情報処理学会論文誌　プログラミング　Vol. 4　No. 3　99 (June 2011)

発表概要

モデル検査法における詳細化概念の導入によるソフトウェア信頼性担保手法

本間毅史[†1]　山本章博[†1]

本研究の目標は，ソフトウェアとその検証過程をあわせた利用者への提示手法を提案することである．提案手法を用いると，利用者がソフトウェアに対する信頼性を確認するために，利用者自身が，開発者が検証したときと同じ過程で再現することが可能になる．検証手法としては，形式的検証手法の 1 つであるモデル検査法を用いる．ソフトウェア検証におけるモデル検査法は，ソフトウェアの動作モデルが制約条件を満足するかどうかを証明するものである．しかし，ソフトウェアに対して完全なモデルを作ることは困難であるとともに，その検証にも膨大な時間がかかる場合があり，これをそのまま利用者に提供してもモデルの理解や検証を行うことが困難になるという問題がある．本研究ではこの問題を解決するために，モデル検査法にモデルの詳細化という手法を導入する．モデルの詳細化とは，単純なモデルの生成とその検証から始め，必要に応じて対話的にモデルを詳細にする手順を繰り返していく手法である．モデルを詳細化する過程は保存されソフトウェアに添付して提示される．これにより，利用者はソフトウェアの検証過程を再現することが可能になる．提案手法を実証するために，モデルの生成・詳細化・検証を一連の流れの中で行うことができるソフトウェアを実装し，提案手法が実現可能であることを示した．また，実際に使用してもらうことにより，ソフトウェアの信頼性が向上するという意見が得られた．

Software Reliability Method by Introduction of Refinement Concept to Model Checking

Takeshi Homma[†1] and Akihiro Yamamoto[†1]

In this research, we propose a method for presenting software unified with its verification process. When users use the proposal method, they can reproduce the verification process by the programmers to confirm the reliability of the software. As the verification method, we choose model checking, which is one of the well-known methods. Model checking in software verification detects whether or not a model expressing software meets constraints, but it is difficult to make a complete model for software. In addition, the verification takes much time when combinatorial explosion occurs. This means that a user has difficulty in understanding and verification. In this research, we introduce refinement of models into the model checking method to solve this problem. In our method the programmers begin with the generation of a simple model and its verification based on it, and they refine the model interactively. They repeat this procedure until they obtain a model refined as they are satisfied. The process of refining the model is saved and presented it with software. As the result, users can reproduce the verification process of the software. We implemented the proposal method and asked several programmers to use it. We received answers from them saying that reliability of the software is improved.

（平成 23 年 1 月 21 日発表）

†1 京都大学大学院情報学研究科知能情報学専攻
Graduate School of Informatics Intelligence Science and Technology, Kyoto University