ソフトウェア品質管理研究会 特別講義 レポート

作 成 日：2024 年 2 月 5 日
書記氏名：松波 知典

日時	2024 年 1 月 26 日（金）9:50 ～ 12:00
会場	(一財) 日本科学技術連盟・東高円寺ビル　地下 1 階講堂　*ハイブリッド開催
テーマ	産業界におけるモデル検査の実践事例と普及活動
講師名・所属	早水 公二 氏（株式会社フォーマルテック 代表取締役）
司会者	田中 桂三 氏（オムロン株式会社）
アジェンダ	・形式手法のなかのモデル検査 ・検査の流れ ・産業界における実践事例 ・モデル検査の普及に向けて
アブストラクト	形式手法と言えば、「時々名称を耳にするけどどんな手法？」「どんなメリットがあるの？」「具体的に何をするの？」等、疑問符（？）ばかりが頭に浮かんでくると思います。そんな疑問に答えるため、本講義では、まず形式手法とその 1 つの手法であるモデル検査について、あまり学問的にならないように実用的な見地から概説します。以降はモデル検査に主眼を置いて、モデル検査ツールを用いたデモで検査の流れを説明し、2002 年から 20 年以上にわたって蓄積してきた多種多様な実践事例を紹介します。最後に、モデル検査の普及に向けて、自身の経験談を交えながら、企業での導入の進め方やモデル検査の教育について紹介します。

第 8 回の特別講義では、「産業界におけるモデル検査の実践事例と普及活動」と題して、早水氏よりご講義をいただきました。

◆冒頭、早水氏よりフォーマルテック社の紹介が有りました。
・フォーマルテックはモデル検査の専門企業
・サービス
　モデル検査の導入支援コンサルティング
　モデル検査業務の請負（第三者検証）
・製品
　NuSMV 支援ツール
　国産モデル検査ツール（開発中）

◆講演の流れ
・形式手法のなかのモデル検査
・検査の流れ
・産業界における実践事例
・モデル検査の普及に向けて
・質疑応答

◆形式手法のなかのモデル検査
(1)形式手法のなかのモデル検査
・モデル検査とは、形式手法（フォーマルメソッド）の一つ
・形式手法は、特定の手法を指すわけではない
　数学・論理学を基盤としたシステムの記述方法や検証手法の総称
(2)形式手法の概要と重要性
・システムをフォーマルに記述あるいは検証する
・論理学／数学にもどついた記法による仕様記述→厳密に規定できる
・仕様の証明は「定理証明」で定理／公理を使って証明する
・モデル検査とは、全状態を網羅的に探索して性質を確認する→しらみつぶしの検査が可能
・形式手法（含モデル検査）が産業界で注目されている理由
　→機能安全に関する国際規格 IEC61508 で推奨
　　対象はコンピュータ技術を用いた安全関連系を使用するすべての産業分野
・ISO26262 では、自動車安全整合性 ASIL C 以上で、検証手法として形式検証の適用が推奨されている
(3)モデル検査とは？
・「専用言語」で記述されたシステムを全自動で網羅的に検査する
　モデルが検査式を満たすか否かを検査する
(4)作業は 2 つだけ
・モデルの作成と検査式の作成
　モデルの作り方：ツールの専用言語で記述
　検査式の作り方：時相理論式で記述
(5)モデルとは
仕様書／ソースコードをモデル検査ツールの専用言語で記述したもの
(6)検査式とは
検査したい性質を時相論理式（CTL 式）で記述したもの
(7)モデル検査の原理
・不具合が見つかる原理
　モデルを検査する→モデルで不具合を発見
　モデルの基（仕様書／ソースコード）にも不具合がある

(8) さまざまなモデル検査ツール
・SMV 系→推奨する（実業務に適用すると大きな状態のモデル検査が必須であるため）
・SPIN
・UPPAAL
(9) SMV について
・状態遷移系を論理式に変換して、論理積や論理和などの記号処理を用いてモデル検査を実行
・SMV の内部データ構造は二分決定グラフ
・SMV は、記号モデル検査＋二分決定グラフ
(10) NuSMV について
SMV の種類は 4 つ

◆検査の流れ
(1) モデル検査のデモ
（ここでデモの説明が有りました）
加速・減速ボタン押下時の表示不正の検知の仕組みを説明頂きました。
(2) 検査の流れ
（火星探査機に搭載されたシステムをサンプルとして説明頂きました）
変数を抽出して、変数が取りうる値を決定する。
仕様を読みながら「変数毎の状態遷移図」を作成する
コーディング
検査式の作成

◆モデル検査の普及に向けて
(1) 社会人向け教育
・トップエスイープロジェクト
（テストと検証・形式仕様記述）
・スマートエスイー
（IoT／AI コース）
(2) 形式手法ワークショップ
・ソフトウェアエンジニアリングシンポジウム 2023
2012 年から形式手法ワークショップを開催
事例・研究発表
情報交換（議論）
モデル検査のチュートリアル
・ウインターワークショップ 2024 イン鹿児島
産学連携によるソフトウェア工学と形式手法の利用推進
(3) モデル検査技術者育成
・モデル技術者育成の流れ
モデル検査初級セミナーの受講
最初に適用するシステムの選定
OJT 形式での人材育成
(4) モデル検査技術者育成
・モデル検査の課題 1：プロセスモデルが必要
モデル検査の適用プロセスの確立
アウトプットの定義→モデル検査報告書
・モデル検査の課題 2：上流と下流の両方で活用したい
上流工程での適用
→設計段階で検査⇔設計を繰り返して品質向上

設計が FIX した時点で設計内容の最終検査
設計からのモデルの自動変換ツールの開発
下流工程での適用
→ソースコードのモデル検査
実際に動作する「もの」の検査が可能
障害の再現や原因究明が可能
・モデル検査の課題 3：状態爆発を抑えたい
検査対象すなわちシステムが取り得る状態空間の増大に伴って、処理時間とメモリ使用量が指数関数的に増大し、現実的な時間でモデル検査ツールが終了しない
→基本はシステムの抽象化と絞りこみ
モデル検査ツールのオプションも活用
(5)企業における導入の進め方
・モデル検査は事前に効果が見えにくい
→説明するより成果でアピール
・社内でどのように知名度を広めたか？
不具合で困っているプロジェクトを探す
常に適用対象を募集
適用結果は報告書にまとめた
事例（成果）が増えたら、成果報告会を開催。また、対外発表を行った。

◆事例紹介
(1)C 言語プログラムの検査
うるう年判定のプログラム
(2)回路図のデモ
回路図からモデル作成

（講義の感想）

今回の講義は、モデル検査に関して、ソースコードの事例も交えながら、検査の流れを詳しく説明頂きました。また、途中で複数のデモを紹介いただき、実践事例に関する理解が深まる講義となりました。講義内容が非常に高度で複雑なものでしたが、具体事例やデモを通して、丁寧に説明いただき、とても参考になりました。
特にモデル検査を通して、実際にバグを検知した経験（事例）を用いて説明頂いたことで、聴講者としても具体的なイメージが湧いたのではないかと思います。
また、後半では教育展開・ワークショップの紹介があり、より深い知識を習得するためのプランなども持つことができる講義でした。
大変有意義な講義、ありがとうございました。

以上