Call/cc を含む型無しラムダ計算における文脈等価性の一証明手法

谷内 太一　住井 英二郎

項の評価文脈を取り出す call/cc 演算子は，大域脱出をはじめ様々な制御を表現することができる強力な機能であるが，その強力さゆえに等価性をはじめプログラムの性質に関する推論が困難になる．環境双模倣は様々な機能をもった言語に適用可能なプログラム等価性証明手法であるが，call/cc 等の制御演算子をもつ言語における環境双模倣はこれまで考えられていなかった．本研究は，call/cc を含むラムダ計算における環境双模倣の変種を提案し，健全性と完全性を証明するとともに，いくつかのプログラム等価性の例を実際に証明した．Call/cc は評価文脈に大域的な影響を及ぼすため，環境双模倣の定義に大幅な変更が必要となった一方，健全性証明は大幅に簡略化された．

1 序論

Call/cc は様々な制御を表現できる強力な演算子である．例えば，以下の関数はリストを受け取り，その要素の積を返すが，要素に 0 があった場合は call/cc を用いて大域脱出を行う．

```
let mul =
  λlist. callcc k.
    fix (λf. λl.
      if length(l)=0 then 1 else
      if hd(l)=0 then k 0 else
      hd(l)*(f tl(l)))
    list
```

`fix` は，`fix` λ`x.`$M \to$ [`fix` λ`x.`M/`x`]Mのような簡約規則をもつ演算子である．直観的には，`fix` λ`x.`M は，`x=`M (M は `x` を含みうる) と再帰的に定義される `x` を表す．

例えばプログラム `mul [2;0;5]` を実行すると，次の簡約列のように，継続 λ`x.throw x` に `k` が束縛され，大域脱出 `throw 0` が起こる．

```
    mul [2;0;5]
→* callcc k. ... if ... then k 0 else ...
→   ... if ... then (λx.throw x) 0 else ...
→* 2 * throw 0
→   0
```

Call/cc 演算子は強力ではあるが，簡約の際にまわりの評価文脈が無視できない．つまり，評価文脈を E とすると，$M \to N$ であっても，$E[M] \to E[N]$ となるとは限らない．そのため，文脈等価性をはじめ，プログラムの性質の推論が困難になる．

環境双模倣 [2–6] は，型抽象や参照のあるラムダ計算など，様々な言語に適用可能なプログラム等価性証明手法である．本研究では，call/cc を含む型無しラムダ計算における，環境双模倣に基づくプログラム等価性証明手法を提案し，健全性および完全性を証明する．

Call/cc 演算子は文脈の影響を受けるため，これまでの環境双模倣に大幅な変更を必要とする．具体的には，関数の等価性を証明する際，本体に call/cc 演算子があると，関数適用のまわりの文脈が無視できない

---

* A Method for Proving Contaxtual Equivalence in Untyped λ-Caluculus with Call/cc
This is an unrefereed paper. Copyrights belong to the Authors.

Taichi Yachi, 東北大学, Tohoku University.
Eijiro Sumii, 東北大学, Tohoku University.

ため，任意の評価文脈の下での適用を考慮する必要がある．

本論文の以降の構成は次のとおりである．2 節は対象言語についての説明，3 節は我々の等価性証明手法の定義，4 節は up-to technique の定義と健全性・完全性，5 節は我々の手法の健全性と完全性，6 節は我々の手法を用いた証明の例である．7 節は結論である．

2 対象言語

対象言語の抽象構文と簡約関係 $\overset{\text{top}}{\to}$ の定義を表 1 に示す．(評価文脈ではなく一般の) 文脈 C は，(0 個以上の自由変数を持つ) 単なる項で表す．`callcc` $k.M$ は，k を現在の継続に束縛して M を実行する．`throw` M は，現在の評価文脈を捨てて M を実行する．それ以外は標準的なラムダ計算である．また，これ以上簡約できない項 M を正規形という．$\overset{\text{top}}{\to\!\!\!\!\to}$ は $\overset{\text{top}}{\to}$ の反射的推移的閉包である．$\exists V.M \overset{\text{top}}{\to\!\!\!\!\to} V$ を $M\downarrow$ と書く．

この論文では列の略記としてオーバーラインを用いる．例えば，$x_1,\ldots,x_n$ は $\overline{x}$ と表し，$(V_1,V_1'),\ldots,(V_n,V_n')$ は $(\overline{V},\overline{V'})$ と表す．

以下は簡約にかかわる補題である．

補題 2.1 (評価文脈と instruction の一意性) $E_1[I_1] = E_2[I_2] \Rightarrow E_1 = E_2 \wedge I_1 = I_2$

証明 E_1 の構造に関する帰納法で示せる． □

補題 2.2 (簡約の一意性) $M \overset{\text{top}}{\to} N \wedge M \overset{\text{top}}{\to} N' \Rightarrow N = N'$

証明 $M \overset{\text{top}}{\to} N$ の規則による場合分けを行う．補題 2.1 より，$M = E[I]$ となる E, I は一意に定まり，簡約規則は I の形により一つに定まるので明らか． □

補題 2.3 (文脈の簡約) $FV(C_1) \subseteq \{\overline{y}\} \wedge C_1$ は正規形でない $\Rightarrow \exists C_2.\ FV(C_2) \subseteq \{\overline{y}\} \wedge (\forall \theta = [\overline{V}/\overline{y}].\ \theta C_1 \overset{\text{top}}{\to} \theta C_2)$

証明 C_1 の形で場合分けする．C_1 が正規形でないので C_1 の形は $E[(\lambda x.M_{12})\ V_2]$, $E[\#_j(\langle V_1,\ldots,V_j,\ldots,V_n\rangle)]$, $E[$`callcc` $k.M_1]$, $E[$`throw` $M_1]$ のいずれかである．

$C_1 = E[(\lambda x.M_{12})\ V_2]$ である場合，$C_1 \overset{\text{top}}{\to} E[[V_2/x]M_{12}]$ となる．$C_2 = E[[V_2/x]M_{12}]$ とすると，$FV(C_1) \subseteq \{\overline{y}\}$ より，$FV(E,V_2) \subseteq \{\overline{y}\}$, $FV(M_{12}) \subseteq \{x,\overline{y}\}$ であるから，$FV(C_2) \subseteq \{\overline{y}\}$ である．任意の $\theta = [\overline{V}/\overline{y}]$ について，$\theta C_1 = (\theta E)[(\lambda x.\theta M_{12})\ \theta V_2] \overset{\text{top}}{\to} (\theta E)[[\theta V_2/x]\theta M_{12}] = \theta C_2$ となる．

他の場合も同様． □

3 停止模倣と adequate relations

本節では環境双模倣の変種である，我々の等価性証明手法を定義する．

定義 3.1 閉じた (すなわち自由変数のない) 値の組の集合を値関係 (value relation) と呼び，$\mathcal{R}$ で表す．$\mathcal{R}^{-1} = \{(V',V) \mid (V,V') \in \mathcal{R}\}$ とする．

直観的には，$\mathcal{R}$ は等価性を証明したい値の組の集合として用いることを意図している．

定義 3.2 値関係 $\mathcal{R}$ に対し，$\{\ ([\overline{V}/\overline{x}]C,\ [\overline{V'}/\overline{x}]C) \mid FV(C) \subseteq \{\overline{x}\},\ (\overline{V},\overline{V'}) \in \mathcal{R}\ \}$ を $\mathcal{R}$ の context closure と呼び，$\mathcal{R}^\star$ で表す．

定義 3.3 停止模倣 (termination simulation) とは，次の条件を満たす最大の関係 $\precsim$ である．任意の $M \precsim M'$ について，

1. $M \overset{\text{top}}{\to} N$ ならば，$M' \overset{\text{top}}{\to\!\!\!\!\to} N'$ なる N' が存在して，$N \precsim N'$
2. $M = V$ ならば $M'\downarrow$

直観的には，$M \precsim M'$ は，M が値となって停止するなら M' は値となって停止することを意図している．簡約の途中の項 (N や N') も考える理由は，後の up-to techniques の定義との統一性のためである．

定義 3.4 $M \precsim M'$ かつ $M' \precsim M$ であることを，$M \sim M'$ と表す．

$\sim$ はいわゆる模倣等価性 (simulation equivalece) であり，双模倣 (bisimulation) とは異なる定義だが，本研究の言語は決定的なので一致する．本研究では，定

表 1　対象言語

M, N, L, C	::=	x	E	::=	$[\,]$
		$\lambda x.M$			$E\ M$
		$M\ N$			$V\ E$
		$\langle M_1, \ldots, M_n \rangle$			$\langle V_1, \ldots, V_{m-1}, E, M_{m+1}, \ldots, M_n \rangle$
		$\#_i(M)$			$\#_i(E)$
		$\texttt{callcc}\ x.M$			
		$\texttt{throw}\ M$			
V, W	::=	x	I	::=	$(\lambda x.M)\ V$
		$\lambda x.M$			$\#_j(\langle V_1, \ldots, V_j, \ldots, V_n \rangle)$
		$\langle V_1, \ldots, V_n \rangle$			$\texttt{callcc}\ x.M$
					$\texttt{throw}\ M$

$E[(\lambda x.M_{12})\ V_2]$	$\overset{\text{top}}{\to}$	$E[[V_2/x]M_{12}]$	E-APPABS
$E[\#_j(\langle V_1, \ldots, V_j, \ldots, V_n \rangle)]$	$\overset{\text{top}}{\to}$	$E[V_j]$	E-PROJTUPLE
$E[\texttt{callcc}\ k.M_1]$	$\overset{\text{top}}{\to}$	$E[(\lambda k.M_1)\ (\lambda x.\texttt{throw}\ E[x])]$	E-CALLCC
$E[\texttt{throw}\ M_1]$	$\overset{\text{top}}{\to}$	M_1	E-THROW

義や証明を簡単にするため，前者を用いる．

次に，停止性に対する停止模倣の健全性・完全性を示す．

補題 3.5 (停止性に対する停止模倣の健全性) $M \precsim M' \Rightarrow (M$ は値となって停止する $\Rightarrow M'$ は値となって停止する)

証明　$M \overset{\text{top}}{\to} V$ と仮定して，簡約のステップ数に関する帰納法による．　□

補題 3.6 (停止性に対する停止模倣の完全性) (M は値となって停止する $\Rightarrow M'$ は値となって停止する) $\Rightarrow M \precsim M'$

証明　前提を満たす (M, M') の集合が $\precsim$ の条件 1, 2 を満たすことを確認する．M が値となって停止するか stuck 状態であるか発散するかで場合分けする．

M が stuck 状態である場合　条件 1, 2 の前提を満たさないので明らか．

M が発散する場合　条件 1 は $M \overset{\text{top}}{\to} N$ となるような N が存在し，補題 2.2 より N は発散するので満たされる．条件 2 は前提を満たさないので明らか．

M が値となって停止する場合　M が値となって停止するので $M' \downarrow$ である．M が値であるかそうでないかで場合分けする．

M が値である場合　条件 1 は前提を満たさないので明らか．条件 2 は $M' \downarrow$ より満たされる．

$M \overset{\text{top}}{\to} N$ なる N が存在する場合　補題 2.2 より $N \downarrow$ であるから条件 1 は満たされる．条件 2 は前提を満たさないので明らか．　□

定義 3.7 次の条件を満たすとき，$\mathcal{R}$ は adequate であるという．

1. 任意の $(V, V') \in \mathcal{R}$ について，(V が関数 $\Leftrightarrow V'$ が関数) $\wedge$ (V が組 $\Leftrightarrow V'$ が組)
2. $(\lambda x.M,\ \lambda x.M') \in \mathcal{R}$ ならば任意の $(W, W') \in \mathcal{R}^\star$，$(\overline{V}, \overline{V'}) \in \mathcal{R}$，$FV(E) \subseteq \{\overline{y}\}$ に対し $[\overline{V}/\overline{y}]E[[W/x]M] \sim [\overline{V'}/\overline{y}]E[[W'/x]M']$
3. $(\langle V_1, \ldots, V_n \rangle,\ \langle V_1', \ldots, V_n' \rangle) \in \mathcal{R}$ ならば任意の $i \in \{1, \ldots, n\}$ に対し $(V_i, V_i') \in \mathcal{R}$

条件の対称性より，$\mathcal{R}$ が adequate ならば $\mathcal{R}^{-1}$ も adequate である．

定義 3.8 (文脈等価性) 閉じた値 V, V' が次を満たすとき，V と V' は文脈等価であるといい，$V \equiv V'$ と書く．

$\forall C.\ FV(C) = \{x\} \Rightarrow ([V/x]C\downarrow \Leftrightarrow [V'/x]C\downarrow)$

この定義では閉じた値のみ考えたが，開いた項に関しても既存研究 [6] と同じように扱えると思われる．

定理 5.3 で示すとおり，閉じた値 V,V' が文脈等価であることと，$(V, V') \in \mathcal{R}$ なる adequate な $\mathcal{R}$ が存在することは同値である．すなわち，二つの（閉じた）値の文脈等価性を示すには，それらの組が属する adequate な $\mathcal{R}$ を構成すればよい．

4 Up-to techniques

この節では，我々の手法による等価性証明を容易にする up-to techniques を示す．

4.1 Up-to reduction

まず up-to reduction を示す．直観的には，up-to reduction は簡約の途中を省略できる模倣である．

定義 4.1 Up-to reduction の停止模倣 (termination simulation up-to reduction) とは，次の条件を満たす最大の関係 $\precsim^{\rightarrow}$ である．任意の $M \precsim^{\rightarrow} M'$ について，

1. $M \overset{\text{top}}{\rightarrow} N$ ならば，N が発散するか，$M' \overset{\text{top}}{\twoheadrightarrow} N'$ なる N' が存在して，$N\downarrow \wedge N'\downarrow$ または $\exists L, L'.\ N \overset{\text{top}}{\twoheadrightarrow} L \wedge N' \overset{\text{top}}{\twoheadrightarrow} L' \wedge L \precsim^{\rightarrow} L'$
2. $M = V$ ならば $M'\downarrow$

定義 4.2 $M \precsim^{\rightarrow} M'$ かつ $M' \precsim^{\rightarrow} M$ であることを，$M \sim^{\rightarrow} M'$ と表す．

Up-to reduction の停止模倣の健全性と完全性を示す．健全性は，up-to reduction の停止模倣が，元の停止模倣を含意する，という性質である．完全性はその逆である．

補題 4.3 (Up-to reduction の停止模倣の健全性) $\precsim^{\rightarrow} \subseteq \precsim$

証明 $R = \{(M_0, M') \mid M_0 \overset{\text{top}}{\twoheadrightarrow} M \wedge M \precsim^{\rightarrow} M'\}$ が $\precsim$ の条件 1, 2 を満たすことを確認する．任意の $(M_0, M') \in R$, $M_0 \overset{\text{top}}{\twoheadrightarrow} M$, $M \precsim^{\rightarrow} M'$ について，以下の条件により場合分けする．

M_0 が stuck 状態である場合 $\precsim$ の条件 1, 2 の前提を満たさないので自明．

$M_0 \overset{\text{top}}{\rightarrow} M_1 \overset{\text{top}}{\twoheadrightarrow} M$ である場合 $(M_1, M') \in R$ より $\precsim$ の条件 1 を満たす．条件 2 は前提を満たさないので自明．

$M_0 = V$ である場合 $\precsim$ の条件 1 は前提を満たさないので自明．$M = V$ すなわち $V \precsim^{\rightarrow} M'$ より $M' \overset{\text{top}}{\twoheadrightarrow} V'$ なので条件 2 も満たす． □

補題 4.4 (Up-to reduction の停止模倣の完全性) $\precsim \subseteq \precsim^{\rightarrow}$

証明 $\precsim^{\rightarrow}$ の条件 1, 2 は $\precsim$ より弱いので明らか． □

定義 4.5 次の条件を満たすとき，$\mathcal{R}$ は adequate up-to reduction であるという．

1. 任意の $(V, V') \in \mathcal{R}$ について，(V が関数 $\Leftrightarrow$ V' が関数) $\wedge$ (V が組 $\Leftrightarrow$ V' が組)
2. $(\lambda x.M,\ \lambda x.M') \in \mathcal{R}$ ならば任意の $(W, W') \in \mathcal{R}^{\star}$, $(\overline{V}, \overline{V'}) \in \mathcal{R}$, $FV(E) \subseteq \{\overline{y}\}$ に対し $[\overline{V}/\overline{y}]E[[W/x]M] \sim^{\rightarrow} [\overline{V'}/\overline{y}]E[[W'/x]M']$
3. $(\langle V_1, \ldots, V_n\rangle,\ \langle V_1', \ldots, V_n'\rangle) \in \mathcal{R}$ ならば任意の $i \in \{1, \ldots, n\}$ に対し $(V_i, V_i') \in \mathcal{R}$

4.2 Up-to reduction and context

次に，up-to reduction and context を示す．Up-to reduction and context は，up-to reduction に加え，比較している値に対する共通の文脈を省略できる模倣である．

定義 4.6 Up-to reduction and $\mathcal{R}$-context の停止模倣 (termination simulation up-to reduction and $\mathcal{R}$-context) とは，次の条件を満たす最大の関係 $\precsim_{\mathcal{R}}$ である．任意の $M \precsim_{\mathcal{R}} M'$ について，

1. $M \overset{\text{top}}{\rightarrow} N$ ならば，N が発散するか，$M' \overset{\text{top}}{\twoheadrightarrow} N'$ なる N' が存在して，$N\downarrow \wedge N'\downarrow$ または $\exists L, L'.\ N \overset{\text{top}}{\twoheadrightarrow} L \wedge N' \overset{\text{top}}{\twoheadrightarrow} L' \wedge (L \precsim_{\mathcal{R}} L' \vee (L, L') \in \mathcal{R}^{\star})$
2. $M = V$ ならば $M'\downarrow$

定義 4.7 $M \precsim_{\mathcal{R}} M'$ かつ $M' \precsim_{\mathcal{R}^{-1}} M$ であることを，$M \sim_{\mathcal{R}} M'$ と表す．

定義 4.8 次の条件を満たすとき，$\mathcal{R}$ は adequate up-

to reduction and context であるという．

1. 任意の $(V, V') \in \mathcal{R}$ について，(V が関数 $\Leftrightarrow V'$ が関数) $\wedge$ (V が組 $\Leftrightarrow V'$ が組)
2. $(\lambda x.M,\ \lambda x.M') \in \mathcal{R}$ ならば任意の $(W, W') \in \mathcal{R}^\star,\ \forall(\overline{V}, \overline{V'}) \in \mathcal{R},\ FV(E) \subseteq \{\overline{y}\}$ に対し $[\overline{V}/\overline{y}]E[[W/x]M] \sim_{\mathcal{R}} [\overline{V'}/\overline{y}]E[[W'/x]M']$
3. $(\langle V_1, \ldots, V_n\rangle,\ \langle V_1', \ldots, V_n'\rangle) \in \mathcal{R}$ ならば任意の $i \in \{1, \ldots, n\}$ に対し $(V_i, V_i') \in \mathcal{R}$

Up-to reduction and context の健全性と完全性を示す．

補題 4.9 $\mathcal{R}$ は adequate up-to reduction and context $\wedge\ (M, M') \in \mathcal{R}^\star \Rightarrow M \precsim_{\mathcal{R}} M'$

証明 $R^\star \cup \precsim_{\mathcal{R}}$ が $\precsim_{\mathcal{R}}$ の条件 1, 2 を満たすことを示す．任意の $(M, M') \in R^\star \cup \precsim_{\mathcal{R}}$ を考える．$(M, M') \in \precsim_{\mathcal{R}}$ である場合は明らか．$(M, M') \in R^\star$ である場合を考える．$\mathcal{R}^\star$ の定義より，$M = [\overline{V}/\overline{y}]C$, $M' = [\overline{V'}/\overline{y}]C$, $(V, V') \in \mathcal{R}$, $FV(C) \subseteq \{\overline{y}\}$ である．

条件 2 については，$M = V$ ならば，$C = \lambda x.M_0$ または $\langle V_1, \ldots, V_n\rangle$ または y_i となる．よって，M' も値であるから満たされる．

条件 1 については，$M \overset{\text{top}}{\to} N$ として，C の形で場合分けする．$M \overset{\text{top}}{\to} N$ を導出する規則を考えると，C は正規形でないか，$C = E[x_i\ V]$ (V_i は関数) か，$C = E[\#_j(x_i)]$ (V_i は組) である．

C が正規形でない場合　補題 2.3 より，$\exists C_2.\ (FV(C_2) \subseteq \{\overline{y}\}) \wedge (\forall\theta = [\overline{V}/\overline{y}].\ \theta C \overset{\text{top}}{\to} \theta C_2)$ である．したがって，$N = [\overline{V}/\overline{y}]C_2$, $M' \overset{\text{top}}{\to} N'$, $N' = [\overline{V'}/\overline{y}]C_2$ となる．よって，$(N, N') \in \mathcal{R}^\star$ となる．

$C = E[x_i\ V]$ $(FV(E, V) \subseteq \{\overline{y}\})$ である場合 $M \overset{\text{top}}{\to} N$ より，$V_i = \lambda x.M_0$ とおいて，$M \overset{\text{top}}{\to} [\overline{V}/\overline{y}]E[[[\overline{V}/\overline{y}]V/x]M_0] = N$ である．$\mathcal{R}$ は adequate up-to reduction and context であるから条件 1 より，$V_i' = \lambda x.M_0'$, $M' \overset{\text{top}}{\to} [\overline{V'}/\overline{y}]E[[[\overline{V'}/\overline{y}]V/x]M_0'] = N'$ である．条件 2 より，任意の $(W, W') \in \mathcal{R}^\star$, $(\overline{V}, \overline{V'}) \in \mathcal{R}$, $FV(E) \subseteq \{\overline{y}\}$ に対し $[\overline{V}/\overline{y}]E[[W/x]M_0] \sim_{\mathcal{R}} [\overline{V'}/\overline{y}]E[[W'/x]M_0']$ である．すなわち，$N \precsim_{\mathcal{R}} N'$ となる．

$C = E[\#_j(x_i)]$ $(FV(E) \subseteq \{\overline{y}\})$ である場合 $M \overset{\text{top}}{\to} N$ より，$V_i = \langle W_1, \ldots, W_n\rangle$ とおいて，$M \overset{\text{top}}{\to} [\overline{V}/\overline{y}]E[W_j] = N$ である．$\mathcal{R}$ は adequate up-to reduction and context であるから条件 1 より，$V_i' = \langle W_1', \ldots, W_n'\rangle$, $M' \overset{\text{top}}{\to} [\overline{V'}/\overline{y}]E[W_j'] = N'$ である．条件 3 より，任意の $i \in \{1, \ldots, n\}$ に対し $(W_i, W_i') \in \mathcal{R}$ である．よって，$(N, N') \in \mathcal{R}^\star$ となる．□

補題 4.10 (Up-to reduction and $\mathcal{R}$-context の停止模倣の健全性) $\mathcal{R}$ は adequate up-to reduction and context $\Rightarrow \precsim_{\mathcal{R}} \subseteq \precsim^{\to}$

証明 $\precsim_{\mathcal{R}}$ が $\precsim^{\to}$ の条件 1, 2 を満たすことを確認する．条件 2 は同じなので満たされる．条件 1 については，$M \overset{\text{top}}{\to} N$ とする．

N が発散するか，$M' \overset{\textbf{top}}{\twoheadrightarrow} N'$ なる N' が存在して，$N\downarrow \wedge N'\downarrow$ または $\exists L, L'.\ N \overset{\textbf{top}}{\twoheadrightarrow} L \wedge N' \overset{\textbf{top}}{\twoheadrightarrow} L' \wedge L \precsim_{\mathcal{R}} L'$ である場合　$M \precsim^{\to} M'$ の条件 1 と同じなので満たされる．

$M' \overset{\textbf{top}}{\twoheadrightarrow} N'$ なる N' が存在して，$\exists L, L'.\ N \overset{\textbf{top}}{\twoheadrightarrow} L \wedge N' \overset{\textbf{top}}{\twoheadrightarrow} L' \wedge (L, L') \in \mathcal{R}^\star$ である場合　補題 4.9 より $L \precsim_{\mathcal{R}} L'$ である．よって $M \precsim^{\to} M'$ の条件 1 を満たす．□

補題 4.11 (Up-to reduction and $\mathcal{R}$-context の停止模倣の完全性) $\precsim^{\to} \subseteq \precsim_{\mathcal{R}}$

証明 $\precsim_{\mathcal{R}}$ の条件 1, 2 は $\precsim^{\to}$ より弱いので明らか．□

5 主定理

この節では我々の等価性証明手法の健全性と完全性を示す．

補題 5.1 (adquate relation の健全性) $FV(V, V') = \emptyset$ とする．$(V, V') \in \mathcal{R}$ なる adequate な $\mathcal{R}$ が存在すれば，$V \equiv V'$ である．

証明 $\mathcal{R}$ は adequate であるから $\mathcal{R}^{-1}$ も adequate である．よって補題 4.4, 4.11 より $\mathcal{R}$ と $\mathcal{R}^{-1}$ は adequate up-to reduction and context である．$\mathcal{R}^\star$ の定義より，$FV(C) = \{x\}$ なる任意の C について，$([V/x]C, [V'/x]C) \in \mathcal{R}^\star$, $([V'/x]C, [V/x]C) \in (\mathcal{R}^{-1})^\star$ となる．補題 4.9 より $[V/x]C \precsim_{\mathcal{R}} [V'/x]C$,

$[V'/x]C \precsim_{\mathcal{R}^{-1}} [V/x]C$ である．補題 4.10 と補題 4.3 より $[V/x]C \precsim [V'/x]C$, $[V'/x]C \precsim [V/x]C$ である．よって補題 3.5 より $V \equiv V'$ である． □

補題 5.2 (adequate relation の完全性) $FV(V, V') = \emptyset$ とする．$V \equiv V'$ ならば，$(V, V') \in \mathcal{R}$ なる adequate な $\mathcal{R}$ が存在する．

証明 $\mathcal{R} = \{(V, V') \mid FV(V, V') = \emptyset \wedge V \equiv V'\}$ とし，$\mathcal{R}$ が adequate であることを確かめる．

まず条件 1 を確かめる．$C = E[\#_i(x)]$ という文脈を考えると，V が組 $\Leftrightarrow V'$ が組である．同様に，$C = E[x\ W]$ という文脈を考えると，V が関数 $\Leftrightarrow V'$ が関数である．

次に条件 3 を確かめる．$(V_1, \ldots, V_n)$ と $(V_1', \ldots, V_n')$ を文脈等価な組とすると，$FV(C') = \{z\}$ なる任意の C' に対し，$C = (\lambda y.[y/z]C')\ \#_i(x)$ を考えれば，それぞれの第 i 要素 V_i と V_i' も文脈等価であることがわかる．

最後に条件 2 を確かめる．$\lambda x.M$ と $\lambda x.M'$ を文脈等価な関数とする．$(\overline{V}, \overline{V'}) \in \mathcal{R}$, $(W, W') \in \mathcal{R}^\star$ も文脈等価なので，補題 3.6 より，$[\overline{V}/\overline{y}]E[[W/x]M] \precsim [\overline{V'}/\overline{y}]E[[W'/x]M']$ が成り立つ．逆向きも同様． □

定理 5.3 $FV(V, V') = \emptyset$ とする．$(V, V') \in \mathcal{R}$ なる adequate な $\mathcal{R}$ が存在すれば，$V \equiv V'$ である．また，逆も成り立つ．

6 例

我々の手法を用いた等価性証明の例を示す．1 節でみた `mul` と次に示す `mul'` の等価性を証明する．型エラーを無視する便宜上，ここでのリストは整数のリストにかぎるとする．

```
let mul' =
  λlist.
    fix (λf. λl.
      if length(l)=0 then 1 else
      hd(l)*(f tl(l)))
    list
```

$\mathcal{R} = \{(\texttt{mul}, \texttt{mul'})\}$ が adequate up-to reduction and context であることを示す (そうすれば up-to techniques の健全性より $\mathcal{R}$ が adequate であることもわかる)．関数 `mul`, `mul'` の本体をそれぞれ M, M' とすると，$E[[W/\texttt{list}]M] \sim_{\mathcal{R}} E'[[W'/\texttt{list}]M']$ であることを確認すればよい (E, E' は $\mathcal{R}$ の分だけ違ってもよい評価文脈で，W, W' は $\mathcal{R}$ の分だけ違ってもよい値とする)．

W, W' がリストでない場合は，左右どちらのプログラムも stuck 状態となる．よって，$E[[W/\texttt{list}]M] \sim_{\mathcal{R}} E'[[W'/\texttt{list}]M']$ である．

W, W' が (整数の) リストの場合，$(W, W') \in \mathcal{R}^\star$ より，$W = W'$ である．W, W' が 0 を含むか含まないかで場合分けする．

W, W' が 0 を含む場合 左辺は，$E[[W/\texttt{list}]M] \overset{\text{top}}{\twoheadrightarrow} E[\ldots\ *\ \texttt{throw}\ E[0]] \overset{\text{top}}{\to} E[0]$ となり，右辺は，$E'[[W'/\texttt{list}]M'] \overset{\text{top}}{\twoheadrightarrow} E'[\ldots\ *\ 0\ *\ \ldots] \overset{\text{top}}{\twoheadrightarrow} E'[0]$ となる．$(E[0], E'[0]) \in \mathcal{R}^\star$ より，$E[[W/\texttt{list}]M] \sim_{\mathcal{R}} E'[[W'/\texttt{list}]M']$ である．

W, W' が 0 を含まない場合 W の第 i 要素を w_i ($i \in \{1, \ldots, n\}$) とおく．左辺は，$E[[W/\texttt{list}]M] \overset{\text{top}}{\twoheadrightarrow} E[w_1\ *\ \ldots\ *\ w_n\ *\ 1]$ となり，右辺は，$E'[[W'/\texttt{list}]M'] \overset{\text{top}}{\twoheadrightarrow} E'[w_1 * \ldots * w_n * 1]$ となる．$(E[w_1 * \ldots * w_n * 1], E'[w_1 * \ldots * w_n * 1]) \in \mathcal{R}^\star$ より，$E[[W/\texttt{list}]M] \sim_{\mathcal{R}} E'[[W'/\texttt{list}]M']$ である．

7 結論

Call/cc を含む型無しラムダ計算におけるプログラム等価性の，環境双模倣の変種を用いた健全かつ完全な証明手法を提案した．

今後の課題としては，logical relation に基づく証明手法 [1] との比較や，より多くの例の証明，および対象言語の拡張などが挙げられる．

参考文献

[1] Dreyer, D., Neis, G., and Birkedal, L.: The impact of higher-order state and control effects on local relational reasoning, *J. Funct. Program.*, Vol. 22, No. 4-5(2012), pp. 477–528.

[2] Sumii, E.: A Complete Characterization of Observational Equivalence in Polymorphic *lambda*-Calculus with General References, *Computer Sci-*

ence Logic, 23rd international Workshop, CSL 2009, 18th Annual Conference of the EACSL, Coimbra, Portugal, September 7-11, 2009. Proceedings, 2009, pp. 455–469.

[3] Sumii, E. and Pierce, B. C.: A bisimulation for dynamic sealing, *Proceedings of the 31st ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL 2004, Venice, Italy, January 14-16, 2004*, 2004, pp. 161–172.

[4] Sumii, E. and Pierce, B. C.: A bisimulation for type abstraction and recursion, *Proceedings of the 32nd ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL 2005, Long Beach, California, USA, January 12-14, 2005*, 2005, pp. 63–74.

[5] Sumii, E. and Pierce, B. C.: A bisimulation for dynamic sealing, *Theor. Comput. Sci.*, Vol. 375, No. 1-3(2007), pp. 169–192.

[6] Sumii, E. and Pierce, B. C.: A bisimulation for type abstraction and recursion, *J. ACM*, Vol. 54, No. 5(2007).