論文名: Integrating Animation-Based Inspection Into Formal Design Specification Construction for Reliable Software Systems
著者名: Mo Li and Shaoying Liu
掲載雑誌名: IEEE Transactions on Reliability, 65(1), pp. 88~106, 2016

概要:

形式仕様記述はソフトウェアの高信頼性を獲得するための有効な手段であり、設計の品質および信頼性を各段向上させることができる。しかしながら、形式仕様においては仕様記述言語を用いた複雑な数理表現が必要とされるため、実際には設計者とユーザ間のコミュニケーションを可視化することが難しく、しかも形式仕様の妥当性を正確に検証することも困難であることが長年の課題であった。

この問題点を現実的に解決するために、本論文では、仕様のアニメーションに基づくインスペクション技術を形式仕様記述過程に融合し、設計者とユーザ間のコミュニケーションを可視化することに成功しており、さらに形式仕様の妥当性の検証をより効率的に行うための新たな手法を提案している。具体的には、形式仕様アニメーション技術をインスペクションの reading 技術として利用し、ソフトウェアの形式設計仕様を進化しながら仕様の妥当性の検証を行うための基本原理と応用技術を提案している。この中で、形式仕様の妥当性はユーザ要求を反映する非形式仕様および形式仕様の一致性によって定義されている。このような妥当性性質は、形式仕様の中で関連する形式表現のアニメーションを実施しながらその内容が正しいかどうかを厳密的にインスペクションし、含まれたエラーを検出する。また、提案手法を実務において有効に使用するために、ソフトウェア支援ツールを開発しており、その構造や機能などを分かりやすく解説している。最終的に、開発された支援ツールを用いた事例研究を通じて、支援ツールと提案手法が実際の形式仕様に対して有効に機能することが示されている。

本論文の学術的に貢献する点は、次の三つである。第一に、仕様アニメーションを用いることで、厳密なインスペクション技術をシステム設計の形式仕様作成過程に統合し、設計者とユーザ間のコミュニケーションを可視化するとともに、形式仕様の妥当性も検証できるアジャイル形式仕様作成手法を世界に先駆けて確立した。第二に、形式仕様アニメーション化技術とソフトウェア品質を保証するインスペクション技術を有機的に統合し、実行できないソフトウェア仕様と設計を厳密かつ正確に検証するアプローチを提案した。第三に、提案されたアニメーションに基づくインスペクション技術の支援ツールのプロトタイプを開発し、ソフトウェアの信頼性向上に向けた実践的なプラットフォームを確立した。

本論文では重要な学術進歩を達成したが、大規模ソフトウェア開発への適用性を向上させるために改善しなければならない問題点が残っている。一つは開発された支援ツールの機能を入出力データのアニメーションや形式数理式のアニメーションなどまで更に拡大し、ツールの品質も改善することが必要である。もう一つは実際のソフトウェア開発現場で提案された技術を客観的に評価することが必要である。