様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　３１　年　　４　月　２７　日現在

機関番号：　１１３０１
研究種目：　挑戦的萌芽研究
研究期間：　2016～2018
課題番号：　１６Ｋ１２４０９

研究課題名（和文）継続と文脈の概念にもとづく新しい関係的プログラム意味論

研究課題名（英文）New reational program semantics based on the notion of continuations and contexts

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）　　2,800,000円

研究成果の概要（和文）：「難解な専門用語の使用はできるだけ避けるか…適宜説明を加えて」「最大300文字」との指示に従って述べる。「継続」とは、計算機プログラムを実行している途中の「残りの計算」を指す概念である。「文脈」とは、プログラム中のある部分に対し、そのまわりの部分（前者を[]という記号で置き換えた、「穴」のあるプログラム）を指す。本研究では、「継続」を扱う機能の一つであるcall/ccという演算を含む関数型（式の値を計算する「評価」以外の、いわゆる「副作用」がない）プログラムの等価性（動作の等しさ）を証明するための理論を「環境双模倣」という手法にもとづき確立し、その知見を他の研究にも活かすことができた。

研究成果の学術的意義や社会的意義
現代社会において計算機を中心とする情報処理システムの重要性は言をまたないが、多くの計算機ソフトウェアの理論的基礎は薄弱であり、毎日のように「不具合」（という名の誤動作）を起こして社会的問題となっている。本研究のような「プログラミング言語理論」は、狭義の「プログラム」のみならず、広義の「計算モデル」も含め、数理論理学的基礎による堅固な理論の確立・発展・応用を目指している。本研究もその一つであり、前述の「継続」と「文脈」という、広義の計算機プログラムにおいて重要な概念を扱った、「二つのプログラムの動作が等しい」という基本的な性質を証明する手法の成果である。

研究成果の概要（英文）：A theory for proving program equivalence, based on environmental bisimulations, has been developed in a foundational calculus modelling a functional programming language with the undelimited continuation operator "call/cc" (call-with-current-continuation).

研究分野：　プログラム理論

キーワード：　継続　（評価）文脈　プログラム等価性　call/cc　λ計算　（環境）双模倣

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９、ＣＫ－１９（共通）

１．研究開始当初の背景

ある計算に対する継続とは、その計算が終わった後の「残りの計算」を表す概念である。例えば１＋２×３＋４という式において、２×３という計算の継続は、その計算の結果が入るべき穴(hole)を[ ]とすると、1+[ ]+4のように表すことができる。このように継続は1+[ ]+4のような「現在実行中のプログラムのまわりのプログラム」を表す評価文脈、あるいは引数xを受け取って式１＋ｘ＋４の値を返す関数λx．１＋ｘ＋４と対応させることができる。

継続の概念は 1960 年代に Algol 60 をめぐって発見され[Reynolds, "The Discoveries of Continuations", Lisp and Symbolic Computation (1993)]、goto 文によるジャンプや大域脱出(global exit)、例外(exception)、関数呼び出しからの復帰(return)、コルーチン、スレッド、バックトラック、非決定的選択など多種多様な制御構造を統一的かつ関数的(functional)に表せることから、特に Scheme 等の関数型プログラミング言語において盛んに研究されてきた[Steele, Felleisen, Appel, 亀山, 浅井, Kiselyov 他多数]。

一方、応募者は環境双模倣(environmental bisimulation)の着想により、高階(higher-order)計算やデータ抽象、状態(state)、並行性(concurrency)、参照(reference)などの現代的な機能を備えた様々な言語における健全かつ完全なプログラム等価性の理論を初めて確立し、POPL 2004, POPL 2005, Journal of the ACM (2007), LICS 2007, ESOP 2009, LICS 2012 等の top conference および top journal において発表を行なった。さらに、それらの業績が国内外で評価され、主要国際学会(ML Workshop 2008, FLOPS 2014, ICFP 2016)プログラム委員長や日本ソフトウェア科学会(JSSST)プログラミング論研究会(PPL)主査、情報処理国際連合(IFIP) WG 2.8 (functional programming)正メンバー（日本人初）を務めるとともに、日本学術振興会賞、日本 IBM 科学賞、MSR 日本情報学研究賞（全世界のマイクロソフト研究所で審査）、船井学術賞、情報処理学会ソフトウエアジャパンアワード等を受賞した。

２．研究の目的

本研究では、継続および評価文脈の概念と環境双模倣のアイディアを融合し、新たな関係的プログラム意味論(relational program semantics)の確立を目指す。それにより、例えば古典的な継続演算子である call-with-current-continuation (call/cc)を持つλ計算において（最も一般的なプログラム等価性である文脈等価性(contextual equivalence)に対して）初の健全かつ完全なプログラム等価性の理論等を確立する。

３．研究の方法

継続ならびにプログラム等価性に関する研究は、計算機科学の初期である 1960 年代から数多く行われており[Reynolds, "The Discoveries of Continuations", Lisp and Symbolic Computation (1993)][Morris, "Lambda-Calculus Models of Programming Languages", 1968]、それぞれが一大分野をなしている。単に既存研究のサーベイを行うことが本研究の目的ではないが、それらの全体像を十分に把握し、本研究に有用な知見を得るとともに、従来のアプローチの問題点と本研究の学術的新規性を明確にするため、膨大な文献の中から特に重要なものをできるだけ網羅して精査する。現時点では、具体的には以下のような研究を想定している。

・Felleisen らによる C オペレータに関する研究[Felleisen et al., "A Syntactic Theory of Sequential Control", Theoretical Computer Science (1987)][Felleisen and Hieb, "The Revised Report on the Syntactic Theories of Sequential Control and State", Theoretical Computer Science (1991)]。E[callcc M] → E[M(λx.abort E[x])]のように呼び出し時の継続

すなわち評価文脈 E を維持する call/cc と異なり、C オペレータは E[CM] → M(λx.abort E[x]) のように外側の E を破棄するが、call/cc と C オペレータは容易に相互変換可能である。

・Sabry らによる call/cc に関する研究[Sabry and Felleisen, "Reasoning about Programs in Continuation-Passing Style", Lisp and Symbolic Computation (1993)][Sabry, "Note on Axiomatizing the Semantics of Control Operators, 1996]。先に触れたとおり、Felleisen や Sabry らの理論は継続渡し形式(CPS)変換後のβη等価性に対する健全性・完全性しか成り立たず、より一般的な文脈等価性とは一致しない。

・限定継続、特に shift, reset 演算子に関する理論[Danvy and Filinski, "Abstracting Control", Lisp and Symbolic Computation (1990)][Kameyama and Hasegawa, "A Sound and Complete Axiomatization of Delimited Continuations", ICFP 2003][Downen and Ariola, "Compositional Semantics for Composable Continuations", ICFP 2014][Biernacki and Lenglet, "Environmental Bisimulations for Delimited-Control Operators", APLAS 2013]（他多数）。特に、最後に挙げた研究は、申請者の環境双模倣のアプローチを用いた研究である。call/cc によって取り出される継続は、限定継続と異なり適用時の評価文脈を破棄するため(abortive)、これまでは理論的な扱いが難しいと考えられてきた。本研究はそのような困難を打破するものである。

調査と並行して、call/cc を持つ（状態を持たない純粋な）型無しλ計算に対し、環境双模倣をもととするプログラム等価性の理論を確立する。具体的には以下のとおりである。純粋な型無しλ計算における従来の環境双模倣 X とは、以下の条件をすべて満たす集合であった。

1. 各(M,N,R)∈X について、M→M'ならば、ある N'が存在し N→...→N'かつ(M',N',R)∈X

2. 各(V,N,R)∈X について、ある W が存在し N→...→W かつ R∪{(V,W)}∈X

3. 各 R∈X および各(λx.M,λx.N)∈R について、任意の(V,W)∈R*に対し((λx.M)V, (λx.N)W, R)∈X

4. 以上の条件の左辺(M, V, ...)と右辺(N, W, ...)を入れ替えても成り立つ

すると、(V,W)∈R∈X なる関係 R と環境双模倣 X が存在すれば値 V と値 W は文脈等価であり（健全性）、その逆も成り立つ（完全性）のであった。しかし call/cc のような継続演算子のある言語では、M→N であっても E[M]→E[N]とは限らないため、3 番目の条件を以下のように強化する。

3'. 各 R∈X および各(λx.M,λx.N)∈R について、任意の(V,W)∈R*および任意の E に対し(E[(λx.M)V], E[(λx.N)W], R)∈X

それにともない、逆に 2 番目の条件は以下のように緩和する。

2'. 各(V,N,R)∈X について、ある W が存在し N→...→W

従来の環境双模倣の定義では 3.における関数適用と 2.における評価が相互に循環していたところ、新たな定義では 3'.は依然として関数適用の結果が X に属することを要求するが、2'.において評価結果を R に追加する必要がなくなり、相互循環が断ち切られている点が特徴的である。なお、3'.において任意の E を考えなければならない点は、従来の環境双模倣と同様の"up-to context technique"により吸収可能で、多くの場合は問題にならない（問題になるのは call/cc が本質的に用いられているケースのみである）。

以上のように定義された新たな理論の（文脈等価性に対する）健全性と完全性を証明するとともに、任意の式 M と式 M;M の等価性など、従来の理論では扱えなかった例を示す。

４．研究成果

上述のアイディアにもとづき研究を実施し、call/cc を持つλ計算において初の健全かつ完

全な環境双模倣の理論を確立した。また、本研究により得られた評価文脈に関する知見を、名前呼び評価と必要呼び評価との対応関係や、セキュリティ型付きλ計算における条件分岐（if-then-else 式）の扱いの本質的な改良等に活かすことができた。

５．主な発表論文等

〔雑誌論文〕（計２件）

[1] Masayuki Mizuno, Eijiro Sumii: Formal Verification of the Correspondence Between Call-by-Need and Call-by-Name. FLOPS 2018: 1-16. 査読有

[2] Taichi Yachi, Eijiro Sumii: A Sound and Complete Bisimulation for Contextual Equivalence in λ-Calculus with Call/cc. APLAS 2016: 171-186. 査読有

〔学会発表〕（計４件）

[1] 遠藤 侑介，松本 宗太郎，上野 雄大，住井 英二郎，松本 行弘: Progress report: Ruby 3 における静的型解析の実現に向けて．PPL 2019

[2] Masayuki Mizuno, Eijiro Sumii: Formal Verification of the Correspondence Between Call-by-Need and Call-by-Name. FLOPS 2018.

[3] Masayuki Mizuno: Formal Verification of the Correspondence between Call-by-Need and Call-by-Name. TPP 2017

[4] Taichi Yachi, Eijiro Sumii: A Sound and Complete Bisimulation for Contextual Equivalence in λ-Calculus with Call/cc. APLAS 2016

６．研究組織

(1)研究分担者

なし（事務上、同一研究室の教員および学生は分担金の配分が不要ないし不可能なため）

(2)研究協力者

研究協力者氏名：松田 一孝
ローマ字氏名：Kazutaka Matsuda

研究協力者氏名：オレッグ キセリョーヴ
ローマ字氏名：Oleg Kiselyov

ならびに研究代表者を指導教員とする複数の学生（本報告書は公開を前提としており、研究協力者の氏名は必須ではないので記載しない）

※科研費による研究は、研究者の自覚と責任において実施するものです。そのため、研究の実施や研究成果の公表等については、国の要請等に基づくものではなく、その研究成果に関する見解や責任は、研究者個人に帰属されます。