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　５ 年　 ５ 月 ３１ 日現在

機関番号：１３３０２
研究種目：若手研究(B)
研究期間：2017～2022
課題番号：１７Ｋ１７７６３

研究課題名（和文）実現可能性必要条件に基づいた協調的リアクティブシステム自動合成

研究課題名（英文）Cooperative Reactive System Synthesis Based on Necessary Conditions of Realizability

研究代表者

冨田　尭（Tomita, Takashi）

北陸先端科学技術大学院大学・情報社会基盤研究センター・講師

研究者番号：８０７４９２２６

交付決定額（研究期間全体）：（直接経費）　　3,200,000円

研究成果の概要（和文）：本研究では仕様の実現可能性必要条件に基づき協調的リアクティブシステムを自動合成する手法の開発に取り組んだ．
新たに8つの必要条件群を発見し，既知の必要条件群も含めた統一的な特徴付けと階層定理群を与えた．これらの必要条件群は網羅性，保存性，安定性及び戦略化可能性の4つの観点から体系的に分類でき，その観点から仕様の欠陥についての分析と，協調が発生し得ることを導出できる．そして，必要条件群の特性について，判定手続きを構成するサブルーチンの共通性及び類似性からも分析するとともに各必要条件判定の期待計算量を導出し，実現可能性必要条件に基づく協調的リアクティブシステム自動合成手法の基礎を確立した．

研究成果の学術的意義や社会的意義
本研究成果は，より現実的・一般的な自動合成技術の基盤を与えたという点で学術的・社会的な意義がある．
古典的なリアクティブシステム自動合成では敵対的な環境を想定するという過度に厳しい安全性に基づいていたが，本研究では協調の発生を想定し緩和された安全性に基づく自動合成に注目し，合成可能性の基盤となる実現可能性必要条件群について分析した．その結果，実現可能性必要条件群の判定手続きの期待計算量は大きいものの，体系的な特徴付け・分類により，要求仕様の欠陥や協調不調についてのより詳細な分析が可能なことが明らかになったため，仕様修正の容易化を期待できる．

研究成果の概要（英文）：In this research, we tackled the development of an automatic synthesis method of a cooperative reactive system from a formal requirement specification, based on necessary conditions of realizability of the specification.
We found eight new necessary conditions of the realizability, gave a systematic characterization for the new conditions and also existing ones, and proof a hierarchy theorem among the conditions. The conditions are systematically categorized with four viewpoints: exhaustivity, strategizability, preservability and stability. In these viewpoints, we can analyze defects of specifications and also imply the possibility of cooperation between a reactive system and external environment. We also revealed expected complexities of checking problems for the necessary conditions, based on the similarity among subroutines of their checking procedures. That is, we established the basis of cooperative reactive system synthesis methods based on necessary conditions of realizability.

研究分野：計算科学

キーワード：ソフトウェア工学　ソフトウェア検証　形式手法　協調的リアクティブシステム　実現可能性　自動合成

１．研究開始当初の背景

リアクティブシステム（RS）とは，利用者などの外部環境と継続的に相互作用し続けるシステムであり，組込みシステムや制御システムなどの高い安全性が求められるオープンシステムである．誤りなく RS を構成するための手法として，不具合混入の元となる人手によるコーディング工程を持たない自動合成(実現可能性の構成的証明に相当)は古くから提唱されてきた. そして，定性的検証から定量的検証へ，そして検証から最適化への形式的検証技術の発展と合わせて，自動合成においても定量的な拡張が提案され，最適 RS 自動合成手法の研究も活発化しており，RS 自動合成への注目はますます高まっている．

しかしながら，従来の RS 自動合成の問題設定は，現実的には必ずしも妥当ではない．従来の RS 自動合成では環境が敵対的であると仮定することでいかなる状況下でも要求仕様を満たすことを保証しているが，現実的には環境は敵対的でないことも多い．また，分散システム（個々のサブシステムからみると他のシステムは環境）においても，システム全体で１つの目的を達成するのではなく，各サブシステムが自然に協調して互いの目的を満たせるように設計されることもある．そのため，協調関係も考慮することで，与えられた要求仕様が従来観点では欠陥があり実現不能とされる場合であっても，現実的には欠陥なく自動合成できる場合がある．

２．研究の目的

本研究の目的は，従来手法とは異なり，システムと環境の協調関係に焦点を当て，実現可能性必要条件に基づき，協調的 RS を自動合成する手法及びツールを開発することである．

特に，RS-環境間に協調関係が発生するための条件と協調的 RS の自動合成の効率化に有効な技術を明らかにすることを目指す．

３．研究の方法

まず，実現可能性必要条件について考察しその特徴付けを行う．そして実現可能性必要条件に基づいてリアクティブシステム（RS)と環境の間の協調関係について考察しその特徴付けを行い，協調的 RS 自動合成手法の試作・実装・評価，従来型自動合成手法の効率化手法の適用のほか，協調関係を考慮するが故の効率化手法を模索する．

４．研究成果

（1）実現可能性必要条件群の特徴付けと新しい実現可能性必要条件群の発見

既知の 4 つの実現可能性必要条件（充足可能性，強充足可能性，保存的充足可能性，保存的強充足可能性）が入力接頭辞，入力接尾辞，出力接頭辞及び出力接尾辞に対する限量に基づいて定義されていることから，この限量の仕方（限量行列表現）に基づいて実現可能性必要条件群を体系的・階層的に特徴付けることで，新たに接頭的半強充足可能性，接尾的半強充足可能性，真接尾的半強充足可能性，真強充足可能性，真保存的充足可能性，安定的充足可能性，真安定的充足可能性，安定的強充足可能性の 8 つの実現可能性必要条件を新たに発見した．

これらの実現可能性必要条件群は，接頭構造（有限長言語）と接尾構造（無限長言語）の非対称性，入力（RS 制御不可）と出力（RS 制御可）の非対称性に基づいた自然な限量順序を網羅している他，（反例が存在する場合）説明が用意な反例を持つ必要条件群から成り，与えられた要求仕様が実現不能な場合でも，どの必要条件を満たしているかによってどの程度実現可能に近いかを明らかにすることが可能となった．

（2）実現可能性必要条件群の階層定理の証明

実現可能性必要条件群の特徴付けに用いた限量行列表現より，既知の 4 つの実現可能性必要条件群と新しい 8 つの実現可能性必要条件は，入力の網羅性，出力の戦略化可能性，実行前期での充足可能性の保持性（保存性），実行後期での充足可能性の保持性（安定性）の 4 つの観点で体系的・階層的に分類でき，要求仕様が実現可能性であるときには網羅性・戦略化可能性・保存性・安定性のすべてを完全に満たすことに相当することを明らかにした．

また，実現可能性必要条件群を満たす要求仕様クラス間の包含関係（階層定理）を証明した（図 1）．接頭構造と接尾構造の非対称性と入力と出力の非対称性により単純ではない階層をもつことが明らかになった．

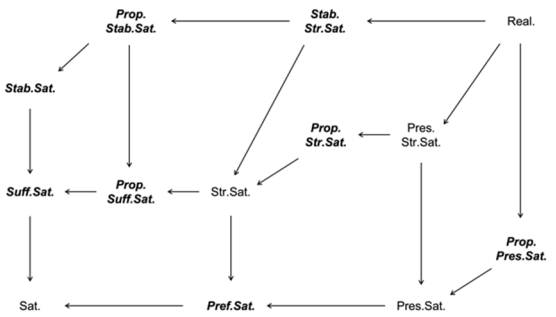

図 1：実現可能性必要条件群を満たす要求仕様クラスの包含関係（太字は新たに発見した 8 つの実現可能性必要条件）

（3）実現可能性必要条件群の判定問題の期待計算量の導出
新たに発見された実現可能性必要条件群は既知の実現可能性必要条件群及び実現可能性と類似の定義構造を持っており，その判定手続きも既知の実現可能性必要条件群及び実現可能性の判定手続きと同様の工程を持つ．そして，判定手続き中に取り扱われるオートマトンに対する数種の遷移変更操作，状態変更操作及び受理条件変更操作を組み合わせることで，新たに発見された実現可能性必要条件群も判定することが可能であることを示した．
また，新実現可能性必要条件群と既知実現可能性必要条件群の類似性と既知実現可能性必要条件群の判定手続き計算量から，各判定問題の計算量は，要求仕様が線形時相論理（LTL）で与えられている場合，接頭的半強充足可能性，接尾的半強充足可能性及び真接尾的半強充足可能性 EXPSPACE 困難，真強充足可能性，真保存的充足可能性，安定的充足可能性及び真安定的充足可能性は 2EXPTIME 困難，安定的強充足可能性は 2EXPSPACE 困難であると予想される．実現可能性必要条件群の判定手続きの期待計算量は大きいものの，体系的な特徴付け・分類により，要求仕様の欠陥や協調不調についてのより詳細な分析が可能なことが明らかになったため，仕様修正の容易化を期待できる．

（4）実現可能性判定手続きにおける部分記号化アプローチの開発
協調的 RS 自動合成手法及びツールの開発に向け，従来型自動合成手法の効率化手法として，部分記号化手法を開発した．
既存の従来型自動合成手法では合成手続き中に取り扱われるオートマトンの状態空間及び繊維関係のすべての二分決定図（BDD）で表現する完全記号化アプローチがしばしば採用されているが，記号化を部分的にするアプローチを提案した．また，プロトタイプツールを実装し，既存ツールとの比較実験を通して，効率化が見込めることを確認した．

５．主な発表論文等

〔雑誌論文〕　計1件（うち査読付論文　1件／うち国際共著　0件／うちオープンアクセス　1件）

１．著者名 Takashi Tomita, Shigeki Hagihara, Masaya Shimakawa, Naoki Yonezaki	４．巻 E105-D(10)
２．論文標題 A Characterization on Necessary Conditions of Realizability for Reactive System Specifications	５．発行年 2022年
３．雑誌名 IEICE Transaction on Information and Systems	６．最初と最後の頁 1665-1677
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transinf.2021FOP0005	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 －

〔学会発表〕　計3件（うち招待講演　0件／うち国際学会　2件）

１．発表者名 冨田　尭
２．発表標題 リアクティブシステム実現可能性必要条件の判定手続き
３．学会等名 日本ソフトウェア科学会第37回大会
４．発表年 2020年

１．発表者名 Takashi Tomita, Shigeki Hagihara, Masaya Shimakawa, 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（国際学会）
４．発表年 2018年

１．発表者名 Masaya Shimakawa, Atsushi Ueno, Shohei Mochizuki, Takashi Tomita, Shigeki Hagihara, Naoki Yonezaki
２．発表標題 Towards Efficient Implementation of Realizability Checking for Reactive System Specifications
３．学会等名 8th International Conference on Software and Computer Applications（国際学会）
４．発表年 2018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

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