Case Studies with a Combined Formal System Verification Technique

Weiqiang Kong (weiqiang@jaist.ac.jp)

Graduate School of Information Science
Japan Advanced Institute of Science and Technology (JAIST)

1 Research Aim

In my previous research, a combined formal system verification technique has been proposed to enjoy the best from both interactive theorem proving and model checking techniques when conducting formal system analysis. In this combined technique, two methodologies for such combination, which are called Induction-Guided Falsification (IGF) and Combined Falsification and Verification (CFV), has been proposed, and an environment for making the two methodologies possible has been implemented.

The aim of my current research is to investigate the usability and effectiveness of the proposed methodologies by conducting case studies in different application domains. Three applications are chosen for this research: the Mondex electronic purse system, an e-Government messaging framework, and trace anonymity property of distributed systems.

2 Research Approaches

In the proposed combined technique, the OTS/CafeOBJ method and Maude model checker are chosen as the target techniques/systems providing interactive theorem proving and model checking functionalities, respectively.

The OTS/CafeOBJ method is a modeling, specification and verification method. In this method, modeling is based on Observational Transition System (OTS) models, specification is based on CafeOBJ specification language, and verification is based on induction while using CafeOBJ system as an interactive theorem prover. Maude is a specification and programming language based on rewriting logic that has model checking facilities. Maude can conduct model checking on abstract data types, and is capable to model check systems whose states involve data in data types of infinite cardinality.

In the methodologies for combining the OTS/CafeOBJ method and Maude, IGF is a procedure that can reveal logical errors (falsification) lurking in the CafeOBJ specification as early as possible by employing Maude model checking during the interactive inductive verification of the OTS/CafeOBJ method, and interactive inductive verification of the OTS/CafeOBJ method can be used to reduce the state space needed for Maude to find a counterexample. CFV is a more general combined procedure whose purpose is to enhance the verification

capability of IGF, but such enhancement is based on sacrificing the falsification capability of IGF. Thus the two procedures IGF and CFV have different focus – falsification and verification, respectively. The basis of the methodologies is an automatic translation from CafeOBJ specification into corresponding Maude specification. And the soundness of the translation wrt counterexample has been proved, namely that any counterexample reported by Maude is a true counterexample.

3 Progress in 2007

To examine the usability and effectiveness of the proposed methodologies supported by the automatic translation, we have been conducting case studies in three different application domains.

The Mondex Electronic Purse. Mondex is a payment system that utilizes smart cards as electronic purses for financial transactions. The system has been chosen as a challenge for formal methods. The purpose of setting up this challenge is to see what the current state-of-the-art is in mechanizing the specification, refinement, and proof, and ultimately to contribute to the Grand Challenge – Dependable Software Evolution.

We choose the Mondex problem as our primary case study. In this case study, the methodologies have been shown to be useful in the following two aspects: (1) before carrying out the interactive verification using the OTS/CafeOBJ method, falsification using Maude can help human verifiers to obtain a certain degree of confidence for the correctness (within a finite reachable state space) of the system and property specifications (in case that no counterexample is reported), and (2) during conducting interactive verification, generating good and correct lemmas is not a simple task. Falsification can help in this stage to filter out those generated by essentially incorrect lemmas.

Besides, our work on the Mondex problem provides an alternative way of: (1) modeling the Mondex system in an operational style (in terms of transition system), rather than a relational style employed in related work, and (2) expressing and verifying (and falsifying) security properties of the Mondex system directly in terms of invariants, rather than the simulation relation proof conducted in related work. Our work therefore provides a different way of viewing the Mondex analysis problem and can be used to compare different modeling and proof strategies.

An E-Government Messaging Framework. Electronic Government (e-Government) refers to the use of information and communication technique, particularly the Internet, as a tool to achieve better government. The messaging framework used in this case study was proposed for a real e-Government project to provide citizens seamless services (services are offered through cross-agency collaboration, however, such collaboration is not known by citizens). The messaging framework is to support transferring messages between registered members

through dynamically created channels. A member is a registered user of the framework, usually a government angency. Basic idea of the framework is that: Messages can be transferred between registered members through channels. To send/receive messages from a channel, members should subscribe the channel. A channel can be created by a member, and the member who creates the channel, is the owner of the channel, and is automatically subscribed to the channel.

In this case study, we modeled the framework as an OTS and tried to analyze three basic consistency properties of the OTS. However, we found two problems: (1) when unregister a member (say A), the member's registration ID (say IDA) is not removed from the subscribing list of the channel (say C) that A subscribed. This may cause the problem that another member (say B) who registers the framework using IDA may receive messages from C without subscribing it. (2) an owner of a channel can unsubscribe the channel. This may cause the problem that an owner of a channel loses control of the channel that it owned. We are going to further discuss the two issues with the project members and check if the two problems found are real problems of the framework.

Trace Anonymity. The issue of anonymity occurs in many real-life activities such as voting and donation, in which people may not want their identities to be disclosed. However, the use of formal methods for analysis of anonymity property is still in its elementary stage and only a few studies exist in the literature.

A notion of trace anonymity has been proposed by Kawabe et al. from NTT Communication Science Laboratories based on trace notations of I/O automaton. An inductive verification technique based on a notion of anonymous simulation is then proposed. It is shown that the existence of an anonymous simulation leads to trace anonymity. The formal verification that an infinite-state system satisfies trace anonymity is carried out using Larch prover. In this case study, we follows the definition of trace anonymity and its inductive proof technique proposed by Kawabe et al, but using OTSs and CafeOBJ instead of I/O automaton and Larch prover.

In this research, we have revised the original definition of OTSs to define trace notations, and consequentially to formalize trace anonymity. We have also made a small revision to the proof technique proposed by Kawabe et al to make the proof steps for trace anonymity more explicit. This research demonstrated that the proof score based verification technique could be used for anonymity analysis. This research is also a starting point for our further research on formal analysis of anonymity, and more broadly, formal analysis of privacy related properties of distributed systems. As to the issue that how the proposed methodologies could be used for anonymity analysis, we are going to do further studies.

4 Future Directions

My future work is classified into three aspects as follows according to the three application domains.

In the Mondex case study, I did not consider intruder purses that may send faked messages based on possibly gleaned information. My first future work is to extend the modeling and verification by considering possible intruder purses under a cryptographically secured communication protocol. Besides, I am going to investigate the technical issue in falsification that how many entities (such as purses) are enough to uncover possible counterexamples when the number of the entities has to be made finite for falsification.

In the e-Government messaging framework case study, what I have analyzed is only the core messaging framework. This core framework can be extended to provide more secure and reliable transfer of messages. I am going to use the two methodologies to analyze the extensions of the core messaging framework, and further discuss the two problems found with the project members.

In the trace anonymity case study, the satisfaction of a distributed system to trace anonymity is proved by showing the existence of an anonymous simulation ralation. However, coming up with such simulation relation is a non-trival task. If anonymity can be formalized as an invariant property, then the already well-studied proof technique for invariants could be directly used for the analysis of anonymity. This leads to my future work of proposing a way to formalize anonymity as invariant properties.

5 Publications in 2007

Journal paper

1. Masaki Nakamura, Weiqiang Kong, Kazuhiro Ogata, and Kokichi Futatsugi: "*A Complete Specification Translation from OTS/CafeOBJ into OTS/Maude*", IEICE Transactions on Information and Systems, Accepted, to appear in 2008.

Conference papers

2. Weiqiang Kong, Kazuhiro Ogata, Jian Cheng, and Kokichi Futatsugi: "*Trace Anonymity in the OTS/CafeOBJ Method*", submitted for publication, 2008.
3. Weiqiang Kong, Kazuhiro Ogata, and Kokichi Futatsugi: "*Algebraic Approaches to Formal Analysis of Mondex Electronic Purse System*", In: the 6th International Conference on Integrated Formal Methods (iFM 2007), LNCS 4591, Springer, pp. 393-412, 2007.
4. Weiqiang Kong, Kazuhiro Ogata, and Kokichi Futatsugi: "*Algebraic Approaches to Formal Analysis of Mondex Electronic Purse System*", Research Report, IS-RR-2007-004, JAIST, 2007.
5. Xiaoyi Chen, Weiqiang Kong, and Kokichi Futatsugi: "*Formal Support of e-Government Design with Transparency Consideration*", In: the 1st International Conference on Theory and Practice of Electronic Governance (ICEGOV 2007), ACM press, pp. 20-29, 2007.
6. Xiaoyi Chen, Jianwen Xiang, Weiqiang Kong, and Kokichi Futatsugi: "*Formalization and Analysis of Public Administration Domain with the OTS/CafeOBJ Method*", In: the 3rd International Conference on e-Government (ICEG 2007), pp. 77-86 2007.