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　元 年　 ６ 月 ２５ 日現在

機関番号：１３６０１
研究種目：基盤研究(C)（一般）
研究期間：2016～2018
課題番号：１６Ｋ００９４

研究課題名（和文）モデルと制約に基づくソフトウェア開発に関する研究

研究課題名（英文）Software Development based on Models and Constraints

研究代表者
岡野　浩三（OKANO, KOZO）

信州大学・学術研究院工学系・准教授

研究者番号：７０２５２６３２

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）：要求仕様書からの状態遷移の導出方法について、ツールを具体的に作成した。形態素を構文解析し、全解析結果をXML形式で保持する。「話題沸騰ポット」の要求仕様記述の状態遷移記述に相当する仕様記述文章群に対して状態遷移の導出を行い、状態変数、状態遷移を高再現率で導出することに成功した。また、クラス図の類似性をクラスの属性から判断する方法を提案し、クラスの共通親クラスを音声合成でレビュー支援するシステムを作成した。再帰構造体を用いたプログラムに対するSAWを用いた振る舞い等価性検証手法を提案している。STAMP/STPAとモデル検査を統合した安全性検査について研究会等で発表を行っている。

研究成果の学術的意義や社会的意義
自然語要求記述からコンピュータで解析できる動作モデルを自動導出できることを限定されたドメインと記述スタイルであれば可能であることを示した。またプログラムコードレベルでの比較的小さな機能単位である関数が異なったアルゴリズムで同一の計算をしている場合に、その関数がリストやバイナリツリーのような再帰データを扱うような複雑なものであっても網羅的に動作の等価性を限定されたサイズ内で全自動で調べることはできることを示した。またこのようなモデル検査をSTAMP/STPAという安全検査手法と結びつける成果を一部提供できた。

研究成果の概要（英文）：We developed a tool to derive the state transitions from the requirement specification. Morphemes and parsing results are stored in XML format. The state transitions are derived from the specification description sentences of the "electric pot", and the state variables and the state transitions are successfully derived at a high recall rate. In addition, we proposed a method to determine similarity of class diagrams from class attributes, and developed a review support system where synthesized voice feedbacks the review results. We have proposed a behavioral equivalence verification method using SAW for a program using a recursive structure. We have also made presentations at safety analyzing methods integrated STAMP/STPA and model checking.

研究分野：ソフトウェア工学

キーワード：仕様記述　検証　モデル

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９、ＣＫ－１９（共通）

１．研究開始当初の背景

近年注目を浴びているサイバーフィジカルシステム(CPS) や IoT においては, 車載組み込みシステムや大量のデータを扱うソフトウェアシステムのように，高信頼性（安全性）と開発期間の短縮化の両方が望まれている．このようなシステムの設計においては仕様レベルでの品質保証が極めて重要である．ソフトウェアの上位仕様の品質保証ができたとしても，上位仕様と実際のコード記述には大きなギャップが存在し，一般には上位仕様の品質を，コード記述まで詳細化する過程で保証することは容易でない．そのギャップを埋めるために，モデル駆動開発技術やコード記述への検証技術が種々提案されている．コード記述に対する正しさの保証技術として，例えば，オブジェクトの特定のメソッド(equals メソッドや hashCode メソッド) についてその正しさを論理的に検査する技法が研究されており，研究代表者のグループでもその研究を行ってきた．一方，モデル駆動型開発では各記述レベルにおける成果物をそのメタモデルに基づき，自動変換できる技術をそのコアにしている．自動変換が主体であるため，人為的なバグを混入しにくいという特徴を持つ．研究代表者の研究グループでは通常のコード変換ではなく，仕様記述の変換を対象に，UML の標準アノテーション言語である OCL から Java のコードレベルでのアノテーション言語である JML への変換技術について研究を行ってきた．

２．研究の目的

安心・安全なソフトウェア開発を行うための，日本語仕様からの形式仕様記述導出，モデル検査技法を活用した開発方法を，モデル変換技術，モデル駆動開発と連動させて，総合的に確立していくことをこの研究の目的とする．

３．研究の方法

(1). 日本語で記述された仕様への形式的手法の適用可能性を調べる．具体的には日本語で記述された要求仕様記述に対して，以下を行い，日本語による要求仕様記述の解析方法論を考案する．また，変換過程の半自動化手法を確立する．

(a) 形態要素解析技術などの技術をもちいて中間記述表現に変換する(自然語仕様解析).

(b) 中間記述表現からモデル変換の技術をもちいてAlloy に変換する(自然語仕様変換).

(c) 変換された要求記述の論理的矛盾性や仕様記述の不完全性をAlloy のための論理解析ツールAlloy Analyzer を用いて検出する(仕様検査).

(2). モデルや制約指向を再利用したモデル駆動型開発によるコードの一部自動生成(コード生成),

(3). コードレベルでのモデル検査技術を活用したコード無矛盾性検証(コード検査),

(4). コードレベルでのモデル検査技術を活用した仕様発掘技術とBug Localization の研究(仕様発掘・バグ同定).

４．研究成果

要求仕様書から状態遷移を導出方法について状態変数と状態値を導出するツールを具体的に作成した。この導出にあたっては、単語の解析をkuromojiと呼ばれるJava用の日本語形態

素解析ライブラリを用いている。また導出された形態素をCYKアルゴリズムにより構文解析し、全解析結果をXML形式で内部表現として保持している。そこから状態変数候補、遷移条件候補、動作内容候補などを抽出する方法をとっている。また状態遷移記述用に文章構造を限定された構文を設定し、そこの構文で記述されていている前提で、SESSAMIが公開している「話題沸騰ポット」の要求仕様記述の状態遷移記述に相当する仕様記述文章群に対して状態遷移の導出を行い、状態変数、状態遷移まで高再現率で導出することに成功した。その結果を国際会議JCKBSE2018において発表した。
その後、各状態変数に対し状態値の獲得ができるよう中間表現のXML形式とプログラムの見直しを行い、ルールとXPATH表現でこれらの情報をフィルターリングするよう導出プログラムを改善した。また、概念モデルにおけるクラス図の類似性をクラスの属性使用用語から判断する方法を提案し、そのうえで、クラスの共通親クラスの設定をレビューとして音声合成するレビュー支援システムを具体的ツールとして作成し、評価実験を行った。属性使用用語から判断するために、kuromojiを用い、類似性判定にはjaccard距離を用いている。実装はAstah Proのプラグインの形で行った. これらの結果については2019年度に国際会議等で発表する。コードレベルの矛盾性検証についてはリストやバイナリツリーなど再帰構造体を用いたプログラムに対するSAWを用いた振る舞い等価性検証手法を提案している。
またSTAMP/STPAとモデル検査を統合した安全性確認についていくつか研究会等で発表を行っている。

５．主な発表論文等

〔雑誌論文〕（計 2 件）

(1) Kozo Okano, Shinji Kusumoto, and Yukihiro Sasaki: “Effective Derivation of a Mapping of Variables in a Loop Structure,” International Journal of Informatics Society, Vol.10, No.2, pp.75-83 (2018) 査読あり

(2) Chikyu Yanagisawa, Shinpei Ogata, and Kozo Okano: “On the Generation of Human-oriented
Counter-examples using a Test Automaton,”
International Journal of Informatics Society, Vol.9, No.1, pp.41-50 (2017) 査読あり

〔学会発表〕（計 11 件）

(1) 岡野浩三, 楊盼, 辛島凛, 小形真平:“STAMP/STPA における振舞いモデル記述の効用について” ウィンターワークショップ2019・イン・福島飯坂(2019-01) 査読なし

(2) 岡野浩三, 楊盼, 辛島凛, 小形真平:“STAMP/STPAとモデル検査との連携について—

鉄道踏切「とりこ検知」例題をもとに—” 第3 回STAMP ワークショップ(2018-12) 査読なし

(3) 辛島凛, 原内聡, 小形真平, 岡野浩三: “再帰的な構造体を用いたプログラムに対するSAWを用いた振る舞い等価性検証手法の考案と評価”, 日本ソフトウェア科学会「ソフトウェア工学の基礎」研究会第15 回ワークショップFOSE2018, レクチャーノート・ソフトウェア学44 ソフトウェア工学の基礎XXV, pp.91-96 (2018-11) 査読あり

(4) Kozo Okano, Satoshi Harauchi, Shin Maruyama, and Shinpei Ogata: “Applying SAW to regression verification for C functions with recursive data structure,” Proceedings of International Workshop on Informatics 2018 (IWIN2018), pp.125-132 (September 2018) 査読あり

(5) Kozo Okano, Kazuma Takahashi, Shinpei Ogata, and Toshifusa Sekizawa: “Analysis of Specification in Japanese using Natural Language Processing,” Proceedings of the 12th Joint Conference on Knowledge-Based Software Engineering (JCKBSE 2018), pp.12-21, Springer (August 2018) 査読あり

(6) 楊盼, 辛島凛, 小形真平, 岡野浩三: “STAMP/STPA の鉄道踏切「とりこ検知」例題に対するモデル検査適用と考察”, 電子情報通信学会技術研究報告, Vol.118, No.137, pp.31-36 (2018-9) 査読なし

(7) 岡野浩三, 小形真平, 楊盼, 岡本圭史: “STAMP/STPA 単線列車例題に対する時間オートマトンモデル検査の適用と考察”, 電子情報通信学会技術研究報告, Vol.117, No.477, pp.1-6 (2018-3) 査読なし

(8) 岡野浩三, 高橋一真, 仲悠介, 小形真平, 関澤俊弦: “自然語解析技術を用いた和文要求仕様の解析と音声によるレビュー支援法”, 電子情報通信学会技術研究報告, Vol.117, No.465, pp.79-84 (2018-3) 査読なし

(9) 丸山森, 原内聡, 小形真平, 岡野浩三: “再帰構造体に対するsaw を用いた有界検証手法の考察” 第24 回ソフトウェア工学の基礎ワークショップFOSE2017 (2017-11) 査読あり

(10) Kozo Okano, Shinji Kusumoto, and Yukihiro Sasaki: “Derivation of a map of variables in a loop structure,” Proceedings of International Workshop on Informatics 2017 (IWIN2017), pp.129-134 (September 2017) 査読あり

(11) 田幸玄陽, 小形真平, 岡野浩三, 関澤俊弦: “Kuromoji と構文解析による要求仕様書から状態遷移系への自動変換の試み”, ウィンターワークショップ2017・イン・飛騨立山論文集, pp.45-46 (2017-01) 査読なし

〔図書〕（計　0 件）

〔産業財産権〕
○出願状況（計 0　件）

○取得状況（計 0　件）

〔その他〕

６．研究組織

(1)研究分担者

研究分担者氏名：関澤　俊弦
ローマ字氏名：Toshifusa Sekizawa
所属研究機関名：日本大学
部局名：工学部
職名：准教授
研究者番号（8 桁）：10549314

研究分担者氏名：小形　真平
ローマ字氏名：Shinpei Ogata
所属研究機関名：信州大学
部局名：学術研究院工学系
職名：助教
研究者番号（8 桁）：10589279

(2)研究協力者