Systematic design and verification method based on verification pattern

Hayato Kanai (410031)

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

February 9, 2005

Keywords: model checking,SPIN,verification pattern,software pattern.

Recently,our society is deeply dependent on embedded software, and the quality of the software becomes problems. On the other hand, the complexity and the size of embedded systems become lager and lager, conventional development style is no more suitable. Against these background, we believe that, in software verification, it is necessary to utilize not only conventional verification techniques but also formal verification techniques.

One of promising formal verification techniques is model checking technique. This verification technique is an automatic technique for verifying the property of the target system represented as finite state concurrent systems. The properties to be verified are given as logical formula. Using model checking technique for verification of UML models, we can expect to attain highly reliable software design. However,in order to verify UML model using a model checking tools, we need to convert UML model into a specification language acceptable by tools. Also it is necessary to define properties that the design must satisfy utilizing temporal logic. The specification is given in some temporal logic. The representation of properties depends on how we represent UML model in specification language. These work is hard for ordinarily software engineers, as they have to learn not only grammars of specification language and temporal logic and but also description techniques.

We have observed that, in software formal verification, there are patterns in software specification and logical formula. Therefore, it is useful for software engineers to show these patterns. Logical properties are deeply depend on the target system description. Therefore, we believe that it is useful to provide patterns of system description along with patterns of logical formula that describe properties to be verified. In this paper, we use SPIN model checker as a model checking tool.

That problems in formal software verification can be summarized as follows;

- It is difficult for software engineer to convert a properties into temporal logical formula.
- There are no common way to convert UML into a specification language, and this affect the above logical formula.

In order to solve the first problem, we have provided patterns of logical formula. There already proposed patterns of logical formula, but these previous work are independent from the system description. As mentioned above, the formula depends on system description, our pattern is provided as a set of patterns of software structure (system description) and properties (logical formula).

For the second problem, we have proposed a conversion techique from UML model to PROMELA language. We have carefully examine the technique so as to important properties on UML model can be expressed as LTL formula on PROMELA language. Based on our conversion rule, we can easily express UML properties such as "receiving message".

In order to evaluate our patterns, we have apply our patterns in verifying software design provided by a company, and demonstrate that we can systematically verify the properties of the system.

This structure of this paper is as follows. Chapter 2 describes objectives of this paper. Chapter 3 describes the fundamental overview of Model Checking technology and SPIN. Chapter 4 describes that verification patterns and converting rules proposed by this paper. Chapter 5 describes evaluation of our patterns based on a case study. Chapter 6 describes conclusions and possible future works.