様式 C-19

科学研究費補助金研究成果報告書

平成２１年４月１０日現在

研究種目：基盤研究（Ｃ）
研究期間：2006～2008
課題番号：18500019
研究課題名（和文）　証明支援系とモデル検査器を効果的に利用できる環境と方法論

研究課題名（英文）　Methodology and Environment for Effectively Using Theorem Provers and Model Checkers

研究代表者
緒方　和博　（OGATA KAZUHIRO）
北陸先端科学技術大学院大学・情報科学研究科・准教授
研究者番号：30272991

研究成果の概要：証明支援系とモデル検査器を効果的に利用できるよう、定理証明向きのシステム仕様をモデル検査向きのシステム仕様に自動変換する方法を考案した。変換により、モデル検査向きのシステム仕様が大きくなりすぎて効果的にモデル検査ができなくなることを防ぐための工夫を行った。提案した変換方法の有効性を確認するため、電子商取引プロトコル iKP と Mondex の検証実験に適用した。また、変換を支援する変換ツールの拡張性の高い実装方法も提案した。この実装方法では、複数の変換規則をモジュラーに組み入れることを可能にする。

交付額

（金額単位：円）

	直接経費	間接経費	合　計
２００６年度	1,100,000	0	1,100,000
２００７年度	1,300,000	390,000	1,690,000
２００８年度	1,200,000	360,000	1,560,000
年度			
年度			
総　計	3,600,000	750,000	4,350,000

研究分野：形式手法
科研費の分科・細目：情報学・ソフトウエア
キーワード：仕様記述、仕様検証、モデル検査、仕様変換、観測遷移システム、CafeOBJ、Maude、メタプログラミング

１．研究開始当初の背景

我々の生活はコンピュータシステムに深く依存するようになってきた。このため、安心して生活を送るには、を安全にすることは不可欠である。コンピュータシステムを安全にするには、開発の各工程でコンピュータシステムの安全性を確認しつつ開発すればよい。開発の上流工程（仕様書の作成や設計）でコンピュータシステムの安全性を確認する方法の一つは、形式手法（formal methods）である。形式手法は、コンピュータシステムの数学モデルを作成し、モデルが所望の性質を有すこと等を科学的に確かめることにより、安全性を確認する方法である。

形式手法を支援する多くのツール（ソフトウェア）も開発されている。主に使われているものは大きく二つに大別できる。モデル検査器（model checkers）と証明支援系（interactive proof assistants）である。モデル検査器と証明支援系は、以下のように、補完的な関係にある。

1. コンピュータシステムを（状態空間が十分に小さい）有限状態機械としてモデル化できれば、モデル検査器は、モデルが所望の性質を有すことを自動で確認できる。
2. 有限状態機械が所望の性質を有しない場合、モデル検査器は自動で反例を提示する。
3. 証明支援系は、無限状態機械が所望の性質を有すことも確認できる。ただし、ユーザは証明支援系との対話を必要とする。
4. 証明支援系との対話により、隠れた事実（補題等）を発見することができ、対象であるコンピュータシステムの理解をさらに深めることができる。

しかし、両方のツールを効果的に利用できる環境は整っていない。このため、両方のツールを利用するには、コンピュータシステムの数学モデルを別々に記述する必要がある。つまり、二つのドキュメントを作成する必要がある。二つのドキュメントを作成するのは時間の浪費になるかもしれない。さらに、記述の途中で、二つのドキュメント間に不整合が混入するかもしれない。

モデル検査器と証明支援系はコンピュータシステムの安全性を確認するための相補関係にある基盤技術であり、それらを効果的に利用できることは 21 世紀の高度情報化社会において本質的に重要であるという認識に基づき、本提案研究を行った。

２．研究の目的

証明支援系のために記述されたコンピュータシステムの数学モデルのドキュメント（仕様書あるいは設計書）を、モデル検査器用のドキュメントに自動変換することで、両方のツールを効果的に利用できる環境を提供し、両方のツールを効果的に利用できることを明らかにすることが、本提案研究の目的である。

３．研究の方法

研究代表者（緒方）は、北陸先端科学技術大学院大学の二木教授の研究グループにおいて、適切な抽象度・詳細度でコンピュータシステムをモデル化することを可能とする観測遷移システム（あるいは振舞仕様）によるコンピュータシステムの解析法（検証法）の研究に従事してきた。観測遷移システムは振舞仕様の特殊形である。観測遷移システムによる解析法は、北陸先端科学技術大学院大学の二木教授を中心に開発された代数仕様言語・処理系 CafeOBJ を、数学モデルの記述言語ならびに証明支援系として用いる。CafeOBJ による数学モデルの記述は、もっとも基本的な論理式である等式を用い、CafeOBJ による証明(解析あるいは検証)は、他の方法と比べ理解・習得が容易な、書き換えによる等式推論に基づく。

また、研究代表者は、米国 SRI International 研究所および University of Illinois の Urbana-Champaign 校で開発された Maude の提供するモデル検査機能による観測遷移システムの解析方法に関する研究にも従事してきた。CafeOBJ と Maude は、最も有名な代数仕様言語・処理系の１つである OBJ3 の継続である。このため、CafeOBJ と Maude は姉妹言語・処理系の関係にある。

本提案研究では、CafeOBJ を証明支援系として、Maude をモデル検査器として用いた。観測遷移システムの定理証明向きの CafeOBJ 仕様を、モデル検査向きの Maude 仕様に自動変換することで、証明支援系とモデル検査器を効果的に利用できる方法論と環境の開発を目指した。

４．研究成果

(1) 変換法

観測遷移システムの定理証明向き CafeOBJ 仕様（振舞仕様）を、モデル検査向きの Maude 仕様（書換え論理仕様）に素直に変換を試みると、有限の Maude 仕様では表現できないものがあることがわかった。これは、振舞仕様では、１回の状態遷移により、無限個の値を変更するようなことを容易に記述できるのに対し、有限の書換え論理仕様では、基本的に、１回の状態遷移により変化させることのできるのは有限個の値に限られるからである。

振舞仕様を書換え論理仕様に変換した後で、モデル検査を実際に行うには、システムやプロトコルに参加するプロセスや主体の数を決める必要がある。仕様を変換した後で決めるのではなく、変換する時点で決めるようにすれば、上記の問題を回避できることがわかった。

この方針に則った変換方法を形式化し、この変換方法は「変換によって得られる書換え論理仕様に反例があれば、変換前の振舞仕様にも対応する反例がある」という性質を満たしていることの証明を行った。

ただし、この変換では、遷移等のパラメータを変換時に具現化するため、多くの書換え規則を生成することになり、変換によって得られる書換え論理仕様が大きくなりすぎる

という点も併せ持っている。このため、モデル検査を効果的に行えない可能性がある。

もし、１回の状態遷移で変化する値の数が有限であれば、システムやプロトコルに参加するプロセスや主体の数を変換時に決める必要はなくなる。研究代表者がこれまでに扱ったすべての実例において、１回の状態遷移で変化する値の数は有限であった。たま、ほとんどの実例においてもそうであろうと予想できる。このような条件のもとで、変換時にプロセスや主体の数等のパラメータを具現化しなければ、観測遷移システムの各遷移を１つの書換え規則で表現でき、変換によってえられる書換え論理仕様が大きくなるのを防ぐことができる。

ただし、この変換方法では、各書換え規則に遷移のパラメータの情報を含める必要があり、状態を表す項が大きくなりすぎる可能性がある。特に、電子商取引プロトコル等のセキュリティプロトコルを観測遷移システムでモデル化した場合、効果的にモデル検査ができないほどに状態を表す項が巨大になってしまう。

そこで、書換え規則に含まれている遷移のパラメータの表現方法を工夫すること等で、状態を表す項が巨大になりすぎないようにした。

（２）変換器の実装

変換を支援するためのツール（変換器）を、最初、Java を用いて実装した。というのは、ガーベージコレクションを備えているため、メモリ管理をプログラマが明示的に行わなくてもよいこと、オブジェクト指向の考えに基づき、モジュラーな実装が可能であること等のためであった。ただし、構文解析器等の変換に本質的に関係ないものも実装する必要があるため、変換そのものだけに注意を注ぐことができなかった。

一方、Maude は、モデル検査機能だけでなく、メタプログラミング機能も備えている。この機能により、Maude 上に各種のツールを構築することができる。これまでにも、実時間システムの仕様記述や解析を行うための Real-Time Maude やデータ型の性質を証明するための Inductive Theorem Prover（ITP）等がこの機能を用いて実装されている。

この機能は構文解析器生成系を備えており、この機能を用いて変換器を実装することで、変換そのものに注意を注ぐことができる。

Maude のメタプログラミングを用いた変換器のモジュラーな実装方法を考案した。この方法では、１つの変換器内に、複数の変換規則を埋め込むことを可能する。つまり、１つの振舞仕様に対し、複数の異なるスタイルの書換え論理仕様を生成することができる。状況に応じて、適切な書換え論理仕様も異なってくると思われるので。このような変換器は実用上も有用であると思われる。

（３）事例研究

iKP(i = 1,2,3)は、IBM の Yorktown Heights および Zurich 研究所の研究者により設計された電子支払プロトコル族である。既存のクレジットカードによる支払に基づいている。MasterCard International 社および Visa International 社を中心に設計・開発された SET（Secure Electronic Transactions）に影響を与えたプロトコルとしても知られている。

iKP の参加者は、買い手（B）、売り手（S）および銀行（A）の３つのグループである。1KP、2KP および 3KP の違いは、どのグループが公開・私有鍵の組を保持するかである。1KP では銀行のみが、2KP では銀行と売り手が、3KP ではすべてのグループが保持する。

買い手が売り手の支払をする場合、以下のメッセージ送受信により行う。銀行は、既存のクレジットカード支払機構を利用し、買い手が使用するクレジットカードによる支払が可能かどうかを調べる。

Initiate. B → S : ID_B
Invoice. S → B : Clear, $[_{2,3}\ Sig_S]$
Payment. B → S : EncSlip, $[_3\ Sig_B]$
Auth-Request. S → A :
Clear, EncSlip, $[_{2,3}\ Sig_S]$, $[_3\ Sig_B]$
Auth-Response. A → S : RESPCODE, Sig_A
Confirm. S → B : RESPCODE, Sig_A

$[_3 \cdots]$ で囲まれたものは 3KP でのみ用いられ、$[_{2,3} \cdots]$で囲まれたものは 2KP と 3KP でのみ使われる。

プロトコルで使われている値は以下のとおりである。ID_Bは、B のクレジットカード番号と乱数の組のハッシュ値で、B の擬似識別子である。Clear は、S の識別子、ノンス、それに支払額や ID 等のハッシュ値から構成される複合値である。EncSlip は、B のクレジットカード等を A の公開鍵で暗号化した暗号文である。RESPCODE は、支払のクレジットカード支払機構による審査結果である。Sig_S、Sig_BおよびSig_Aは、それぞれ、支払に対する S、B および A の私有鍵による電子署名である。

研究代表者の研究グループでは、3KP を観測遷移システムでモデル化し、CafeOBJ で証明譜を記述することで、3KP がある性質を満たすことの検証を試みているとき、反例を発見した。検証対象の性質は、「銀行が支払を許可した場合、この支払に関係する買い手と売り手はともにこの支払に合意している」、というものである。この性質を支払合意性と

呼ぶ。ただし、検証を開始して3KPが支払合意性を満たさないであろうと気づくのに１０日ほどかかり、それから反例を構築するのに数日を要した。

この経験が元になり、定理証明による検証を支援するモデル検査利用のためのシステム仕様の変換方法を考案した。我々の目的は、モデル検査を以下のように使うことである：（1）プロトコルやシステムがある性質を満たすことの定理証明による検証を試みる前に、モデル検査を用いて反例がないことを確認すること、および、（2）定理証明による検証で必要となる補題に反例がないことを確認することである。このため、定理証明向きのモデル（システム仕様）からモデル検査向きのモデル（システム仕様）に変換することが適切かる実現可能な方法であるとの結論に至り、変換方法を考案し、iKPに適用した。

観測遷移システムの遷移を、Maudeの書換え規則で素直に記述すると、状態を表現する項に遷移に関する情報を陽に含める必要がある。このため、状態を表す項が巨大になってしまう。遷移が多くのパラメータを取ればとるほど、状態を表す項が大きくなる。iKP等の電子商取引プロトコルを観測遷移システムでモデル化した場合、遷移は多くのパラメータを持つ。たとえば、侵入者があるメッセージを偽造することに対応する遷移fkvm5は、５つのパラメータを持つ。遷移fkvm5をMaudeの書換え規則で素直に記述すると以下のようになる。

```
crl [rule-fkvm5] :
fkvm5(S,B,N,PR,HBN) (nw: NW)
(nonces: Ns') (hbans: HBNs')
=> fkvm5(S,B,N,PR,HBN)
  (nw: (vm(is,S,B,CK,GS) NW))
  (nonces: Ns') (hbans: HBNs')
if N ¥in Ns' /¥ HBN ¥in HBNs' /¥
  HC := hcom(com(PR,S,N,HBN)) /¥
  CL := clear(S,N,HC) /¥
  GS := sigs(is,HC) .
```

ここで、Ns'とHBNs'は、それぞれ、侵入者が取得したノンスと買い手の擬似識別子の集合である。条件の最初の２つの連言肢は、ノンスNと擬似識別子HBNが、それら２つの集合に含まれていることを意味する。

遷移fkvm5の５つのパラメータが、それぞれ、n_1、n_2、n_3、n_4およびn_5個の値を取りうるとすると、状態を表す項には、fkvm5から始まる項を$n_1 \times n_2 \times n_3 \times n_4 \times n_5$個含める必要がある。効果的にモデル検査のできるMaude仕様にするには、書換え規則に含める遷移のパラメータの数をなるべく少なくする必要がある。規則を変換することで、遷移のパラメータの数を減らす方法を考案した。

まず、規則の条件の最初の２つの連言肢を規則の左辺に埋め込む。つまり、(nonces: Ns')と(hbans: HBNs')を、それぞれ、(nonces: (N Ns'))と(hbans: (HBN HBNs'))にし、N ¥in Ns'とHBN ¥in HBNs'を削除する。(N Ns')は、侵入者が取得したノンスにNが含まれていることを意味し、もとの条件N ¥in Ns'と同じことを表す。この変換により、NとHBNが、遷移のパラメータ以外の左辺にも現れることになったので、遷移のパラメータから、これら２つを削除できる。つまり、規則に２回現れるfkvm5(S,B,N,PR,HBN)をfkvm5(S,B,PR)にすることができる。

規則におけるfkvm5(S,B,PR)の役割は、３つの値S,B,PRを規則で利用できるようにすることである。そこで、fkvm5(S,B,PR)の代わりに、(sellers: (S Ss))、(buyers: (B Bs))および(prices: (PR PRs))を用いることができる。これにより、規則に現れる遷移からすべてのパラメータを削除することができ、遷移そのものも削除することができる。

このような変換方法により、iKP等の電子商取引プロトコルの定理証明向きのモデル（システム仕様）から効果的にモデル検査可能なモデル（システム仕様）を得ることが可能となった。3KPに適用した結果、２週間かかった反例発見は、一瞬で行うことができることがわかった。

Mondex（http://www.mondex.com/）は、英国のNational Westminster銀行が中心となり設立したMondex International社によって設計・開発された電子財布（貨幣）プロトコル(システム)である。Mondex社は、現在、クレジットカード大手のMasterCard International社の子会社である。Mondexは、（通常、小額の）金額情報を保有するカード間で、その金額情報をやり取りするためのプロトコルである。Mondexが望みの性質を満たすことの証明支援系による検証を、変換よりえられる書換え論理仕様に対してモデル検査を行うことで支援した。これにより、成り立つと思われた補題の１つに反例があることがわかり、検証の負荷をいくぶん減らすことができた。

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　２　件）

① Masaki Nakamura, Weiqiang Kong, Kazuhiro Ogata and Kokichi Futatsugi: A Specification Translation from Behavioral Specifications to Rewrite Specifications, IEICE TRANSACTIONS on Information and Systems, E91-D(5): 1492-1503, IEICE, 2008.査読有

② Kazuhiro Ogata and Kokichi Futatsugi: Comparison of Maude and SAL by Conducting Case Studies Model Checking a Distributed Algorithm, IEICE TRANSACTIONS on Fundamental of Electronics, Communications and Computer Science, E90-A(8): 1690-1703, IEICE, 2007.査読有

〔学会発表〕（計　３　件）

① Weiqiang Kong, Kazuhiro Ogata and Kokichi Futatsugi: Algebraic Approaches to Formal Analysis of the Mondex Electronic Purse System, Proceedings of the 6th International Conference on Integrated Formal Methods (6th IFM), LNCS 4591, Springer, pp.393-412 (2007), 査読有, 2007年7月2日～5日, Oxford, UK.

② Kazuhiro Ogata, Weiqiang Kong and Kokichi Futatsugi: Falsification of OTSs by Searches of Bounded Reachable State Spaces, Proceedings of the 18th International Conference on Software Engineering and Knowledge Engineering (18th SEKE), Knowledge Systems Institute, pp.440-445 (2006), 査読有, 2006年7月5日～7日, San Francisco, USA.

③ Kazuhiro Ogata, Masahiro Nakano, Weiqiang Kong and Kokichi Futatsugi: Induction-Guided Falsification, Prceedings of the 8th International Conference on Formal Engineering Methods (8th ICFEM), LNCS 4260, Springer, pp.114-131 (2006), 査読有, 2006年6月1日～3日, Macao.

６．研究組織
(1)研究代表者
緒方　和博（OGATA KAZUHIRO）
北陸先端科学技術大学院大学・情報科学研究科・准教授
研究者番号：30272991

(2)研究分担者

(3)連携研究者