氏　　名	野口秀人		
学位の種類	博士(情報科学)		
学位記番号	博情第 332 号		
学位授与年月日	平成 27 年 9 月 24 日		
論文題目	モデル検査を用いたフォールトアナリシス手法の提案		
論文審査委員	主査　青木　利晃	北陸先端科学技術大学院大学	准教授
	平石　邦彦	同	教授
	鈴木　正人	同	准教授
	岡野　浩三	信州大学	准教授
	粂野　文洋	日本工業大学	准教授

論文の内容の要旨

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

論文審査の結果の要旨

この博士論文では，ソフトウェア開発において発生する故障に対し，その原因を特定するフォールトアナリシスを，モデル検査を用いて支援する手法およびツールを提案している．

並行性を持つソフトウェアでは，故障発生時と同様の条件のもとで再実行しても，その再現が困難な場合が多い．本博士論文では，そのような故障の原因を特定するために，モデル検査の技術を応用している．ソースコードを再実行しながら故障原因を特定するのではなく，ソースコードから故障が存在すると予想している部分を抜き出し，その部分をモデル検査可能な記述に変換して網羅的に探索することにより，故障原因を特定するのである．

一方で，このような抜き出しとモデル検査の実施は試行錯誤しながら繰り返し行われる．そこで，本博士論文では，ソースコードからモデル検査可能な記述への変換を支援する手法とツール POM/MC を提案している．POM/MC では，変換規則を与えると，その規則に基づいて C のソースコードからモデル検査ツール Spin のための記述へと自動的に変換する．また，MOF におけるメタモデルの考え方を取り入れており，試行錯誤を行いやすい仕組みを提案している．本博士論文では，さらに，このようなフォールトアナリシスを実施するプロセスの形式化も行っている．提案手法では試行錯誤を行い故障を特定していくが，それを科学的な実験と捉え，仮説演繹法に基づいて故障原因箇所を絞り込んでいく過程を形式的に定義している．

本博士論文の貢献は，企業において実際に発生している困難な問題に対して，先進的な方法を組み合わせて解決する手法を提案していることである．再現性が低い挙動にまつわる故障の原因特定には，非常に高いコストがかかる．この問題に対して，モデル検査の技術を応用して，効率的に故障の原因特定を行えるようにした．さらに，その過程を明確にするために，科学哲学分野の仮説演繹法を下地として，提案手法に基づいたプロセスを形式的に定義し，科学的にも妥当であることを示した．また，モデル検査の技術は，誤りの検出を目的としているが，提案手法では，誤りがあることを前提として，その原因箇所の特定にモデル検査を応用している点が独創的である．さらに，フォールトアナリシスプロセスを形式的に定義しているのも本研究が最初である．これらのことから，本博士論文では，十分な有効性，妥当性，独創性を持つ手法が提案されていると言える．

以上，この博士論文では，再現が困難な故障に対して，その原因を効率的に特定する実践的な手法を提案しており，学術的に貢献するところが大きい．よって，博士（情報科学）の学位論文として十分に価値があるものと認めた．