

「モデルチェッキングの調査と実験」

064番 森 勝也

1. はじめに

モデルチェッキングはとても注目を浴びている技術であり、すでにハードウェア面ではおおきな成果を上げてきた。

特に近年では組み込みソフトウェアやWEB サービスソフトウェア開発への実用化がされつつある。

例えばマイクロソフト社の「SLAM」プロジェクトでは「SDV」というモデル検査を用いてコンパイル時にドライバのエラーを発見するツールを開発した。

2. モデルチェッキングとは

従来システムが仕様を満たすことの数学的な証明は手動で行われ、さまざまな公理や推論を用いて構成されていた。

そしてそれは手作業で行われていた。

そこで状態数有限のシステムではその必要は無く、命題的時相論理と抽象化されたモデルにより仕様を満たすか否かを機械的に決定する方法のことである。

具体的にはシステムを Kripke 構造と呼ばれる構造体を用いてグラフ化し、モデルチェッカを用いて仕様を満たすかどうかを決定する。

言語の仕様は命題的で、**computation tree logic (CTL)** と呼ばれる分岐時相論理を用いる。

3. 今回の研究内容

モデルチェッキングについてその理論を調査し、実際に SMV というモデルチェッキングツールを用いて簡単なモデルが仕様を満たすかどうか検証する。

4. 参考文献

[1]“Automatic Verification of Finite-State Concurrent Systems Using Temporal Logic Specifications “

E. M. CLARKE Carnegie Mellon University
E. A. EMERSON University of Texas, Austin and
A. P. SISTLA GTE Laboratories, Inc.

[2] Model Checking @CMU

<http://www.cs.cmu.edu/~modelcheck/index.html>