様式 C-19

科学研究費補助金研究成果報告書

平成 23 年 6 月 10 日現在

機関番号：26402
研究種目：若手研究(B)
研究期間：2009～2010
課題番号：21700045
研究課題名（和文）　マルチスレッド再帰プログラムの自動検証のための形式モデル

研究課題名（英文）　Formal models for verifying multi-threaded recursive programs

研究代表者
高田　喜朗（TAKATA YOSHIAKI）
高知工科大学・工学部・准教授
研究者番号：60294279

研究成果の概要（和文）：Java 仮想機械等のプログラム実行系にはスタック検査と呼ばれる汎用的なアクセス制御機構が導入されている．プログラム中，重要な資源にアクセスする箇所の直前にアクセス権検査文を置くことで，信頼されていないモジュールがその資源にアクセスすることを防止できる．本研究では，スタック検査の拡張である履歴ベースアクセス制御(HBAC)を対象に，与えられたセキュリティ仕様を満たすようにアクセス権検査文を自動的にプログラムに挿入する方法について検討した．まずアクセス権検査文挿入問題の枠組を定義した後，この問題の co-NP 困難性を示した．また，プッシュダウンシステムのモデル検査法を利用してこの問題を解くアルゴリズムを示し，試作システムを例題に適用した．

研究成果の概要（英文）：In this study, we proposed a method for automatically inserting check statements for access control into a given recursive program according to a given security specification. A history-based access control (HBAC) was assumed as the access control model. A security specification is given in terms of information flow. We say that a program P satisfies a specification S if P is type-safe when we consider each security class in S as a type. We first defined the problem as the one to insert check statements into a given program P to obtain a program P' that is type-safe for a given specification S. This type system is sound in the sense that if a program P is type-safe for a specification S, then P has noninterference property for S. Next, the problem was shown to be co-NP-hard and we proposed a fix-point computation algorithm for solving the problem. The experimental results based on our implemented system showed that the proposed method can work within reasonable time.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2009 年度	1,700,000	510,000	2,210,000
2010 年度	1,100,000	330,000	1,430,000
総　計	2,800,000	840,000	3,640,000

研究分野：ソフトウェア検証
科研費の分科・細目：情報学・ソフトウェア
キーワード：自動検証，モデル検査，形式モデル，プッシュダウンシステム

１．研究開始当初の背景

計算機システムが社会基盤として浸透し，同時に，それらの不具合がもたらす影響も非常に大きくなっている．計算機システムやそのソフトウェアの不具合により金銭的・時間的に大きな損失を生じた例は，近年枚挙にいとまがない．それに伴い，計算機システムお

よびそのソフトウェアの無欠陥性がますます強く求められるようになっている．システムの無欠陥性を確認する方法として通常は試験が実施されるが，試験には「まれな事象によって発現する不具合を発見するのが困難」という問題がある．それを補うものとして近年，計算機性能の目覚ましい向上を背景に，モデル検査等の形式的自動検証技術が注目されるようになってきた．

現在普及している Spin，SMV 等のモデル検査ツールは有限状態モデルに基づくものであり，ソフトウェアシステム等の無限状態システムを扱うには有限状態モデルへの近似が必要である．しかし，有限状態に近似したことにより検証に失敗する（システムが仕様を満たすにも関わらず，「仕様を満たしているとは言えない」と答える）場合が生じる（図 1）．そのため，無限の状態空間を持つ，より表現能力の高いモデルが必要となるが，一方 Turing 機械と等価な計算モデルを用いてしまうと，モデルの能力が高すぎて有用な検証は一切不可能になってしまう．検証可能であり，かつ，現実のシステムやプログラムの記述に適した表現能力のより高い形式モデルの開発が重要である．

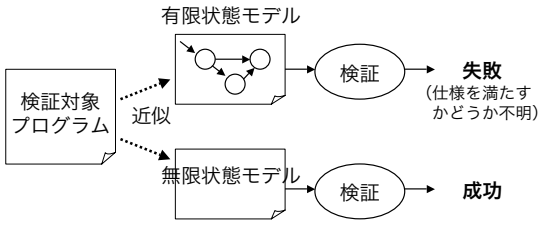

図 1：有限状態モデルと無限状態モデル

ソフトウェアで構成されるシステムは一般に無限の状態空間を持つため，現在普及している有限状態モデルに基づくモデル検査ツールでは，システムの振る舞いを有限状態モデルに近似する必要があり，そのために検証に失敗する場合が生じる．これに対し，プッシュダウンシステム(PDS)などの無限状態モデルに対するモデル検査法の研究が近年注目されるようになってきた．無限状態モデルを用いることで，システムの振る舞いをより正確に表現することが可能となる．例えば，モデル検査を応用して情報流解析と呼ばれる解析を行う例題について，有限状態モデル検査器では解析に失敗し PDS モデル検査器では解析に成功することが報告されている [伊藤，関; 2008]．

一方，これまでの PDS に基づくモデル検査法では，複数のスレッドが並行動作するマルチスレッドプログラムをうまく扱うことができなかった．近年ではマルチスレッドプログラムは多くのアプリケーションで用いられており，また，並行システムはタイミングに起因する発見しにくい不具合を含みやすく，自動検証による恩恵が大きいことから，マルチスレッドプログラムを扱えるようにモデル検査法を拡張することは重要と考えられる．しかし，有限状態機械の並行合成はやはり有限状態機械であるのに対し，複数のスタックを持つプッシュダウンシステムは Turing 機械と等価なモデルとなるため，単純な拡張では検証不可能なモデルとなってしまう．

応募者らは以前，Java 仮想機械(JVM)や共通言語ランタイム(CLR)で提供されている言語組み込みアクセス制御機能に着目し，この機能を用いたプログラムに対する形式モデルとモデル検査法の開発などを行ってきた．[Nitta, Takata, Seki; 2001]では文脈自由文法の拡張であるインデクス文法に基づくモデル検査法を提案し，[高田，王，関; 2008]では文脈自由文法に基づくモデル検査法およびその最適化法を提案した．これらは単一スレッドプログラムに対するものであるが，インデクス文法のほかにも文脈自由文法の拡張でかつ各種の判定問題が決定可能であるような形式文法がいくつか知られており，これらを応用することで，マルチスレッドプログラムに適用可能な形式モデルを構築できる可能性がある．

２．研究の目的

本研究では，自動検証可能でかつシステムの振る舞いをより正確に表現できる形式モデルの開発を目的として，これまで再帰プログラムの形式モデルとして用いられてきた PDS を拡張し，マルチスレッドの再帰プログラムの振る舞いを表現できる形式モデルとそのモデル検査法の開発を目指す．

PDS 等の無限状態モデルに対するモデル検査法の研究は近年注目を浴びるようになってきたが，複数のスタックを持つ PDS は Turing 機械と等価となってしまうことから，検証可能なままマルチスレッド向けに拡張することは容易でない．本研究では，多重文脈自由文法などの形式文法に関する知見を活用し，検証可能性を失わずにマルチスレッド再帰プログラムのためのモデルを構築しようとする点が特色である．

また近年，モデル検査は，単にシステムが振る舞い仕様を満たすかどうか調べるだけでなく，自己合成法に基づく情報流解析などのように，さまざまなプログラム解析への応用が試みられている．マルチスレッドプログラムの振る舞いをより正確に表現するモデ

ルとそのモデル検査法を開発することにより，モデル検査による検証の精度を向上させると同時に，これらの各種解析の精度を向上させることができると予想される．

３．研究の方法

本研究では具体的に，与えられたセキュリティ仕様に基づいて，必要なアクセス制御実行文を自動的にプログラムに挿入する方法を，プッシュダウンシステムモデルによるモデル検査を基礎として検討した．すなわち，アクセス制御機能の呼び出しのないプログラムとセキュリティ仕様を入力として，セキュリティ仕様を満たすように，必要なアクセス制御実行文を追加する．

セキュリティ仕様をどのような形で表現するかが問題となるが，ここでは，情報流(information flow)に関する仕様として記述することにする．すなわち，プログラムの各入力および各出力の機密度(security class)（例えばconfidential，unclassifiedなど）を指定する．このとき，例えば，confidentialである入力を使って計算された値がunclassifiedである出力先に出力されるなら，セキュリティ違反となる．情報流は必須アクセス制御(mandatory access control，MAC)と関係が深い．アクセス制御の目的を「どの利用者にどのような情報を提供するかを管理し，望ましくない情報漏洩を防ぐこと」と考えれば，セキュリティ仕様として情報流に関する仕様を用いるのは自然と考えられる．

本研究ではまず，アクセス権検査文の挿入対象であるプログラムの構文と操作的意味を定義した．このプログラム言語は，HBACによるアクセス権検査文を持つ単純な手続き型言語であり，図2のような制御フローグラフの形で表現される．また，その操作的意味論は図3のような呼び出し制御スタックの遷移によって定義される．次に，本研究における情報流仕様について定義するとともに，PDSモデル検査に基づいて情報流仕様に対する違反（型エラー）を検出する方法を示した．型エラーの検出とアクセス権検査文の挿入とを繰り返すことで，アクセス権検査文挿入問題を解くことができる．そして，アクセス権検査文挿入問題を定義し，この問題がco-NP困難であることを示した．ここでは問題を簡単にするため，関数呼び出し時・復帰時におけるアクセス権の操作は予め与えられ固定されているという仮定をおき，その仮定の下で議論を行った．なお，アクセス権検査文挿入問題は「アクセス権検査文のないプログラムに検査文を挿入する問題」ではなく，「予め配置されたアクセス権検査文に対し，必要な引数を設定する問題」として定義した．これは，すべての出力文の直前にcheck文を配置するといったことは困難ではなく，各check文の引数（アクセス権の部分集合）を過不足なく決定することが問題の本質であるからである．最後にこの問題を解くアルゴリズムを示し，例題に対して本アルゴリズムの実装を適用する実験を行った．

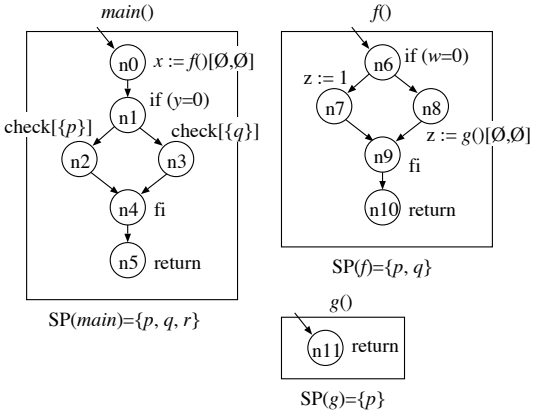

図2：制御フローグラフ

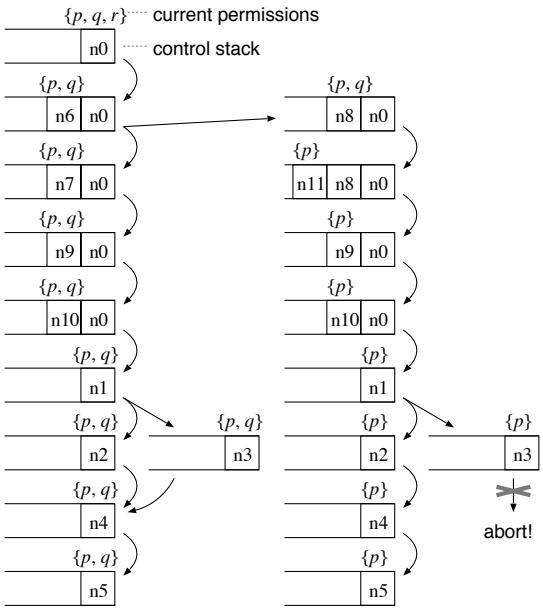

図3：呼び出し制御スタックの遷移

４．研究成果

PDSモデル検査に基づいて，与えられたHBACプログラムが情報流仕様に対して違反（型エラー）を起こす可能性のある箇所を検出する方法を示し，検出アルゴリズムの健全性を証明した．すなわち，本アルゴリズムによって型エラーが検出されなければ，与えら

れたプログラムは情報流仕様に違反しないことが保証される．

また，アクセス権検査文挿入問題を定義し，この問題が co-NP 困難であることを示した．これは，3SAT 問題の補問題が，図 4 のような HBAC プログラムに対するアクセス権検査文挿入問題に帰着される，すなわち，型エラーがなくなるようにアクセス権検査文を設置できるとき，かつそのときのみ，3SAT インスタンスが充足不能であることを示すことで得られた．

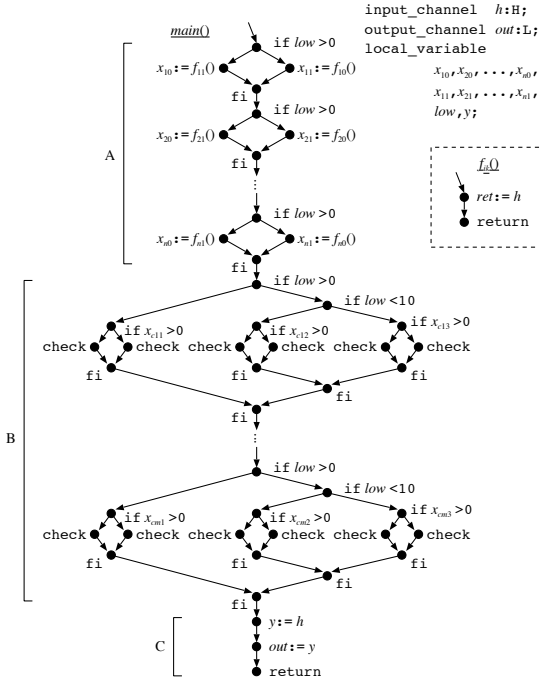

図 4：co-NP 困難性を示すためのプログラム

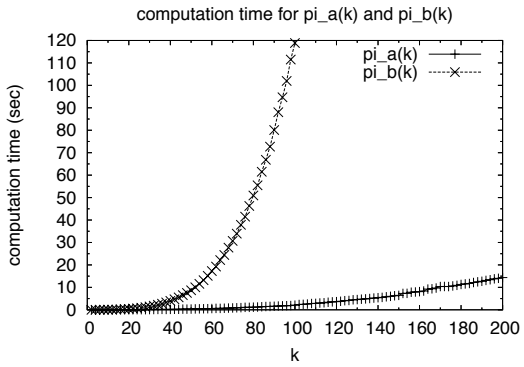

図 5：例題に対する実行時間

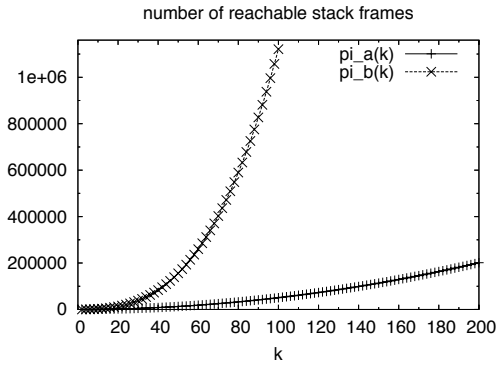

図 6：到達可能スタック数

最後に，アクセス権検査文挿入問題に対し，不動点計算に基づく求解アルゴリズムを示した．また，on-the-fly 状態生成に基づいて比較的効率のよいプログラムを実装した．このプログラムは到達可能スタックフレーム数と最終的に得られる check 文の引数の総数の積のオーダに従う．例題に適用することでこのことを確認した（図 5，6）．

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 1 件）

① Yoshiaki Takata, and Hiroyuki Seki, Automatic generation of history-based access control from information flow specification, Automated Technology for Verification and Analysis, ATVA 2010, 査読有, Lecture Notes in Computer Science, Vol.6252, pp.259–275, 2010.

〔学会発表〕（計 1 件）

① 高田喜朗，情報流仕様に基づくアクセス権検査文自動挿入法，日本ソフトウェア科学会第 12 回プログラミングとプログラミング言語ワークショップ，2010 年 3 月 4 日，香川県琴平温泉．

６．研究組織

(1)研究代表者

高田　喜朗（TAKATA YOSHIAKI）

高知工科大学・工学部・准教授

研究者番号：60294279