要 旨

モデル検査器 Java Pathfinder における実行トレース出力の改善

菅 優也

プログラムの検証手法の 1 つに，モデル検査がある．モデル検査とは，形式システムをアルゴリズム的に検証する方法であり，ハードウェアやソフトウェアの設計から導出されたモデルが形式仕様を満たすかどうかについて網羅的に検証を行う．

Java プログラムのモデル検査を行うモデル検査器の 1 つに Java Pathfinder がある．Java Pathfinder は通常の Java 仮想マシン上に独自の仮想マシンを構築し，その上で対象プログラムそのものの網羅探索を行うため，モデル記述言語を用いたモデルの作成が不要である．

Java Pathfinder ではエラー検出の際，経路情報のみが表示され，エラー検出時の状況が把握し辛い．そこで，本研究では状況の把握とエラー原因の特定を容易にするため，実行開始からエラー検出までの各地点の情報を表示する方法を提案した．この実現方法として，探索終了後の仮想マシン自体を操作して情報を取得する方法と，探索時に情報を収集し，エラー検出時に収集した情報から状況を再現する方法の 2 通りの方法を試した．

結果として，後者の方法により実行開始からエラー検出時までのトレース情報の表示を実現することができた．また，被験者に実際に使用してもらった結果，検出したエラー情報の追加や，地点変更時に変更のあった変数情報の強調表示，表示項目自体の説明などが必要との意見があり，表示項目についてさらなる改善が必要であることがわかった．

キーワード　モデル検査, Java Pathfinder, 網羅探索

Abstract

Improvement of the execution trace output of Java Pathfinder

Kan Yuya

Model checking is one of the techniques to formally verify a program. Model checking performs an exhaustive verification in which a model derived from the specification of hardware and software is verified whether it satisfies a formal specification.

Java Pathfinder is one of software model checking tools that performs verification for Java programs. Java Pathfinder has own virtual machine on the Java virtual machine. Java Pathfinder does not require a user to create a model using a model description language because it can perform exhaustive verification of the target program on its own virtual machine.

For users of Java Pathfinder, it is not easy to grasp what happens when an error is detected, because it shows only routing information for the error. To facilitate understanding the situation and identifying the cause of the error, in this study we have proposed a method to display information for each point of the error trace from the initial point to the error point. We tried two implementations. One is to obtain information by operating the virtual machine itself after the end of the search, and the other is to recreate the state information using collected information at the time of error detection. As a result, we were able to achieve the display of trace information from the initial point to the error point by the latter method.

In addition, human subjects gave some comments on the proposed tool. For example, a subject said that the tool have to highlight the variable information which has changed. The comments suggest that there is a need for further improvement on the

displayed items.

key words model checking, Java Pathfinder, exhaustive verification