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　 ５ 月 ２８ 日現在

機関番号：３２６７５
研究種目：基盤研究(A)（一般）
研究期間：2014～2018
課題番号：２６２４０００８

研究課題名（和文）ソフトウェア開発の高信頼アジャイル形式工学手法に関する研究

研究課題名（英文）Research on Highly Reliable Agile Formal Engineering Methods

研究代表者
劉　少英（LIU, Shaoying）

法政大学・情報科学部・教授

研究者番号：９０２６４９６０

交付決定額（研究期間全体）：（直接経費）　　22,000,000円

研究成果の概要（和文）：本研究では、既存のソフトウェア開発手法の短所を大幅に改善して、生産性と信頼性を共に確保する最新のソフトウェア開発技術とした「SOFLアジャイル形式工学手法」を確立して、次の具体的な成果を達成した。（１）SOFLアジャイル形式工学手法のフレームワーク、（２）SOFL仕様のアニメーション化手法、（３）仕様アニメーションとプログラムのテスト用のテストデータの自動生成手法とアルゴリズム、（４）定理証明とモデル検査の融合技術とアニメーション化手法,（５）仕様アニメーションの可視化表現手法、（６）仕様アニメーションの支援ツールとテストデータの自動生成の支援ツールのプロトタイプの開発。

研究成果の学術的意義や社会的意義
本研究はソフトウェアの進化による開発手法と形式仕様記述によるソフトゥエア開発手法を適切に統合することによって双方の利点を生かすことができ、実用性がより高い厳密的なソフトウェア開発手法を確立することで、ソフトウェア工学方法論を大きく前進させ、将来のソフトウェア工学の発展の新たな方向を示すことができ、学術的意義が大きい。
一方、このような新しいソフトウェア開発手法が企業で採用されることによって、IT産業の生産性を向上させることができ、開発されるソフトウェアの信頼性の確保も可能であるため、より安全安心なシステムと社会を構築することが可能になる。

研究成果の概要（英文）：In this research, we have established a new technology known as SOFL Agile Formal Engineering Method that significantly improves the existing software development methods in terms of offering a great capability of enhancing both software productivity and reliability. Specifically, the technology includes the following aspects:
(1) a framework of the SOFL Agile Formal Engineering Method, (2) a new method for carrying out the animation of hybrid specifications, (3) a new method and the related algorithms for automatically generating test data for both specification animation and specification-based program testing, (4) a method for combining theorem proving with model checking and a tool support for model checking process animation, (5) prototypes of software tools to support the automatic test data generation for both specification animation and specification-based program testing.

研究分野：ソフトウェア工学

キーワード：アジャイル開発手法　形式工学手法　ハイブリッド仕様　仕様アニメーション　ソフトウェアテスト　ソフトウェア検証　ソフトウェア品質保証　高信頼ソフトウェア開発

１．研究開始当初の背景

自動運転車、新幹線、飛行機、インターネット、携帯電話など様々な現代の先進技術を安全安心に利用するために、その中で採用されたソフトウェアシステムにおいて欠陥がないことが重要である。誤った要求・設計仕様は、欠陥を引き起こす、ソフトウェア開発コストを増大する主因だと見られている。この問題に対応するために、モデル駆動、アジャイル、形式手法、形式工学手法などいくつかのソフトウェア開発手法が提案されている。

モデル駆動開発手法では、モデルを作成した上で、ソフトウェアの実装を行う。メリットはシステムの機能や性質などを十分に理解した上で実装を行うことで、要求された機能と制約などを満たさない間違いを避けることが可能である。デメリットとしては、モデルと実装されたコードとの一致性を守るために、モデルとコードを頻繁に修正する必要がある。その結果、費やされる時間と労力が大きくなってしまう。アジャイル開発手法では、進化的なプロトタイピングアプローチを強調し、動くソフトウェアシステムを構築しながらカスタマとのコミュニケーションを強め、カスタマの要求を正しく理解する上で、システムを更に進化させ、静的なレビューと動的なテストによって構築されたソフトウェアの検証を行う。この手法は、モデルとコードの一致性を守る作業の必要がないため、時間とコストを節約できるけれども、大規模ソフトウェアの進化には、コードの理解に工夫が必要で手間がかかる可能性が高く、新たな欠陥をシステムに導入しやすい傾向がある。形式手法は論理学や代数など数学に基づく設計された形式仕様記述言語を用いて、ソフトウェアシステムの機能仕様と非機能的な制約を明確に定義した上で､厳密な検証を行いながら､正しさを保証するプログラムを作成することができる。但し、大規模複雑なソフトウェア開発への適用は困難であるため、現実に利用されたケースが少ない。この問題点を解決するために、形式工学手法という厳密的かつ系統的に使いやすいソフトウェア開発手法が提案された。形式工学手法は、分かりやすい形式仕様を系統的に作成した上で、仕様に基づくプログラムの作成、厳密的な検査（インスペクション）、および厳密的なテストを行うことを強調している。その代表的な事例は､本研究者が設計した SOFL(Structured Object-Oriented Formal Language) 形式仕様記述言語を基に形成された SOFL 手法である。条件データフロー図（CDFD）とモジュールを利用するため、形式仕様の作成は従来の形式仕様より簡易になっているが、実務者にとってまだバリアが高い。

２．研究の目的

本研究では、高生産性と高信頼性を共に達成することが可能である「アジャイル形式工学手法」という新たなソフトウェア開発手法の確立を目指す。具体的には、次の目標を達成する。（１）アジャイル形式工学手法の基本原理を確立する。（２）仕様の自動又は半自動アニメーション化技術を提案する。（３）仕様アニメーション用テストデータの自動生成手法とアルゴリズムを開発する。（４）定理証明ならびにモデル検査の短所を緩和する技術を提案する。（５）アニメーションの中で操作の振る舞いの可視化表現方法とテストデータ生成プロセスの可視化技術を開発する。（６）仕様パターンを提案し、パターンにより仕様を作成かつ進化する手法を確立する。（７）仕様アニメーションとテストデータの自動生成手法の支援ツールのプロトタイプを開発する。

３．研究の方法

SOFL 形式仕様記述言語と代数に基づく仕様言語（代数仕様言語）CafeOBJ に基づき、前述した課題を研究してきた。

アジャイル形式工学手法の基本原理を確立するために、既存のアジャイル手法のマニフェ

ストに提案された四つのソフトウェア開発の基本原則と SOFL 形式工学手法を適切に統合することを研究してきた。形式仕様の理解し難い問題を緩和するために、GUI,半形式仕様および形式仕様を融合したハイブリッド仕様の新しい概念を創出、各種の仕様方式の構造、構文、役割、および作成方法などを設計した。また、仕様のモジュール単位によってプログラムを増分的に構築しながら、構築されたプログラムで厳密な検査とテストを行うという小さな開発サイクルを提案した。仕様の自動又は半自動アニメーション化技術に関しては、SOFL 仕様の条件データフロー図 CDFD によって全ての機能シナリオを自動的に抜き出して、その上で機能シナリオごとにアニメーションを行う技術を明らかにした。一つの機能シナリオは、CDFD の入力から出力までの一つのデータフローパスである。このような機能シナリオのアニメーションというのは、関連する入力変数に具体的な値を代入し、機能シナリオに含まれる操作の形式仕様によって出力変数の期待される値を生成するプロセスを動的に表現することである。仕様アニメーション用テストデータの自動生成手法およびアルゴリズムを開発するために、操作の事前条件と事後条件を生かして、原子述語、複合述語、各データ型に定義された演算子が含まれる述語論理式を満たすことによってテストデータの生成方法とアルゴリズムを開発した。

定理証明ならびにモデル検査の短所を緩和する技術を提案するために、代数に基づく仕様言語（代数仕様言語）ならびにそれらの処理系 CafeOBJ と Maude を用いる。CafeOBJ と Maude は、OBJ3 の直接の後継言語である。Maude は、仕様言語のみならず、ソフトウェアツールのプロトタイプを開発可能なプログラミング言語の側面も併せ持つ。主に Maude を用いて、ソフトウェアツールの開発ならびに事例研究を行った。

アニメーションの中で操作の振る舞いの可視化表現方法とテストデータ生成プロセスの可視化技術を開発するため、入力と出力のデータ項目の構造と特徴、入力と出力の対応関係、および述語論理式を満たすテストデータの生成プロセスを GUI と動画によって可視化を達成した。主な研究課題は、各種機能の可視化の表現方法と可視化の効果の測定である。仕様パターンの定義とパターンにより仕様を作成かつ進化する手法に関しては、アルゴリズムに使われる基本的な操作、例えば、検索、ソート、算術計算、データの比較などを SOFL 言語で表現する様々な可能な仕様パターンをデータ型に分けて定義、その上で、仕様パターンを適用するプロセスの中で必要な仕様の表現を引き出す。仕様アニメーションとテストデータの自動生成手法の支援ツールのプロトタイプを開発するために、C#と Java 言語を用いて、SOFL 仕様アニメーションの支援ツールおよびテストデータの自動生成手法の支援ツールを研究開発してきた。仕様アニメーションの支援ツールでは、CDFD から機能シナリオを自動的に抽出し、選択された機能シナリオのアニメーションプロセスをコントロール、関連する入出力の可視化を適切に表現するなど機能を支援する。仕様アニメーションのために必要なテストデータの自動生成の支援ツールでは、集合、列、写像など各データ型に定義された演算子を含む原子述語と複合述語論理式を満たす、特に論理積を満たすテストデータの自動生成プロセスの可視化表現を実現し、テストデータの生成が成功か失敗かを自動的に示す機能を支援する。

以上の各課題の研究には、事例研究から始め、理論分析を加え、その上でより大きい規模の事例研究と実験を行い、提案された概念または開発された技術の実用性と効果を評価した。

４．研究成果

本研究では、既存のソフトウェア開発手法の短所を大幅に改善して、生産性と信頼性を共に確保する最新のソフトウェア開発技術とした「SOFL アジャイル形式工学手法」を確立し、次の具体的な成果を達成した。

（1）SOFL アジャイル形式工学手法のフレームワークを確立した。このフレームワークでは、使いやすい「三段階技術」で分かりやすいハイブリッド仕様を作成した上で、仕様によりプログラムを増分的に実装しながら、自動的または半自動的な検査とテストによりエラーを検出する開発プロセスを実現できる。（2）SOFL 仕様のアニメーション化手法を設計した。この手法で仕様のアニメーションを二つのレベルで行う。まず、モジュールに定義された操作間の依存関係を定義する CDFD から、全ての可能なシステム機能シナリオを自動的に抽出する。一つのシステム機能シナリオは、CDFD の入力から出力まで関連操作の実行序列である。次は、抽出されたシステム機能シナリオ一つずつに対してアニメーションを行う。アニメーションは、構文レベルのアニメーションと意味レベルのアニメーションに分けて実施される。（3）仕様アニメーションとプログラムのテスト用のテストデータの自動生成手法とアルゴリズムを開発した。操作の事前条件と事後条件によって形成された機能シナリオ群を基に仕様アニメーション用テストデータおよび実装されたプログラムのテスト用テストデータと共に生成するカバレッジ基準が定義された。この上で、機能シナリオから入力変数のみが含まれるテスト条件を抜き出し、そのテスト条件を原子述語、論理積、論理和に分割して、それぞれの述語論理式によってテストデータを自動生成するアルゴリズムが開発された。（4）定理証明とモデル検査の融合技術とアニメーション化手法を提案した。Maude 言語を用いて CafeOBJ 証明支援系を含む CafeOBJ を実装した上で、証明スコアから証明支援系用の証明スクリプトを自動生成した。分散相互排除プロトコルや通信プロトコルが公平性のもとで活性を満たすことをモデル検査に適用することで有用性を確認し、事例研究を行ってきた。（5）仕様アニメーションの可視化表現手法を提案した。これは次の三つのレベルのアニメーションの可視化表現手法を提案した。第一に、CDFD から抽出されたシステム機能シナリオのアニメーションの可視化表現である。このレベルの可視化表現では、操作の入力と出力の関係を仕様の構文による可視化表現を実現する。第二に、一つの操作の入力と出力の対応関係の可視化表現である。第三に、様々な型の入力と出力データの可視化表現である。特に、変数のデータの可視化では、SOFL 言語の様々なデータ型およびその型に定義された演算子の効果の可視化表現方法も実現した。また、データ項目の可視化を実施しながら、そのデータ項目の性質について自動的に生成された音声解釈も実現した。（6）仕様アニメーションの支援ツールとテストデータの自動生成の支援ツールのプロトタイプを開発した。仕様アニメーションの支援ツールでは、形式仕様の CDFD からシステム機能シナリオの自動抽出、一つの機能シナリオのアニメーション、およびデータ項目のアニメーションなど機能を実現した。また、操作の事前条件と事後条件の内容とその操作の入出力の多重ポートの構造を自動的に分析し、アニメーション用の入力と出力のテストデータの自動生成アルゴリズムを開発した。この自動生成手法とアルゴリズムは、仕様により実装したプログラムのテストにも適用できる。この上で、仕様に基づく実装されたプログラムの自動テストのために、テストスクリプトの自動生成、テスト結果の自動分析などの機能を支援ツールに加えた。

５．主な発表論文等

〔雑誌論文〕（計　11　件）全て査読有

① Adrian Riesco, Kazuhiro Ogata, “Prove it! Inferring Formal Proof Scripts from CafeOBJ Proof Scores”, ACM Transactions on Software Engineering and Methodology (ACM TOSEM), 27(2), 2018, pp. 6:1-6:32.

② Yu Chen and Shaoying Liu, “DESIGN AND IMPLEMENTATION OF AUTOMATED VISUALIZATION FOR INPUT / OUTPUT FOR PROCESSES IN SOFL FORMAL

SPECIFICATIONS", International Journal of Software Engineering & Applications (IJSEA), 9(4), 2018, pp. 139-157.

③ Kazuhiro Ogata, "Model Checking the iKP Electronic Payment Protocols", Journal of Information Security and Applications, No. 36, 2017, pp. 101-111.

④ Adrian Riesco, Kazuhiro Ogata, Kokichi Futatsugi, "A Maude Environment for CafeOBJ", Formal Aspects of Computing, Springer, 29(2), 2017, pp. 309-334.

⑤ Mo Li and Shaoying Liu, "Integrating Animation-Based Inspection into Formal Design Specification Construction for Reliable Software Systems", IEEE Transactions on Reliability, 65(1), 2016, pp. 88-106.

〔学会発表〕(計 50 件) 全て査読有

① Shaoying Liu, "Agile Formal Engineering Method for Software Productivity and Reliability", The 14th Central and Eastern European Software Engineering Conference Russia (CEE-SECR 2018), ACM press, Moscow, 2018, pp. 64-69.

② Ha Thi Thu Doan, Francois Bonnet, Kazuhiro Ogata, "Specifying a Distributed Snapshot Algorithm as a Meta-program and Model Checking it at Meta-level", 37th IEEE International Conference on Distributed Computing Systems (37th ICDCS), IEEE press, Atlanta, 2017, pp.1586-1596.

③ Tam Thi Thanh Nguyen, Kazuhiro Ogata, "Graphical Animations of State Machines", 15th IEEE International Conference on Dependable, Autonomic and Secure Computing (15th DASC), IEEE Press, Orlando, 2017, pp.604-611.

④ Xuan-Linh Ha, Kazuhiro Ogata, "Writing Concurrent Java Programs Based on CafeOBJ Specifications", 24th Asia-Pacific Software Engineering Conference (APSEC 2017), IEEE press, Nanjing, 2017, pp.618-623.

⑤ Shaoying Liu, "Testing-Based Formal Verification for Theorems and Its Application in Software Specification Verification", Proceedings of 10th International Conference on Tests and Proofs (TAP 2016), Springer, Vienna, 2016, pp. 112-129.

⑥ Shaoying Liu, Xi Wang, and Weikai Miao, "Supporting Requirements Analysis Using Pattern-Based Formal Specification Construction", 17th International Conference on Formal Engineering Methods (ICFEM 2015), Springer, Paris, 2015, pp. 100-115.

⑦ Shaoying Liu, "Automatic Selection of System Functional Scenarios for Formal Specification Animation", 22nd Asia-Pacific Software Engineering Conference (APSEC 2015), IEEE CS Press, New Delhi, 2015, pp. 72-79.

〔図書〕(計 5 件)

① Kazuhiro Ogata, Mark Lawford, and Shaoying Liu (eds), "Formal Methods and Software Engineering", 18th International Conference on Formal Engineering Methods (ICFEM 2016), LNCS 10009, Springer, Tokyo, Japan, Nov. 14-18, 2016, No. of Pages: 508.

〔招待講演〕（計　3　件）

① Shaoying Liu, “Testing and Inspection for Software Quality Assurance”, 2015 IEEE International Conference on Software Quality, Reliability & Security (QRS 2015), Vancouver, Canada, 2015.

② Shaoying Liu, “Testing-Based Formal Verification: A New and Practical Approach for Software Quality Assurance”, 19th International Conference on Engineering of Complex Computer Systems (ICECCS 2014), Tianjin, China, 2014.

６．研究組織

(1) 研究分担者
研究分担者氏名：児玉　靖司
ローマ字氏名：（KODAMA, yasushi）
所属研究機関名：法政大学
部局名：経営学部
職名：教授
研究者番号（8 桁）：30266910

研究分担者氏名：緒方　和博
ローマ字氏名：（OGATA, kazuhiro）
所属研究機関名：北陸先端科学技術大学院大学
部局名：先端科学技術研究科
職名：教授
研究者番号（8 桁）：30272991

研究分担者氏名：荒木　啓二郎
ローマ字氏名：（ARAKI, keijiro）
所属研究機関名：熊本高等専門学校
部局名：
職名：校長
研究者番号（8 桁）：40117057

(2) 研究協力者
研究協力者氏名：玉井　哲雄
ローマ字氏名：（TAMAI, tetsuo）

研究協力者氏名：二木　厚吉
ローマ字氏名：（FUTATSUGI, kokichi）

研究協力者氏名：中島　震
ローマ字氏名：（NAKAJIMA, shin）

研究協力者氏名：粂野　文洋
ローマ字氏名：（KUMENO, fumihiro）

および他の２２名の研究者と大学院生