情報処理学会論文誌　プログラミング　Vol. 2　No. 1　19 (Jan. 2009)

発表概要

大規模システムソフトウェアのモデル検査器の設計と実装

松田元彦[†1]　前田俊行[†1]　米澤明憲[†1]

本発表では，デペンダブル組み込み OS に対する静的プログラム解析の一部として開発中のモデル検査器の概要を報告する．一般に述語抽象をベースにするモデル検査方式が有望であるが，適用規模が OS 等のシステムソフトウェアに及ばない．そこで規模の大きなソフトウェアにモデル検査器を適用するため，検証項目はアサーション等の基本な性質に限るが，効率や規模を重視するモデル検査器の開発を行っている．処理規模の拡大にはクラスタ計算機による分散処理を念頭に，並列化が可能な構成を選択する．また，抽象状態の遷移計算には近年性能向上の著しい SMT ソルバを利用できる方式を選択する．モデル検査器に与えるアサーションの記述には，デペンダブル組み込み OS で提案されている記述方法を利用する．P-Bus と呼ばれる OS 内部のレイヤ間で抽象化インタフェースが定義されており，それに対するアサーション記述が提案されている．その記述に対してモデル検査を行う．

Design and Implementation of a Model Checker for Large-scale System Software

Motohiko Matsuda,[†1] Toshiyuki Maeda[†1]
and Akinori Yonezawa[†1]

A model checker is under development as one of the static program verifiers for the forthcoming Dependable Embedded Operating System. Our model checker is designed with priority for scalability, because model checking based on predicate abstraction is promising, but it is not yet applicable to large system software like operating systems. A trade-off is taken not for verifiable properties, but for efficiency and scalability, and verifiable properties are currently simple assertions. Our model checker is designed for parallel processing with cluster computers, and utility of recently advanced SMT solvers. Assertions are described based on the P-Bus interface, which is a proposed abstract interface internal to the kernel that cleanly separates functionalities in operating systems. Our model checker works on the properties attached to the interface.

（平成 20 年 8 月 6 日発表）

†1 東京大学大学院情報理工学系研究科
Graduate School of Information Science and Technology, The University of Tokyo