JAIST Repository
https://dspace.jaist.ac.jp/

Title	モデル検査のための環境モデリング手法に関する研究
Author(s)	西端，浩和
Citation	
Issue Date	2009-03
Type	Thesis or Dissertation
Text version	author
URL	http://hdl.handle.net/10119/8103
Rights	
Description	Supervisor:青木利晃，情報科学研究科，修士

JAIST
JAPAN
ADVANCED INSTITUTE OF
SCIENCE AND TECHNOLOGY

Japan Advanced Institute of Science and Technology

モデル検査のための環境モデリング手法に関する研究

西端 浩和 (710054)

北陸先端科学技術大学院大学 情報科学研究科

2009 年 2 月 5 日

キーワード: モデル検査, SPIN, 形式的手法, モデリング手法, Promela.

1 はじめに

近年、ソフトウェアの信頼性確保の手段の一つとしてモデル検査が注目されている。モデル検査を行うためには、検査する対象をモデル化した検査対象モデル、検査する性質を論理式により記述する検査項目が必要である。さらにモデル検査を行う際には、これらだけでなく検査対象への入出力などを記述した外部環境のモデルも必要である。この外部環境の振舞いを記述したものを検査モデルと呼ぶこととする。検査モデルを生成するには2つの問題点がある。信頼性向上のためには検査したい機能ごとに検査モデルを組み合わせて、検出したい誤りを発見できる事が望ましい。しかしながら、検査モデルを組み合わせるには複雑な制約があるため整理して記述する必要がある点が一つめである。また、多重度による組み合わせや、実体化する属性の値によっては検査モデルの組み合わせのパターン数が膨大になると想定される。そのすべてにおいて検査モデルを生成し、モデル検査を実施するのは困難である点がもう一つである。

本研究の目的はモデル検査に適した外部環境のモデリング手法を提案する事である。モデリングの際に制約を整理して記述する事により 1 つめの問題を解決する。多重度や属性を実体化する際に、同じ振舞いをすると考えられる組み合わせを同意義パターンを定義して削減する事により 2 つめの問題点を解決する。

2 環境モデリング手法

提案手法では一般的に広く使われるモデリング言語である UML を用いて環境をモデル化する。提案する環境のモデル化の記述に十分なように UML の記述能力の拡張を行う。提案手法では検査したい機能毎に外部環境をモデル化する。外部環境を UML を用いてモデル化したものを環境モデルと呼ぶこととする。各外部環境を組み合わせてモデル検査を行うためには、環境モデルの振舞いを統合した検査モデルを生成する必要がある。統合さ

Copyright © 2009 by Nishibata Hirokazu

れた検査モデルを生成するために、環境モデルの組み合わせに対する制約を状態遷移の遷移条件として記述する事とした。

提案手法の流れを説明する。提案手法ではまず、環境モデルの状態から遷移する可能性のある遷移に着目する。状態毎にすべての遷移を遷移抽出図と呼ぶダイアグラムに記述する。環境モデリングではUMLクラス図とステートマシン図の2つのダイアグラムを用いる。検査対象システムと外部環境の静的な関係性をモデル検査用クラス図に記述する。遷移抽出図を元にモデル検査用ステートマシン図を記述する。各遷移についてクラスレベルの遷移条件表を記述する。遷移により他の遷移が誘導される場合がある。そのような誘導遷移の情報を誘導遷移表として記述する。また、モデル検査用クラス図を実体化する際、膨大な種類のオブジェクトが想定される。すべてのオブジェクトを検査モデルに生成する事は困難である。よって、同じ振舞いをすると考えられるオブジェクトを、同意義パターンを定義して除去する。同意義パターン除去は多重度同意義パターン、属性同意義パターンの2段階で行う。除去後、残ったオブジェクトをモデル検査用オブジェクトとする。モデル検査用オブジェクトの情報を元に環境統合アルゴリズムにより検査モデルを生成する。環境統合アルゴリズムにより検査モデルを生成するために、遷移条件表と誘導遷移表を実体化する。得られた検査モデルはステートマシン図記述であるため、Promelaに変換する必要がある。よって、本研究ではステートマシン図記述の検査モデルとPromela記述の検査モデルとの対応を明示する。

3　例題に対しての適用実験

モデル検査手法は、レビューや試験では確認が難しいシステムの検査に適している。それらのシステムとしてマルチタスクやマルチスレッドなどの並行動作するシステムや、非同期イベント処理や通信プロトコルなどのタイミングによって動作が変化するシステムが挙げられる。提案手法の適用対象をこれらの特徴を持つReal Time Operating System (以下RTOS) であるOSEK/VDX仕様とする。OSEK/VDX仕様とは自動車におけるエンジンコントロールユニットで用いられるRTOSの業界標準仕様である。

本研究では、提案手法における検査対象をタスク、資源の振舞いを決定するOSEKのスケジューラ機能とした。タスク、資源を外部環境として環境モデルング手法を適用した。各環境モデルにクラスレベルの遷移の情報を記述した。生成する検査モデルの組み合わせパターンをタスクが1つか2つ、資源が0から2つ、各優先度が高低の2値の場合とした。実体化したオブジェクトの組み合わせパターンを、同意義パターンを定義した。同意義パターン定義より、334パターン想定された組み合わせパターン数が35パターンにまで削減された。組み合わせパターン毎に各遷移の情報をインスタンス化した。インスタンスレベルの遷移の情報を環境統合アルゴリズムの入力とし、検査モデルを生成した。生成した検査モデルを元に検査実験を行った。検査モデルの状態数は一番多い検査モデルの場合で17状態であった。

4　まとめ

提案手法では検査モデル生成の困難さの解決法として、環境モデリング手法、同意義パターン定義の 2 つを提案した。環境モデリング手法では、モデル検査用クラス図とモデル検査用ステートマシン図の 2 種類を用いて環境モデリングを行う。同意義パターン定義では、同じ振舞いすると考えられるオブジェクトを同意義パターンとして定義し、組み合わせパターン数を削減する。機械的に環境モデルを統合し、検査モデルを生成する環境統合アルゴリズムを提案した。生成した検査モデルと、モデル検査器 SPIN の記述言語である Promela との対応関係を示した。提案手法を OSEK/VDX 仕様に適用し、検査モデルを生成した。生成した検査モデルにより不具合を発見できる事を確認した。