

平成 27 年 6 月 19 日現在

機関番号：15301

研究種目：基盤研究(C)

研究期間：2012～2014

課題番号：24500016

研究課題名(和文) 能動的オブジェクトのストリーミング転送を行う並行計算系の理論に関する研究

研究課題名(英文) Study on the theory of concurrent systems with code streaming

研究代表者

村上 昌己 (Murakami, Masaki)

岡山大学・情報統括センター・教授

研究者番号：60239499

交付決定額(研究期間全体)：(直接経費) 1,900,000円

研究成果の概要(和文)：近年のネットワーク技術の進歩・普及にともない、パソコンまたは携帯端末といった機器が、日常的なソフトウェアの実行の中でプログラムの転送しそれを実行するという処理が行われる。またこのようなネットワーク上のプログラムの転送は、異種の機器やOS、あるいは異なる言語により実装された機器の間で発生するものであることが多々あり、従来の単一のプログラムやソフトウェアの解析手法では、扱うことが困難なものである。本研究では、プログラムの転送動作のうち、転送と実行を同時進行で行うような機能について、計算モデルを設計し、システムの等価性を定義し、その妥当性を示した。

研究成果の概要(英文)：In recent years, it is common to send and receive programs using the internet. The capability of sending/receiving of program codes during the computation is represented using the notion of higher-order communication. The design, analysis and verification of the system with higher-order communication is not easy with the methods for the softwares that are executed on one closed computer system. A formal model of concurrent system that is equipped with capabilities of non-atomic higher-order communication is presented. The model is based on a graph rewriting system. We defined an equivalence relation on the model and showed that the equivalence is a congruent.

研究分野：情報学基礎

キーワード：並行計算 プロセス代数 計算モデル

1. 研究開始当初の背景

研究開始当初の技術的背景としては、ネットワークを利用してプログラムの送受信をとまなうアプリケーションにおいて、転送が完了する前に実行を開始するような形態の実装は既に一部に取り入れられていたといえる。我々はこのような通信を行うシステムの解析・検証は技術的な困難さを伴うものであることを指摘し、このようなシステムの検証・解析の基礎となる形式的モデル、すなわちストリーム型の高階通信であるコード・ストリーミングを伴う並行システムを記述するモデルをプロセス代数の拡張として提案していた。

また我々は、プロセス代数に基づくモデルが、システムの通信チャンネル名の有効範囲の表現において十分な表現力をもたないことを指摘していた。さらにこのことがシステムのセキュリティの解析・検証に問題であることより、プロセス代数に代わるモデルの必要性を示し、代替としてグラフ書換に基づくモデルが有効であることを示していた。

一方研究開始当時は、グラフ書換に基づくモデルに類する並行計算のモデルとして、Milner らによる bigraph が最も注目された結果であった。特に bigraph によるモデル化の上でシステムの等価関係を定義することによって、その等価性が合同関係となり、システムの検証・解析に有用であることが知られていた。しかしながら、このモデルでは、従来の移動型並行計算のモデルやプロセス代数によってあらわされるシステムに対して、拡張したグラフ書換系を用いた表現を取り入れたものが示されているに留まっていた。

したがってストリーム型の高階通信を行う並行システムは、このようなグラフ書換による定式化は行われていなかった。またこのことは、ストリーム型の高階通信を行う系に対する通信チャンネル名の有効範囲の表現力を備え、かつ合同関係であるような等価性を定義できるモデルは、存在していなかった。

2. 研究の目的

この研究の目的は、上記の背景を踏まえ能動的オブジェクトのストリーミング転送の機能を、チャンネル名の有効範囲に関する表現力を十分に備えたモデルで定式化することであった。すなわち、通信チャンネル名の有効範囲の表現においては、bigraph などのグラフ書換を基にしたモデルが有効であり、本研究ではこれを採用することとした。すなわち能動的オブジェクトのストリーミング転送の機能を、グラフ書換の規則によって定式化し、その書換規則をもとにラベル付きの遷移系を定義し、さらにその遷移系をもとに双模倣等価関係を定義し、それが合同であること

を示すことを目的とした。

我々は先に同期型の高階通信を含む並行計算システムのグラフ書換モデルに対して、双模倣等価をもとにしたより強い等価関係として、チャンネルの有効範囲の変化にも対応する等価関係を定義している。これはシステムにおける機密性をもつ情報の伝搬のモデル化と考えられる。まこのような過去の研究による知見をもとに、本研究で扱ったストリーム型の高階通信を行うシステムに対して、本研究で得られた合同性をもつ双模倣等価関係を基に、チャンネルの有効範囲に関する等価性を定義することを目指す。

また我々は高階通信を含まないシステムに対して、プログラムの部分計算法を拡張した手法、特に部分計算によって保存される振る舞いと等価性と、部分計算の前後で差を生じるような順序関係によって、システムのセキュリティを強化もしくは脆弱化させることが可能であることを示している。本研究で得られたストリーム型の高階通信を行うシステムの双模倣等価は、このような系に対する妥当な部分計算法の基礎となるものであり、上のチャンネルの有向範囲の定式化と合わせて、システムのセキュリティの強化手法の定式化を、能動的オブジェクトの送受信を含む場合に対しても拡張するための基礎とあうことを目的としている。

3. 研究の方法

本研究は、まずストリーム型の高階通信を行うシステムの bigraph もしくはそれと類似のグラフ構造によって表現することに着手した。ここでは計算の主体となるプロセスを、動作部分をあらかず behavior 部分と、通信チャンネルにあたる部分をあらかず channel に分け、それらが二部グラフとして結合される形で表現した。Behavior 部分は、入れ子構造をもつノードの集まりによって表現した。これは bigraph でいうところの place graph と同様な構造である。また高階通信を扱うため、送信動作をあらかずノードの引数部分に、グラフ構造そのものを含めることを許す構造とした。このグラフ構造で表現されたシステムにおける能動的オブジェクトの送受信に関して、グラフ書換系による操作的意味論を与えた。ここで与えた操作的意味論において、特に特徴的であるのは、ストリーミング通信がアトミックな動作ではないことに着目し、通信によって引き渡された引数値が、システム全体に波及するまでのタイムラグを表現するため、遅延型の 変換を定義したことである。

加えて、bigraph における合同な双模倣等価関係の構築に重要な役割を果たすコンテキスト型ラベルを用いた遷移系意味論の研究を進めた。コンテキスト型ラベルを用いた遷移系については、アンビエント計算、計算などの従来の並行計算モデルに対して、

その公理系を構築を試みそれを拡張することによって、グラフ書換系に対する公理系の構築の基礎とした。具体的には、アンビエント計算に対しては、構造合同の公理, in, out, open の3つの動作に対応する公理、およびラベルとリデックスの間でコンテキストを移動するための公理を導入することにより、遷移系の公理化を行った。これによって定義された遷移系による各振る舞いに対応して、従来の書換系による簡略が存在すること、すなわち遷移系の健全性を示した。また逆にリデックスとコンテキストが与えられたとき、それらを合成して得られたグラフに対する各簡略操作に対して、それに対応する遷移がそのリデックスとコンテキストによって可能であること、すなわち遷移系の完全性を示した。またこの遷移系による操作的意味論をもとに双模倣等価性を定義し、それが合同関係となっていることを示した。

また 計算に対しても、同様に入出力、並列合成、名前制限、複製に対応する公理をしめし、操作的意味論を定義した。さらにアンビエント計算の場合と同様に、遷移系による意味論の完全性と健全性を示した。加えて、この遷移系による操作的意味論を元に、双模倣等価関係を定義し、それは合同であることの証明を行った。

以上によって得られた知見を基に、ストリーム型の高階通信を行うグラフ書換系についてのコンテキスト型ラベル付きの遷移系の公理系を構築した。グラフ書換系に対するコンテキスト型のラベルの定義のために、グラフの合成操作を定義した。この合成操作は bigraph におけるカテゴリ論的合成の特殊な場合であることが示される。この合成操作を用いることにより、グラフ書換におけるコンテキスト型ラベル付き遷移の概念を定義した。さらにストリーム型高階通信における基本的な動作であるチャンネルの結合、グラフの転送、チャンネルの切断といった動作に対応して、グラフのラベル付き遷移のための公理を導入し操作的意味論を定めた。このように定義された遷移系による意味論に対して、先に定義した書換系における簡略関係との整合性を示した。すなわちリデックスのグラフとコンテキストのグラフが与えられた時、それらの合成によって得られるグラフの任意の簡略に対して、対応する遷移がそのリデックスとコンテキストに対して存在すること、すなわち遷移系の完全性を示した。また逆にあたえられた任意のリデックスおよびコンテキストに対して遷移が存在するとき、それらを合成して得られるグラフの簡略が存在すること、すなわち遷移系意味論の健全性を示した。

最後にその遷移系を基に合同な双模倣等価関係を定義するという手順によって進めた。

4 . 研究成果

本研究では、上の研究の方法に示した通り、高階のストリーム通信を行うグラフ書換モデルを定式化し、その書換意味論を示した。ここで提案した書換意味論により、現存する web アクセスにおける従来の並行計算モデルでは記述できなかった非同期な動作が、表現できることを示した。すなわち能動的オブジェクトの非同期な転送を行う系においては、オブジェクトの転送が終了する前に、その実行が開始され、その結果オブジェクトの送信元に対して通信が発生することにより、送信元の動作が影響を受ける可能性がある。このような現象は、従来のオブジェクトは一括して転送されるとした高階通信を前提にした系では発生しない。しかしながら現に存在するシステムにおいては、起こりうる現象であり、その意味では従来の高階通信を扱うモデルは、現実のシステムのモデルとしては表現力が十分ではなかった。本研究で示したモデルは、この点に対して対応できる表現力を備えたものであることを示した。

またコンテキスト型ラベルの研究結果として、アンビエント計算および 計算に対して、コンテキスト型ラベルの遷移系を定義する公理系を示し、それらが従来の書換型意味論に対する健全性および完全性を示した。また遷移系を用いてアンビエント計算、計算のそれぞれに対する双模倣等価関係を定義し、さらにそれらの合同性を示した。アンビエント計算に対する等価関係は、簡略の最終形態の相違にのみ着目するものが主流であり、双模倣等価のような振る舞いの経緯の相違にも着目できるものとしては、十分な結果が得られてはいなかった。本研究で得られた双模倣等価関係は、合同性を持つものであり、その意味において従来より進んだ等価関係を定義しえたといえる。また 計算の双模倣等価関係については、合同性を確保するためにその構文に制限を加え、送信のあとは直ちに停止するプロセスのみを扱う手法が主に用いられてきていた。本研究では送信プフィクスを許す 計算を対象としており、この範囲を扱う双模倣等価関係としては、従来より進んだ結果を得たといえる。

また、高階のストリーム通信を行うグラフ書換系に対するコンテキスト型ラベルを用いた遷移系意味論を定義し、先に示した書換型意味論に対する健全性および完全性を示した。また現時点で未発表ではあるが、この遷移系を用いて双模倣等価関係が定義できること、およびその等価関係が合同となるという結果が得られている。このことは、能動的オブジェクトのストリーム通信を行う系の、解析・検証手法、もしくは部分計算法などの最適化手法に対して理論的な基礎を与えるものである。

さらに上記の目的で述べたように、双模倣

等価を用いて、チャンネル名の有向範囲に関する等価関係の定義の基礎となる。これは上で延べた部分計算法の拡張と合わせて、システムの脆弱性の解析、検証，強化手法の基礎となるものと考えられる。

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)

[学会発表](計5件)

1. A Contextual Transition Semantics for Graphical Concurrent System with Higher-Order Streaming Communication". M. MURAKAMI, 3rd International Conference on CIRCUITS, SYSTEMS, COMMUNICATIONS, COMPUTERS and APPLICATIONS (CSCCA '14), Florence, Italy, 2014年11月(査読有)
2. "Contextual Transition System for π -calculus", M. MURAKAMI and T. Sasaki, Science and Information Conference 2014, London UK, 2014年8月(査読有)
3. A Graphical Structure Rewriting Model for Concurrent System with Higher-Order Streaming Communication", M. MURAKAMI, 3rd Int. Conf. on Innovative Computing Technology 2013, London UK, 2013年8月(査読有)
4. "Congruent Bisimulation Equivalence of Ambient Calculus Based on Contextual Transition System", M. MURAKAMI, 2013 Int. Symp. on Theoretical Aspects of Software Engineeringm Birmingham UK, 2013年7月(査読有)
5. "Contextual Transition System for Ambient Calculus" S. YAMAZAKI and M. MURAKAMI, 12th Int. Conf. on Software Engineering, Parallel and Distributed Systems, Cambridge UK. 2013年2月(査読有)

6. 研究組織

(1)研究代表者

村上 昌己 (Masaki Murakami)
岡山大学情報統括センター 教授
研究者番号：60239499