プログラミング-言語・基礎・実践- 21－9
(1995. 3. 9)

ブロードキャスト用プロセス代数(CCB)のための観測的合同関係

磯部 祥尚, 佐藤 豊, 大蒔 和仁

電子技術総合研究所 情報アーキテクチャ部 情報ベース研究室
〒305 茨城県つくば市梅園 1-1-4

あらまし　我々はブロードキャストに適したプロセス代数としてCCBを提案している。ブロードキャストでは送信者は受信者を指定しないため、拡張性の高いシステムの構築が可能である。CCBの最も重要な特徴は、ブロードキャスト後に、送信者がその受信者数を知ることができることにある。この受信者数を知ることによって、送信者は全ての受信者からの情報を確実に受けとることが可能になる。

CCBはCCSの拡張として与えられているが、CCSで定義されている観測合同がCCBでは合同関係にならないことが示されている。そこで、CCBのための観測的な合同関係を得ることが課題となっていた。

本報告書では、CCBの観測的な合同関係として**弱監視合同**を定義し、有限エージェントの弱監視合同に対する健全で完全な公理系を与える。この弱監視合同は観測合同に含まれ、かつ最も大きな合同関係である

キーワード　プロセス代数, ブロードキャスト, 観測的合同関係, 公理系

Observational Congruence Relations in a Calculus of Communication with Broadcasting

Yoshinao ISOBE, Yutaka SATO, Kazuhito OHMAKI

Information Base Section, Computer Science Division, Electrotechnical Laboratory
1-1-4 Umezono, Tsukuba, Ibaraki 305, Japan
E-mail: isobe@etl.go.jp, ysato@etl.go.jp, ohmaki@etl.go.jp

Abstract　In this paper we propose **weak monitor congruence** as an observational congruence relation for **CCB** (a Calculus of Communication with Broadcasting) which has been proposed by us, and give a sound and complete axiom system for the weak monitor congruence of finite agents. Weak monitor congruence is the largest congruence relation included in *observation congruence* which is defined in CCS.

CCB is a process algebra for broadcasting. Because a transmitter of broadcasting do not specify receivers, it is useful for constructing extensible systems. The advantage of CCB is that a transmitter can know the number of receivers after broadcasting. Thereby the transmitter can certainly get information from *all* the receivers.

Though CCB is a extension of CCS, we can show that observation congruence is not a congruence relation in CCB. Therefore observational congruence relations for CCB have been required.

key words　process algebra, broadcast, observational congruence relation, axiom system

1 はじめに

プロセス代数は分散した並行プロセス (エージェントと呼ぶ) を解析するための数学的道具として知られている。我々はブロードキャスト方式によるエージェントの結合モデルの解析を行なっており、その基盤としてプロセス代数を採用している [13, 14]。ここでブロードキャストは、「送信者がイベントを送信したとき、そのイベントの受信希望者は全てそれを受信する」通信方式を意味している。このような通信方式を記述できるプロセス代数として、CBS[6, 7, 8, 9]、CSP[4]、LOTOS[5]、などがあげられるが、特に CBS はブロードキャストのために開発されたプロセス代数である。しかし、これらのプロセス代数では、イベントの送信後にそのイベントの受信者数を知ることができない。

利用者が自由にエージェントを追加修正できる場合、あるイベントの受信者数を固定することはできない。また、1 つのエージェントにおいても、状況に応じて受信を希望するイベントを変える可能性もある。そこで、その受信者数を動的に (実行時に) 数えることができることが求められる。例えば、我々は次のような動作を記述できることを要求している。

- エージェント P はイベントをブロードキャストして他のエージェントを起動し、起動された全てのエージェントの終了を待ってから次の処理に進む。

このとき、P がそのイベントの受信者数 (すなわち、起動されたエージェントの数) を知ることは不可欠である。

我々は、イベントのブロードキャスト後に、そのイベントの受信者数を知ることができるプロセス代数として **CCB** (a Calculus of Communication with Broadcasting) を提案している [13, 14]。CCB は次の 2 つを考慮して CCS を拡張したプロセス代数である。

1. イベントの受信希望者は全てそれを受信する。
2. 送信後、その受信者数を知ることができる。

CBS は上の 1. を考慮して CCS を拡張したプロセス代数としてとらえることができる。CCB と CBS では、1. の実現方法に違いが見られるが[1]、その結果得られる効果は同等であり差はない。

2. を実現するために我々は CCB の定義の段階で受信者数を考慮している。これによって、ブロードキャスト後その送信者はその受信者数を知ることが可能となっている。しかしその反面、CCS で定義されていた観測合同 [1] が、CCB では合同関係ではなくなることが明らかになった。CBS では観測合同は合同関係であるから [7]、このことに CCB と CBS の明確な違いが現われている。

本報告書で、我々は CCB のための観測的な合同関係である**弱監視合同**を定義する。弱監視合同は観測合同に含まれる最大の CCB の合同関係である。さらに弱監視合同のための唯一解の存在を示す命題を与え、有限エージェントに対する健全で完全な公理系を与える。

以下、2節で CCB を非形式的に紹介し、3節と 4節で CCB の定義を与える。5節で観測的な 2 つの同値関係を定義し、6節で観測的な 2 つの合同関係を定義する。さらにそれらの健全で完全な公理系を与える。7節では関連研究として従来のプロセス代数と CCB を比較し、8節でまとめと今後の課題について述べる。

2 CCB の紹介

CCB ではブロードキャストの他に、受信者数を指定して送信することもできる。我々はこの送信方式をマルチキャストと呼んでいる。このマルチキャストは SCCS でも容易に記述でき、CCB 固有の特徴ではない。

CCB のイベントは $a\theta\langle x\rangle(y)$ の形をもち、ここで a はイベント名、θ はイベントの属性、$\langle x\rangle$ は受信者数、(y) はこのイベントによって渡されるメッセージである[2]。イベントの属性 θ は、マルチキャストの送信用 ! と受信用 ?、ブロードキャストの送信用 ‼ と受信用 ⁇ の計 4 種類である。特に、属性が ! で同期数が 0 であるイベント $a!\langle 0\rangle$ を内部イベントと呼ぶ (CCS の τ に相当する)。内部イベントは外部から観測も制御もできないイベントである。

CCB の特徴をより抽象的に表現すれば、**「あるイベントを受信可能なエージェントの数を知ることができる」**ということができる。これは他のプロセス代数では困難である。例えば、次のように定義されるシステム SYS を考える[3]。

$$SYS \equiv (a.\mathbf{0}|b.\mathbf{0}|a.\mathbf{0}|a.\mathbf{0}|b.\mathbf{0}|P)\backslash\{a,b\}$$

SYS ではイベント a と b を受信可能なエージェントが各々 3 個と 2 個含まれている。これらの個数を数えた後、イベント out によってその結果を外部に報告するように、エージェント P を定義することは容易ではない。CCS、SCCS[3]、π-Calculus[2]、CBS をはじめ、イベントにプライオリティ [11] を付加しても困難であると考えられる[4]。

この例に対する CCB の記述例を与えておく。

$$\begin{array}{rcl} SYS & \equiv & (a⁇.\mathbf{0}|b⁇.\mathbf{0}|a⁇.\mathbf{0}|a⁇.\mathbf{0}|b⁇.\mathbf{0}|P)\backslash\{a,b\} \\ P & \equiv & a‼\langle x\rangle.b‼\langle y\rangle.out!(x,y).\mathbf{0} \end{array}$$

[1] CBS ではディスカードと呼ばれる特殊なイベントを導入したのに対し、CCB では監視関数という関数を導入している。

[2] 1 の受信者数 ⟨1⟩、空のメッセージ ( ) は省略されることがある。

[3] この記法は CCS に従っている。$a.\mathbf{0}$ はイベント a を受信して停止するエージェントを表し、| はエージェントの並列合成演算子、\ は制限演算子である。また ≡ はシンタクティクに等しいことを意味する。

[4] $A \stackrel{\mathrm{def}}{=} a.A$ のようなエージェントがある場合、無限ループに落ちる可能性がある。

このとき、等式 $SYS \approx out!(3,2).\mathbf{0}$ が証明できる[5]。P の最初のイベント $a‼\langle x\rangle$ は、イベント名 a でブロードキャストした後に束縛変数 x をその受信者数 3 に束縛することを意味している。次のイベント $b‼\langle y\rangle$ も同様である。そして最後の $out!(x,y)$ で、2つの受信者数を外部に報告している。

3 Core-CCB の定義

この節では CCB の基礎となる Core-CCB のシンタックスとセマンティクスを形式的に定義する [14]。Core-CCB は値変数をもたないプロセス代数であり、CCB の定義は Core-CCB を基にして 4節で与えられる。

3.1 シンタックス

この小節では Core-CCB のシンタックスを定義する。まず、我々は名前の集合 $\mathcal{N} = \{a,b,c,\cdots\}$ が与えられていると仮定する。このとき、イベントの集合 $Event$ は次の集合として与えられる。

$$Event = \{a\theta^n : a \in \mathcal{N}, \theta \in \mathcal{T}, n \in \mathcal{I}\} \\ -\{a?^0, a⁇^0 : a \in \mathcal{N}\}$$

ここで、$\mathcal{I}$ は非負の整数の集合 $\{0,1,2,\cdots\}$、$\mathcal{T}$ はイベント属性の集合 $\{!,?,‼,⁇\}$ である。$\mathcal{T}$ の要素は $\theta,\phi,\cdots$ によって表される。特に任意の a について、$a!^0$ を**内部イベント**と呼ぶ (CCS の τ に相当する)。

Core-CCB のシンタックスを次のように定義する。

定義 3.1 *Core-CCB のエージェント式の集合 $\mathcal{E}$(要素を $E,F,\cdots$ で表す) は次の BNF 記法に従って定義される*[6]。

$$E ::= X \mid A \mid \mathbf{0} \mid a\theta^n.E \mid E+E \mid E|E \mid E[S] \mid E\backslash L$$

ここで、$X \in \mathcal{X}$、$A \in \mathcal{K}$、$a\theta^n \in Event$、$S \in \mathcal{F}$、$L \subseteq \mathcal{N}$ であり、$\mathcal{X}$ と $\mathcal{K}$ は各々エージェント変数とエージェント定数の集合、$\mathcal{F}$ はリネイミング関数 $(S:\mathcal{N}\to\mathcal{N})$ の集合である。 ∎

エージェント変数を含まないエージェント式を**エージェント**と呼び、エージェントの集合を $\mathcal{P}$ で表し、その要素を $P,Q,\cdots$ で表す。**エージェント定数**は**定義式**によって意味を与えられるエージェントである。実際に全てのエージェント定数 A について、$A \stackrel{\mathrm{def}}{=} P$ $(P \in \mathcal{P})$ の形の定義式があると仮定する。さらに、P の中で A は**弱ガードされている**と仮定する[7]。弱ガードされていないエージェントの動作は明確でなく実用的ではない。

[5] $\approx$ は観測等価 [1] である

[6] 今後、$\sum_{i\in I} P_i$ は、$I \neq \emptyset$ ならば $P_1 + P_2 + \cdots$、$I = \emptyset$ ならば $\mathbf{0}$ を意味する。

[7] 全ての X が E の部分式 $a\theta^n.F$ の中に含まれているならば、X は E の中でガードされているという。

3.2 セマンティクス

まず、エージェント式から名前の部分集合への関数である**監視関数** (monitor function) を定義する。

定義 3.2 各エージェント式 E について、**監視関数** $mon : \mathcal{E} \to 2^{\mathcal{N}}$ を次のように帰納的に定義する。

$$\begin{aligned}
mon(\mathbf{0}) &= \emptyset \\
mon(a\theta^n.E) &= \begin{cases} \{a\} & (\theta = ⁇) \\ \emptyset & (otherwise) \end{cases} \\
mon(E+F) &= mon(E) \cup mon(F) \\
mon(E|F) &= mon(E) \cup mon(F) \\
mon(E[S]) &= \{S(a) : a \in mon(E)\} \\
mon(E\backslash L) &= mon(E) - L \\
mon(A) &= mon(P) \qquad (A \stackrel{\mathrm{def}}{=} P) \\
mon(X) &= \emptyset
\end{aligned}$$

∎

エージェント定数は弱ガードされているので、この関数 mon は効果的に計算可能である。

CCS と同様に、Core-CCB のセマンティクスも次のラベル付遷移システムによって与えられる。

$$(\mathcal{E}, Event, \{\xrightarrow{a\theta^n} : a\theta^n \in Event\})$$

例えば、$E \xrightarrow{a\theta^n} E'$ はエージェント式 E がイベント $a\theta^n$ を実行でき、その実行後はエージェント式 E' になることを意味している。

定義 3.3 エージェント式間の遷移関係 $\xrightarrow{a\theta^n}$ は次の推論規則を満たす最小の関係である。ここで、横棒の上が 0 個以上の仮定、右横が条件、下が結果を表している。

$$\textbf{Event}\,\frac{}{a\theta^n.E \xrightarrow{a\theta^n} E}$$

$$\textbf{Choice}_1\,\frac{E \xrightarrow{a\theta^n} E'}{E+F \xrightarrow{a\theta^n} E'}$$

$$\textbf{Choice}_2\,\frac{F \xrightarrow{a\theta^n} F'}{E+F \xrightarrow{a\theta^n} F'}$$

$$\textbf{Ren}\,\frac{E \xrightarrow{a\theta^n} E'}{E[S] \xrightarrow{S(a)\theta^n} E'[S]}$$

$$\textbf{Res}_1\,\frac{E \xrightarrow{a\theta^n} E'}{E\backslash L \xrightarrow{a\theta^n} E'\backslash L}\ (a \notin L)$$

$$\textbf{Res}_2\,\frac{E \xrightarrow{a\theta^0} E'}{E\backslash L \xrightarrow{a!^0} E'\backslash L}\ \left(\begin{array}{c}\theta \in \{!,‼\},\\ a \in L\end{array}\right)$$

$$\textbf{Con}\,\frac{P \xrightarrow{a\theta^n} P'}{A \xrightarrow{a\theta^n} P'}\ (A \stackrel{\mathrm{def}}{=} P)$$

$$\mathbf{Para_1}\ \frac{E \xrightarrow{a\theta^n} E'}{E|F \xrightarrow{a\theta^n} E'|F} \left(\begin{array}{l} \theta \in \{!,?\} \text{ or} \\ a \notin mon(F) \end{array} \right)$$

$$\mathbf{Para_2}\ \frac{F \xrightarrow{a\theta^n} F'}{E|F \xrightarrow{a\theta^n} E|F'} \left(\begin{array}{l} \theta \in \{!,?\} \text{ or} \\ a \notin mon(E) \end{array} \right)$$

$$\mathbf{Para_3}\ \frac{E \xrightarrow{a\theta^m} E' \qquad F \xrightarrow{a\phi^n} F'}{E|F \xrightarrow{a\theta^{(m-n)}} E'|F'} \left(\begin{array}{l} \theta \in \{!,!!\}, \\ \phi = @(\theta), \\ m \geq n \end{array} \right)$$

$$\mathbf{Para_4}\ \frac{E \xrightarrow{a\phi^n} E' \qquad F \xrightarrow{a\theta^m} F'}{E|F \xrightarrow{a\theta^{(m-n)}} E'|F'} \left(\begin{array}{l} \theta \in \{!,!!\}, \\ \phi = @(\theta), \\ m \geq n \end{array} \right)$$

$$\mathbf{Para_5}\ \frac{E \xrightarrow{a\theta^m} E' \qquad F \xrightarrow{a\theta^n} F'}{E|F \xrightarrow{a\theta^{(m+n)}} E'|F'} \ (\theta \in \{?,??\})$$

ここで、@ は次のように定義される $\mathcal{T}$ から $\mathcal{T}$ への関数である：$@(!) = ?$, $@(?) = !$, $@(!!) = ??$, $@(??) = !!$ ∎

この定義のもとで、監視関数は「各エージェントが次に受信可能なイベントの集合」を計算する関数であることが、次の命題により示される

命題 3.1 $E \overset{a??^n}{\not\longrightarrow}$ *for any n* **iff** $a \notin mon(E)$ ∎

4 CCB の定義

4.1 CCB のシンタックス

CCB のシンタックスは次のように定義される。

定義 4.1 *CCB* のエージェント式の集合 $\mathcal{E}^+$ は次の *BNF* 記法に従って定義される。

$$\begin{aligned} E ::= X \mid A(e_1, \cdots, e_n) \mid \mathbf{0} \mid a!\langle c_0\rangle(e).E \mid a!!\langle x\rangle(e).E \\ \mid a?\langle c_1\rangle(x).E \mid a??\langle c_1\rangle(x).E \mid E+E \mid E|E \\ \mid E[S] \mid E\backslash L \mid [\![b]\!]E \end{aligned}$$

x は値変数、b は真偽式、e, c_0, c_1 は式である。ただし、c_0 の値域は 0 以上の整数、c_1 の値域は 1 以上の整数でなければならない。さらに、式 b, e, c_0, c_1 の中の全ての値変数は、それらの出現の左側で、すでに束縛されていなければならない。 ∎

n 引数をもつ各エージェント定数は、$A(\tilde{x}) \overset{\text{def}}{=} E$ の形の定義式をもつと仮定する。ここで、E は変数 $\tilde{x}(= x_1, \cdots, x_n)$ 以外の自由変数を含まず、エージェント変数も含まないとする。

4.2 CCB のセマンティクス

CCB のエージェント式 $E \in \mathcal{E}^+$ の意味は、core-CCB のエージェント式 $\mathcal{B}(E)$ によって与えられる。ここで、$\mathcal{B}$ は次のように定義される CCB から Core-CCB への変換関数である。

定義 4.2 関数 $\mathcal{B} : \mathcal{E}^+ \to \mathcal{E}$ は次のように定義される。

$$\begin{aligned} \mathcal{B}(X) &= X \\ \mathcal{B}(A(e_1, \cdots, e_n)) &= A_{e_1, \cdots, e_n} \\ \mathcal{B}(\mathbf{0}) &= \mathbf{0} \\ \mathcal{B}(a!\langle c\rangle(e).E) &= a_e!^c.\mathcal{B}(E) \\ \mathcal{B}(a!!\langle x\rangle(e).E) &= \textstyle\sum_{n \in \mathcal{I}} a_e!!^n.\mathcal{B}(E\{n/x\}) \\ \mathcal{B}(a?\langle c\rangle(x).E) &= \textstyle\sum_{v \in V} a_v?^c.\mathcal{B}(E\{v/x\}) \\ \mathcal{B}(a??\langle c\rangle(x).E) &= \textstyle\sum_{v \in V} a_v??^c.\mathcal{B}(E\{v/x\}) \\ \mathcal{B}(E+F) &= \mathcal{B}(E) + \mathcal{B}(F) \\ \mathcal{B}(E|F) &= \mathcal{B}(E)|\mathcal{B}(F) \\ \mathcal{B}(E[S]) &= \mathcal{B}(E)[S'] \\ \mathcal{B}(E\backslash L) &= \mathcal{B}(E)\backslash L' \\ \mathcal{B}([\![b]\!]E) &= \begin{cases} \mathcal{B}(E) & \mathit{if}\ b = \mathit{true} \\ \mathbf{0} & \mathit{otherwise} \end{cases} \end{aligned}$$

ここで、全ての値は集合 V に含まれていると仮定している。また、$S'(a_v) = S(a)_v$、$L' = \{a_v : a \in L, v \in V\}$ である。さらに、エージェント定数の定義式 $A(\tilde{x}) \overset{\text{def}}{=} E$ は、定義式の集合 $\{A_{\tilde{v}} \overset{\text{def}}{=} \mathcal{B}(E\{\tilde{v}/\tilde{x}\}) : \tilde{v} \in V^n\}$ に変換される。 ∎

5 観測的な同値関係

Core-CCB にも CCS と同様に観測的な合同関係を要求する。しかし、CCS で定義された**観測合同** $=$ が、次の例に示されるように Core-CCB では合同関係にならないことが重要な問題である。

$$P_1 = P_2, \quad P_1|Q \neq P_2|Q$$

ここで、各成分は次のように定義されている。

$$P_1 \overset{\text{def}}{=} a??^1.b!^0.P_1, \qquad P_2 \overset{\text{def}}{=} a??^1.P_2$$
$$Q \overset{\text{def}}{=} a!!^0.out0!^1.Q + a!!^1.out1!^1.Q$$

$b!^0$ は内部イベントであるので、P_1 と P_2 は観測合同となる。しかし、その各々に Q を合成するとその結果は観測合同にならない。それは、P_2 は常に a を受信可能であるのに対し P_1 は受信できないときがあるためである。そこで、観測合同に条件を付加して Core-CCB のための観測的な合同関係を定義する必要がある。

5.1 2 つの監視等価

この小節では観測的な同値関係を定義し、その特性について述べる。まず、この定義に必要な記法を準備する。

$Event^*$ を空列 ε を含むイベント列の集合とする。$t = a_1(\theta_1)^{n_1} \cdots a_k(\theta_k)^{n_k} \in Event^*$ について、もし $E \xrightarrow{a_1(\theta_1)^{n_1}} \cdots \xrightarrow{a_k(\theta_k)^{n_k}} E'$ ならば、$E \overset{t}{\Longrightarrow} E'$ と書く。特に、$E \overset{\varepsilon}{\Longrightarrow} E'$ ならば $E' \equiv E$ である。また、もしあるイベント名 a で、$E \xrightarrow{a!^0} E'$ ならば、$E \xrightarrow{\tau} E'$ と書く。このとき、次の状態遷移関係を定義する。

定義 5.1 $t = a_1(\theta_1)^{n_1} \cdots a_k(\theta_k)^{n_k} \in Event^*$ とする。もし、$E(\xrightarrow{\tau})^* \xrightarrow{a_1(\theta_1)^{n_1}} (\xrightarrow{\tau})^* \cdots (\xrightarrow{\tau})^* \xrightarrow{a_k(\theta_k)^{n_k}} (\xrightarrow{\tau})^* E'$ ならば、$E \overset{t}{\Longrightarrow} E'$ と書く。ここで $(\xrightarrow{\tau})^*$ は *0* 回以上の内部イベントによる状態遷移を意味している。 ∎

この状態遷移関係を用いて、CCS の**弱双模倣** (weak bisimulation) に相当する CCB の弱双模倣関係を定義する。以下、$(P, Q) \in \mathcal{S}$ を意味するために $P\mathcal{S}Q$ の記法を用いる。

定義 5.2 エージェント上の関係 $\mathcal{S}$ が**弱監視双模倣** *(weak monitor bisimulation)* であるとは、$P\mathcal{S}Q$ ならば、任意の $a\theta^n \in Event$ について、次の *4* つの条件が成り立つことである[8]。

- (i) $P \xrightarrow{a\theta^n} P'$ ならば、ある Q' が存在して、
  $Q \overset{\widehat{a\theta^n}}{\Longrightarrow} Q'$ かつ $P'\mathcal{S}Q'$ を満たす。
- (ii) $Q \xrightarrow{a\theta^n} Q'$ ならば、ある P' が存在して、
  $P \overset{\widehat{a\theta^n}}{\Longrightarrow} P'$ かつ $P'\mathcal{S}Q'$ を満たす。
- (iii) $a \notin mon(P)$ ならば、ある Q', Q'' が存在して、
  $Q \Rightarrow Q' \Rightarrow Q''$, $a \notin mon(Q')$, $P\mathcal{S}Q''$ を満たす。
- (iv) $a \notin mon(Q)$ ならば、ある P', P'' が存在して、
  $P \Rightarrow P' \Rightarrow P''$, $a \notin mon(P')$, $P''\mathcal{S}Q$ を満たす。

∎

弱監視双模倣は弱双模倣に条件 $(iii)(iv)$ を追加して得られる関係である。この弱監視双模倣を用いて弱監視等価を定義する。

定義 5.3 もし、ある弱監視双模倣 $\mathcal{S}$ において $(P, Q) \in \mathcal{S}$ ならば、エージェント P と Q は**弱監視等価**であるといい、$P \approx_m Q$ と書く。 ∎

次の命題に示されるように、弱監視等価は CCS の観測等価 $\approx$ に含まれ、かつ Core-CCB の並行合成演算子 $|$ によって保存される最も大きな関係である。

命題 5.1 $P_1 \approx_m P_2$ **iff** $\forall Q.\ P_1|Q \approx P_2|Q$ ∎

弱監視等価は同値関係であるが、選択演算子 $+$ によって保存されないため合同関係ではない。ただし、選択演算子を除く全ての演算子によっては保存される。弱監視等価の特性を顕著に表した等式として次の命題を与えておく。

命題 5.2 $a_1!^0.P \approx_m a_2!^0.a_3!^0.P + P$ ∎

この等式は定義 5.5で定義される強監視等価では成り立たず、弱監視等価固有の特性を表している。

[8] $\hat{t}$ はイベント列 t の内部イベントを全て除いたイベント列である。

ここで、弱監視双模倣の条件 $(iii), (iv)$ において、$P \equiv P' \equiv P''$, $Q \equiv Q' \equiv Q''$ の特殊な場合を考えておく。これは、内部イベントによる状態遷移を許さない場合であり、弱監視双模倣に対して強監視双模倣として定義できる。

定義 5.4 エージェント上の関係 $\mathcal{S}$ が**強監視双模倣**であるとは、$P\mathcal{S}Q$ ならば、任意の $a\theta^n \in Event$ について、次の *3* つの条件が成り立つことである。

- (i) $P \xrightarrow{a\theta^n} P'$ ならば、ある Q' が存在して、
  $Q \overset{\widehat{a\theta^n}}{\Longrightarrow} Q'$ かつ $P'\mathcal{S}Q'$ を満たす。
- (ii) $Q \xrightarrow{a\theta^n} Q'$ ならば、ある P' が存在して、
  $P \overset{\widehat{a\theta^n}}{\Longrightarrow} P'$ かつ $P'\mathcal{S}Q'$ を満たす。
- (iii) $mon(P) = mon(Q)$

∎

強監視双模倣を用いて強監視等価を定義する。

定義 5.5 もし、ある強監視双模倣 $\mathcal{S}$ において $(P, Q) \in \mathcal{S}$ ならば、エージェント P と Q は**強監視等価**であるといい、$P \simeq_m Q$ と書く。 ∎

強監視等価に対しては命題 5.2は成り立たない。それは $a \in mon(P)$ のような a が存在するとき、(iii) の条件を満たすことができないためである。弱監視等価に対しては条件 $(iii), (iv)$ の中で内部イベントによる状態遷移を許しているため、命題 5.2の等式の右辺を 1 回状態遷移して、左辺と同じ式を得ることが可能である。

強監視等価も弱監視等価と同様、同値関係ではあるが選択演算子 $+$ によって保存されないため合同関係ではない。

5.2 $\approx_m$ を除いて弱監視双模倣

弱監視等価の証明を容易にするために、$\approx_m$ を除いて弱監視双模倣 (weak monitor bisimulation up to $\approx_m$) を定義する。

定義 5.6 エージェント上の関係 $\mathcal{S}$ が、**$\approx_m$ を除いて弱監視双模倣**であるとは、$P\mathcal{S}Q$ ならば、任意の $a\theta^n \in Event$ について、次の *4* つの条件が成り立つことである[9]。

- (i) $P \overset{a\theta^n}{\Longrightarrow} P'$ ならば、ある Q' が存在して、
  $Q \overset{\widehat{a\theta^n}}{\Longrightarrow} Q'$ かつ $P' \approx_m \mathcal{S} \approx_m Q'$ を満たす。
- (ii) $Q \overset{a\theta^n}{\Longrightarrow} Q'$ ならば、ある P' が存在して、
  $P \overset{\widehat{a\theta^n}}{\Longrightarrow} P'$ かつ $P' \approx_m \mathcal{S} \approx_m Q'$ を満たす。

[9] $P \approx_m \mathcal{S} \approx_m Q$ は、ある P', Q' で $P \approx_m P', P'\mathcal{S}Q', Q' \approx_m Q$ を表している。

(iii) $P \Rightarrow P' \Rightarrow P''$ かつ $a \notin mon(P')$ ならば、
ある Q', Q'' が存在して、$Q \Rightarrow Q' \Rightarrow Q''$,
$a \notin mon(Q')$, $P'' \approx_m \mathcal{S} \approx_m Q''$ を満たす。

(iv) $Q \Rightarrow Q' \Rightarrow Q''$ かつ $a \notin mon(Q')$ ならば、
ある P', P'' が存在して、$P \Rightarrow P' \Rightarrow P''$,
$a \notin mon(P')$, $P'' \approx_m \mathcal{S} \approx_m Q''$ を満たす。 ∎

このとき次の命題が得られる。

命題 5.3 もし $\mathcal{S}$ が、$\approx_m$ を除いて弱監視双模倣ならば、$\mathcal{S} \subseteq \approx_m$ ∎

つまり、2つのエージェント P と Q が弱監視等価であることを示すためには、(P,Q) を含む、$\approx_m$ を除いて弱監視双模倣を見つければ十分である。

しかし、定義5.6の条件 $(i),\cdots,(iv)$ の仮定は、定義5.2の条件 $(i),\cdots,(iv)$ の仮定よりも弱くなっているため、より多くの場合をチェックしなければならない。そこで次の命題は、$\approx_m$ を除いて弱監視双模倣を見つけるために有効であると考えられる。

命題 5.4 エージェント上の関係 $\mathcal{S}$ について、$P\mathcal{S}Q$ ならば、任意の $a\theta^n \in Event$ について、次の *4* つの条件が成り立つとする。

(i) $P \xrightarrow{a\theta^n} P'$ ならば、ある Q' が存在して、
$Q \stackrel{\widehat{a\theta^n}}{\Longrightarrow} Q'$ かつ $P' \sim \mathcal{S} \approx_m Q'$ を満たす。

(ii) $Q \xrightarrow{a\theta^n} Q'$ ならば、ある P' が存在して、
$P \stackrel{\widehat{a\theta^n}}{\Longrightarrow} P'$ かつ $P' \approx_m \mathcal{S} \sim Q'$ を満たす。

(iii) $a \notin mon(P)$ ならば、
ある Q', Q'' が存在して、$Q \Rightarrow Q' \Rightarrow Q''$,
$a \notin mon(Q')$, $P \simeq_m \mathcal{S} \approx_m Q''$ を満たす。

(iv) $a \notin mon(Q)$ ならば、
ある P', P'' が存在して、$P \Rightarrow P' \Rightarrow P''$,
$a \notin mon(P')$, $P'' \approx_m \mathcal{S} \simeq_m Q$ を満たす。

このとき $\mathcal{S}$ は、$\approx_m$ を除いて弱監視双模倣である。 ∎

ここで、$\sim$ と $\simeq_m$ は各々強等価 [1] と強監視等価である。命題5.4は命題6.3の証明に使われる。ただし、命題6.4の証明では直接、定義5.6の条件を証明した方が容易である。

6 観測的な合同関係

次の例は弱監視等価が選択演算子によって保存されないことを示している。

$$P_1 \approx_m P_2, \quad P_1 + c!^1.\mathbf{0} \not\approx_m P_2 + c!^1.\mathbf{0}$$

ここで、各成分は次のように定義されている。

$$P_1 \equiv a_1!^0.b?^1.\mathbf{0}$$
$$P_2 \equiv a_2!^0.a_3!^0.b?^1.\mathbf{0} + b?^1.\mathbf{0}$$

$P_1 \approx_m P_2$ は命題5.2によって証明される。この例では、P_1 と P_2 は観測合同でもあることに注目すべきである。つまり、観測等価から観測合同を得たように演算子 ^ を省くだけでは弱監視等価から合同関係は得られない。

以下、弱監視等価と強監視等価に最も弱い条件を付加して合同関係を与え、公理系について考察する。

6.1 2つの監視合同

まず、無数に存在する内部イベント間の違いを無視するため、イベント上の同値関係 $\doteq$ を導入する。

定義 6.1 イベント等価 $\doteq$ は、次の集合として定義されるイベント上の *2* 項関係である。

$\{(a!^0, b!^0) : a, b \in \mathcal{N}\} \cup \{(a\theta^n, a\theta^n) : a\theta^n \in Event\}$ ∎

弱監視等価を用いて弱監視合同を定義する。

定義 6.2 もし、任意の $a\theta^n \in Event$ について、次の *3* つの条件を満たすならば、P と Q は**弱監視合同**であるといい、$P =_m Q$ と書く。

(i) $P \xrightarrow{a\theta^n} P'$ ならば、ある Q', b が存在して、
$Q \stackrel{b\theta^n}{\Longrightarrow} Q'$, $P' \approx_m Q'$, $a\theta^n \doteq b\theta^n$ を満たす。

(ii) $Q \xrightarrow{a\theta^n} Q'$ ならば、ある P', b が存在して、
$P \stackrel{b\theta^n}{\Longrightarrow} P'$, $P' \approx_m Q'$, $a\theta^n \doteq b\theta^n$ を満たす。

(iii) $mon(P) = mon(Q)$ ∎

弱監視等価の定義と比較して、演算子 ^ が落されている他に、弱監視等価の条件 $(iii),(iv)$ が $mon(P) = mon(Q)$ に強められていることがわかる。次の命題に示されるように、弱監視合同は弱監視等価 $\approx_m$ に含まれ、かつ Core-CCB の選択演算子 $+$ によって保存される最も大きな関係である。

命題 6.1 $P_1 =_m P_2$ **iff** $\forall Q.\ P_1 + Q \approx_m P_2 + Q$ ∎

今までエージェント上に弱監視合同を定義してきたが、ここでエージェント変数を含むエージェント式に拡張しておく。

定義 6.3 エージェント式 E または F に含まれるエージェント変数を $X_1,\cdots,X_n$ (以後 $\tilde{X}$ と書く) とする。このとき、もし全ての $\tilde{P}$ について、$E\{\tilde{P}/\tilde{X}\} =_m F\{\tilde{P}/\tilde{X}\}$ ならば、$E =_m F$ とする。 ∎

弱監視合同は次の命題が示すように全ての演算子によって保存され、再帰表現によっても保存される。

命題 6.2 もし $E_1 =_m E_2$ ならば、$a\theta^n.E_1 =_m a\theta^n.E_2$, $E_1+F =_m E_2+F$, $E_1|F =_m E_2|F$, $E_1\backslash L =_m E_2\backslash L$, $E_1[S] =_m E_2[S]$ である。 ∎

命題 6.3 $\tilde{E}$ と $\tilde{F}$ は高々変数 $\tilde{X}$ を含んでいるとする。このとき、もし $\tilde{A} \stackrel{\mathrm{def}}{=} \tilde{E}\{\tilde{A}/\tilde{X}\}$ かつ $\tilde{B} \stackrel{\mathrm{def}}{=} \tilde{F}\{\tilde{B}/\tilde{X}\}$ かつ $\tilde{E} =_m \tilde{F}$ ならば、$\tilde{A} =_m \tilde{B}$。 ∎

さらに、再帰をもつエージェントが弱監視合同であることを証明するために有効な、唯一解の存在を示す命題を与える。

命題 6.4 エージェント式 $\tilde{E}$ は高々エージェント変数 $\tilde{X}$ を含むとし、$\tilde{X}$ は $\tilde{E}$ のなかでガード[10]され、かつ逐次的[11]であるとする。このとき、もし、$\tilde{P} =_m \tilde{E}\{\tilde{P}/\tilde{X}\}$ かつ $\tilde{Q} =_m \tilde{E}\{\tilde{Q}/\tilde{X}\}$ ならば、$\tilde{P} =_m \tilde{Q}$ である。 ∎

次のように定義する強監視合同についても、弱監視合同と同様の議論をすることができる。

定義 6.4 もし、任意の $a\theta^n \in Event$ について、次の *3* つの条件を満たすならば、P と Q は**強監視合同**であるといい、$P \cong_m Q$ と書く。

(*i*) $P \xrightarrow{a\theta^n} P'$ ならば、ある Q', b が存在して、
$Q \stackrel{b\theta^n}{\Longrightarrow} Q'$, $P' \simeq_m Q'$, $a\theta^n \doteq b\theta^n$ を満たす。

(*ii*) $Q \xrightarrow{a\theta^n} Q'$ ならば、ある P', b が存在して、
$P \stackrel{b\theta^n}{\Longrightarrow} P'$, $P' \simeq_m Q'$, $a\theta^n \doteq b\theta^n$ を満たす。

(*iii*) $mon(P) = mon(Q)$ ∎

6.2 2 つの監視合同に対する公理系

この節の残りで、我々は有限エージェントの 2 つの監視合同に対する健全で完全な 2 つの公理系 $\mathcal{A}_1, \mathcal{A}_2$ を与える。有限エージェントとはエージェント定数を含まない (再帰をもたない) エージェントのことである。

定義 6.5 *2* つの有限エージェント P と Q の等価性が公理系 $\mathcal{A}_1$ から推論されるならば、$\mathcal{A}_1 \vdash P = Q$ と書く。ここで、公理系 $\mathcal{A}_1$ は次の等式から構成される。

- **M1** $P_1 + P_2 = P_2 + P_1$
- **M2** $(P_1 + P_2) + P_3 = P_1 + (P_2 + P_3)$
- **M3** $P = P + P$
- **M4** $P = P + 0$
- **T1** $a\theta^n.(b!^0.P + P) = a\theta^n.P$
- **T2** $P + R + a!^0.(P + Q) = R + a!^0.(P + Q)$ *if* $mon(P) \subseteq mon(R)$
- **T3** $a\theta^n.(P + b!^0.Q) + a\theta^n.Q = a\theta^n.(P + b!^0.Q)$
- **T4** $a!^0.P = b!^0.P$
- **E1** $(\sum_{(i\in I_1)} a_i(\theta_i)^{m_i}.P'_i)|(\sum_{(i\in I_2)} b_i(\phi_i)^{n_i}.Q'_i)$
$= \sum_{(i\in I_1)}\{a_i(\theta_i)^{m_i}.(P'_i|Q) : \theta_i \in \{!, ?\}\ or\ a_i \notin mon(Q)\}$
$+ \sum_{(i\in I_2)}\{b_i(\phi_i)^{n_i}.(P|Q'_i) : \phi_i \in \{!, ?\}\ or\ b_i \notin mon(P)\}$
$+ \sum_{(i\in I_1)}\sum_{(j\in I_2)}\{a_i(\theta_i)^{(m_i-n_j)}.(P'_i|Q'_j) : a_i = b_j, \theta_i \in \{!, !!\}, \phi_j = @(\theta_i), m_i - n_j \geq 0\}$
$+ \sum_{(i\in I_1)}\sum_{(j\in I_2)}\{b_j(\phi_j)^{(n_j-m_i)}.(P'_i|Q'_j) : a_i = b_j, \phi_j \in \{!, !!\}, \theta_i = @(\phi_j), n_j - m_i \geq 0\}$
$+ \sum_{(i\in I_1)}\sum_{(j\in I_2)}\{a_i(\theta_i)^{(m_i+n_j)}.(P'_i|Q'_j) : a_i = b_j, \theta_i = \phi_j \in \{?, ??\}\}$
- **E2** $(\sum_{(i\in I)} a_i(\theta_i)^{n_i}.P'_i)\backslash L$
$= \sum_{(i\in I)}\{a_i(\theta_i)^{n_i}.(P'_i\backslash L) : a_i \notin L\}$
$+ \sum_{(i\in I)}\{a_i!^0.(P'_i\backslash L) : a_i \in L, \theta_i \in \{!, !!\}, n_i = 0\}$
- **E3** $(\sum_{(i\in I)} a_i(\theta_i)^{n_i}.P'_i)[S]$
$= \sum_{(i\in I)} S(a_i)(\theta_i)^{n_i}.(P'_i[S])$ ∎

定義 6.6 *2* つの有限エージェント P と Q の等価性が公理系 $\mathcal{A}_2$ から推論されるならば、$\mathcal{A}_2 \vdash P = Q$ と書く。ここで、公理系 $\mathcal{A}_2$ は次の等式から構成される。

- **M1-M4, T1-T4, E1-E3**
- **T5** $a\theta^n.(P + \sum_{(i\in I)} a!^0.(Q_i + P_i))$
$= a\theta^n.(a!^0.(P + \sum_{(i\in I)} a!^0.(Q_i + P_i)) + P + \sum_{(i\in I)} P_i)$
- **T6** $a\theta^n.(R + a!^0.(P + \sum_{(i\in I)} a!^0.(Q_i + P_i)))$
$= a\theta^n.(a!^0.(R + a!^0.(P + \sum_{(i\in I)} a!^0.(Q_i + P_i))) + P + \sum_{(i\in I)} P_i)$
if $mon(R) \subseteq mon(P) \cup \bigcup_{(i\in I)} mon(P_i)$ ∎

M1-M4、**T1-T6**、**E1-E3** は各々 CCS のモノイド規則、τ 規則、 展開規則に相当する。特に、弱監視合同と強監視合同の差を知るために **T5** と **T6** は重要である。**T5** と **T6** は共に $\sum_{(i\in I)} P_i$ を内部イベントの内側に吸収するための式であり、基本的には命題 5.2の等式の形に似ている。

これら公理系 $\mathcal{A}_1$ と $\mathcal{A}_2$ は、次の定理が示すように、各々有限エージェントの強監視合同と弱監視合同に対して健全で完全である。

定理 6.1 P と Q を有限エージェントとする。このとき、

$$P \cong_m Q \ \textbf{iff}\ \mathcal{A}_1 \vdash P = Q. \quad ∎$$

定理 6.2 P と Q を有限エージェントとする。このとき、

$$P =_m Q \ \textbf{iff}\ \mathcal{A}_2 \vdash P = Q. \quad ∎$$

[10] X の全ての出現が $a\theta^n.F$ の形をもつ E の部分式のなかにあるならば、X は E のなかでガードされているという、ただし、$a\theta^n$ は内部イベントであってはならない。

[11] もし、X を含む E の全ての部分式 (X 自身は除く) が $a\theta^n.F$ か $\sum \tilde{F}$ の形をもつならば、X は E のなかで、逐次的であるという。

7 関連研究

1節で述べたように、ブロードキャストのためのプロセス代数としてCBSが提案されている。ブロードキャストを導入するためには、「各エージェントが受信を希望していないイベント」を扱うことが重要である。一般にそれは負の状態遷移によって表されるが、CBSではディスカードと呼ばれる特殊なイベントによる(正の)状態遷移を用いている。このディスカードよる状態遷移を使う利点は同期代数(synchronization algebra)[12]の枠組を適用できることにある。

我々は負の状態遷移の代わりに監視関数monを採用している。この監視関数の利点は、等式の条件として監視関数を使えることにある。例として、公理系の等式**T2**, **T6**の条件に監視関数が使われており、これによって公理系をより簡単に構築することができた。

ディスカードを用いても監視関数を用いてもその結果に差はない。CCBとCBSの重要な違いは受信者数にある。CCBではイベントをブロードキャストしたエージェントはそのイベントの受信者数を知ることができるが、CBSではそれは困難である。一般にプロセス代数には時間の概念がないため、タイムアウトとループを用いて受信者数を数えることができない[9]。

TCCS[10]のように、時間の概念をもつプロセス代数も提案されている。TCCSは1対1通信であるが、タイムアウトを用いてブロードキャストを模倣できると考えられる。すなわち、ブロードキャスト機能をもつ並列言語の開発にTCCSのようなプロセス代数は大変有効であると考えられる。他方、我々はそのような並列言語を用いて記述されたソフトウェアシステムを可能な限り簡単に解析することを望んでいる。このような目的に対してCCBは適している。

他のプロセス代数によるブロードキャストの記述に関する研究として[9]があげられる。この研究では、CBSのエージェントをSCCSのエージェントに変換する方法を示し、CBSとSCCSの関係を明らかにしている。同様にしてSCCSによるCCBの解釈も考え得る。可能ならばCCBの監視合同が、SCCSでどのように解釈されるかに興味がもたれる。

8 おわりに

我々はブロードキャスト後にその受信者数を知ることができることを要求し、そのようなブロードキャストの記述に適したプロセス代数として**CCB**を提案している。しかし、CCBでは観測合同が合同関係にならないことが問題になっていた。

本報告書で、我々は弱監視等価と弱監視合同を定義した。弱監視等価は観測等価に含まれ、かつCCBの並行合成演算子$|$によって保存される最も大きな関係である。また、弱監視合同は弱監視等価に含まれる最も大きな合同関係である。そして、弱監視等価の証明に有効な、$\approx_m$を除いて弱監視双模倣について考察し、弱監視合同の唯一解の存在を明らかにした。さらに、有限エージェントの弱監視合同に対する健全で完全な公理系$\mathcal{A}_2$を与えた。

今後は、さらにCCBの特性を明らかにしていくとともに、CCBに空間的距離の効果を導入して拡張することを検討中である。

参考文献

[1] R.Milner, "Communication and Concurrency", Prentice-Hall, 1989.

[2] R.Milner, J.Parrow and D.Walker, "A Calculus of Mobile Processes, I and II", Information and Computation, 100, pp.1 - 40 and pp.41 - 77, 1992.

[3] R.Milner, "Calculi for Synchrony and Asynchrony", Journal of Theoretical Computer Science, Vol.25, pp.267 - 310, 1983.

[4] C.A.R.Hoare,"Communicating Sequential Processes", Prentice-Hall, 1985.

[5] ISO 8807: "Information Processing Systems–Open System Interconnection–LOTOS–A formal description technique based on the temporal ordering of observational behavior", Feb. 1989.

[6] K.V.S.Prasad, "A Calculus of Broadcasting Systems", TAPSOFT'91, Vol.1:CAAP, LNCS 493, Springer-Verlag, pp.338 - 358, 1991

[7] K.V.S.Prasad, "A Calculus of Value Broadcasts", PARLE '93, LNCS 694, Springer-Verlag, pp.391 - 402, 1993

[8] K.V.S.Prasad, "Programming with Broadcasts", CONCUR'93, LNCS 715, Springer-Verlag, pp.173 - 187, 1993

[9] Uno Holmer, "Interpreting Broadcast Communication in SCCS", CONCUR'93, LNCS 715, Springer-Verlag, pp.188 - 201, 1993

[10] F.Moller and C.Tofts,"An overview of TCCS", Proceedings of EUROMICRO'92, Athens, June 1992.

[11] L.Aceto, B.Bloom, and F.Vaandrager "Turning SOS Rules into Equations", Proc. Seventh Annual IEEE Symposium on Logic in Computer Science, pp.113 - 124, 1988.

[12] G.Winskel, "Synchronization trees", Journal of Theoretical Computer Science, Vol.34, pp.33 - 82, 1984.

[13] 磯部祥尚, 佐藤豊, 大蒔和仁, "CCB: ブロードキャスト機能をもつプロセス代数の提案", 情報処理学会研究報告, PRG19-3, pp.19 - 26, 1994.

[14] 磯部祥尚, 佐藤豊, 大蒔和仁, "ブロードキャストに適したプロセス代数", 第1回ソフトウェア工学の基礎ワークショップ(FOSE '94) 論文集, pp.33 - 40, 1994.