Combination of verificaiton by deduction and verification by searching

Yoshihisa Kawasaki (0610027)

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

February 05, 2009

Keywords: Formal Method, CafeOBJ, Model Checker, Interactive Prover.

1 Introduction

Recently, high reliability and safety should be verify enough because these are most important on software and information system. Now, there are generally two verification methods in software and information system. One is verification method by searching by using model checker. The other is reasoning based verification method by deduction. Two verification methods have the different properties, advantages and disadvantages each other. These properties is such as that when you verify the infinite state system by using model checker, it is necessary to abstract to the finite state system. But reasoning based verification by deduction can verify infinite state system. On the other hand, reasoning based verification by deduction needs more works by human than verification by searching.

Therefore, The purpose of this research is to propose more efficient verification method, that is the combinationof advantages between verification by deduction and searching, than verification method used now.

2 Approach

Algebra specification language CafeOBJ is order-sorted specification language, and can calculate by interpreting equation as rewriting rule. CafeOBJ has two verification methods, which are corresponding verification by deduction and verification by searching. One is verification method by proof score, the other is model checking by search command. System can be specified based on OTS(Observational Transition System) by using CafeOBJ. CafeOBJ/OTS can be verified by proof score and model checking by search command, It is not necessary to translate between two verification methods because both verification method can be used simultaneously. When you use model checker by using search command, CafeOBJ has two methods. One is (1)method by withStateEq and observationa equivalence. The other is (2)method by equational abstraction. (1) is method to search all states checking equality of each state on observational equivalence. It is important to define observational equivalence for (1). (2) is method to search all states abstracted by some equations, which stand for state-abstraction, that is proved to justification by proof score. It is important to discover equations for (2). It is can be considered that (2) is combination method between verificaiton by deduction and veriication by searching, which is purpose of this research. (1)and (2) are already proved efficiency on mutual exclusion protocol QLOCK. (2) is proved search time is shorter than (1) on QLOCK. But(2) is not experimented on the other protocol except to QLOCK. So, It is considered that it is necessary to get more efficiency by experimenting the other protocol. Moreover, to discover equations for abstraction is difficult in spite of fact that equation is important because to discove is intelligent works by human on (2) Therefore, this research does the following

- Apply to communication protocol SCP
- Analyze and classify pattern of equations and discovery method for equations.

3 Conclusion

The combination method between verification by deduction and verification by searching could be proved efficiency on SCP. I can systemize calssification of equations and guide to discover equations. As future works, It is considered application of ABP, which is more complex protocol than SCP.