An Interactive Theorem Proving Framework for Declarative Cloud Orchestration

Hiroyuki Yoshida
School of Information Science,
Japan Advanced Institute of Science and Technology

March 2017

Abstract

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 human 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 exhaustively 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 Proving, Framework, Proof Scores, CafeOBJ**