

平成 30 年 5 月 26 日現在

機関番号：14401

研究種目：基盤研究(C) (一般)

研究期間：2014～2017

課題番号：26330083

研究課題名(和文)再合成可能な半順序分割による分散システムの振る舞いモデル自動合成

研究課題名(英文)Automatic Synthesis of Behavioral Models in Distributed Systems by Reconstructible Decomposition of Acyclic Relations

研究代表者

宮本 俊幸 (MIYAMOTO, Toshiyuki)

大阪大学・工学研究科 准教授

研究者番号：00294041

交付決定額(研究期間全体)：(直接経費) 3,500,000円

研究成果の概要(和文)：高信頼ソフトウェアの開発は、安心・安全な社会を実現する上で必要不可欠である。本研究では、抽象的な要求仕様から分散システムを構成するモジュールの振る舞いモデルを自動合成する問題に取り組んだ。非循環関係の再合成可能な分割という新たな概念を導入し、パレート効率な状態機械を合成するアルゴリズムを開発した。また、提案手法をUMLモデリングツールのプラグインとしてソフトウェア実装した。提案手法はモデルの理解しやすさの点で既存手法より優れていた。

研究成果の概要(英文)：Development of high reliability software is indispensable to achieve safe and secure society. This research program addressed the problem of automatically synthesizing the behavioral model of each module composes a distributed system from an abstract specification. A new notion called "reconstructible" decomposition of acyclic relation is introduced and an algorithm synthesizing Pareto efficient state machines is developed. The proposed method has been implemented as a plug-in of a UML modeling tool. The proposed method is superior to the former method in terms of intelligibility of model.

研究分野：分散システム

キーワード：ソフトウェア開発効率化・安定化 ソフトウェア工学 アルゴリズム 情報システム

1. 研究開始当初の背景

組み込みシステムやインターネットなど今日の我々の便利な生活を支えるあらゆるものにおいて、ソフトウェアが重要な役割を果たしている。しかしながら、ソフトウェアの不具合(バグ)が様々な物理的事故や経済的損失を引き起こしており、高信頼性ソフトウェア構築技術が求められている。

また、最近のソフトウェアは単体で動作するのではなく、自動車における車載ネットワークを使った制御ソフトウェアや情報通信システムにおけるサービス指向アーキテクチャ(SOA)のように、ネットワークで繋がった複数のプロセスが連携しながらタスクを実行する。いわゆる、分散システムである。制御分野では、物理システムとネットワーク化された情報システムが密接に結合したシステムをサイバーフィジカルシステムと名付けて、欧米を中心に新たな研究分野として展開されている。このように、今後ますます重要となる分散システムにおける高信頼性ソフトウェア開発は安心安全な社会を実現する上で重要な課題となる。

ソフトウェアの信頼性を高める一つの方法として、プログラムの自動合成がある。良い仕様から仕様を満足するプログラムを自動合成することができれば、信頼性の高いソフトウェアが開発される。

研究代表者らはシナリオを UML 2.X のコミュニケーション図によって与え、コミュニケーション図から階層型状態機械を合成する手法を提案している。この手法には状態機械が不必要に複雑になる問題例が見られるという改善の余地があり、さらなる検討が必要であった。

2. 研究の目的

これまでの手法では、シナリオで定義されている振る舞いを忠実に実現するために、シナリオを「射影」することによりモジュールの振る舞いモデルを合成している。しかし、これまでに提案した手法では、モジュールの状態機械が不必要に複雑になる問題例が見られた。そこで、シナリオを「分割」してから、モジュールの振る舞いモデルを合成する手法を提案する。このとき、分割によってシナリオの定義と違えることが無いよう「再合成可能」な分割について理論的に考察する。

以上より、本研究では研究期間内に次の(1)~(3)の項目を明らかにすることを目的とする。

(1) シナリオ分割の必用十分条件の導出

シナリオを分割したときに得られる状態機械がシナリオで定義される振る舞いを模倣するための条件を理論的に考察する。

(2) パレート効率な状態機械導出アルゴリズムの設計

(1)の成果を元に状態機械の理解しやすさの意味で最適な状態機械を導出するためのアルゴリズムを設計する。この時、状態機械の理解しやすさには複数の指標が考えられるため、パレート効率な状態機械を導出するアルゴリズムを設計する。

(3) 提案アルゴリズムの評価

(2)の成果を UML モデリングツールのプラグインとして実装し、評価実験により提案手法の有効性を明らかにする。

3. 研究の方法

まず、シナリオの再合成可能な分割について理論的に考察する。数学的にはシナリオは非循環関係と見なせるので、非循環関係の再合成可能な分割について必用十分条件を導出する。

次に、シナリオを状態機械に変換するアルゴリズムを開発する。再合成可能な分割が複数存在するため、合成される状態機械に自由度がある、そこで状態機械の理解しやすさの仕様を使った最適化アルゴリズムとして定式化し、パレート効率な状態機械を導出するアルゴリズムを開発する。

最後に、シナリオから状態機械を自動合成するアルゴリズムを開発し、ソフトウェア実装する。そして、いくつかのサンプルシステムを使って開発したアルゴリズムの評価を行う。

4. 研究成果

(1) シナリオ分割の必用十分条件の導出

非循環関係の再合成可能な分割という新たな概念を提案し、再合成となるための必用十分条件を与えた。

また、シナリオをモジュール毎の仕様に分割する上で再合成可能な分割の概念を利用し、モジュール毎の仕様に上限および下限があることを示した。これにより、上限と下限に挟

まれた範囲から状態機械を合成してもよいことが明らかになった。

(2) パレート効率的な状態機械導出アルゴリズムの設計

(1)の成果により複数の候補から最も良い状態機械を合成すれば良いことになる。状態機械の理解しやすさの指標は複数あるため、トレードオフの関係が起こりえる。そのため、全ての候補を列挙して、パレート効率的な状態機械を合成するアルゴリズムを開発した。

(3) 提案アルゴリズムの評価

(2)の成果を UML モデリングツール (IBM Rational Software Architect) のプラグインとして実装した。

図1に開発したソフトウェアの実行画面を示す。提案手法ではコミュニケーション図を使ってシナリオを記述する。左上の図がコミュニケーション図である。コミュニケーション図ではシステムを構成するモジュールとモジュール間で通信されるメッセージの順序関係を定義する。提案手法では、与えられた順序関係を満足する状態機械を合成する。右上および下が開発したソフトウェアによって自動的に合成された状態機械である。なお、このソフトウェアは研究代表者のホームページで一般公開している。

図2に以前の研究により開発された手法で合成された状態機械を、図3に提案手法で

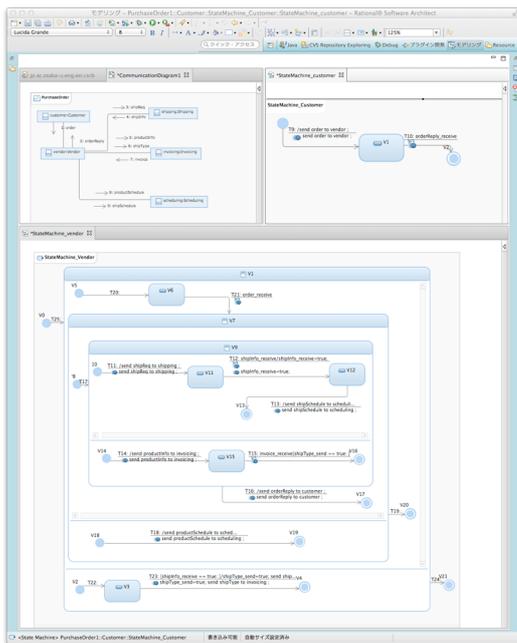


図1：開発ソフトウェアの実行画面

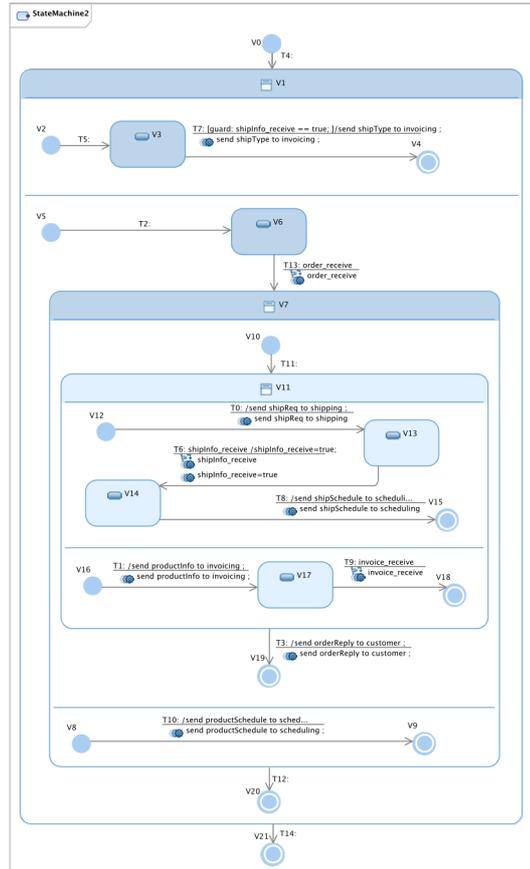


図2：既存手法で合成された状態機械

合成された同じ例に対する状態機械を示す。

表1に Cruz-Lemus らによって提案されている状態機械の理解しやすさに関する指標による比較を示す。NSS は単純状態の数、NT は遷移の数、NG はガードの数、ND は階層数であり、いずれも値の小さい方が理解しやすいと言われている。既存手法の状態機械と提案手法の状態機械を比較すると、階層数が異なる。提案手法の方が、階層が1層少なく構造が単純な動作を理解しやすい状態機械を合成している。また NT において 27%の削減に成功しており、この結果は提案手法の有効性を示している。

5. 主な発表論文等

[雑誌論文] (計2件)

- ① Toshiyuki Miyamoto, Synthesizing Pareto Efficient Intelligible State Machines from Communication Diagram, IEICE Trans. Inf. & Syst., 査読有り, Vol. E100-D, 2017, 1200-1209
DOI: 10.1587/transinf.2016FOP0002

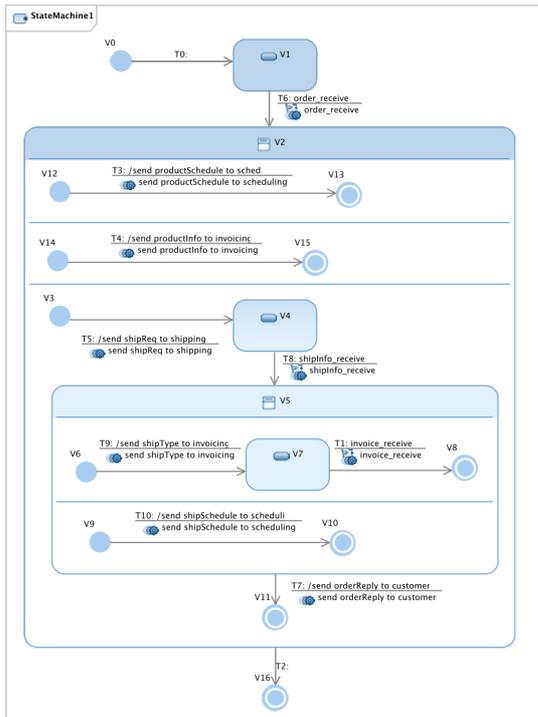


図3：提案手法で合成された状態機械

② Toshiyuki Miyamoto, Choreography Realization by Re-Constructible Decomposition of Acyclic Relations, IEICE Trans. Inf. & Syst., 査読有り, Vol.E99-D, 2016, 1420-1427
DOI: 10.1587/transinf.2015FOP0001

[学会発表] (計 10 件)

- ① Toshiyuki Miyamoto, Modified Rules for Modular Reachability Analysis of Petri Nets for Multiagent Systems, SICE Annual Conference 2017, 2017年9月20日, 金沢大学 (石川県・金沢市)
- ② 木下聖基, 宮本俊幸, 二つのシナリオで定義されるコレオグラフィの実現可能性の検討, 第30回 回路とシステムワークショップ, 2017年5月11日, 北九州国際会議場 (福岡県・北九州市)
- ③ 木下聖基, 宮本俊幸, 二つのコミュニケーション図からなるコレオグラフィの実現可能性の検討 - 仕様間に競合がある場合の考察 -, 電子情報通信学会システム数理と応用研究会, 2017年1月26日, 京都工芸繊維大学 (京

表1：評価実験の結果

	NSS	NT	NG	ND
既存	5	15	1	4
提案	3	11	0	3

都府・京都市)

④ 木下聖基, 宮本俊幸, 二つのコミュニケーション図からなるコレオグラフィの実現可能性の検討, 電子情報通信学会基礎・境界ソサイエティ大会, 2016年9月20日, 北海道大学 (北海道・札幌市)

⑤ Toshiki Kinoshita and Toshiyuki Miyamoto, A Study on Synthesizing State Machines from Multiple Communication Diagrams, International Technical Conference on Circuits/Systems, Computers and Communications, 2016年7月11日, 自治会館 (沖縄県・那覇市)

⑥ Toshiyuki Miyamoto, CSCB Tools: A Tool to Synthesize Pareto Optimal State Machine Models from Choreography Using Petri Nets, International Workshop on Petri Nets and Software Engineering, 2016年6月20日, ニコラス・コペルニクス大学 (トルン・ポーランド)

⑦ 宮本俊幸, 非循環関係の再合成可能な分割によるコレオグラフィ実現 - バレート最適な状態機械の合成について -, 電子情報通信学会システム数理と応用研究会, 2016年1月25日, しいのき迎賓館 (石川県・金沢市)

⑧ Toshiyuki Miyamoto, CSCB Tools: Tool for Supporting the Design of Systems Based on SOA, IEEE 4-th Global Conference on Consumer Electronics, 2015年10月27日, 大阪国際会議場 (大阪府・大阪市)

⑨ 宮本俊幸, 非循環関係の再合成可能な分割によるコレオグラフィ実現, 電子情報通信学会システム数理と応用研究会, 2015年6月17日, 小樽商科大学 (北海道・小樽市)

⑩ 老邑博行, 宮本俊幸, サービス指向アーキテクチャに基づくシステムの整合性検証に関する研究, 電子情報通信学会システム数理と応用研究会, 2015年1月27日, プランナール三朝 (鳥取県・三朝町)

[その他]

ホームページ等

<http://is.eei.eng.osaka-u.ac.jp/miyamoto/index.php?CSCB>

6. 研究組織

(1) 研究代表者

宮本 俊幸 (MIYAMOTO, Toshiyuki)
大阪大学・大学院工学研究科・准教授
研究者番号：00294041