Title	A survey of formal verification of Paxos and a case study with an algebraic specification language [課題研究報告書]
Author(s)	Apasuthirat, Thanisorn
Citation	
Issue Date	2014-09
Type	Thesis or Dissertation
Text version	author
URL	http://hdl.handle.net/10119/12263
Rights	
Description	Supervisor:Kazuhiro Ogata, School of Information Science, Master

A survey of formal verification of Paxos and a case study with an algebraic specification language

Thanisorn Apasuthirat (1210201)

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

August 7, 2014

Keywords: software verification, Paxos, OTS/CafeOBJ, theorem proving.

Software sometimes has some bugs or errors since made by human. Some systems may run correctly even it contains some errors, while some systems can cause the damage to life even containing a tiny error. Therefore, we need to check that system does not contain any fault by doing the software verification. Software verification is an vital part for checking the correctness of system. It consists of two techniques for doing verification; model checking and theorem proving. Model checking involves automatically exploring the set of reachable states of model to ensure that some formulas needed to check holds. On the other hand, theorem proving uses some theories to prove, and the theorem to be proved need to be formulated as formulas involving some mathematics. The theorem proving technique needs the guidance of human taking the form of lemmas while the model checking can be automatically done. However, model checking can cause the state explosion problem since it searches in the state space of the complex system.

This research aims to verify an algorithm for solving consensus problem in distributed system. The algorithm for solving consensus is called consensus algorithm. The consensus we focused is Paxos algorithm which is a family of consensus algorithms. We conduct the Paxos model and specify it on both CafeOBJ language (by OTS) and maude language. Then we verify

Paxos that enjoys agreement property, which is a property of consensus algorithms, by using proof scores in OTS/CafeOBJ and CITP in maude which considered as a theorem proving technique.

Futhermore, we survey the related formal verification of an similar consensus algorithm with Paxos (called LastVoting algorithm). They proposed the way to reduce the verification problem to a small model checking problem by involving single phases of algorithm configuration. They used some notions of round-based model to model asynchronous consensus algorithm and reduced the model checking problem of some properties such as agreement and termination to the satisfiability problem for a formula in some logic. They used a Yices (Satisfiability Module Theories) to check the satisfiable of the formula. In their experimental result, they only successfully verified the number of processes up to around 10 processes. Difference from our approach that use theorem proving, we do not need to bound any number of processes and it can be proved infinite number of processes.