構成し、欠陥情報抽出手法ではこれを用いる。

(4) 欠陥情報抽出手法の構成は、形式手法により行い、得られた抽出手続きに対して、正当性の証明をそれぞれ与え、その計算量も特定する。さらに、得られた手続きを計算機上に実装し、有用性を確認する。

４．研究成果

(1) 仕様の欠陥情報抽出手法の構成・実装

① 誤り原因を表す情報の抽出手法

組み込み仕様が欠陥を持つ場合に、その原因情報である環境制約を、直感的でシンプルな式の形で導出する方法を与え、その手続きの正当性と有用性を示した。手続きの計算量も明らかにした。さらに、その手続を実装し、現実規模に近い仕様についても欠陥情報を正確に抽出できることを示した。

② 誤り箇所を表す情報の抽出手法

組み込み仕様が欠陥を持つ場合に、その欠陥の範囲を特定する手法を構成し、その手続きの健全性、完全性を証明し、手続きの計算量を特定した。さらに、本手法を実装した後、現実的な仕様に適用し、現実時間で欠陥箇所が特定できることを示した。

これらの研究は、仕様を検証・修正しながら、誤りのない仕様を作成していくという仕様記述の理想的なプロセスを現実的にする大きな成果である。

(2) 時間論理式からオートマトンへの高速な変換器の実装

時間論理で記述されたシステム仕様の欠陥情報抽出には、時間論理式から等価な Büchi オートマトンへの変換が用いられる。この変換を高速に行なうことが、現実規模の仕様を取り扱うために必要不可欠である。本研究では、時間論理式から Büchi オートマトンへの高速な変換法を構成・実装した。オートマトンの遷移関係に二分決定グラフを用いて、演算速度の高速化及び使用メモリを効率化し、さらに、等価な状態を一つの状態としてまとめる工夫と、不必要な状態を作成しない工夫をそれぞれ行った。これらにより、世界最速の変換器と競合できるくらい高速化に成功した。この変換器は、ソフトウェアの検証や合成に、幅広く利用されるため、本成果のインパクトは非常に大きい。

(3) 組み込みシステム仕様記述言語 T の提案とコンパイラの構成
時間論理は構造を持たないため、パラメータや構造を持つ組み込みシステムの仕様を時間論理をそのまま用いて記述するのは困難であった。本研究では、パラメータ付きのシステム仕様を記述するためのオブジェクト指向言語の提案とそのコンパイラの構成を行った。言語仕様とコンパイラの実装方法を論文にまとめた。

(4) 時間論理で記述された組み込みシステム仕様の検証にかかる計算量の特定
実現可能性の必要条件であり、近似ともみなせる性質、強充足可能性について、性質判定にかかる計算量を特定し、それら EXPSPACE 完全であることを明らかにした。これにより、実現可能性（計算量は 2EXPTIME 完全）よりも少ない計算で強充足可能性が判定できることになり、現実規模の仕様の検証に道筋をつけた。

(5) 組み込みシステム仕様の実現可能性判定器の実装
組み込みシステム仕様が実現可能性を満たすかどうか判定する判定器を実装した。実装した判定器の大きな特徴は、Büchi オートマトンやゲームの遷移表現に BDD を用いることである。これにより、オートマトンの決定化やゲームへの変換が効率的に行えるようになり、他の世界最速のツールにも引けをとらない性能を出している。

(6) 環境許容性のある組み込みシステム合成法
環境の振る舞いが予め仮定されている前提でシステムを合成する場合、環境の振る舞い仮定を仕様に含めた仕様からシステムを合成する。ところが、センサーの故障など環境が仮定通りに振る舞わない場合でも、仕様をできるだけ満たすシステムが得られることが望ましい。本研究では、そのような組み込みシステムを合成する手法の研究を行った。この手法では、仕様から変換されたゲームの勝利戦略の中で可能な限り仕様を満たす戦略を選択する。この手法をプロトタイプ実装し、いくつかの仕様で環境許容性のある組み込みシステムを合成できることを確認した。これにより、より実際的に利用可能なシステム合成が可能となった。

(7) システム合成に適した時間論理式で記述された仕様の分割法
時間論理で記述された組み込みシステム仕様からシステムを自動的に合成可能であるが、その問題の計算量は２重指数時間完全であるため、仕様を分割して効率的に検証する方法がこれまで研究されてきた。ところが、仕様をどう分割すれば効率的に合成できるかは自明ではなかった。本研究では、この分割方法について研究を行った。本研究では、作成される中間生成物である決定性ωオートマトンの大きさを同じくらいにする分割が適していることを明らかにし、そのような分割が得られるアルゴリズムを構成した。この手法をいくつかの仕様に適用し、有効性を確認した。

(8) 時間論理で記述された仕様からの組込みシステム自動生成
これまで述べた、時間論理で制約的に記述された組み込み仕様からの欠陥情報抽出手法や、組み込みシステム自動合成手法を用いて、誤りのない組み込みシステムを構成する手法を提案した。提案手法は次の 4 つのステップからなる。(1)形式仕様を記述する。(2)形式仕様をハードウェアにあわせて詳細化する。(3)詳細化された形式仕様から、仕様の実現可能性判定器を用いて。プログラムを表す状態遷移系に変換する。(4)形式仕様で用いた命題とプログラムで用いる命令や条件式との対応を与え、状態遷移系をプログラムに変換する。組み込みシステムとして、センサーと独立駆動可能なタイヤを 2 つ持つロボットを対象として、それをライントレーサとして動作させるプログラムを提案手法で生成し、本方法の有効性を示した。

(9) 平均利得式が記述可能な時間論理の充足可能性判定器の実装
システム仕様には、定性的な性質に加え、頻度など定量的な性質も記述される。定量的な性質が記述可能な時間論理 LTLMP を定義し、充足可能性判定手続きを構成した。この充足可能性判定では、平均利得制約を線形不等式の充足問題に帰着する。さらに、充足可能性判定手続きを実装し効率化を行った。本実装では、線形不等式の充足問題を SMT ソルバに解かせている。変換される線形不等式の大きさを小さくするいくつかのヒューリスティックを導入し、効率化を行った。これにより、定量的性質を含む仕様の無矛盾性を効率的に証明できるようになった。

５．主な発表論文等

〔雑誌論文〕（計 7 件）

① 冨田尭，萩原茂樹，伊藤宗平，米崎直樹．確率頻度時間論理の統計的モデル検査，コンピューターソフトウェア，査読有，岩波書店，Vol. 31，No. 3，pp. 336-356，Aug. 2014. DOI:10.11309/jssst.31.3_336

② Masaya Shimakawa, Shigeki Hagihara, Naoki Yonezaki. Bounded Strong Satisfiability Checking of Reactive System Specifications, IEICE Transactions on Information and Systems, 査読有, A Publication of the Information and Systems Society, Vol. E97-D, No. 7, pp. 1746-1755, Jul. 2014.

DOI:10.1587/transinf.E97.D.1746

③ 冨田尭，萩原茂樹，米崎直樹．平均利得時間論理とそれを用いた検証・最適化手法，コンピューターソフトウェア，査読有，岩波書店，Vol. 31，No. 2，pp. 93-117，Apr. 2014. DOI:10.11309/jssst.31.2_93

④ 安藤崇央，萩原茂樹，米崎直樹．SAT solver を用いる LTL タブロー構成法とその評価，情報処理学会論文誌，査読有，Vol. 55，No. 2，pp. 909-921，Feb. 2014.

⑤ Masaya Shimakawa, Shigeki Hagihara, Naoki Yonezaki. Complexity of Strong Satisfiability Problems for Reactive System Specifications, IEICE Transactions on Information and Systems, A Publication of the Information and Systems Society, 査読有, Vol. E96-D, No. 10, pp. 2187-2193, Oct. 2013. DOI:10.1587/transinf.E96.D.2187

⑥ Sohei Ito, Takuma Ichinose, Masaya Shimakawa, Naoko Izumi, Shigeki Hagihara, Naoki Yonezaki. Modular analysis of gene networks by linear temporal logic, Journal of Integrative Bioinformatics, 査読有, Vol. 10, No. 2, 216, 2013. DOI:10.2390/biecoll-jib-2013-216

⑦ Shigeki Hagihara, Hiroaki Oguro, Naoki Yonezaki. Kripke semantics for Epistemic Logic of Relational Information between Ciphertexts, Philippine Computing Journal, 査読有, Vol. 7, No. 2, pp. 23-32, Dec. 2012.

〔学会発表〕（計 16 件）

① 上野篤史，冨田尭，島川昌也，萩原茂樹，米崎直樹．環境許容性のあるリアクティブシステム合成法，電子情報通信学会ソフトウェアサイエンス研究会，信学技報，Vol. 114，No. 510，pp. 7-12，Mar. 2015，沖縄県青年会館（沖縄県那覇市）．

② Yoshiharu Fushihara, Shigeki Hagihara, Masahiko Tomoishi, Naoki Yonezaki. A new approach to analysis of access tendency of web server using Poisson distribution, 15h Philippine Computing Science Congress (PCSC 2015), Proceedings of the 15th Philippine Computing Science Congress, pp. 14-19, Mar. 2015, Tuguegarao (Philippines).

③ Shohei Mochizuki, Masaya Shimakawa, Shigeki Hagihara, Naoki Yonezaki. Fast Translation from LTL to Büchi Automata via Non-transition-based Automata, Formal Methods and Software Engineering, 16th International Conference on Formal Engineering Methods, ICFEM 2014, Lecture Notes in Computer Science, Springer, Vol. 8829, pp. 364-379, Nov. 2014, Luxembourg.

④ Kenji Osari, Shigeki Hagihara, Naoki Yonezaki. Discussion on modularization of specifications for efficient synthesis of reactive systems, 7th Symposium on Mathematical Aspects of Computer Science, SMACS2014, pp. 27-32, Nov.2014, Naga (Philippines).

⑤ Takashi Tomita, Takahito Kimura, Shigeki Hagihara, Naoki Yonezaki. An Efficient Implementation of Satisfiability Checking for LTL with Mean-Payoff Constraints, Workshop on Computation: Theory and Practice (WCTP 2014), pp. 30-42, Oct. 2014, Manila (Philippines).

⑥ Shigeki Hagihara, Naoki Egawa, Masaya Shimakawa, Naoki Yonezaki. Minimal strongly unsatisfiable subsets of reactive system specifications, Proceedings of the 29th ACM/IEEE international conference on Automated software engineering (ASE2014), ACM New York, pp. 629-634, Sep. 2014, Västerås (Sweden).

⑦ 萩原茂樹，江川直毅，島川昌也，米崎直樹．リアクティブシステム仕様の極小強充足不能部分計算に関する考察，情報処理学会第 99 回プログラミング研究発表会，Jun. 2014，旭川市民文化会館（北海道旭川市）．

⑧ Shigeki Hagihara, Masahiko Tomoishi, Naoki Yonezaki. On Constructing Unification-based Proof Methods for Modal Logics with First-order Undefinable Frames, 14th Philippine Computing Science Congress (PCSC 2014), pp. 22-27, Mar. 2014, Davao (Philippines).

⑨ 萩原茂樹，江川直毅，島川昌也，米崎直樹．強充足不能なリアクティブシステム仕様における欠陥範囲の特定，ソフトウェア工学の基礎 XX，日本ソフトウェア科学会 FOSE 2013，近代科学社，pp. 143-152，Nov. 2013，ゆのくに天祥（石川県加賀市）．

⑩ Kenji Osari, Takuya Murooka, Kiyotaka Hagiwara, Takahiro Ando, Masaya Shimakawa, Sohei Ito, Shigeki Hagihara, Naoki Yonezaki. An object-oriented language for parameterised reactive system specification based on linear temporal logic, Workshop on Computation: Theory and Practice (WCTP 2013), pp. 94-113, Sep. 2013, Manila (Philippines).

⑪ 上野篤史，望月翔平，島川昌也，萩原茂樹，米崎直樹．LTL 式で記述されたリアクティブシステム仕様の高速な実現可能性判定器の実装に関する研究，日本ソフトウェア科学会第 30 回大会講演論文集，Sep.

2013，東京大学本郷キャンパス（東京都文京区）

⑫ Masaya Shimakawa, Shigeki Hagihara, Naoki Yonezaki. SAT-Based Bounded Strong Satisfiability Checking of Reactive System Specifications, Information & Communication Technology - EurAsia Conference 2013 (ICT-EurAsia 2013), Information and Communicatiaon Technology, Lecture Notes in Computer Science, Vol. 7804, pp. 60-70, Mar. 2013, Yogyakarta (Indonesia).

⑬ 望月翔平，島川昌也，萩原茂樹，米崎直樹. LTL 式から Büchi オートマトンへの高速な変換法，第 19 回 ソフトウェア工学の基礎ワークショップ FOSE 2012，ソフトウェア工学の基礎 XIX，日本ソフトウェア科学会 FOSE 2012，近代科学社，pp. 91-100，Dec. 2012，ゆふいん山水館（大分県由布市）.

⑭ Takashi Tomita, Shin Hiura, Shigeki Hagihara, Naoki Yonezaki. A Temporal Logic with Mean-Payoff Constraints, 14th International Conference on Formal Engineering Methods, ICFEM 2012, Lecture Notes in Computer Science, Springer, Vol. 7635, pp. 249-265, Nov. 2012, Kyoto (Japan).

⑮ Masaya Shimakawa, Shigeki Hagihara, Naoki Yonezaki. Complexity of Checking Strong Satisfiability of Reactive System Specifications, International Conference on Advances in Information Technology and Communication, AIT 2012, pp. 42-51, Sep. 2012, Dubai (UAE).

⑯ Shigeki Hagihara, Takahiro Arai, Masaya Shimakawa, Naoki Yonezaki. Developing Embedded Systems from Formal Specifications Written in Temporal Logic, Proceedings of the Third International Conference on Trends in Information, Telecommunication and Computing, Lecture Notes in Electrical Engineering, Springer, Vol. 150, pp. 107-113, Aug. 2012, Bangalore (India).

〔図書〕（計 1 件）

① 萩原茂樹. 論理的検証法，応用数理ハンドブック，朝倉書店，pp. 238-239，Oct. 2013.

６．研究組織

(1)研究代表者

萩原　茂樹（HAGIHARA, Shigeki）

東京工業大学・大学院情報理工学研究科・助教

研究者番号：７０３３４５４７

(2)研究協力者

島川　昌也（SHIMAKAWA, Masaya）

東京工業大学・大学院情報理工学研究科・研究員

研究者番号：００７４９１６１