Title	モデル検査を用いたフォールトアナリシス手法の提案
Author(s)	野口，秀人
Citation	
Issue Date	2015-09
Type	Thesis or Dissertation
Text version	ETD
URL	http://hdl.handle.net/10119/12968
Rights	
Description	Supervisor:青木　利晃，情報科学研究科，博士

Abstract

A fault analysis process is discussed in this paper. Fault analysis is an activity to detect the fault that caused a failure, which has occurred during software testing. The objective of this work is to provide an effective fault analysis method especially for the ``hard-to-reproduced" failure. In order to achieve this objective, a failure reproduction method using model extraction and model checking techniques is proposed in this paper. Moreover, a fault analysis process including the failure reproduction is also proposed. Assumed target of this work is so-called embedded software, which is embedded in the devices that control physical, electrical or electronic world outside the devices.

In late years, the purpose of embedded software is to add value of the products by using software, which realizes intellectual control depending on the situation, cooperation action of the plural devices or cooperation with the information service. Therefore, concurrency of the systems and complexity of embedded software in such systems increase rapidly. In addition, the behavior of world outside the systems, which embedded software controls through devices, is nondeterministic, and it is difficult to assume whole behavior of the systems beforehand.

One of the issues of such embedded software development is fault analysis. To detect the fault according to an observed failure, the developer generally tries to reproduce the failure by executing the system again under the same condition as that in the case of failure. However, the failure reproduction is sometimes quite difficult, since behavior of the target system is not constant because of above-mentioned concurrency and nondeterminism. This paper proposes an effective method of fault analysis for such a hard-to-reproduced failure.

Primarily, model checking technique is proposed to be applied to failure reproduction. Model checking is a powerful technique to decide whether the behavior model of the system models the predefined property, which is conventionally used during software development to find the unknown and unexpected behavior of the target system. One of the characteristics of this work is to use model checking technique for detecting behavior that reaches the observed failure that has occurred during testing.

Then, a model extraction method from source code is proposed for model checking against source code. One of the problems in practical use of model checking is a huge cost for constructing the behavior model of the target system. POM (Program-Oriented Modeling) framework that extracts a model from source code is proposed to solve this problem. The POM/MC tool that is a tool performing model extraction and model checking using the POM framework is also proposed. POM/MC enable its user to explicitly appoint the method for model extracting. This feature supports the failure reproduction in trial-and-error-manner experiments both to keep information necessary for fault analysis and to avoid state explosion in model checking.

Moreover, the fault analysis process is defined in formal manner. The fault analysis model that formalizes concepts of failure, fault and fault analysis is proposed. Then fault analysis is constructed from view of the hypothetico-deductive method, and an experimental fault analysis process based on hypothesis and predictions is formalized. This process is implemented by using POM/MC. Finally, feasibility of effective fault analysis by using the proposed method is shown through some case studies.

Keywords

fault analysis, model extraction, model checking, system testing, hypothetico-deductive method