様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成 ２７ 年　 ５ 月 ２６ 日現在

機関番号：１１３０１
研究種目：基盤研究(B)
研究期間：2010～2014
課題番号：２２３０００００５

研究課題名（和文）高階オープンシステムの数理的検証

研究課題名（英文）Formal Verification of Higher-Order Open Systems

研究代表者
住井　英二郎（SUMII, Eijiro）

東北大学・情報科学研究科・教授

研究者番号：００３３３５５０

交付決定額（研究期間全体）：（直接経費）　　11,300,000円

研究成果の概要（和文）：複数のプロセスが並行に動作して、プロセス自身を通信することができ（高階）、かつ位置（ロケーション）の概念のある計算モデル（高階分散プロセス計算）において、「二つのシステムを外部から観察したときの動作が等しい」という振る舞い等価性を数理的に証明する、世界初の健全かつ完全な理論（環境双模倣）を確立、理論計算機科学のトップコンファレンスの一つACM/IEEE LICS 2012等に厳しい査読を経て論文が採択され、発表を行なった。

研究成果の概要（英文）：We developed the first sound and complete theory for proving behavioral equivalence ("makes the same actions" when observed externally) in higher-order (processes themselves can be communicated), concurrent and distributed ("has the notion of locations") computation model (process calculus), and published the results in refereed venues such as LICS 2012, a top conference on theoretical computer science.

研究分野：プログラミング言語理論

キーワード：環境双模倣　並行・分散プロセス計算モデル　プログラム理論　形式手法　理論計算機科学

１．研究開始当初の背景

（国内・国外の動向・位置づけ）　コンピュータシステムが「どこにでもある」現代社会において、プログラムないしソフトウェアの不具合（バグ）は重大な問題となっている。もはや一般的全国紙の第一面だけでも、社会的問題となった重大不具合の実例には事欠かない。特に大きな不具合かつソフトウェア的原因に限っても、以下のような事例がある。

・ウイルスバスターの不具合により企業や官公庁の PC 17 万台が停止（2005 年 4 月）
・東京証券取引所システム不具合により 400 億円の誤発注の取り消しが失敗（2005 年 12 月）
・三菱東京 UFJ 銀行キャッシュカードのコンビニ ATM での取引 2 万件が失敗（2008 年 5 月）
・日本航空チェックインシステム不具合による遅延・欠航で 1 万 5 千人に影響（2009 年 6 月）

いわゆる「セキュリティホール」の大半も、ソフトウェアのバグが原因である。セキュリティホールはしばしば不正アクセスに悪用され、やはり重大な社会問題となっている。

現在、ソフトウェアのバグは、「テスト」や「レビュー」など、人手による確認で防止することが通常である。しかし、コンピュータプログラムは一般に非常に多数の状態をとりうるため（指数個あるいは無限個）、それらをすべて人手で確認することは、非現実的ないし不可能である。このため、論理式による仕様記述や、モデル検査（効率的な状態探索）、型システム（論理学的推論規則によるプログラム解析）などの、数理論理学的ソフトウェア検証手法が注目されている。（モデル検査の第一人者である Clarke 氏ら 3 名は、2007 年チューリング賞を受賞した。抽象データ型システムの祖である Liskov 女史は、2008 年チューリング賞を受賞した。）

数理的手法は産業界においても注目され、国外では航空機制御ソフトウェアの検証など多数、国内でも電力設備保全システムのモデル検査によるデバッグや、次世代モバイル FeliCa の形式仕様記述などの事例がある。（日経エレクトロニクス 2005 年 12 月 19 日号特集「ソフトウェアは硬い」、情報処理 2008 年 5 月号特集「フォーマルメソッドの新潮流」など）

しかしながら、従来の数理的ソフトウェア検証手法は、オープンでないシステムや一階(first-order)のシステムを対象としており、高階(higher-order)かつオープンなシステムをうまく扱うことができなかった。ここでいう「高階かつオープンなシステム」とは、いわゆるインターネットのような公開通信路を介して、（必要であれば暗号化ないし電子署名された）プログラム自身を送受信・実行するようなシステムのことである。例えば以下のようなシステムが「高階かつオープンなシステム」にあたる。

・ソフトウェアを定期ダウンロードし自動インストールするシステム（Windows Update など）
・Web ブラウザがサーバからプログラムをダウンロードして実行するシステム（Gmail など）
・ユーザがネットワーク上のサーバにプログラムを送信して実行させるシステム

（それまでの研究成果）　研究代表者の住井は、「暗号λ計算」（暗号プリミティブを備えた高階言語）や、多相λ計算（抽象データ型や総称型を備えた高階言語）において、「与えられた二つのプログラムの振る舞いが等しい」という性質（プログラム等価性）を検証する完全(complete)な理論を世界で初めて与えた。プログラム等価性は、システムの機能的正当性・安全性や、情報の機密性・真正性なども包含する、重要な基本的性質である。

これらの研究は高く評価され、計算機科学分野の最高峰とされる国際論文誌 Journal of the ACM や、プログラム理論分野の最高峰とされる国際会議 POPL、計算機論理学における最高峰とされる国際会議 LICS などに、厳しい査読を経て採録された。住井は 34 歳（2010 年 4 月時点）で POPL 2008 を含む 20 件以上の国際学会プログラム委員やプログラム委員長、サマースクール講師、国内外の論文誌編集委員等を務めている。

（着想に至った経緯）　住井は上述の理論（環境双模倣）を発展させ、メモリ確保・解放プリミティブを備えた高階命令型言語や、公開鍵暗号系など任意の代数プリミティブを備えた高階並行言語にも適用した。そのような言語は従来の理論（「表示的意味論」や「論理関係」、従来の双模倣など）では扱うことができなかったが、住井の理論により、高階オープンシステムの数理的検証に向けた基礎が初めて構築された。

２．研究の目的

本研究では、以上の成果をさらに発展させ、より現実的なシステムの数理的検証を可能とすることを目指した。具体的には、単なる並行計算(concurrent computation)ではなく、位置(location)に依存するプリミティブを備えた分散計算(distributed computation)のための環境双模倣の理論を確立する。

ここでいう「プログラム」や「言語」とは、C 言語や Java といった狭義のプログラミング言語だけでなく、「λ計算」や「π計算」といった一般的計算モデルを含む。したがって、実装レベルのコードだけでなく、（人間や自然、ハードウェア等の外部動作も含め

た）仕様レベルのモデルを記述・検証することも可能である。

数理的検証手法の実用化にあたっては、以上のような理論的問題だけでなく、「いかに技術者にとってわかりやすい／使いやすいインターフェースを提供するか」「今現在のソフトウェア開発プロセスにどう取り入れるか」といった、さらに現実的・社会的な問題に取り組むことも非常に重要である。これらは産業総合技術研究所や九州大学などにおいて、企業と連携した複数の研究が行われており、本研究の中では直接は扱わない。

３．研究の方法

高階分散プロセス計算に対する環境双模倣の定義と健全性・完全性証明を行う。位置依存プリミティブのない高階並行プロセス計算に対しては、すでに住井らにより環境双模倣の定義と健全性・完全性証明が与えられている。しかしながら、位置の概念がある言語に対する環境双模倣の定義は自明でない。

例えば、標準的な高階並行プロセス計算である高階π計算(*1)に、位置の概念と、局所的システムダウン(location faliure)をつけ加えた計算体系を考える。通常の高階π計算においては、

P = c!<R> | *R

というサーバプロセスと、

Q = c!<0> | *R

というサーバプロセスは等価である。ただしc!<R>は通信チャネル c へプロセス R を送信するプロセス、*R は (UNIX の fork のように) プロセス R を複製するプロセス、0 は何もしないプロセス、|は並行実行を表す。ところが、位置の概念があると、

c?(X).m[run X]

のように、チャネル c から受け取ったプロセス X を位置 m の下で実行するクライアントプロセスが考えられる。ここで、R が例えば複数の動作を逐次実行するようなプロセスであり、その途中で位置 m がシステムダウンした場合、P と Q は等価にならない。これは現実のシステムにおいては、大域的な不整合状態やデッドロック等の恐れがあることを意味する。

このように、位置の概念がある分散計算には、単なる並行計算では捉えられない不具合の可能性がある。理論的にも、高階プロセス計算に位置依存プリミティブを導入すると、従来の環境双模倣は不健全となる。そのため、位置の概念に対応する条件を環境双模倣の定義に追加する必要があるが、

・どのような条件を追加すればよいか
・そのように拡張した環境双模倣の健全性・完全性をどうやって証明するか

は自明でないことが、それまでの研究からわかっている。これらの問題を解決することを目指した。

分散プロセス計算はその現実的重要性のため、欧米などの多数のグループにより従来から研究されている。しかし、プロセス自身を送受信・実行する高階分散プロセスやその等価性問題は、理論的に取り扱いが難しく、いまだに検証手法が確立されていなかった。例えば 2009 年 9 月に発表された当時の最新の研究では、いたるところで無限に多くのプロセスを考える必要があり、実際に自明でない検証を行うことはできなかった。前述の環境双模倣の拡張が実現すれば、「オープンな」（＝事前に全参加者を検査する必要がない）高階分散システムに対する、世界初の数理的検証手法となる。

４．研究成果

以上の背景・目的・方法にもとづいて研究を行ない、位置の概念と名前制限もしくは名前生成のある高階π計算に対する、健全かつ（名前制限ではなく名前生成がある場合は）完全な環境双模倣を定義し、FOSSACS 2011 および理論計算機科学に関するトップコンファレンスの一つである LICS 2012 の予稿集に査読つきフルペーパーが採択、合わせて口頭発表も行なった。

さらに、環境双模倣および高階・分散計算に関する国際共同研究等を行ない、複数の査読つき論文等を発表した。

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６件）

① Eijiro Sumii, Yuji Sato: A Multi-Role Translation of Protocol Narration into the Spi-Calculus with Correspondence Assertions. FCS'13: Workshop on Foundations of Computer Security (Informal Proceedings): 66-82 (2013)（査読有）

② Adrien Piérard, Eijiro Sumii: A Higher-Order Distributed Calculus with Name Creation. LICS 2012: 531-540（査読有）

③ Vasileios Koutavas, Paul Blain Levy, Eijiro Sumii: From Applicative to Environmental Bisimulation. Electr. Notes Theor. Comput. Sci. 276: 215-235 (2011) doi:10.1016/j.entcs.2011.09.023（査読有）

④ Davide Sangiorgi, Naoki Kobayashi, Eijiro Sumii: Environmental bisimulations for higher-order languages. ACM Trans. Program. Lang. Syst. 33(1): 5 (2011)（査

読有）

⑤ Adrien Piérard, Eijiro Sumii: Sound Bisimulations for Higher-Order Distributed Process Calculus. FOSSACS 2011: 123-137（査読有）

⑥ Eijiro Sumii: A bisimulation-like proof method for contextual properties in untyped lambda-calculus with references and deallocation. Theor. Comput. Sci. 411(51-52): 4358-4378 (2010)（査読有）

〔学会発表〕（計５件）

① Akinori Abe, Eijiro Sumii: A Simple and Practical Linear Algebra Library with Static Size Checking. ACM SIGPLAN ML Family Workshop 2014
2014 年 9 月 4 日、ヨーテボリ（スウェーデン）

② Eijiro Sumii: Environmental Bisimulation and Its Open Problems. IFIP Working Group 2.8
2013 年 10 月 14 日、オッソワ（フランス）

③ Eijiro Sumii: A Multi-Role Translation of Protocol Narration into the Spi-Calculus with Correspondence Assertions. FCS'13: Workshop on Foundations of Computer Security 2013
2013 年 6 月 29 日、ニューオーリンズ（アメリカ）

④ Adrien Piérard, Eijiro Sumii: A Higher-Order Distributed Calculus with Name Creation. LICS 2012
2012 年 6 月 25 日、ドブロヴニク（クロアチア）

⑤ Adrien Piérard, Eijiro Sumii: Sound Bisimulations for Higher-Order Distributed Process Calculus. FOSSACS 2011
2011 年 3 月 28 日、ザールブリュッケン（ドイツ）

〔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〕
ホームページ
http://www.kb.ecei.tohoku.ac.jp/~sumii/

６．研究組織
(1)研究代表者
住井　英二郎（SUMII, EIJIRO）
東北大学・大学院情報科学研究科・教授
研究者番号：00333550

(2)研究分担者
寺内　多智弘（TERAUCHI, TACHIO）
北陸先端科学技術大学院大学・情報科学研究科・教授
研究者番号：70447150

(3)連携研究者