Verification oriented software design method using model checking

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

January 8, 2010

Abstract

In this study, we propose a verification oriented design method that facilitates UML design verification based on model checking techniques. It is not efficient to verify models that are designed without considering the ease of verification, e.g. the definition of verification properties on such model becomes difficult. Hence, in designing software, it is important to recognize important properties for the software and develop design model considering how to develop verification model based on the design model and how to verify the verification model. In this study, we propose two techniques that support the development of verification model and also propose a design method that systematically utilize these techniques to facilitate design verification.

Firstly, we propose a technique to utilize verification patterns each of them supports the development of verification model that facilitate the verification of specific design property. As verification properties are defined utilizing the modeling elements defined in the verification model, the ease of the definition strongly depends on the verification model. We observe that there are typical techniques to develop verification model that facilitate the verification of specific properties, and it is useful to define a verification pattern as a set of properties, verification model and verification properties. Among some existing verification patterns such as patterns of properties, our verification pattern is unique as it is defined as a set of software structure and properties.

Secondly, we propose an aspect-oriented modeling technique that supports the modification of verification model. In verifying design model by model checking techniques, it is common to partially modify a design model with respect to verification properties. It is also common that these modifications cross cut the model. It is bothersome and error-prone to do such modification ad hoc. In actual software development such ad hoc modification becomes unrealistic, as software developers incrementally develop design model and repeatedly verify various properties. In this study we propose an aspect-oriented UML modeling technique and its support environment that facilitates such modification.

Lastly, we propose a verification oriented design method that systematically utilize above techniques in order to facilitate the design verification utilizing model checking techniques.

Key Words: **Model checking, Verification pattern, Temporal logic, Aspect-oriented modeling, Software architecture**