様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成２５年　６月１０日現在

機関番号：51303
研究種目：基盤研究（Ｃ）
研究期間：2010 年度～2012 年度
課題番号：22500021
研究課題名（和文）形式手法のための論理の構築と、一階拡張が満たす性質に関する研究

研究課題名（英文）Research on Construction of a Logic for Formal Methods and Properties of First-Order Extensions

研究代表者
岡本　圭史（OKAMOTO　KEISHI）
仙台高等専門学校・情報システム工学科・准教授
研究者番号：00308214

研究成果の概要（和文）：対象を形式的に記述することで，それらの対象を自動的に検証できるようになる．しかし，形式的に記述・検証するためには，「論理」という枠組みが必要となる．本研究では，Jackson モデルを基にした要求管理を目的とした論理や Milk-run 物流システムの経路探索を目的とした論理を構築した．また，検証用論理として提案された一階様相μ計算に関する性質として，モデル論的性質や表現力比較に関するいくつかの性質をしめした．

研究成果の概要（英文）：If we formalize a target system then we can verify whether the system satisfy desired property. For formal description and verification, we must construct a mathematical logic that is a framework for description and verification. We propose a logic for requirements management based on Jackson's Reference Model and a logic for automated route planning for milk-run transport logistics. Besides, we proved model-theoretic property and expressiveness results for first-order modal mu-calculus.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2010 年度	500,000	150,000	650,000
2011 年度	500,000	150,000	650,000
2012 年度	500,000	150,000	650,000
総　計	1,500,000	450,000	1,950,000

研究分野：総合領域
科研費の分科・細目：情報学・情報学基礎
キーワード：数理論理学，形式手法，命題様相μ計算，　一階様相μ計算，モデル，表現力

１．研究開始当初の背景

現在の社会では，携帯電話や銀行システムなど，多くの産業基盤が情報システムによって支えられている．このようなシステムの規模は年々増大しており，大規模化したシステムは様々な問題(自動車のエンジン制御プログラムの不具合や航空機の自動操縦システムの不具合等)を引き起こしている．

このような問題を解決するためのアプローチのひとつに「形式手法」がある．形式手法は，数理論理学や代数学に基づき，検証対象をモデル化(形式的仕様記述)したり，さらに，そのモデルを検証(形式的検証)したりする手法の総称である．従来の形式手法では，命題線形時相論理(LTL)等の命題時相論理，高階論理，Hennessy-Milner Logic(HML)等の論理を用いて，モデル化や検証を行っていた．

複雑化するシステムをモデル化するために，より表現能力の高い論理が必要になってきており，一階時相論理の部分論理(Decidable fragments of first-order temporal logics, Hodkinson, Wolter and Zakharyaschev, Annals of Pure and Applied

Logic, Vol.106, pp.85-134, 2000)やambient logic の拡張(A Predicate mu-Calculus for Mobile Ambitens, Huimin Lin, Journal of Computer Science and Technology, 2005)等, 新しい論理に関する研究が行われてきた．報告者も，命題様相μ計算の一階への拡張である「一階様相μ計算」を構築し，その研究を行ってきた．

報告者らは，命題様相μ計算を拡張し，一階様相μ計算を定義した．さらに，その論理を用いて，既存の命題様相μ計算では形式化できない対象システムを形式化及び検証し，一階様相μ計算の応用面での有用さを示した．(Formal Verification in a First-Order Extension of Modal μ-calculus, Computer Software, Vol. 26, No. 1 (2009), pp. 103-110, 2009) また，東京工業大学 鹿島氏との共同研究として，一階様相μ計算の一般モデルに対する完全性を証明し，一階様相μ計算の理論的性質の一部を明らかにした．(General Models and Completeness of First-Order Modal μ-calculus, Journal of Logic and Computation, Vol.18, No.4 pp.497-507, 2008)

続いて，これまでの研究成果の今後の発展の方向性について述べる．発展の方向性は，大きく分けて，（１）一階様相μ計算を発展させて形式手法のための新しい論理を構築し，その適用例を例示すること，（２）一階様相μ計算の理論的性質を明らかにすること，の二つが考えられる．（１）の方向性の必要性に関しては，既に述べた．

（２）の方向性の必要性については，応募者らが構築してきた論理は形式手法のための論理であり，論理の意味論の妥当性を研究する①“モデル理論”，形式的仕様記述を行うのに適切な記述力があるか否かを判断するのに必要な性質である②“表現力”や(モデル検査や定理自動証明といった)形式的検証の基礎に必要な性質である③“計算可能性”といった，論理の理論的性質を明らかにする必要がある．したがって，（２）の方向へ研究を発展させることは，論理の応用を考える上でも重要である．また，（１）を行うためには，既に構築した論理の限界を研究する必要があり，それには（２）を行うことが必要である．

２．研究の目的

本研究の内容は，形式手法のための新しい論理の構築と，その論理の性質を明らかにすることである．新しい論理を構築することで，従来の論理では形式的に扱えなかった対象が形式的に扱えるようになり，より多くの製品の信頼性を高めることに貢献できる．また，構築した論理の性質を明らかにすることで，形式手法を適用する際の指針を与えることができる．例えば，新しい論理のクラスの表現力の強弱関係を明らかにすることで，各対象に対し，適切な表現力を持つ論理を選択できるようになる．

３．研究の方法

本研究は，（１）検証のための新しい論理の構築と（２）一階様相μ計算の理論的性質を明らかにすることの二つに分けることができる．

（１）では，既存の論理を拡張することで，新しい論理を構築する．具体的には，Hennessy-Milner Logic(HML)等を拡張し，value-passing CCSやappliedπのための論理を構築する．

（２）では，一階様相μ計算の理論的性質のうち，モデル理論(モデルに関する性質)と表現力(文法に関する性質)を明らかにする．
（２）①モデル理論の研究では，一般モデルと標準モデルの関係に関する研究を行う．
（２）②表現力の研究では，新たな帰納法を提案し，既存の論理を一階拡張したもの達の表現力の強弱を明らかにする．

４．研究成果

(1) 形式手法のための新しい論理構築

①要求仕様の参照モデルとして有名なJackson モデルを基にした（要求管理を目的とした）形式手法のためのモデル及び論理を構築した（雑誌論文２，３及び学会発表４，６）．本参照モデルでは，要求とシステム仕様の関係にドメイン知識の概念を取り入れ，その三つ組みで要求とシステム仕様の関係を定式化するものである．また，本手法では，形式的議論，及び計算機支援実現のための仕組みとして（形式）論理を用いている．具体的には，要求変更が起きた際の「仕様の最弱条件」という概念を定義し，それを計算機により自動的に導くことにより，要求変更のインパクトを測り，要求変更の管理を支援する技法を開発した．さらに，飛行機の着陸時制御システムの要求管理に本手法を適用し，その有効性を示した．(北村は関連成果で，2011年度情報処理学会山下記念研究賞を受賞)

②Milk-run 物流システムの分析・検証のための論理の構築及び，その論理の計算機上で

の実装を行った（雑誌論文１，学会発表２）．本研究では，Milk-run 物流システム複雑性を低減するため，システムの分析・検証の向け論理言語（DR-SL: Delivery Requirements Specification Language）を構築した．さらに，DR-SL から時相論理 LTL（Linear Temporal Logic）の変化形への変換規則を考案した．また，形式文法のみならず時相論理 LTL の変化形の意味論を策定した．加えて，その意味論に基づき，その変化形の計算機上に実装を行った．この議論と DR-SL から LTL への変換規則により，DR-SL の計算機上での実行が可能になった．

（２）一階拡張が満たす性質の調査

① モデル理論

「与えられた有限な一般モデルに対し，それと論理式の真偽に関して等価な標準モデルの構築できること」を，筑波大学坪井氏らとの共同研究で示した（学会発表５）．この結果は，「一般モデルで充足可能な命題様相μ計算の論理式は，標準モデルでも充足可能か？」という本研究項目の主な目標の部分的解決を与えている．

上述の主な目標を解決するために，与えられた一般モデルから，それと論理式の真偽に関して等価な標準モデルを構築することに関する研究を行った．初期の段階で，「与えられた有限な一般モデルに対し，それと論理式の真偽に関して等価な標準モデルの構築できること」を，筑波大学坪井氏らとの共同研究で示した（学会発表５）．

上述の既に示した主張「与えられた有限な一般モデルに対し，それと論理式の真偽に関して等価な標準モデルの構築できること」内の有限という仮定を取り除くことが出来れば，本研究項目の目的を達成できる．そこで，無限モデルから有限モデルへの等価性を保った対応をつけるための研究を実施したが，本研究期間内では未解決である．

② 表現力

命題時相論理の一階拡張達間の表現力比較結果を示した（雑誌論文５及び学会発表１，３）．一階様相μ計算と似た論理を経由することで命題様相μ計算のモデル検査の効率を上げる研究などがある．本研究成果により，一階様相μ計算の部分論理である一階時相論理達の表現力が明らかになることで，記述能力・計算量の観点から，形式的検証などで利用する際に適切な論理を選択出来るようになることが期待できる．

CTL^*の表現力が命題様相μ計算の表現力よりも真に弱いことを示す証明を拡張し，それぞれの一階拡張である，$FOCTL^*$の表現力が一階様相μ計算の表現力よりも真に弱いことを示した（雑誌論文５）．従来の CTL^*及び命題様相μ計算の表現力比較の証明では，論理式の構成に関する帰納法を用いて証明を行う．そこで，（構文的に拡張されている）一階拡張における証明へ拡張するために，帰納法で示す主張を拡張した形式の帰納法による証明を用いて証明を行った．

前述の結果は，$FOCTL^*$の表現力が一階様相μ計算の表現力よりも弱いことを論理式の構成に関する帰納法で証明し，さらに，一階様相μ計算の論理式で $FOCTL^*$の論理式と等価にならない論理式（とそれらが等価にならない構造）を具体的に示すという二つの部分から構成される．他の一階拡張に関しても，ある一階拡張が他の一階拡張の構文的拡張であれば，表現力が強いことは明らかである．したがって，課題は二つの論理が等価でないことを示す論理式を示すことである．

命題時相論理 CTL,LTL,CTL^*の一階拡張（一階時相論理）を，それぞれ FOCTL,FOLTL,$FOCTL^*$とする．このとき，命題時相論理間の表現力比較と同様の結果が成り立つことを示した（学会発表１，３）．具体的には，FOCTL＜$FOCLT^*$，FOLTL＜$FOCTL^*$，FOLTL≦FLCTL，FOCTL≦FOLTL が成り立つことを，文献 ”Sometimes” and ”Not Never” revisited: on branching versus linear time temporal logic, Emerson, Halpern で用いられている証明の構造・帰納法を一階へ素朴に拡張して証明した．

（３）今後の展望

① 形式手法のための新しい論理構築

Milk Run 問題以外にも，時相論理式による制約記述が有効な分野を調査する．有効と思われる分野に対し本研究で構築した論理を適用・改良し，各種の制約が充足されるか否かを検証する方法を合わせて開発する．これらの研究により，従来は検証が困難であった対象・性質に対しても，自動検証が可能となることが期待される．

② モデル理論

一般モデルと標準モデルの充足性に関しては，モデルが有限であるという仮定の下での等価性を，筑波大学坪井氏らとの共同研究において示した．そこで，Finite Model Property の成り立つ条件を精査し，無限モデ

ルから有限モデルへの対応をつけることで，無限モデルと有限モデルのギャップを埋めるための研究を行う．この研究により，一般モデルに対する充足可能性と，標準モデルに対する充足可能性が等価になることを目指す．

③ 表現力

表現力比較の一般論を模索する．具体的には，時相論理 L1 と L2 が L1≦L2 を満たす時，L1 と L2 に同じ論理記号を付加することで拡張して得られる論理 L1 ' と L2 ' が L1 ' ≦L2 ' となるための条件を調査する．この研究により，論理の拡張を行う毎に表現力比較結果を証明せずとも，論理記号を付加する段階で表現力の強弱が不変であることが保証されるようになる．

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 5 件）

1. Takashi Kitamura and Keishi Okamoto, Automated route planning for milk-run transport logistics with the NuSMV model checker, The IEICE Transactions on Information and Systems, Special Section on Parallel and Distributed Computing and Networking, 査読有, 条件付き採録

2. Takashi KITAMURA, Keishi Okamoto, Makoto TAKEYAMA, Formal Validation and Requirements Management Based on the Jackson's Reference Model for Requirements and Specifications, Proceedings of the 16th IEEE Pacific Rim International Symposium on Dependable Computing, 査読有, Published electronically, 2010

3. 北村崇師, 岡本圭史, 武山誠, Jackson の要求・仕様参照モデルに基づく要求追跡の形式手法, Proceedings of the IPSJ/SIGSE ソフトウェアエンジニアリングシンポジウム, 査読有, 2010, 149～154

4. Keishi Okamoto, Formal Verification in a First-Order Extension of Modal μ-calculus, Information and Media Technologies, 査読有, 5(1), 2010, 40～47

5. Keishi Okamoto, Comparing expressiveness of first-order modal μ-calculus and first-order CTL*, 京都大学数理解析研究所講究録, 査読無, 1708, 2010, 1～14

〔学会発表〕（計 6 件）

1. 岡本圭史, 一階時相論理の表現力について, 日本数学会 2013 年度年会, 2013 年 3 月, 京都大学

2. Takashi Kitamura, Keishi Okamoto, An automated route planning for milk-run transport logistics using model checking 4th International Workshop on Parallel and Distributed Algorithms and Applications, 2012 年 12 月, Okinawa, Japan

3. 岡本圭史, 命題時相論理の一階拡張について, 2010 年日本数学会秋季総合分科会, 2012 年 3 月 27 日, 東京理科大学

4. Takashi KITAMURA, Keishi Okamoto, Makoto TAKEYAMA, Formal Validation and Requirements Management Based on the Jackson's Reference Model for Requirements and Specifications, The 16th IEEE Pacific Rim International Symposium on Dependable Computing, 2010 年 12 月 15 日, National Institute of Informatics, Tokyo, Japan

5. Yuki ANBO, Keishi OKAMOTO and Akito TSUBOI, Toward a Concise Proof of Completeness Theorem for Propositional Modal \mu-calculus, 2010 年日本数学会秋季総合分科会, 2010 年 9 月 22 日, 名古屋大学

6. 北村崇師, 岡本圭史, 武山誠, Jackson の要求・仕様参照モデルに基づく要求追跡の形式手法, ソフトウェアエンジニアリングシンポジウム 2010, 2010 年 9 月 1 日, 東洋大学

〔その他〕
なし

６．研究組織
(1)研究代表者
岡本　圭史（OKAMOTO　KEISHI）
仙台高等専門学校・情報システム工学科・准教授
研究者番号：00308214

(2)研究分担者
北村 崇師（KITAMURA TAKASHI）
産業技術総合研究所・セキュアシステム研究部門・研究員
研究者番号：70530484