氏　　名　奥殿 貴仁

学位(専攻分野)　博士(情報学)

学 位 記 番 号　総研大甲第 2240 号

学位授与の日付　2021年3月 24日

学位授与の要件　複合科学研究科 情報学
学位規則第6条第1項該当

学 位 論 文 題 目　Algebraic Abstraction in Formal Methods

論 文 審 査 委 員　主　査　蓮尾 一郎
情報学専攻 准教授
井上 克巳
情報学専攻 教授
杉山 麿人
情報学専攻 准教授
関山 太朗
情報学専攻 助教
南出 靖彦
東京工業大学 情報理工学院 教授

（様式３）

博士論文の要旨

氏　　名　奥殿 貴仁

論文題目　Algebraic Abstraction in Formal Methods

Formal methods are development techniques to describe and analyze systems and specifications mathematically and help to ensure the safety of systems. As computer programs are being used in safety-critical systems, formal methods are becoming increasingly important. Model checking is a style of formal methods. For a system described as an automaton and a specification for the system, model checking constructs a proof of safety in an algorithmic manner. By transforming a program into an automaton in a proper way, model checking can be applied to verifying program, and program verification by model checking is realized. As model checking automatically constructs safety proofs, it needs less expertise in formal methods to use than other formal methods, but it has problems with applicability to complex systems and scalability.

This thesis aims to expand the range of problems that model checking can be efficiently applied to by looking at algebraic structures underlying target systems. We expect that it improves the applicability of formal methods and encourages the industry to use model checking. There are multiple benefits of using the properties of algebraic structures in model checking. Firstly, writing a target system as an algebraic system leads to the algebraic description of the abstract states, i.e., the subsets of the memory states of the systems. Algebraic descriptions of the abstract states allow us to manipulate them so that we can check the properties of the system computationally. Secondly, as many algebraic structures satisfy the associative law, if a system is compatible with an algebraic structure, the exhaustive search of the system can be done efficiently with memoization or parallelization. Thirdly, we researchers can get an insight by inspecting the underlying structure of a target system and connecting it with other mathematical objects.

In Chapters 3 and 4, we develop methods of interpolant generation, which can be regarded as abstraction methods in program verification. Interpolants (or Craig interpolants) are considered to be essential predicates to analyze the properties of programs, and commonly used in model checking of various types of programs. Chapter 3 aims to improve interpolant generation for programs with polynomials. Dai et al.'s technique could not generate interpolants when the given data are “barely disjoint.” We make the technique works in this situation by (1) proposing a substructure of the polynomial ring $\mathbb{R}[\vec{X}]$, called the strict cone, and by (2) proposing a simplification of ratios to deal with numerical erros that occurs in interpolant generation. Chapter 4

aims to improve interpolant generation in the bit-vector theory for programs in which integer variables cause the overflow and wraparound. For this task, Griggio's technique uses an interpolant generation in the linear integer arithmetic, and it has an advantage that it generates interpolants while preserving the semantics of the program. However, they reported that it sometimes fails at generating interpolants by failing to deal with the overflow. We look at the group $(\mathbb{Z}/\ n\mathbb{Z})^d$, which represents the memory space, combine it with a torus, and propose a new technique, called *boxing and gapping*, for this task.

Chapters 5 and 6 aim to approximate a complex system with a weighted finite automaton (WFA). A WFA is a quantitative extension of a deterministic finite automaton, and models a function from words to real numbers. Applying model checking to complex systems is often impractical. We advocate that the scenario of applying a formal method to an approximated system to certify the safety of the approximated system is useful to know the partial safety of the original system. Chapter 5 aims to approximate a recurrent neural network with a weighted finite automaton over $\mathbb{R}$. For this task, we propose a method to compare a candidate approximated WFA with an recurrent neural network to be approximated. The approximation is driven by Balle and Mohri's algorithm, which learns a weighted finite automata from given data, and the comparing method is used as a subroutine of Balle and Mohri's algorithm. Chapter 6 aims to extend Balle and Mohri's algorithm for general semirings, including the max-plus semiring, and improve the flexibility of techniques to approximate complex systems with weighted finite automata. We show that the naive extension of Balle and Mohri's algorithm outputs an “unfaithful” weighted finite automaton, which ignores some given data, as some properties of fields do not necessarily hold in general semirings. We prove that *column-closedness* is necessary to ensure “faithfulness,” and propose a new algorithm to assure the column-closedness.

Form8・Separate Sheet
（様式８・別紙１）

Results of the doctoral thesis screening

博士論文審査結果

Name in Full
氏　　名　奥殿 貴仁

Title
論文題目　Algebraic Abstraction in Formal Methods

本論文は「Algebraic Abstraction in Formal Methods（形式手法における代数的抽象化）」と題し，形式手法 formal methods の研究分野において代数学の数学的成果を活用することで，より実効的な手法・アルゴリズムを樹立することを目指した研究の成果を述べている．形式手法の主要な目的は，ソフトウェアや情報システムの振る舞いが所与の望ましい性質（仕様）を充足することを数学的に証明することである．その証明手法のうち特にモデル検査とよばれる手法群は，対象システムのモデルを有限的に表現した上で自動の網羅的検査を行うことにより，仕様充足の証明を自動で行う手法群である．モデル検査の諸手法・アルゴリズムは自動で動作するという大きな利点がある一方，その実効性は対象システムの有限的表現の形式及びサイズに大きく依存しており，実効的なモデル検査のためにはシステム表現とアルゴリズムの両者の注意深い検討が必要となる．本論文の全体を貫く指針は，先に述べた課題に対し，代数学の諸成果を活用した抽象化の利点を追求する，というものである．より具体的に，本論文では代数的抽象化を形式手法に応用した４つの研究成果が述べられている．

本論文は７つの章から構成され英語で書かれている．第１章では形式手法とモデル検査について研究の背景が述べられたあと，代数的抽象化という本論文全体の指針が例を挙げながら説明され，４つの具体的研究成果の概要が述べられている．第２章では，４つの具体的研究成果のいくつかに通底して用いる既存の技術的内容，具体的にはオートマトン学習と補間論理式によるプログラム検証について，予備的議論がなされている．

第３章では本論文の４つの提案手法の１つ目として，プログラム検証における述語抽象化のための補間論理式の生成の新たな手法を提案している．ここでは Dai らによる既存手法が知られており，実代数幾何学（特に Positivstellensatz）の応用が試みられていた．本章では Dai らの手法の限界を明らかにした上で（２つの領域が接している場合には補間論理式を生成できない），これを克服するための新たな代数学的知見を導入し（具体的には positive cone の概念と，連分数展開の拡張たる比の簡単化アルゴリズム），これらを新たな補間論理式生成アルゴリズムとして統合して，その実効性を実験によって評価している．

第４章では本論文の４つの提案手法の２つ目として，ビットベクトルの代数的理論における補間論理式生成の新たな手法を提案している．ビットベクトルはプログラミング言語の処理系でよく用いられる整数表現であり，この場合のプログラム検証においては，ビットベクトルのオーバーフローという特有の困難に対処する必要がある．本章の提案手法は，ビットベクトルの理論における補間論理式生成のために boxing と gapping という新たなアイデアを導入するものであり，Griggio による既存手法との比較において性能向上を実現している．また，上記の提案手法は，ビットベクトルの持つ代数構造の特徴づけ（トー

ラス）に基づいている．

第５章では本論文の４つの提案手法の３つ目として，再帰ニューラルネットワーク（RNN）を重み付き有限状態オートマトン（WFA）として近似するためのオートマトン学習アルゴリズムを提案している．RNN から有限状態オートマトンを抽出すると，後者を単純な近似モデルとしてさまざまな形式手法で解析することにより，RNN の振る舞いの近似的解析が可能になる．本章で提案する手法は Weiss らによる既存研究（重みのない DFA を抽出）を重み付きに拡張するものである．ここでは Angluin の L*アルゴリズムの重み付き拡張たる Balle らによる重み付きオートマトン学習アルゴリズムをもとにしているが，特に equivalence query への返答において RNN 内部状態の回帰による近似を用いることが新規性となっている．提案手法の実効性は実験によって評価されている．

第６章では本論文の４つの提案手法の４つ目として，max-plus semiring 上の重み付きオートマトンの L*型学習アルゴリズムを提案している．Angluin の L*アルゴリズムは，その数学的クリーンさによって代数的拡張が容易であり，一般の semiring への拡張が知られていた．本章では，この拡張を max-plus semiring に適用した場合に起こる望ましくない現象を同定し（学習されるオートマトンの出力と以前の membership query への回答は一致すべきだが，一致しない場合がある），その原因を解析して，これに対処すべく column closedness という一般的概念を提案している． 本章の主貢献は column closedness を保つべく変更した L*型学習アルゴリズムであり，max-plus semiring へ適用した際の実効性が実験によって評価されている．

最後に，第７章では本論文の貢献をまとめ，今後の研究課題と展望を示している．

本論文にまとめられた研究の成果は査読付き国際会議予稿集のフルペーパー3 篇として発表されている．これらの論文を含めた出願者の出版業績は以下の通りである： 主著者となる査読付きトップ国際会議予稿集フルペーパー2 件，その他の主著者となる査読付き国際会議予稿集フルペーパー1 件，以上の他に共著者となるトップ国際会議予稿集フルペーパー1 件．

公開発表会では博士論文の章立てに従って発表が行われた．その後に行われた論文審査会及び口述試験では，審査委員からの多数の質疑に対し的確に回答がなされた．ここでの回答は，論文全体や分野全体・他分野を俯瞰した包括的内容から，個々の技術的詳細及びその背景・関連研究に関わる個別の内容まで多岐にわたり，出願者の当該研究内容に対する深い理解を十分に示すものであった．

質疑応答後に審査委員会を開催し，審査委員で議論を行った．審査委員会では，出願者の博士研究について，代数的抽象化という大きな指針を元に様々な具体的成果を積み重ねたものであり，ソフトウェア科学の数学的研究に対して優れた貢献を行うものであることが評価された．

以上を要するに本論文は，ソフトウェアの信頼性に数学的証明を与えるという形式手法の研究分野において，４つの新手法の提案を通じて代数的抽象化という方法論の有効性を示したものである．本論文の４つの具体的貢献は，形式手法の新規なアルゴリズムを提案するのみならず，関連する代数学の数学的理論を発展させるものにもなっており，その学術的価値および実用上のポテンシャルは大きいと認められる．

以上の理由により審査委員会は，本学位論文が学位の授与に値すると判断した．