The University of Osaka
Institutional Knowledge Archive

| | |
|---|---|
| Title | A Study of Model Checking Techniques with Emphasis on Program Verification and Probabilistic Analysis |
| Author(s) | 関澤, 俊弦 |
| Citation | 大阪大学, 2009, 博士論文 |
| Version Type | |
| URL | https://hdl.handle.net/11094/49701 |
| rights | |
| Note | 著者からインターネット公開の許諾が得られていないため、論文の要旨のみを公開しています。全文のご利用をご希望の場合は、<a href="https://www.library.osaka-u.ac.jp/thesis/#closed">大阪大学の博士論文について</a>をご参照ください。 |

*The University of Osaka Institutional Knowledge Archive : OUKA*

https://ir.library.osaka-u.ac.jp/

The University of Osaka

【11】

| | |
|---|---|
| 氏　　名 | 関　澤　俊　弦（せき　ざわ　とし　ふさ） |
| 博士の専攻分野の名称 | 博　士（情報科学） |
| 学　位　記　番　号 | 第　２３０５４　号 |
| 学位授与年月日 | 平成 21 年 3 月 24 日 |
| 学位授与の要件 | 学位規則第４条第１項該当<br>情報科学研究科情報システム工学専攻 |
| 学　位　論　文　名 | A Study of Model Checking Techniques with Emphasis on Program Verification and Probabilistic Analysis<br>（プログラム検証と確率解析に重点をおいたモデル検査に関する研究） |
| 論　文　審　査　委　員 | （主査）<br>教　授　菊野　　亨<br>（副査）<br>教　授　尾上　孝雄　　教　授　楠本　真二　　准教授　土屋　達弘 |

## 論　文　内　容　の　要　旨

モデル検査は形式手法の代表的な手法の一つである．モデル検査は，検証対象を表わすモデルと論理式で記述した検証項目を入力として，検証項目がモデル上で成り立つか否かを網羅的な全数探索により検証する．モデル検査は様々なシステムの検証に適用されてきた．近年では，ソフトウェアのプログラムを検証するプログラム検証や，情報科学と他分野との境界領域への適用も試みられつつある．本論文は，プログラム検証と確率モデル検査の境界領域への適用に関する研究成果を述べる．

〈プログラム検証〉

プログラム検証は，プログラムが仕様を満たしていることを検証する．近年，プログラム検証は成功を収めつつあるが，未だ解決が困難な問題も多い．特に，ポインタ操作はヒープ構造を破壊的に操作するため検証が困難である．また，遷移系の大きさが爆発的に増加する状態数爆発も問題である．

第 2 章で，ヒープ構造における空間的な性質を記述する時相論理 2CTL を導入し，その充足可能性判定器の性能評価のためのベンチマーク用論理式生成法を提案する．提案手法は，自然数のパラメータをもつ時相論理式を体系的に生成する手法であり，恒真な論理式から複雑な論理式を帰納的に生成することが特徴である．結果，性能評価のためのベンチマーク論理式生成が容易となる．提案手法を用いて生成したベンチマークを用いて 2CTL の充足可能性判定器の性能評価を行なった結果を示す．提案手法は 2CTL に限らず他の時相論理式にも適用可能である．

第 3 章では，ポインタ操作を含むプログラム検証を目的とした，述語抽象化手法を用いた抽象遷移系生成器 MLAT の詳細を述べる．提案手法では，ポインタ構造と呼ぶ構造と，プログラムの性質を記述可能な時相論理 2CTLN を導入する．ここで，2CTLN 式は，述語抽象化の述語の記述にも用いる．MLAT の要素技術として，簡易プログラミング言語，抽象遷移系生成手法とその正当性，高速化技法に関しても述べる．最後に，片方向リストを操作するプログラムの検証結果を示す．

〈境界領域への適用〉

近年，モデル検査技法を情報科学と他の領域との境界領域に適用する試みがなされているがこれらの研究は途上である。第 4 章では、確率モデル検査の境界領域への適用可能性を調べることを目的として，確率モデル検査を用いた磁性体の簡易モデルである 1 次元イジングモデルの解析を記す．解析に続き，確率モデル検査が物理系の解析に適用可能であることを示し，その妥当性を評価する．本論文では，検証対象を物理現象に限定しているが，イジングモデルはその簡易な定義より，社会学などの他の領でも利用されているモデルであるため，手法の応用性は広い．

## 論文審査の結果の要旨

モデル検査は形式手法の一つであり、ソフトウエアやハードウエアが仕様を満たしているか否かを検証する．本論文は，ポインタ操作を含むプログラムを検証するためのモデル検査の実用化研究の成果と物理現象の解析への確率モデル検査の適用に関する事例研究の成果をまとめている．

先ず，充足可能性判定器の性能評価でベンチマーク用として利用するための時相論理式を体系的に自動生成することに挑戦している．具体的には，ポインタ操作の対象となるヒープメモリの構造

に関する性質を表現するために新たに時相論理２CTL を導入した．その上でベンチマークとして使用するための論理式の条件を明確にした．提案手法は２CTL だけでなく他の時相論理 LTL や CTL にも適用可能である．

次に，状態爆発を解消するための代表的技法である抽象化に注目し，ポインタ操作を含むプログラムの検証を目的としたツールの開発を目指した．開発したツール MLAT ではプログラムとヒープメモリの関係を記述するために時相論理２CTLN を導入したことが特徴となっている．時相論理２CTLN はプログラムの性質が記述できるように２CTL を拡張したものである．片方向リストを操作するプログラム Concatenate を例題としてツール MLAT の評価実験を行った結果，想定されるすべての入力に対して期待される結果が得られることを検証できた．

最後に，境界領域への適用可能性を探るという挑戦のために磁性体の簡易モデルとして知られている１次元イジングモデルの解析を試みた．与えられたイジングモデルから DTMC モデルを構築し，検証すべき物理的特性を PCTL で記述する．次に，確率モデル検査器 PRISM を動かして検証を実行している．DTMC モデルの構築では検証ツールの効率化を特に考慮しており，PCTL の記述では平衡状態に着目することで解析を容易化している．

以上のように，本論文はモデル検査の実用化と適用分野の開拓に関して重要な貢献を果たしている．よって，博士（情報科学）の学位論文として価値のあるものと認める．