モデル検査事例演習

平成２４年度シラバス

２０１２年　１月　４日

国立情報学研究所

TOPSE プロジェクト

代表者　本位田　真一

１．講座名

モデル検査事例演習

２．担当者

早水　公二

３．本講座の目的

本講座の目的は、企業におけるモデル検査推進者の育成である。講座では、モデル検査を実システムに適用する、すなわち業務としてモデル検査の適用を実施する際に必要な技術やノウハウ、さらにモデル検査の成果や有効性をアピールするための報告書の作成方法等を、講師による概略的な指導のもとで、受講者自身が実践と経験を通して自力で会得する。受講生は、教育の場ではあくまで「教わる立場」であるが、企業に帰任すれば、社内で自らモデル検査を実践、推進し、逆に「教える立場」となる必要がある。したがって、本講座では、実践に備えた準備段階や練習ではなく、「実践の場＝現場」そのものを想定したシミュレーション形式で講義を進める。シミュレーションとして想定する状況は、受講生が社内の他の技術者からモデル検査の適用を依頼されたという状況である。また、受講生が成果を経営層にアピールし、モデル検査を社内で本格導入させるために自身が推進者となることを希望するという状況も含んでいる。また、モデル検査を適用する題材は、適用しやすいようにあらかじめ整理された題材ではなく、実際の製品に関する資料（仕様書、ソースコード等）に基づいた題材とすることで、より実践に近い経験を積むことができる。

４．本講座のオリジナリティ

本講座では、モデル検査の適用技術の習得に加えて、「経験」の蓄積と、推進者としてモデル検査を社内で普及させる「戦術」の習得を目指している。本講座のオリジナリティを表すキーワードとして、シミュレーション／実機に基づいた題材／モデル検査報告書の 3 つが挙げられる。モデル検査の技術習得に主眼を置いた講座については、従来多くの同様な講座が開講されている。しかし、それらの講座では、受講生が企業の現場ですべきこと、実務としてモデル検査適用を行う難しさ、導入を推進する戦略等まではカバーしていない。本講座では、それらの問題点を解消し、本講座受講後、企業内のモデル検査推進者になれるように配慮している。

表 1 に、既存の講座の問題点と、本講座における解を示す。

表１　既存の講座の問題点と、本講座における解

既存の講座の問題点	本講座における解
講師と受講生は、教える側と教わる側に完全に分かれており、受講態度やモチベーションが受動的になりがちである。	適用現場でのシミュレーションであるため、講師は、適用を依頼した技術者、業務を評価する管理者の役も担っている。受講生は社内のモデル検査推進希望者の役を担っており、能動的に参加する環境を実現している。
現実的な問題をそのまま使用せず、抽象化・簡略化されたトイ例題を題材にしているため、実際のシステム開発に対する有用性を実感するのが難しい。	2 つの題材は実製品の仕様書とソースコードに基づいており、必ずしも簡単に解けるとは限らないが、逆に、実際のシステム開発に適用した際の難しさを体感した上で、モデル検査の有用性を自ら模索し、実感することができる。
技術に主眼が置かれており、業務としての適用、コストを踏まえた運用、営利を目的とした企業での導入、他者を巻き込んでの戦略等はカバーしていない。	モデル検査報告書や、適用の成果を PR するための発表資料の作成方法、事例を蓄積するための題材の探し方など、技術だけでなく、企業内で戦略についても習得できる講座としている。

５．本講座で扱う難しさ

産業界で注目を集めている形式手法であるが、最近では、製品であるソフトウェアの品質確保の手段としてモデル検査技術を導入し、一名あるいは複数名の技術者が専任として検査業務にあたる企業も出現している。そこで、実システムにモデル検査を適用することを企業内の自主研究や基礎研究ではなく、業務として扱う際の課題が明らかになってきた。導入企業では、開発者が自身の製作した仕様書やソフトウェアにモデル検査を適用するスキームは稀であり、多くは、開発者とは異なる第三者が適用して結果を報告するスキームを採用する傾向にある。後者のスキームを 1 つのプロジェクトと捉えたときに課題となるのが、プロジェクト自体の管理と、ソフトウェア開発者や検査の依頼者、その他の関係組織への報告である。業務として進める限りは、どのような計画、体制で、何の作業を実施したのか、結果や費用はどうであったか等をドキュメントに明文化する必要がある。しかしながら、これまで管理方法や検査結果の報告書にまで言及した事例報告はなく、モデル検査の適用プロセスについても明確になっていない。本講座では、上記のように過去に前例のない事項を扱っており、モデル検査技術そのものが普及段階にある中で、その適用プロセスや結果報告の手法を習得する難しさがあるが、反面、受講生にとっては本講座でしか得られない経験やノウハウを獲得する良い機会である。

６．本講座で習得する技術

本講座で習得する技術は大きく 3 つに分類することができる。

■モデル検査の適用プロセス
ソフトウェアの開発者以外の第三者によって、実システムにモデル検査を適用する際のプロセスとノウハウを習得する。習得するプロセスはモデル化、検査式の作成、検査という概略的な作業事項ではなく、以下に示すように適用の開始から終了までを網羅した標準的なプロセスである。
＜モデル検査適用プロセス＞
　－仕様調査・不具合調査
　－モデル検査の方針立案
　　モデル化の方針
　　検査項目の方針
　－検査対象の絞り込みと抽象化
　－モデル設計
　－モデル製作
　－CTL 式製作

－モデル検査実行と反例解析
－報告書作成

■モデル検査報告書の作成方法
モデル検査報告書は、ソフトウェアの試験工程における事項のみを記載した既存の試験仕様書や試験成績書とは異なり、上記適用プロセスの要点を、順を追って報告する統括的なドキュメントである。報告書はプロセスの作業順序に沿った目次構成となっており、本講座では、章毎に記載すべき事項、注意点を、演習課題を進めながら受講生自身が報告書を作成することによって、その技術を習得する。

■自社での導入を推進するためのノウハウ
受講生が所属する組織は、既に本格導入を完了した企業ではなく、これからモデル検査の導入を検討する企業である場合が多い。本講座では、受講生が自社内でモデル検査推進者となって、導入を推進する際のノウハウを習得する。企業が新しい技術を全社的に導入するためには意思決定者すなわち経営層に対する成果の PR が必須である。本講座を受講することで、成功確率の高い事例と検査対象の選び方、良い結果が得られた場合の効果的な PR 方法等も習得することができる。

本講座ではモデル検査ツールとして SMV を使用する。SMV の特徴は次の通りである。

二分決定グラフ(Binary Decision Diagram, BDD)と呼ばれる、状態空間の効率的なデータ表現を扱うため、高性能な検証が可能
GUI により、実行とレースの状態遷移の追跡が容易
実適用事例が豊富(プラント制御、IEEE 1394 プロトコルなど)

７．前提知識

本講座の受講生は「設計モデル検証(応用編)」講座を受講済みであるか、SMV の操作方法とモデルの作成方法、CTL（Computation Tree Logic）式の作成方法を全て習得済みである必要がある。

８．講義計画

概要

第 1 回：導入、モデル検査器 SMV 復習課題
第 2 回：仕様調査・不具合調査
第 3 回：モデル検査の方針立案
第 4 回：検査範囲の絞込みと抽象化
第 5 回：モデル設計(1)
第 6 回：モデル設計(2)
第 7 回：モデル製作(1)
第 8 回：モデル製作(2)
第 9 回：CTL 式製作
第 10 回：モデル検査実行と反例解析(1)
第 11 回：モデル検査実行と反例解析(2)
第 12 回：報告書作成
第 13 回：発表資料作成
第 14 回：成果発表(1)
第 15 回：成果発表(2)

詳細

第 1 回：導入、モデル検査器 SMV 復習課題

■本講座について
- ・位置付け
- ・本講座の目的
- ・講座形式と受講条件
- ・シミュレーションについて
- ・成果の PR
- ・円滑な進め方・報連相
- ・講師の立場紹介
- ・題材について
- ・事例（業務）の獲得方法

■モデル検査器 SMV の復習課題
- ・課題１ ： 多重割り込みのシステム
- ・課題２ ： 状態遷移表の検査

・課題３ ：回路図の検査

第 2 回：仕様調査・不具合調査

- ■ 仕様調査　：題材の仕様書の説明
- ■ 不具合調査：題材のプログラムの説明と質問・確認事項への回答
- ■ 題材はどちらか一方を選択する

第 3 回：モデル検査の方針立案

- ■ 何を検査するために適用するのか？
- ■ デッドロックを起こすのは悪いプログラムか？
- ■ 前提条件／仮定・推測
- ■ モデル化の方針
- ■ 検査項目の方針

第 4 回：検査範囲の絞込みと抽象化

- ■ 絞込み（具体的な箇所に絞る）
- ■ 抽象化（例）
- ■ 抽象化（詳細）

第 5 回：モデル設計(1)

- ■ 自然言語からのモデル化（具現化）
- ■ 変数と値の割り当て
- ■ 状態遷移表（図）

第 6 回：モデル設計(2)

- ■ ソースコードからのモデル化
- ■ フローチャートから SMV コード

第 7 回：モデル製作

- ■ モデルのコーディング

第 8 回：モデル製作

- ■ モデルの妥当性検査

第 9 回：CTL 式製作

- ■ 検査項目の意義

■ CTL 式のコーディング

第 10 回：モデル検査実行と反例解析(1)

■ モデル検査器について

■ CadenceSMV について

第 11 回：モデル検査実行と反例解析(2)

■ 反例解析（仮定・推測の妥当性の確認）

■ 依頼者への説明

第 12 回：報告書作成

■ 記載内容とフォーマット

■ 概要の報告例

第 13 回：発表資料作成

■ 誰が聞いてくれるか？誰に聞いてほしいか？

■ 発表の目的は？

■ ゴールはどこにあるのか？

第 14 回：成果発表(1)

■ 受講生によるモデル検査の成果発表(1)

第 15 回：成果発表(2)

■ 受講生によるモデル検査の成果発表(2)

９．教育効果

本講座の目的は、企業におけるモデル検査推進者の育成である。座学による学習に加えて、講義全般にわたって、開発現場における適用場面を想定したシミュレーションの形態を採用することで、企業における OJT（On-the-Job Training）に相当する教育効果があると考えられる。講座のなかでは、検査依頼者への対応方法や業務を円滑に進めるためのマナーなど、コミュニケーション能力の向上や、検査業務に臨むにあたってのモチベーションの維持・向上にも言及している。技術教育の延長線上にある人材育成にまで踏み込んだ講座であり教育効果は高い。

１０．使用ツール

SMV：モデル検査ツール

■使用する上での難しさ

検証モデル記述、および CTL 検証式による記述が難しい

検証の結果がエラーの場合、反例を設計モデル修正に反映するのが難しい

■使用上必要なノウハウ

□検証モデル記述ノウハウ

状態の表現

遷移の表現

通信の表現

非同期プロセス実行の表現

□検証式記述ノウハウ

検証項目の種類(安全性、生存性など)

検証式パターン

□検証モデル抽象化

内部動作の除去

データ領域の有限化

□検証効率化

部分順序法

状態削減

□反例分析

変数値追跡

■選択理由、実用性：大きな状態を高速で扱うことが可能で実用性が高い。また、フリーツールのバージョンも存在し入手しやすい。

１０．実験及び演習

モデル検査の題材は、実システムの仕様書とソースコードに基づいた題材である。受講生は仕様書とソースコードの題材のうち、どちらか一方を選択することができる。演習は原則として単独で取り組む。シミュレーションでは、社内でモデル検査知識を有するのは受講生のみと想定しているからである。また、モデル検査報告書と、成果を PR するための発表資料の作成、経営層が聴講していることを想定した成果発表も演習課題としている。

１２．評価

作業レポート、モデル検査報告書、プレゼン発表、出席日数を総合して評価する。
題材の違いによる評価の差は設けない。

１３．教科書/参考書

■B. Berard et al, “Systems and Software Verification: Model-Checking Techniques and Tools,” Springer Verlag, 2001.

モデル検査手法を利用したソフトウェア検証について、入門から実践までの一通りが述べられており、この講義に最適である。

■E. M. Clarke et al, “Model Checking,”, MIT Press, 2000.

モデル検査手法の原理を理論的に述べたものであり、上記教科書を補うのに最適である。

■K. L. McMillan, “Symbolic Model Checking,” Kluwer Academic Publishers, 1993.

モデル検査ツール SMV に関する理論的背景とツールの利用法が述べられており、モデル検査ツールを用いた演習に最適である。