Title	モデル検査のための環境モデリング手法に関する研究
Author(s)	西端，浩和
Citation	
Issue Date	2009-03
Type	Thesis or Dissertation
Text version	author
URL	http://hdl.handle.net/10119/8103
Rights	
Description	Supervisor:青木利晃，情報科学研究科，修士

Research on environmental modeling method for model checking

Hirokazu Nishibata (710054)

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

February 5, 2008

Keywords: model checking,SPIN,formal method,modeling method,Promela.

1 Introduction

In late years ,model checking attracts attention as one of the means of the reliability security of the software. The subject to inspection model that modeled an object to inspect and The inspection item which describes a property to inspect by logic formulas are necessary to perform a model checking. Furthermore, when you inspect by model checking, not only these but also the outside environmental model that described input and output to subject of examination is necessary. I decide to call the thing which described this outside environmental behavior an check model. There are two problems to generate an check model. For reliability improvement, I put an check model together every function that I want to inspect, and it is desirable that I can discover an error to detect. However, the point where it is necessary I arrange it so that there is complicated limitation to put an check model together, and to describe it is the first. In addition, depending on a combination by the multiplicity and the value of the attribute by dicided, it is assumed that the number of the patterns of the combination of the check model becomes enormous. The point that is difficult as for generate an check model in the all, and carrying out model inspection one more. A purpose of this reserch is to suggest outside environmental modeling method suitable for model checking. It solves the first problem by I arrange limitation in the case of modeling, and describing it. When I do materialization of multiplicity and an attribute, it solves the second problems by I define an equivalence pattern, and reducing the combination that it is thought that I do the same behavior.

2 Environment modeling method

By the suggestion technique, environment modeled by UML which is a modeling language used widely. I expand the ability for description of UML to be enough for a description of the environmental modeling to suggest. Suggestion method model outside environment every function that I want to inspect. I decide to call the thing which modeled outside environment with UML an environmental model. It is necessary to generate the check model that unified the behavior of the environmental model I put each outside environment together, and to perform model checking. I decided to describe limitation for the combination of the environmental model as a transition condition of the transition to generate a unified inspection model. I explain a flow of the suggestion method. At first I pay my attention to transition with the possibility to change from the state of the environmental model. I describe all transition in diagram to call a transition extraction figure every state. I use two UML diagram of a figure of class and the figure of state machine by the environmental modeling. I describe a subject to inspection system and an outside environmental static relationship in a figure of class for model checking. I describe a figure of state machine for model checking in consultation with a transition extraction figure. I describe the transition condition list of the class level about each transition. There is the case that other transition is guided by transition. I describe information of such an instruction transition as an instruction transition list. In addition, the object of an enormous kind is assumed when I do materialization of a figure of class for model checking. It is difficult to generate all objects in an check model. Therefore, I define an equivalence pattern and remove the object that it is thought that I do the same behavior. I perform the equivalence pattern removal with two phases of multiplicity equivalence pattern and attribute equivalence pattern. After the removal, I assume a left object an object for model checking. An environmental unification algorithm generate an check model for the cause by the information of an object for model checking. I do materialization of a transition condition list and an instruction transition list to generate an check model by environmental unification algorithm. Because the provided check model is a figure of state machine description, it is necessary to convert it into Promela. Therefore, I exhibit correspondence with the check model of the figure of state machine description and the check model of the Promela description in this research.

3 The application experiment for the exercise

The model checking is suitable for the inspection of the system that confirmation is difficult by a review and the test. The systems such as multi task or the multi-thread and The system that movement changes by the timings such as asynchronous event processing or the communication protocol are nominated for those systems. I do an application object of the suggestion technique with the OSEK/VDX specifications that are Real Time Operating System(RTOS) with these characteristics. OSEK/VDX specifications are industry-wide standard specifications of RTOS used at an engine control unit in the car. I assumed subject to inspection in the suggestion method a scheduler function of OSEK which decided the behavior of the task and resource. I applied environmental modeling method in a task, resources as outside environment. I described information of the transition of the class level in each environment model. A task is 1 or 2,resource is 2 from 0,each priority high or low by the combination pattern of the check model by generate. By the combination pattern of the object which did materialization, I defined an equivalence pattern. 334 pattern was reduced to 35 pattern by an equivalence pattern definition. I made information of each transition instance every combination pattern. I assumed information of the transition of the instance level input of the environmental unification algorithm and generated an check model. I experimented by the check model that generated. The number of the states of the check model was 17 states in the case of most check models.

4 Summary

I suggested 2 of environmental modeling method and equivalence pattern definition as a solution of the difficulty of the check model generation by the suggestion method. By the environmental modeling method, I use two kinds of the figure of class and figure of state machine for model checking to perform environment modeling. I define the object that it is thought that I make the same behavior by the equivalence pattern definition as an equivalence pattern and reduce the number of the combination patterns. I suggested environmental unification algorithm to unify environmental models automatically. I showed correspondency check model by generated and Promela that description language of the model checker SPIN. I applied suggestion technique to OSEK/VDX specifications and generated an check model. I confirmed that I could discover malfunction by the check model that generated.