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

平成　２９　年　　６　月　１９　日現在

機関番号：　１２６１２
研究種目：　基盤研究(C)（一般）
研究期間：　2014～2016
課題番号：　２６３３００８１

研究課題名（和文）アスペクト指向 models@run.time システムの効率的な実行時形式検証

研究課題名（英文）Efficient runtime formal verification of aspect-oriented models@run.time systems

研究代表者

田原　康之（Tahara, Yasuyuki）

電気通信大学・大学院情報理工学研究科・准教授

研究者番号：３０３９０６０２

交付決定額（研究期間全体）：（直接経費）　　3,700,000円

研究成果の概要（和文）：研究代表者らの既提案の，アスペクト指向 models@run.time システムの形式モデルの枠組に対する，モデルとソースコードが本枠組における抽象化・詳細化関係となるようなコード生成系を開発し，前記形式モデルの枠組に対し，リフレクションを用いてアスペクトの織り込みの定式化である公理の変更規則を新たに公理とすることによる，適応のために実行時にアスペクトを織り込む場合の振舞いを扱えるような拡張を行い，検証・適応系プロトタイプの設計に基づく，コード生成系と検証系を統合した検証・適応系プロトタイプを開発し，例題ウェブ・ユビキタスアプリケーションの実装と実験・評価を行った.

研究成果の概要（英文）：We developed a code generation system that provides an abstraction / refinement relation between the model and the source code based on the framework of the formal model of aspect-oriented models@run.time system proposed by us. We extended the framework of the formal model so that it can deal with the behavior in which aspects are woven at runtime for adaptation, by adding, as new axioms, axiom changing rules that formalize aspect weaving using reflection. We developed a prototype of verification and adaptation integrating the code generation system and the verification system based on the design of the prototype of the verification / adaptation system. We also implemented, conducted experiments of, and evaluated the example web / ubiquitous application.

研究分野：　ソフトウェア工学

キーワード：　ソフトウェア工学　アスペクト指向　models@run.time　形式手法　モデル検査　リフレクション　抽象化　自己適応システム

１．研究開始当初の背景

近年のコンピュータシステムにおいて、システムへの要求や動作環境の急速な変化に対応し、保守運用コストを削減する必要がある。そのための最新の研究動向として、システムが自ら要求や動作環境の変化を監視（モニタ、Monitor）し、対応が必要な変化を検出（分析、Analyze）し、さらにはシステム自らが、自身の動作を極力停止させずに、ソフトウェアのモデルの変更による対応手段を導出（計画、Plan）し、変更後のモデルをプログラムに反映して変化に適応（実行、Execute）する技術が、models@run.time と呼ばれて注目されている。

このような技術の実適用を考えた場合、適応機構が複雑になり、実行前にあらかじめどのような変更が適応時に起こるかの予測が難しいため、システムの振舞いの正しさをテストなどで確認するのは困難となる。そこでシステム稼働中の適応動作実行時に、適応前後の振舞いの正しさを確認する、実行時検証が有効であると考えられている。その上で今後このようなシステムに求められる高い信頼性を保証するためには、特に厳密な検証手法である形式検証の適用が望ましい。しかし形式検証は一般に計算コストが多大であるため、現状では実行時検証への適用は現実的ではなく、研究事例もまだない。そこで本研究では、適応手段の 1 つであるアスペクト指向手法を用いた models@run.time システムにおいて、適応動作時の検証をシステムの部分ごとに行うことにより、検証コストを軽減し、現実的な実行時形式検証の実現を目指す。なおアスペクト指向技術は、プログラムの全体的な変更が必要となるような、高度に複雑な状況への対応を実現するものである。そのために、個々の目的に対するプログラムの変更部分をアスペクトと呼ばれるモジュールにまとめ、プログラム全体にわたってアスペクトで指定された箇所に必要な変更を施す（この操作を織り込みと呼ぶ）。このようにアスペクト指向技術を用いると、よく知られたコンポーネントの切り替えなどよりも、複雑な適応が容易に可能となる。事実、アスペクト指向技術を利用した models@run.time システム構築手法が提案されている。

環境の変化に自ら適応するシステムとして，IBM の Autonomic Computing や無人ロボットカーで知られる DARPA の Urban Challenge，火星探索機 Phoenix，探査機 Rover など，特に米国では莫大な予算のもと，各ドメインでのシステムが現実化されはじめている．学術分野でも，モデル駆動開発の分野で最高峰の会議 MODELS において models@run.time ワークショップが併設されるなど、models@run.time システムに関する研究成果がここ数年で急速に報告されている。

前述のようにアスペクト指向 models@run.time システムでは、適応動作が複雑なものとなるため、実行時検証における形式検証の適用は現実的ではないと考えられる。アスペクト指向 models@run.time システムの実行時検証手法が提案されているが、厳密ではない検証技術を採用している。

２．研究の目的

このような問題に対し本研究では、アスペクト指向システムの効率的な形式検証手法を、アスペクト指向 models@run.time システムの形式モデルに適用することにより、効率的な実行時形式検証手法を確立することを目指す。本研究における具体的な課題は以下の通りである。

(課題 1)検証コストの軽減：前述のように形式検証は一般に計算コストが高い。しかしアスペクト指向システムにおいては、アスペクトごとに検証することで、織り込んだシステムの検証が完了するという手法がある。また、モデル上でアスペクトを織り込むことにより、適応後のモデルを構成する手法もある。そこで本研究では、本手法をアスペクトモデルごとの検証に適用し、織り込んだモデルの正しさを保証することを実現する。

(課題 2)適応後のシステム動作の正しさの保証：アスペクトの織り込みは複雑な過程となるため、適応後のモデルとプログラムとの整合性は必ずしも保証されない。一方研究代表者らが提案した、アスペクト指向システムの形式モデルの枠組は、アスペクトを織り込んだ抽象的なモデルと、プログラムなど抽象度の低いモデルとの整合性を保証するものである。そこでこの枠組を利用し、適応後のプログラムの正しさを保証する。

(課題 3)適応中のシステム動作の正しさの保証：研究代表者らが提案した、アスペクト指向システムの形式モデルの枠組は、システム実行前の織り込みを想定しているため、適応のために実行時に織り込む場合の振舞いの正しさは不明である。そこで本枠組を実行時の織り込みに拡張し、適応中の動作の正しさも保証可能な枠組を確立する。

３．研究の方法

本研究では、アスペクト指向 models@run.time システムの形式モデルを確立し、そのモデルに基づいた実行時形式検証機能とコード生成機能を搭載した適応系のプロトタイプを開発し、具体的なアプリケーションに適用して実験と評価を行う。このために、既に提案しているアスペクト指向の形式モデルの枠組が、書換え論理と呼ばれる論理体系に基づいていることを利用する。本研究は 4 つのテーマに分割して研究を進める．テーマ 1 は課題 1 と 2 に対応し、モデル変換手続きが比較的容易に得られるという書換え論理の特徴を活かし、正確なコード生成アルゴリズムを構築する。テーマ 2 は課題 3 に対応し、書換え論理によるリフレクションのモデルにより、適応中システム動作の形式モ

デルを確立する。さらにテーマ3と4でプロトタイプを開発し、例題に対する適用実験を行う。

４．研究成果

(1)研究代表者らの既提案の、アスペクト指向 models@run.time システムの形式モデルの枠組に対する、モデルとソースコードが本枠組における抽象化・詳細化関係となるようなコード生成系

(2)前記形式モデルの枠組に対し、リフレクションを用いてアスペクトの織り込みの定式化である公理の変更規則を新たに公理とすることによる、適応のために実行時にアスペクトを織り込む場合の振舞いを扱えるような拡張

(3)検証・適応系プロトタイプの設計に基づく、コード生成系と検証系を統合した検証・適応系プロトタイプ

(4)例題ウェブ・ユビキタスアプリケーションの実装と実験・評価結果

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 120 件）

[1] Yuichi Sei, Akihiko Ohsuga: Privacy-Preserving Chi-Squared Testing for Genome SNP Databases, Proc. of IEEE EMBC, to appear (2017) （査読有）

[2] Yasuyuki Tahara, Akihiko Ohsuga and Shinichi Honiden: Formal Verification of Dynamic Evolution Processes of UML Models Using Aspects, Proc. of SEAMS 2017, to appear (2017) （査読有）

[3] 天野和洋, 前田宗宏, 中村泰広, 清雄一, 大須賀昭彦: 1.5 車線的道路整備における待避区間の最適配置に向けた評価手法の検討, 土木学会論文集 D3（土木計画学）, to appear (2017) （査読有）

[4] Yuichi Sei, Hiroshi Okumura, Takao Takenouchi, Akihiko Ohsuga: Anonymization of Sensitive Quasi-Identifiers for l-diversity and t-closeness, IEEE Transactions on Dependable and Secure Computing, to appear (2017) （査読有）

[5] Yuichi Sei and Akihiko Ohsuga: Location Anonymization with Considering Errors and Existence Probability, IEEE Transactions on System, Man, and Cybernetics: Systems, Volume: PP, Issue: 99, pp. 1-12, 2017, 10. 1109/TSMC. 2016. 2564928, （査読有）

[6] 芦川将之, 川村隆浩, 大須賀昭彦: クラウドソーシングワーカーの段階的育成方法の提案, 人工知能学会論文誌, Vol.32, No.3, pp.B-G81_1-13 (2017), 10.1527/tjsai.B-G81, （査読有）

[7] Yuichi Sei and Akihiko Ohsuga: Differential Private Data Collection and Analysis Based on Randomized Multiple Dummies for Untrusted Mobile Crowdsensing, IEEE Transactions on Information Forensics and Security, Vol.12, No.4, pp.926-939 (2017), 10.1109/TIFS.2016.2632069,（査読有）

[8] Yuichi Sei, Hiroshi Okumura, Akihiko Ohsuga: Privacy-Preserving Publication of Deep Neural Networks, Proc. of IEEE DSS, pp.1418-1425 (2016), 10.1109/HPCC-SmartCity-DSS.2016.0202, （査読有）

[9] Shusaku Egami, Takahiro Kawamura, Akihiko Ohsuga: Building Urban LOD for Solving Illegally Parked Bicycles in Tokyo, Proc. of ISW C2016, pp.291-307 (2016), 10.1007/978-3-319-46547-0_28, （査読有）

[10] Hiroyuki Nakagawa, Tatsuhiro Tsuchiya, “A Search-based Constraint Elicitation in Test Design”, IEICE Transactions on Information and Systems, Vol. E99-D, No. 9, pp. 2229-2238, 10.1587/transinf.2015KBP0010, (2016).

[11] 江上周作, 川村隆浩, 清雄一, 田原康之, 大須賀昭彦: 放置自転車問題解決に向けた循環型 LOD 構築システムの提案, 人工知能学会論文誌, vol.31, no.6, pp.AI30-K_1-12 (2016), 10.1527/tjsai.AI30-K（査読有）

[12] Masayuki Ashikawa, Takahiro Kawamura and Akihiko Ohsuga: Quality Improvement by Worker Filtering and Development in Crowdsourcing, Web Intelligence Journal, Vol.14, No.3, pp.229-244 (2016), 10.3233/WEB-160341（査読有）

[13] 本田耕三, 平山秀昭, 中川博之, 田原康之, 大須賀昭彦: ゴール指向洗練パターン駆動によるユースケースモデリング, 電子情報通信学会論文誌 J99-D(3), pp. 238-254, 2016（査読有）

[14] 佐々木隆益, 吉岡信和, 田原康之, 大須賀昭彦, 組込み向け進化型ソフトウェアの効率的な拡張性強化手法, 情報処理学会論文誌, Vol.57, No.2, pp.730-744, 2016（査読有）

[15] 川村 隆浩, 大須賀昭彦, TEXT2LOD ~テキスト情報の LOD 化に向けた Web API の開発~, 人工知能学会論文誌, Vol.31, No.1, 10.1527/tjsai.LOD-21, 2016（査読有）

[16] 清雄一, 稲葉緑, 大須賀昭彦, 安心できるプライバシ指標の調査, 情報処理学会論文誌, Vol.56, No.12, pp.

2230-2243，2015（査読有）
[17] 堀田大貴，本田耕三，平山秀昭，清雄一，中川博之，田原康之，大須賀昭彦，リファインメントパターンを利用したKAOS ゴールモデルから BPMN モデルへの変換，日本ソフトウェア科学会コンピュータソフトウェア，VOL.32，NO.4，pp. 141-160，2015（査読有）
[18] 清雄一,竹之内隆夫,大須賀昭彦，クラウド上の安全で高速なキーワード検索アルゴリズムの提案，情報処理学会論文誌，Vol.56，No.10，pp. 1977-1987，2015（査読有）
[19] 池尻恭介，清雄一，中川博之，田原康之,大須賀昭彦，意外性のあるレシピを推薦するエージェントの提案，電子情報通信学会論文誌，vol.j98-d，no.6，pp. 971-981，10.14923/transinfj.2014SWP0007，2015（査読有）
[20] 江上周作，川村隆浩，藤井章博，大須賀昭彦，BOM エージェントの実現に向けたLODの構築，電子情報通信学会論文誌，vol.j98-d，no.6，pp. 992-1004，10.14923/transinfj.2014SWP0019，2015（査読有）
[21] 横尾亮平,川村隆浩,清雄一,田原康之，大須賀昭彦，語句間の意味的リレーションに基づくキュレーションエージェント，電子情報通信学会論文誌，vol.j98-d，no.6，pp. 982-991，10.14923/transinfj.2014SWP0019，2015（査読有）
[22] 清雄一,大須賀昭彦，確率的ダミー生成による統計的な位置情報収集のためのプライバシ保護手法の提案，電気学会論文誌，vol.135，no.6，pp. 660-670，10.1541/ieejeiss.135.660，2015（査読有）
[23] 清雄一,大須賀昭彦，センシティブ属性値のランダムな追加による l-多様性アルゴリズムの提案，情報処理学会論文誌，Vol.56,No.5，pp. 1377-1387，2015（査読有）
[24] 坂野宏樹，中川博之，小島英春，土屋達弘，組み合わせインタラクションテストにおける BDD を用いた制約処理法の性能評価，電子情報通信学会論文誌，Vol. J98-D，No.3，pp. 384-395，10.14923/transinfj.2014PDP0032，2015（査読有）
[25] 岩崎祐貴，折原良平，清雄一，中川博之，田原康之，大須賀昭彦，CGM における炎上の分析とその応用，人工知能学会論文誌，Vol.30，No.1，pp. 152-160，10.1527/tjsai.30.152，2015（査読有）
[26] 吉岡信和，田辺良則，田原康之，長谷川哲夫，磯部祥尚，モデル検査による設計検証，日本ソフトウェア科学会コンピュータソフトウェア，Vol.31，No.4，pp. 40-65，10.11309/jssst.31.4_40，2014（査読有）
[27] 中村祐貴，本田耕三，中川博之，田原康之，大須賀昭彦，ソフトウェア再利用に向けた共通ゴール判別手法の提案，日本ソフトウェア科学会コンピュータソフトウェア，Vol.31，No.2，pp. 67-84，10.11309/jssst.31.2_67，2014（査読有）
[28] Mian Wang，Takahiro Kawamura，Yuichi Sei，Hiroyuki Nakagawa，Yasuyuki Tahara，Akihiko Ohsuga，Music Recommender Adapting Implicit Context Using ‘ renso ’ Relation among Linked Data，Journal of Information Processing，Vol.22，No.2，pp. 279-288，2014（査読有）

〔学会発表〕（計 43 件）

[1] 中川博之，自ら考え適応するソフトウェアの実現に向けて，大阪大学基礎工学部第 38 回公開講座「未来を拓く先端科学技術」(招待講演)，2016 年 8 月 4 日，大阪大学豊中キャンパス(大阪府豊中市)

〔その他〕

ホームページ等

大須賀・田原研究室

(http://www.ohsuga.lab.uec.ac.jp/)

６．研究組織

(1)研究代表者

田原 康之（TAHARA，Yasuyuki）

電気通信大学・大学院情報理工学研究科・准教授

研究者番号：３０３９０６０２

(2)研究分担者

清 雄一（SEI Yuichi）

電気通信大学・大学院情報理工学研究科・助教

研究者番号：２０７００１５７

中川 博之（NAKAGAWA，Hiroyuki）

大阪大学・大学院情報科学研究科・准教授

研究者番号：４０５０８８３４

大須賀 昭彦（OHSUGA，Akihiko）

電気通信大学・大学院情報理工学研究科・教授

研究者番号：９０３９３８４２

(3)連携研究者

なし

(4)研究協力者

なし