様式 C-19

科学研究費補助金研究成果報告書

平成２２年　６月１８日現在

研究種目：若手研究（Ｂ）
研究期間：2008～2009
課題番号：２０７００００４
研究課題名（和文）　モデル検査における抽象化の再利用

研究課題名（英文）　Reuse of Abstraction in Model Checking

研究代表者
西澤　弘毅（NISHIZAWA KOKI）
鳥取環境大学・環境情報学部・講師
研究者番号：６０４５５４３３

研究成果の概要（和文）：
ソフトウェアやハードウェアの誤動作によって起こる社会的な問題は後を絶たない。そこで、これらのシステムを稼働前に検証するモデル検査の技術が広まりつつある。本研究では、モデル検査で不可欠な「抽象化」と呼ばれる効率化情報を再利用または修正するための理論を与える。ある性質の検証には有効であった抽象化も、別の性質の検証にはまったく役に立たない場合があるため、現在のシステム検証の現場では、抽象化のコストが高い。本研究によって抽象化の再利用が進めば、抽象化のコストを下げることができる。本研究では特にさまざまな多値論理の間で抽象化を再利用するための理論を与える。抽象化の正しさは多値論理と模倣の理論に基づいて数学的に保証する。
研究成果は以下の通りである。４つの多値論理（Frame、DeMorgan Frame、Bilattice、MixedTS）を例に含む一般性の高い不動点論理を提案した。その論理のもとで、「随伴の対」によって抽象化を定義し、この抽象化によって検証結果を引き戻せることを証明した。そして、論理を変えたときに、抽象化を再利用できるための十分条件を与えた。
関連研究として、べき集合を用いた多値論理の上の単項演算子についても分析した。その結果、単項演算子の別表現として知られる「多重関係」の階層構造と、クリーネ代数の階層構造との対応付けを発見した。

研究成果の概要（英文）：
There is no end to the number of problem posed by bugs of software and hardware. Model checking is the technique to verify such systems. We gives a theory to reuse ‘abstraction’ that is efficiency technology in model checking. The cost of abstraction is high, because even if an abstraction is efficient to verify a property, it may be inefficient to verify other properties. If this result allows us to reuse abstractions, it reduces the cost of abstractions. We especially gives a theory to reuse abstractions between different multi-valued logics. The validity of abstractions is mathematically guaranteed by using theories about multi-valued logics and simulations.
The results are as follows. We give a general fixed point logic including four multi-valued logics (Frame, De Morgan Frame, Bilattice, Mied TS) as examples. Under the logic, we formulate abstractions by using ‘the pair of two adjunctions’ and prove that the abstraction allows us to pull back results of verification. Moreover, we give the sufficient condition to reuse such abstractions.
As related work, we also analyze unary operators on multi-valued logics whose truth values form a powerset. We discover the correspondence between the hierarchy of Kleene algebras and the hierarchy of multirelations that is another representation of such unary operators.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
２００８年度	1,000,000	300,000	1,300,000
２００９年度	500,000	150,000	650,000
年度			
年度			
年度			
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：　情報基礎、システム検証、モデル検査、抽象化、多値論理

１．研究開始当初の背景

モデル検査とは、システムＳが性質Ｐを満たすかどうかをコンピュータに自動的に判定させる検証法であり、その基本的なアルゴリズムは、システムの取りうる状態を網羅的に探索することである。そのため、テストとは違って完全な検証が可能である。

しかし現実には巨大で複雑なシステムをモデル検査するためには、抽象化と呼ばれる効率化が必要である。抽象化とは、検証したい複雑なシステムＳに対し、それよりも単純なシステムＴを生成し、検証結果を引き戻せる（Ｔが満たす性質をすべてＳも満たす）ということを数学的に証明しておく手法である。これにより、単純なシステムＴが性質Ｐを満たすことだけモデル検査すればよいことになる。

モデル検査で扱える「性質」とは具体的には様相論理や時相論理の論理式であり、扱える真偽値は長い間「真」「偽」の２値であったが、2000 年ごろから、いろいろな真偽値を扱うための研究が進められている。たとえば、「真」「偽」「未確定」「矛盾」の４値、「0」「0.5」「1」の３値、などの有限個の真偽値を扱えるものから、0 から 1 までの任意の実数を真偽値とするファジー論理や、実数からなる任意の開集合を真偽値とする論理など、無限個の真偽値を扱えるものまである。これにより、不正確な情報を含むシステムの検査や、複数のシステムを重ね合わせたものの検査などが行えるようになった。このように、２値に限らない真偽値を用いるモデル検査を多値モデル検査という。

２．研究の目的

多値モデル検査のおかげで、不正確な情報を含むシステムの検査や、複数のシステムを重ね合わせたものの検査などが行えるようになった。しかし、真偽値の集合が変わると論理そのものが変わる。したがって、ある論理Ｌの中でシステムＴの検証結果をシステムＳに引き戻せても、別の論理Ｌ'の中ではそうとは限らない。そのため現状では、論理Ｌ'のために新たに抽象化をしてシステムＴ'を生成しなければならない。本研究は、そのような抽象化のやり直しのコストを下げるため、抽象化をそのまま再利用可能かどうか判定して、不可能ならば修正するための、理論を与える。

３．研究の方法

真偽値に関する十分条件を簡潔かつ効率的に与えるために、本研究は、抽象化や論理を圏論的な概念を用いて定式化するというアプローチを取る。圏論は、集合と写像、代数と準同型、位相と連続写像、などの対を「対象と射」として統一化した理論体系であり、既存の定理の統一化や一般化に役立つ。

本研究は、抽象化を「随伴の対」を用いて定式化するというアプローチを取る。

随伴とは、対象 f(x)から対象 y への射と、対象 x から対象 g(y)への射が一対一に対応するような、函手 f と g の対のことである。随伴を使って、プログラムの静的解析の理論を

統一的に説明できることや、２値論理での模倣や双模倣といった抽象化を定式化できることは、これまで知られていた。本研究では、随伴を多値論理の抽象化にも応用する。ただし、「A」と「A の否定の否定」が一致しない多値論理においては、抽象化を一つの随伴では定式化できない。本研究では、そのような多値論理での抽象化を「随伴の対」によって定式化できることを明らかにする。

４．研究成果

本研究の成果は、「随伴の対」によって抽象化を定式化したことと、抽象化を再利用できるための十分条件を与えたことである。

扱う論理の前提条件は、真偽値集合が少なくとも完備束の構造を持っていることである。今、真偽値集合がＬであるような論理Ｌを考える。そのもとで、状態集合Ｓをもつシステムと、状態集合Ｔをもつシステムを考える。以降では、ＳからＬへの単調写像全体からなる半順序集合を[S,L]と書き、ＴからＬへの単調写像全体からなる半順序集合を[T,L]と書く。そのうえで、ＴがＳの抽象化であるとは、以下を満たすαとβが与えられることとする。

1. αは[S,L]から[T,L]への写像で、しかも右随伴を持つ。
2. βは[T,L]から[S,L]への写像で、しかも右随伴を持つ。
3. 論理Ｌの論理演算子のうち、束の演算子を除いた残りは、αとβとの間で緩変換条件を満たす（緩変換条件の厳密な定義はここでは省略）。

上記の抽象化が与えられているとき、システムＴからシステムＳへ、検証結果を引き戻すことが可能である。

しかし、ここで別の論理Mに基づいてシステムＳを検証し直そうとすると、一般にはＴがＳの抽象化になるとは限らない。したがって、システムＴの検証結果をシステムＳに引き戻せるとは限らない。本研究では、そのような場合でもＴがＳの抽象化であり続けるための、ＬとMに関する十分条件を与えた。すなわち、抽象化を再利用できるための十分条件である。

それは、ＬとMの間にも「随伴の対」が存在することである。つまり、ＬからMへの写像で右随伴を持つ写像と、MからＬへの写像で右随伴を持つ写像が、与えられることである。

この「随伴の対」があれば、まず[S,L]と[S,M]の間の「随伴の対」を自然に構成できる。それを用いて、ＳによるＬの解釈から、ＳによるMの解釈を構成できる。この構成は Cousot らの抽象解釈の理論を拡張したものである。

同様に、[T,L]と[T,M]の間の「随伴の対」を構成し、それを用いて、ＴによるＬの解釈から、ＴによるMの解釈を構成できる。

こうして得られた、ＳとＴによるMの解釈の間には、抽象化の関係が成り立つ。したがって、システムＴの検証結果をシステムＳに引き戻すことが出来る。

典型的な具体例を紹介する。「真」「偽」からなる２値論理をＬとし、「0」「0.5」「1」からなる３値論理をMとする。このとき、ＬからMへの自然な埋め込みは、「真」を「1」へ、移し、「偽」を「0」に移す写像である。この写像は、右随伴も左随伴も持つ。したがって、これらから「随伴の対」が作られる。

このほかに、関連研究として、べき集合を用いた多値論理の上の単項演算子についても分析した。その結果、単項演算子の別表現として知られる「多重関係」の階層構造と、クリーネ代数の階層構造との対応付けを発見した。

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４件）

H. Furusawa, N. Tsumagari, K Nishizawa、A Non-Probabilistic Relational Model of Probabilistic Kleene Algebras 、 Proc. Relations and Kleene Algebra in Computer Science, LNCS、査読有、Vol.4988、2008、pp.110－122

Y. Kinoshita and K. Nishizawa 、An algebraic semantics of predicate abstraction for PML、コンピュータソフトウェア、査読有、Vol.26、No.2、2009、pp.147－156

H.Furusawa, K.Nishizawa, N.Tsumagari、Multirelational Models of Lazy, Monodic Tree, and Probabilistic Kleene Algebras、Bulletin of Informatics and Cybernetics、査読有、Vol.41、2009、pp.11－24

K. Nishizawa、N. Tsumagari、H. Furusawa、The cube of Kleene algebras and the triangular prism of multirelations 、Relations and Kleene Algebra in Computer Science RelMiCS/AKA (Springer LNCS)、査読有、Vol.5827、2009、pp.276－290

〔学会発表〕(計２件)

津曲紀宏, 西澤弘毅, 古澤仁、二項多重関係の反射的推移的閉包、日本ソフトウェア科学会 25 回大会、2008 年 9 月 11 日、筑波大学

K. Nishizawa、Multi-valued modal fixed point logics for model checking、39th International Symposium on Multiple-Valued Logics、2009 年 5 月 21 日、沖縄産業支援センター、招待講演

〔図書〕(計０件)

〔産業財産権〕

○出願状況（計０件）

○取得状況（計０件）

〔その他〕

なし

６．研究組織
(1)研究代表者
西澤　弘毅（NISHIZAWA KOKI）
鳥取環境大学・環境情報学部・講師
研究者番号：６０４５５４３３

(2)研究分担者

なし

(3)連携研究者

なし