法政大学学術機関リポジトリ
HOSEI UNIVERSITY REPOSITORY

PDF issue: 2025-02-05

A Systematic Inspection Approach to Verifying and Validating Formal Specifications based on Specification Animation and Traceability

LI, Mo / 李, 漠

(開始ページ / Start Page)
1
(終了ページ / End Page)
226
(発行年 / Year)
2015-09-15
(学位授与番号 / Degree Number)
32675甲第367号
(学位授与年月日 / Date of Granted)
2015-09-15
(学位名 / Degree Name)
博士(理学)
(学位授与機関 / Degree Grantor)
法政大学 (Hosei University)
(URL)
https://doi.org/10.15002/00012841

博士学位論文
論文内容の要旨および審査結果の要旨

氏名	李　漠
学位の種類	博士（理学）
学位記番号	第 585 号
学位授与の日付	2015 年 9 月 15 日
学位授与の要件	法政大学学位規則第 5 条第 1 項第 1 号該当者（甲）
論文審査委員	主査　教授　小池　誠彦
	副査　教授　劉　　少英
	副査　教授　雪田　修一
	副査　教授　藤田　悟

A Systematic Inspection Approach to Verifying and Validating Formal Specifications based on Specification Animation and Traceability

１．論文内容の要旨

本論文はソフトウエアのフォーマルな要求定義記述を検証し妥当性チェックを行うため、その前工程とも言える構造化された自然言語で書かれたインフォーマルな要求記述と照らし合わせながら、フォーマル記述の不備、不整合、欠けなどを発見するためのシステム的なインスペクション方式を提案している。フォーマルな要求定義記述を実際に“形式的に実行”することで、とりうる全ての振舞いをアニメーション（シナリオ）として抽出し利用者に提示することで仕様の誤りや欠けを発見することを可能とした。さらにフォーマル要求仕様記述とインフォーマル要求仕様記述の間の対応関係をシステムが把握することができるので、未チェックな要求があればチェックリストとしてシステムが提示し利用者が答える形で、妥当性のあるフォーマル要求定義記述を得ることを可能とするソフトウエアシステム（フレームワーク）を開発している。

システム的なインスペクションとは、構造化された自然言語で書かれたインフォーマル記述とコンディション・データーフロー・ダイヤグラム（CDFD:　Condition Data Flow Diagram）で表現されるフォーマル記述とを突き合わせることで、インフォーマル/フォーマル記述間を追跡し対応づけが可能であることに着目し、仕様記述の不備、不整合などをシステムが指摘するものである。利用者と対話形式に追跡を行いながら、インフォーマル記述とフォーマル記述の整合をとって行く。システムが不整合や未確認な記述を検出すると利用者に質問として対応を求め、その結果が記述に反映されていく。

得られた、フォーマル記述は、CDFD のネットワークに表現されているので形式的に実行が可能となる。この CDFD を流れる実行可能な個々の流れがそれぞれシナリオに対応することになる。本論分ではこのシナリオをアニメーションと呼ぶ。入出力データは形式的（数学的に正確）に記述されているので、実際に実データ群を流す必要が無く効率が良い。従い全てのアニメーションを洗い出すことが可能になる。利用者はそのアニメーションの結果を履歴として GUI で確認できるので未検証なシナリオが容易に発見できる利点がある。CDFD 記述は階層化を前提としているので、それぞれの階層で適切なモジュール（プロセス）の数の繋がりとして切り出して解析できるので提案システムは実用性の面でも規模が大きくなっても有効であると言える。

さらに上記機能を組み込んだ対話的なインスペクション・システムのプロトタイプを構築している。コードサイズはＣ＃で数万行にも及び、SOFL ツール支援システムとして学生の利用に供されている。このフレームワーク上で、複数の仕様バグが混入された例題をについて実際に 55 人の学生が参加し評価実験を行っている。学生群を 3 つに分け、1）経験有で従来のチェックリストによるインスペクション、2）経験有で提案手法のアニメーション/インスペクション、3）初学生が本提案システムを使った場合に分け、バグの発見率で比較し提案手法の有効性を示している。

２．審査結果の要旨

本論文の目的は要求分析・定義過程における困難な作業を軽減させ、後段のソフトウエア設計工程にバグのない仕様を与えるためにインフォーマル仕様記述手法とフォーマル仕様記述手法を融合させた研究である。インフォーマル仕様記述とフォーマル仕様記述の２つを作成することはかなりな負担を利用者に要求することになるが、提案手法によりインフォーマル/フォーマル記述の間の追跡性を可能にし、システムが絶えず仕様間の関係を追跡することができるので、仕様の漏れや誤りを指摘し対話式に修正することが可能となる。また、フォーマル仕様記述は CDFD の形で表現されており、形式的に実行可能であるので、全ての動的な振舞い（シナリオ）をアニメーションと言う形で効率良く切り出すことができるので仕様の漏れや誤りも容易に発見可能となる。このアニメーション機能とトレースに基づくインスペクションの自動化によりフォーマル仕様記述の有用性をアピールすることができたと言える。
さらに、Ｃ＃で数万行に及ぶプロトタイプシステムを開発し、実際にバグが混入された仕様記述を用いて、多数の学生を実験に参加させバグ発見率の指標で提案手法の有効性を実証したことは、実用性の面でフォーマル手法の有用性を示したこととして意義深いと言える。また本人がプログラミング能力など幅広い技術と深い知識を有していることも窺える。

先に行われた予備審査会、および予備審査小委員会会議で指摘された事項に関しては、提出された本論文および、6 月 12 日に行われた公聴会においていずれも、正しく加筆修正が行われていることを確認した。

以上のことより，本審査小委員会は全会一致をもって提出論文が博士（理学）の学位に値するという結論に達した。

（報告様式Ⅲ）