| | | | |
|---|---|---|---|
| 氏名 | 吉田裕之 | | |
| 学位の種類 | 博士(情報科学) | | |
| 学位記番号 | 博情第358号 | | |
| 学位授与年月日 | 平成29年3月24日 | | |
| 論文題目 | An Interactive Theorem Proving Framework for Declarative Cloud Orchestration | | |
| 論文審査委員 | 主査 二木 厚吉 | 北陸先端科学技術大学院大学 | 特任教授 |
| | 緒方 和博 | 同 | 教授 |
| | 青木 利晃 | 同 | 教授 |
| | 廣川 直 | 同 | 准教授 |
| | 中島 震 | 国立情報学研究所 | 教授 |

## 論文の内容の要旨


An interactive theorem proving framework for verifying declarative cloud orchestration is proposed.

Recent rapid progress of cloud computing accelerates the whole life cycle of system usage and requires much flexible automation of system operations. Automation of cloud system operations is called cloud orchestration and correctness of cloud orchestration becomes much crucial for many activities in the hu- man society. However, correctness of automated cloud system operations cannot depend on testing-based quality control because a cloud system is a kind of distributed systems and it is not possible to exhaus- tively test all of its behavior which may occur at various situations in the production environment. Formal approaches are expected to provide systematic ways to guarantee correctness of cloud orchestration.

Formal approaches are mainly classified into two categories, model checking and theorem proving. As opposed to model checking, theorem proving can verify models of arbitrary many number of states and so suitable for proving absence of counter examples. However, when applying to practical problems it requires many human efforts to develop proofs.

This dissertation proposes a framework of interactive proof development for a kind of liveness properties, leads-to property, of cloud orchestration. We say “framework” to mean something like an application framework of software development which brings high productivity by minimizing development efforts and high maintainability by consistent structure of application software.

The proposed framework provides (1) a general way to formalize specifications of different kinds of cloud orchestration tools and (2) a procedure for how to verifying a kind of liveness properties, as well as invariant properties, of formalized specifications. It also provides (3) general templates and libraries of formal descriptions for specifying orchestration of cloud systems and (4) proved lemmas

for general predicates of the libraries to be used for verification.

The framework has been applied to the verification of specifications of AWS CloudFormation and also of OASIS TOSCA, and is demonstrated to be effective for reducing generic routine work and making a verification engineer concentrate on the work specific to each individual system. The case study of OASIS TOSCA shows that the framework can be used to specify, represent, and verify the behavior models of TOSCA where the standard has not yet provided any ways to do so. It also shows a general way to manage dependencies of cloud resources which is a smarter one than that of the most popular tool, CloudFormation.

The major contributions of this dissertation are that (1) it introduces the idea of frameworks from software development to proof development which results in high productivity and high maintainability of proofs and (2) it shows that the framework can be effectively applied to a non-trivial problem, that is, to specify, represent, and verify the behavior models of the standard specification language of cloud orchestration.

Key Words: Cloud Orchestration, System Specification/Verification, Theorem Prov- ing, Framework, Proof Scores, CafeOBJ

## 論文審査の結果の要旨

本論文は、クラウドオーケストレーションという今日的で重要な応用領域に焦点を当て、オブジェクトモデルに基づく形式仕様開発法と仕様検証法を、仕様と証明の再利用性を高める定理証明フレームワークという枠組みとして研究開発した研究成果について述べている。

クラウドサービスの急速な進展にともない、クラウドオーケストレーションと呼ばれるクラウドシステム構築操作の自動化の重要性が高まっている。クラウドシステム構築操作の自動化はテストにより信頼性を確保するのが困難であり、形式検証によりその信頼性を確保することが期待される応用領域である。

システムの性質を前提条件に基づき演繹的に証明する定理証明は、全数検索による反例発見を基本原理とするモデルチェッキングに比べて、より精密な検証ができる利点はあるが、検証者の適切な支援を必要とし証明開発に多くの手間を要するという難点がある。本論文は、定理証明のこの難点を克服すべく、ソフトウェア開発において有効な枠組みとされるフレームワークの考え方を定理証明に導入し、クラウドシステム構築操作の不変性(invariant)と到達可能性(leads-to property)の証明に適用可能であることを実証的に示している。

提案される定理証明フレームワークは、(1)種々のクラウドオーケストレーションの形式化の方法、(2)到達可能性の証明手順、(3)クラウドオーケストレーションの仕様開発に必要な汎用仕様ライブラリ、(4)その汎用リブラリに関する補助定理、などから成り、CafeOBJ 仕様言語システムのライブラリとしてウェッブページ上に公開され、ひろく利用可能な形で公開されている。

本論文では、提案したフレームワークがクラウドオーケストレーションの国際標準であるOASIS TOSCA などに適用した成果が報告され、その有効性が示されている。

以上、本研究は、ソフトウェア開発において効果を上げているフレームワークの枠組みをシステム検証のための定理証明領域に導入し、その有用性をクラウドオーケストレーションという重要な応用領域において実証したものであり、学術的に貢献するところが大きい。よって博士（情報科学）の学位論文として十分価値あるものと認めた。