審 査 の 結 果 の 要 旨

氏　　名　　田辺　良則

従来、グラフ構造により意味論が与えられる論理体系として、様相論理が知られている。特に、Kと呼ばれる様相論理をはじめとして、木構造をモデルとする様相論理の体系は決定可能である。その充足可能性判定手続き、すなわち与えられた論理式が整合的かどうかを判定する手続きは、木構造の解析に広く応用されている。しかし、モデルが木構造に限定されない様相論理体系は必ずしも決定可能ではないため、一般のグラフ構造の解析に様相論理を適用することは行われて来なかった。

そこで本研究では、様相論理Kの決定可能な拡張を提案し、その充足可能性判定手続きとその正しさを示している。さらに、その手続きを木構造に限らないグラフ構造の解析に適用することにより、プログラムの検証やセルオートマトンの解析といった、有益な応用が可能となることも示している。具体的には、Kに対し次の４種類の拡張方法を考える：(i)グラフ構造の解析機能を強化するための、不動点演算子μおよびνの導入、(ii)木構造以外のグラフを扱うための、ノミナルと呼ばれる原子論理式の導入、(iii)プログラムの検証に必要な、逆様相演算子の導入、および(iv)ヒープのような特別なグラフ構造を扱うための、関数型クリプキ構造への制限の導入である。しかし、これらすべての拡張を実施した様相論理は決定不能であることが知られている。一方本研究では、拡張を３種類に絞った場合のうち、応用上重要な３つの組み合わせに対し、従来よりも効率的な充足可能性判定手続きを与えている。そしてその正当性を証明することにより、それらの決定可能性を示している。さらに本研究では、以上で示した様相論理の拡張の充足可能性判定手続きに対し、以下の２件の応用事例を示している。１件目は判定手続きのシェープ解析への応用、すなわちポインタ操作を含んだプログラムの検証への応用である。なお具体的なプログラムとして、Deutsch-Schorr-Waite (DSW)マーキングアルゴリズムを検証している。２件目はセルオートマトンの解析である。

論文は、以下の７つの章から構成されている。

第１章では、まず本論文の研究背景として、応用上の目的であるプログラムの検証における課題として、ポインタを含むような現実的なプログラムの検証の難しさを述べている。次に、前述のKの拡張の充足可能性判定手続き、およびプログラム検証への応用として、自動的なシェープ解析手法、ならびに人手を介したより効率的なシェープ解析手法を提案している。そして別の応用として、一次元セルオートマトンの解析を挙げている。次に、これら充足可能性判定手続きの提案と、プログラム検証への応用の理論とツールの実装が、本研究の独自な貢献であることを主張している。本章の最後に、本論文の構成を示している。

第２章では、本論文で使用する様相論理について、Kの構文論と意味論、前述の４種類の拡張、および決定可能性と木構造との関係について詳述している。意味論では、頂点には要素論理式の成否情報を、また辺にはラベルを付加したグラフ構造である、Kripke構造に基づく意味論を説明している。構文論では、命題論理に対し、Kripke構造のラベルmの付いた辺を通った先の全ての、あるいはある頂点で成り立つ、ということを表す様相演算子を追加した体系を定義している。

第３章では、前述した、様相論理体系Kとその拡張の充足可能性判定手続きについて説明している。基本的には伝統的な判定手続きであるタブロー法に基づいた手続きである。通常のタブロー法では、論理式の集合を頂点とするグラフを作成する。一方本論文では、各頂点を、論理式に∞（無限大）を含む数値を割り当てる関数の組とする。これにより、各ノードにおいて、要素となる論理式の証明にかかるステップ数を記録することができる。またその他にも各種の独自の工夫を施すことにより、対象とするKの各拡張の充足可能性判定を可能としている。本章では、本手続きの健全性と完全性、および計算コストの理論的分析と実験による分析を示している。

第４章では、充足可能性判定手続きを利用したシェープ解析を詳述している。まず、ポインタの形式モデル、CやJavaと同様なポインタ操作が可能な簡単なプログラミング言語ＰＭＬ、およびＰＭＬの性質を記述する言語を紹介している。次に、前述の判定手続きの応用により、検証に必要な最弱事前条件を導出する手続きを示す。そして、それを用いてプログラムの抽象的状態遷移系を生成し、線形時相論理(Linear Temporal Logic, LTL)の式で与えられた要求仕様を満たすかどうかを検証する手続きを示している。さらに、この手続きを実装したＭＬＡＴツールを紹介し、ツールの利用例を示している。ＭＬＡＴの実装では、十分な記述能力を保ったまま、使用する様相論理をCTL (Computational Tree Logic)に制限するなどの効率化を行ってい

る。最後に、シェープ解析手法として既存のものを紹介し、本論文の手法がそれらのものより効率的であることを主張している。

第５章では、前章の述語抽象化手続きで導出した状態遷移系が過大なため、人手でサイズの小さい遷移系を作成し、その作成した遷移系の正しさを確認する方法を説明している。そしてその手法をDSWマーキングという、検証が難しいことで知られるアルゴリズムに適用し、実際に検証を実行した実験結果を示している。

第６章では、一次元セルオートマトンの解析への応用を説明している。まずセルオートマトンの説明をした後、その解析のために用いる論理体系2LTLを提示している。そして、無限個のセルからなるオートマトンを、有限の抽象セルからなるオートマトンに変換することにより、元のオートマトンの性質の解析を行う手法を示している。そして、いくつかの例に適用した実験結果を示し、解析が現実的な時間で可能なことを示している。

第７章では、本論文のまとめを行った後、次のような将来の課題を挙げている。まず決定手続きの改良のため、二分決定グラフ(Binary Decision Diagram, BDD)や、ブール代数式の充足可能性判定手続き(SAT solver)の利用を示唆している。次に、プログラムの検証の改良のため、反例の利用や述語の選択方法の改善という方針を挙げている。さらに、定理証明系との統合や、検証可能な性質の範囲の拡大を課題として示している。

以上のように本論文は、応用的に重要な様相論理の効率的な充足可能性判定手続きを、ベースとなるタブロー手法で扱うデータを独自拡張するという、独創的なアイデアで確立し、これにより、従来よりも効率的な判定手続きを実現した。さらにその応用として、シェープ解析、すなわちポインタを扱うプログラムの検証手法として、従来よりも効率的な手続きを確立することにより、プログラム検証技術の実用化の可能性を高めた。さらに、ＤＳＷマーキングという、検証が難しいことで知られるアルゴリズムに適用し、その有効性を示した。加えて、無限サイズのセルオートマトンの解析手法を確立した。この手法は物理系や生物系への応用が可能であり、これらの分野における新たな解析手法の可能性を秘めている。

本論文は、以上のような独自かつ先進的な成果を挙げたものであり、審査委員会は、その独創性、有効性は、博士号に十分値するものと判断した。

よって本論文は博士（情報理工学）の学位請求論文として合格と認められる。