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

令和　４ 年　 ６ 月 ２１ 日現在

機関番号：２０１０６
研究種目：基盤研究(C)（一般）
研究期間：2016～2021
課題番号：１６Ｋ００００９２

研究課題名（和文）形式手法による定量的制約を満たす組み込みシステムの自動合成

研究課題名（英文）Synthesis of embedded systems satisfying quantitative constraints by formal methods

研究代表者
萩原　茂樹（Hagihara, Shigeki）

公立千歳科学技術大学・理工学部・准教授

研究者番号：７０３３４５４７

交付決定額（研究期間全体）：（直接経費）　　3,400,000円

研究成果の概要（和文）：組み込みシステムは、機能要件などの定性的制約だけでなく、性能要件などの定量的制約を満たすことが強く望まれ、これら制約を必ず満たすシステムを構成する手法が必要不可欠である。厳密な保証が可能な形式手法により、これらの制約を満たす現実的なシステムを合成するための基礎技術を構成した。具体的には、性能要件をできるだけ満たすシステムの合成手法や、現実規模のシステム構成のためのモジュール分割方法などを構成した。

研究成果の学術的意義や社会的意義
現実的な仕様からシステムを系統的に構成する手法の研究は、ソフトウェア工学の分野で盛んに行われてきたが、それらはデータオリエンテッドな対応であり、それらから得られるのは「経験則」であると指摘されてきた。「法則」を得る方法として形式手法が注目されている。これまで形式手法は、解析に要する計算量の膨大さにより、現実規模の仕様に適用するのが困難であった。本研究は現実規模の仕様に対して、形式手法で解析が可能な範囲、即ち「法則」が適用可能な範囲を明確にするという学術的な特色がある。

研究成果の概要（英文）：Embedded systems are desired to satisfy not only qualitative constraints, but also quantitative constraints. Methods are required to develop systems which necessarily satisfy these constraints. We construct several fundamental techniques for synthesis of embedded systems of practical size, which satisfy these constraints by formal methods.

研究分野：ソフトウェア

キーワード：形式手法　組み込みシステム　自動合成　時間論理　検証

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

組み込みシステムは、社会インフラとして至るところで使用されており、厳密な安全性が求められる。組み込みシステムは、機能要件などの定性的制約だけでなく、性能要件などの定量的制約を満たすことが強く望まれ、これら制約を必ず満たすシステムを構成する手法が必要不可欠である。厳密な保証が可能な形式手法により、定性的制約のみを満たすシステムを合成する研究は、これまで国内外の幾つかのグループでなされてきたが、定量的制約も同時に満たすシステムの合成手法、特に現実規模のシステム合成手法の研究は不十分であった。

定性的制約を線形時間論理で記述し、それを満たすプログラムを表す状態遷移系を効率的に自動計算する手法(Safraless 手法)が、2005 年に Hebrew 大学の O.Kupferman らによって提案され、本合成分野がブレイクスルーした。その後、Safraless 手法を元に、幾つかの合成ツールが提案されているが、定性的制約に加え、定量的制約も同時に満たす、現実規模のシステム合成手法は、十分には研究されていなかった。

２．研究の目的

本研究では、形式手法を用いて、定性的制約だけでなく、頻度制約や実時間制約などの定量的制約を満たす現実規模の組み込みシステムを自動合成する手法を構成することを目的とする。

３．研究の方法

これまで、研究代表者の研究グループにより構成・実装された定性的制約のみを満たすシステム合成手法に効率化を行い（オートマトンのサイズ縮小、仕様の構文制限、モジュールを適切に分割する方法など）、定量的制約を満たすシステムを合成する機能を追加し、現実規模のシステムを合成可能とすることを目標とする。ここで、形式手法に基づいたアプローチを取る。即ち、構成した技術に対し、数学的な裏付けを与えるアプローチを取る。

４．研究成果

(1) 環境許容性を持つ組み込みシステムの自動構成

組み込みシステム構成において、システムとインタラクションする環境の振る舞いについて前提を置き、仕様に環境の前提を含めることがある。その場合、環境が前提どおりの振る舞いをしている限りは、合成されたシステムは仕様を満たす振る舞いをする。ところが、一旦環境が前提を満たさない振る舞いをした際、それ以降、合成されたシステムは仕様を満たす振る舞いをしない。一般に、現実的な場合を考慮すると、予期せず環境の振る舞いが前提を満たさないことがありうる。このような場合においても、システムはできるだけ仕様を満たすように振る舞うことが望ましい。この性質を環境許容性と呼ぶ。本研究では、環境許容性の簡潔な定義を与え、この定義にしたがい、環境許容性を持つ組み込みシステムを合成する手法を提案した。この手法では、Safraless 合成手法で得られたセーフティゲームの勝利領域を計算し、仕様を満たすときに利得を与えるような平均利得ゲームに変換する。そして、そのゲームの最適戦略を計算することで、環境許容性を持つシステムを合成できる。この手法を実装し、簡単な押しボタン付きドアの仕様を適用したところ、以下の図のように、ボタンが押され方に異常な状況があっても、それを許容して動作できるような、環境許容性を持つ組み込みシステムを合成できることを確認した。

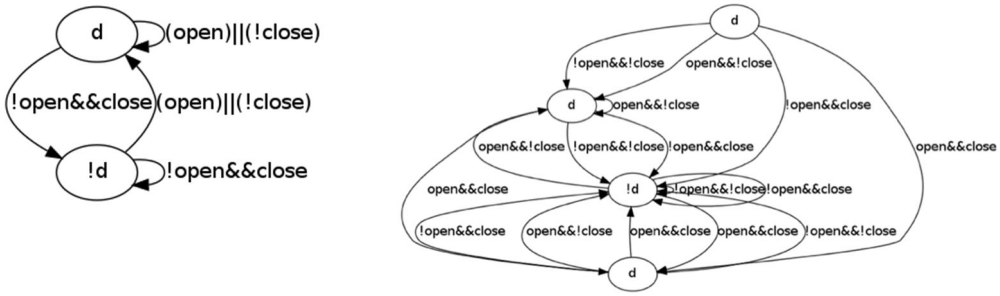

図 合成された組み込みシステム（左：環境許容性を考慮しない場合、右：環境許容性を考慮する場合）

(2) 性能要件をできるだけ満たす組み込みシステムの自動合成
線形時間論理で記述した振る舞い仕様が実現可能である場合、その仕様を満たす組み込みシステムを自動的に合成することが可能である。仕様全体が実現不可能な場合でも、ベストエフォートな組み込みシステムが合成できることが望ましい。すなわち、できるだけ多くの仕様を満たすようなシステムを合成できることが望ましい。本研究では、絶対に満たすべき仕様と、満たすことが望ましい仕様に分け、満たすべき仕様を必ず満たし、満たすことが望ましい仕様をできるだけ多く満たすような組み込みシステムを自動合成する手法を提案した。この手法では、仕様の形を Gϕ（いつも ϕ が成り立つ）とし、ϕ が成り立つ時点の数を最大化するようなシステムを合成するアプローチを取った。成り立つ時点の数を量的に評価するために、平均利得の目的関数を用いた。本手法では、LTL で記述された、満たすことが望ましい仕様から、Safraless アプローチを用いて、その仕様を満たすセーフティゲームを構成する。そのセーフティゲームを平均利得ゲームに変換し、それらのゲームを合成した上、最適戦略を得ることで、組み込みシステムを合成する。

(3) 構成的なシステムに性能要件などの要件を満たさせる方法の研究
システムの仕様を記述する方法には、宣言的に、即ち、制約的に記述する方法と、構成的に記述する方法がある。この２つの方法は、どちらか一方が優れているわけではない。時間軸全体として満たすべき制約として仕様が書かれる場合は、宣言的に記述する方法が適しており、逆に、システムが各時点で次にどのように動作すべきかを記述する場合は、構成的にアルゴリズムを用いて記述する方法が適している。本研究では、仕様を記述する際、宣言的に記述された仕様と、構成的に記述された仕様の両方を満たすシステムを構成する方法を提案した。この方法では、宣言的な記述には線形時間論理を用い、構成的な記述には状態遷移系を用いる。線形時間論理を用いて記述した宣言的仕様をωオートマトンに変換し、構成的な仕様である状態遷移系の上での振る舞いにおいて、ωオートマトンを受理するものを選ぶことにより、システムの振る舞いを得る。

(4) 現実規模の仕様からのシステム合成を可能とするためのモジュール分割法
線形時間論理で記述された仕様から、その仕様を満たす組み込みシステムを自動合成する方法があるが、この方法を現実規模の仕様に対応するためには、時間計算量、空間計算量の大きさゆえ、様々な効率化技術が必要となる。この技術の一つとして、分割検証がある。この技術は、仕様をモジュール分割し、モジュールごとにサブシステムを合成し、得られたそれらのシステムを一つにまとめることで、全体のシステムを得る方法である。このとき、どのようにモジュール分割するかが鍵となる。本研究では、計算時間と計算に使用する空間を爆発させないために、サブシステムを構成する際にモジュールから得られる中間生成物の大きさを見積もり、それらがだいたい同じ大きさになるようにモジュール分割する方法を提案した。モジュール仕様で使われるイベント命題の個数と仕様の大きさで、サブシステムの大きさを見積もり、それらを均等にするようなモジュール分割を k-means 法などで求める。これにより、より現実規模のシステム合成が可能となる。

(5) 定性的仕様からの組み込みシステム合成の効率化
現実規模の組み込みシステム合成を可能とするため、定性的仕様からのシステム合成を効率化する研究にも取り組んだ。システム合成する際、仕様からセーフティゲームを構成し、その上での勝利戦略を求める。勝利戦略の有無を保存しながら、単純なセーフティゲームを構成することで、システム合成を効率化した。さらに、システム自動合成手法の実装において、中間生成物として BDD(二分決定グラフ)と明示的なグラフの両方を適切な箇所で用いることで、システムの自動構成を効率化することに成功した。また、システム自動合成で得られるセーフティゲームの大きさのオーダーを小さくできるような、仕様を記述する構文の制限についても研究した。

５．主な発表論文等

〔雑誌論文〕　計11件（うち査読付論文　11件／うち国際共著　0件／うちオープンアクセス　3件）

１．著者名 三木　潤一，川崎　雄二郎，萩原　茂樹	４．巻 5
２．論文標題 地方公共サービスにおける人員・車両・施設等の最適資源配置問題 ―救急・消防に関する検討―	５．発行年 2021年
３．雑誌名 CIPFA Japan ジャーナル	６．最初と最後の頁 25-35
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 ―

１．著者名 Masaya Shimakawa, Kentaro Hayashi, Shigeki Hagihara and Naoki Yonezaki	４．巻 -
２．論文標題 Towards Interpretation of Abstract Instructions Using Declarative Constraints in Temporal Logic	５．発行年 2020年
３．雑誌名 Proceedings of the 2020 9th International Conference on Software and Computer Applications (ICSCA2020)	６．最初と最後の頁 17-20
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/3384544.3384572	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 ―

１．著者名 Shigeki Hagihara, Masaya Shimakawa and Naoki Yonezaki	４．巻 -
２．論文標題 Verification of Verifiability of Voting Protocols by Strand Space Analysis	５．発行年 2019年
３．雑誌名 Proceedings of the 2019 8th International Conference on Software and Computer Applications (ICSCA2019)	６．最初と最後の頁 363-368
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/3316615.3316629	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 ―

１．著者名 Masaya Shimakawa, Atsushi Ueno, Shohei Mochizuki, Takashi Tomita, Shigeki Hagihara and Naoki Yonezaki	４．巻 -
２．論文標題 Towards Efficient Implementation of Realizability Checking for Reactive System Specifications	５．発行年 2019年
３．雑誌名 Proceedings of the 2019 8th International Conference on Software and Computer Applications (ICSCA2019)	６．最初と最後の頁 347-352
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/3316615.3316634	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 ―

1．著者名 Sohei Ito, Kenji Osari, Shigeki Hagihara and Naoki Yonezaki	4．巻 881
2．論文標題 Compositional Analysis of Homeostasis of Gene Networks by Clustering Algorithms	5．発行年 2018年
3．雑誌名 Biomedical Engineering Systems and Technologies (BIOSTEC 2017), Communications in Computer and Information Science	6．最初と最後の頁 191-211
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/978-3-319-94806-5_11	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Shigeki Hagihara, Yoshiharu Fushihara, Masaya Shimakawa, Masahiko Tomoishi, Naoki Yonezaki	4．巻 -
2．論文標題 Web server access trend analysis based on the Poisson distribution	5．発行年 2017年
3．雑誌名 Proceedings of the 6th International Conference on Software and Computer Applications (ICSCA 2017)	6．最初と最後の頁 256-261
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/3056662.3056701	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Masaya Shimakawa, Kenji Osari, Shigeki Hagihara, Naoki Yonezaki	4．巻 -
2．論文標題 Modularization of formal specifications for efficient synthesis of reactive systems	5．発行年 2017年
3．雑誌名 Proceedings of the 6th International Conference on Software and Computer Applications (ICSCA 2017)	6．最初と最後の頁 208-213
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/3056662.3056702	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Masaya Shimakawa, Shigeki Hagihara, Naoki Yonezaki	4．巻 1955
2．論文標題 Efficiency of the strong satisfiability checking procedure for reactive system specifications	5．発行年 2018年
3．雑誌名 AIP Conference Proceedings	6．最初と最後の頁 40051
掲載論文のDOI（デジタルオブジェクト識別子） 10.1063/1.5033715	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Takashi Tomita, Atsushi Ueno, Masaya Shimakawa, Shigeki Hagihara, Naoki Yonezaki	4．巻 Special Issue on Synthesis
2．論文標題 Safraless LTL Synthesis Considering Maximal Realizability	5．発行年 2016年
3．雑誌名 Acta Informatica	6．最初と最後の頁 1-38
掲載論文のDOI（デジタルオブジェクト識別子） 10.1007/s00236-016-0280-3	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Shigeki Hagihara, Masahiko Tomoishi, Masaya Shimakawa, Naoki Yonezaki	4．巻 126
2．論文標題 Combining Unification and Rewriting in Proofs for Modal Logics with First-order Undefinable Frames	5．発行年 2017年
3．雑誌名 Advances in Engineering	6．最初と最後の頁 676-683
掲載論文のDOI（デジタルオブジェクト識別子） 10.2991/icmmct-17.2017.140	査読の有無 有
オープンアクセス オープンアクセスとしている（また、その予定である）	国際共著 －

1．著者名 Shigeki Hagihara, Atsushi Ueno, Takashi Tomita, Masaya Shimakawa, Naoki Yonezaki	4．巻 -
2．論文標題 Simple synthesis of reactive systems with tolerance for unexpected environmental behavior	5．発行年 2016年
3．雑誌名 Proceedings of the 4th FME Workshop on Formal Methods in Software Engineering (FormaliSE '16)	6．最初と最後の頁 15-21
掲載論文のDOI（デジタルオブジェクト識別子） 10.1145/2897667.2897672	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計7件（うち招待講演　0件／うち国際学会　6件）

1．発表者名 川崎　雄二郎，萩原　茂樹，三木　潤一
2．発表標題 動的モデルによる救急隊配置の最適化手法―山形県酒田地区におけるケーススタディ
3．学会等名 日本応用数理学会第17回研究部会連合発表会
4．発表年 2021年

１．発表者名
Masaya Shimakawa, Shigeki Hagihara and Naoki Yonezaki

２．発表標題
Towards Improvement of Realizability Checking for Reactive System Specifications by Simplification of Infinite Games

３．学会等名
Workshop on Computation: Theory and Practice (WCTP2018)（国際学会）

４．発表年
2018年

１．発表者名
Takashi Tomita, Masaya Shimakawa, Shigeki Hagihara and Naoki Yonezaki

２．発表標題
A Characterization on Necessary Conditions of Realizability for Reactive System Specifications

３．学会等名
Workshop on Computation: Theory and Practice (WCTP2018)（国際学会）

４．発表年
2018年

１．発表者名
Masaya Shimakawa, Shigeki Hagihara, Naoki Yonezaki

２．発表標題
Towards Improvements of Bounded Realizability Checking

３．学会等名
Workshop on Computation: Theory and Practice (WCTP2017)（国際学会）

４．発表年
2017年

１．発表者名
Shigeki Hagihara, Masaya Shimakawa, Naoki Yonezaki

２．発表標題
Discussion on Verification of Voting Protocols

３．学会等名
17th Philippine Computing Science Congress (PCSC 2017)（国際学会）

４．発表年
2017年

１．発表者名 Masaya Shimakawa, Yuji Iwasaki, Shigeki Hagihara and Naoki Yonezaki
２．発表標題 Discussion of LTL Subsets for Efficient Verification
３．学会等名 Workshop on Computation: Theory and Practice (WCTP2016)（国際学会）
４．発表年 2016年

１．発表者名 Shigeki Hagihara
２．発表標題 To develop software without flaws
３．学会等名 Workshop on Computation: Theory and Practice (WCTP2016), Satellite Conference（国際学会）
４．発表年 2016年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究協力者	島川　昌也 (Shimakawa Masaya) (00749161)		
研究協力者	冨田　尭 (Tomita Takashi) (80749226)		
研究協力者	伊藤　宗平 (Ito Sohei) (50708005)		

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関