数理解析研究所講究録 1442 巻 2005 年 76-82

並列合成の論理演算を持つ論理体系

竹内泉 (Takeuti Izumi)
東邦大学理学部 (Faculty of Science, Tôhô University)

要旨

ヘネシーミルナーの様相論理はプロセス代数などの遷移系に対して健全性と完全性を充たす。この結果を、並列合成を含む CCS に拡張するために、論理体系に並列合成を表す論理演算を追加する。

重要語句: ヘネシー・ミルナーの様相論理, プロセス代数, CCS

1 序

ラベル付遷移系の性質を記述する論理体系としては、ヘネシー・ミルナーの様相論理が有名である。[S] これは、K 公理によって規定される様相を持った多重様相命題論理である。この論理はプロセス代数との間に充足関係が定義される。プロセス代数の上の、論理式に対する充足関係の等価性は、公理的同等性、双模倣関係と一致する。また、この充足関係の許でこの論理は健全かつ完全である。即ち、ある論理式が証明可能ならば全てのプロセスで充足され、証明不能ならば反例がある。

プロセス代数に通信と並列合成を追加した理論模型としては、ミルナーの CCS が知られている。[M] プロセスの遷移を見るだけならば、古典論理に様相を付加しただけの様相命題論理で十分であるが、並列合成をもまた論理式によって把握することは興味深い問題である。そこで、従来の様相論理に並列合成を表す論理演算を追加した論理体系を提案する。この論理は健全かつ完全であり、更に、証明探査と反例構成の手続を同時に行なうことが出来るであろことが予想される。

2 プロセス代数

まず、単純なラベル付遷移系の例としてプロセス代数を採り、それに関して説明する。

定義 2.1 (プロセス代数)

遷移要素 $a \in A$ 、有限集合
プロセス式 $P ::= 1 \mid G$
ガード式 $G ::= a.P \mid G + G$

これは後に現れる定義との比較の便宜の為にプロセス式とガード式とによって相互再帰的に定義しているが、

$P ::= a.1 \mid a.P \mid P + P$

と定義したものと同等である。

1 は正常終了を表す。他の文献で 0 と書かれているものと似ている。しかし、一般に 0 は単なる不活性を表すので、その点は異なる。

プロセス式は今後単にプロセスと呼ぶ。

定義 2.2 (遷移関係) プロセスの間の二項関係 $\xrightarrow{a}$ は、以下の規則から生成される。

$$a.P \xrightarrow{a} P$$
$$P \xrightarrow{a} Q \Longrightarrow P+R \xrightarrow{a} Q,\ R+P \xrightarrow{a} Q$$

3 同値関係

プロセスに対して三種の同値関係を導入する。

定義 3.1 (公理的同等性) 以下の規則によって生成される同値関係 $\sim$ を公理的同等性と呼ぶ。プロセス P 、Q 、R 及び遷移 a に対して

$P \sim P+P$ (冪等則)、$P+Q \sim Q+P$ (交換則)、

$P \sim Q \Longrightarrow a.P \sim a.Q,\ P+R \sim Q+R$ (合同則)

定義 3.2 (双模倣) あるプロセス上の二項関係 $\overset{S}{\sim}$ があって、以下の条件を充たし、PSQ が成り立つならば、P と Q は双模倣であるという。

任意のプロセス P 、Q に対して

- $P \overset{S}{\sim} Q \Longrightarrow \forall a \in A.\ \forall P'.\ P \xrightarrow{a} P' \Longrightarrow \exists Q'.\ Q \xrightarrow{a} Q' \wedge P' \overset{S}{\sim} Q'$
- $P \overset{S}{\sim} Q \Longrightarrow Q \overset{S}{\sim} P$

定義 3.3 (論理式) $F ::= 1 \mid \neg F \mid F \wedge F \mid [a]F$

以下の略記法を用いる。

$F \supset G = \neg(F \wedge \neg G)$ 、$F \vee G = (\neg G) \supset F$ 、$F \supset\subset G = (F \supset G) \wedge (G \supset F)$ 、$\langle a \rangle F = \neg[a]\neg F$

定義 3.4 (充足関係)

- $P \models 1 \iff P = 1$
- $P \models \neg F \iff P \not\models F$
- $P \models F \wedge G \iff P \models F \& P \models G$
- $P \models [a]F \iff \forall Q.\ P \xrightarrow{a} Q \Longrightarrow Q \models F$

定義 3.5 (恒真) $\models F \iff \forall P.\ P \models F$

定義 3.6 (充足等価) プロセス P 、Q が充足等価であるとは、$\forall F.\ P \models F \iff Q \models F$ となることを云う。

定理 3.7 公理的同等、双模倣、充足等価の三者は互いに同値である。

4 論理式の公理系

論理式に対して、K 公理による多重様相の公理系によって理論を定める。論理式 F がその理論の定理であることを $\vdash F$ と書く。

補題 4.1 $\not\vdash F \Longrightarrow \exists P.\ P \not\models F$

補題 4.2 $P \models F, \vdash F \supset G \Longrightarrow P \models G$

定理 4.3 *1.* $\vdash F \iff \models F$ *2.* $\vdash F \supset\subset G \iff \forall P.\ P \models F \iff P \models G$

5 並列合成のあるプロセス代数

定義 5.1 (プロセス)

遷移名 $n \in N$ 、有限集合

遷移要素 $a \in A = \{\tau\} \cup N \cup \{\bar{n} \mid n \in N\}$

プロセス式 $P ::= 1 \mid G\ P * P$

ガード式 $G ::= a.P \mid G + G$

$a = \bar{n} \in A$ に対して $\bar{a} = n$ と定める。$\bar{\tau}$ という表現は無い。

記号 $*$ は並列合成を表す演算記号である。他の文献では「|」と書かれることも多い。

定義 5.2 (遷移関係) $\xrightarrow{a}$ は、以下の規則から生成される。

$a.P \xrightarrow{a} P$

$P \xrightarrow{a} Q \Longrightarrow P + R \xrightarrow{a} Q,\ R + P \xrightarrow{a} Q$

$P \xrightarrow{a} Q \Longrightarrow P * R \xrightarrow{a} Q * R,\ R * P \xrightarrow{a} R * Q$

$P \xrightarrow{a} Q,\ P' \xrightarrow{a} Q' \Longrightarrow P * Q \xrightarrow{a} P' * Q'$

$P \xrightarrow{a} Q,\ P' \xrightarrow{\bar{a}} Q' \Longrightarrow P * Q \xrightarrow{\tau} P' * Q',\ Q * P \xrightarrow{\tau} Q' * P'$

定義 5.3 (公理的同等性) 3.1 の規則に以下を追加する。

プロセス P 、Q 、R 及び遷移 a に対して

$P \sim Q \Longrightarrow P * R \sim Q * R,\ R * P \sim R * Q$ (合同則)

$P \sim 1 * P \sim P * 1$ (単位元)

$P = a_1.P_1 + \ldots + a_m.P_m$ 、$Q = b_1.Q_1 + \ldots + b_n.Q_n$ に対して

$P * Q \sim$

$a_1.(P_1 * Q) + \ldots + a_m.(P_m * Q) + b_1.(P * Q_1) + \ldots + b_n.(P * Q_n)$

$+ \tau.(P_{i_1} * Q_{j_1}) + \ldots + \tau.(P_{i_l} * Q_{j_l})$

(分配則)

ここで $\{\langle i_1, j_1\rangle, \ldots, \langle i_l, j_l\rangle\} = \{\langle i, j\rangle \mid a_i = \bar{b}_j\}$

この規則の許で以下が成り立つ。

命題 5.4 $P*Q \sim Q*A$ *(交換則)*、$P*(Q*R) \sim (P*Q)*R$ *(結合則)*

命題 5.5 任意のプロセス P に対して、$*$ を含まないプロセス Q があって $P \sim Q$ 。

定義 5.6 (双模倣、充足関係、充足等価) プロセスの定義が拡張された以外は、 3.2、3.4、3.6 と同一の定義による。

同様の定理が成り立つ。

定理 5.7 公理的同等、双模倣、充足等価の三者は互いに同値である。

6 並列合成を持った論理式

定義 6.1 (論理式) $F ::= 1 \mid \neg F \mid F \wedge F \mid [a]F \mid F \multimap F \mid F * F$

定義 6.2 (充足関係)
- $P \models 1 \iff P = 1$
- $P \models \neg F \iff P \not\models F$
- $P \models F \wedge G \iff P \models F \& P \models G$
- $P \models [a]F \iff \forall Q.\ P \xrightarrow{a} Q \Longrightarrow Q \models F$
- $P \models F \multimap G \iff \forall Q.\ Q \models F \Longrightarrow P * Q \models G$
- $P \models F * G \iff \exists Q, R.\ P \sim Q * R,\ Q \models F,\ R \models G$

定理 6.3 公理的同等、双模倣と充足等価は互いに同値である。

充足関係の定義の中で公理的同等が参照されているので、この定理は左程重要ではない。

7 論理体系

論理式が与えられたときに、それが恒真であるかそれとも反例があるかを判定することは有益である。即ち、論理式 F に対して、もし $\forall P.\ P \models F$ ならば恒真であると答え、もし $P \not\models F$ となる P があるならばその P を答える計算手続を作ることが求められる。

ある適切な論理体系があって、その論理体系で証明されるならばその論理式は恒真であり、その証明探査手続が反例構成手続と一致しているということになれば、先の要求は充たされる。この要請を充たすような論理体系を定義する。

論理体系はゲンツェンの LK に倣って、式を推論していく形を取る。LK に於いては式は左辺と右辺より成っていたが、ここで定義する論理体系は一

段以上の段より成る。各段に左辺と右辺がある。左辺、右辺は論理式の有限集合である。紙面での表記上は有限集合は列で表されるが、その順序や重複には意味がない。

以降、Γ 、Γ_i 、Δ 、等は論理式の有限集合を表す。「F,Γ」、「Γ,Γ'」は $\{F\}\cup\Gamma$ 、$\Gamma\cup\Gamma'$ をそれぞれ表す。Γ と $a\in A$ に対して $\Gamma^a=\{F|[a]F\in\Gamma\}$ 。

定義 7.1 (式) 式とはこのような形をした図式である。

Γ_1	Δ_1
...	...
Γ_n	Δ_n
Γ_0	Δ_0

最下段とそれより上の段とは二重線で仕切られる。二重線の上には 0 段以上の段がある。二重線の下には必ず丁度 1 段ある。各段は左辺と右辺の枡がある。各枡には論理式の有限集合がある。

表の形では書き辛いので、一行の数式による表記法を与えておく。先の表はこのように表記する。

$$(\Gamma_1/\Delta_1)(\Gamma_2/\Delta_2)...(\Gamma_n/\Delta_n)\Rightarrow(\Gamma_0/\Delta_0)$$

この式の直感的な意味はこのようなものである。この式が証明できない場合には、以下を充たすプロセス $P_1*...*P_n$ がある。

$$\forall F\in\Gamma_0.\ P_1*...*P_n\models F)\&\forall F\in\Gamma_i.\ P_1*...*P_n\not\models F$$

$$\forall i\in 1,2,...,n.\ (\forall F\in\Gamma_i.\ P_i\models F)\&\forall F\in\Gamma_i.\ P_i\not\models F$$

特に $\Gamma_0,...,\Gamma_n$ 、$\Delta_1,...,\Delta_n$ が空であり、Δ_0 が唯一つの論理式 F から成る場合には、式は $\Rightarrow(/F)$ となる。この場合には、$\Rightarrow(/F)$ が証明可能ならば $\forall P.\ P\models F$ 、$\Rightarrow(/F)$ が証明不能ならば $\exists P.\ P\not\models F$ となる。

式 $(\Gamma_1/\Delta_1)...(\Gamma_n/\Delta_n)\Rightarrow(\Gamma_0/\Delta_0)$ に於いて、小括弧で括られた (Γ/Δ) は一ヶの段を表す。以下では、二重線より上の 0 段以上の段を纏めて $\tilde{\Gamma}$ 、$\tilde{\Gamma}'$ 等で表す。

$\tilde{\Gamma}=(\Gamma_1/\Delta_1)...(\Gamma_n/\Delta_n)$ に対して

$$\tilde{\Gamma}-(\Gamma_i/\Delta_i)=(\Gamma_1/\Delta_1)...(\Gamma_{i-1}/\Delta_{i-1})(\Gamma_{i+1}/\Delta_{i+1})(\Gamma_n/\Delta_n)$$

定義 7.2 (推論規則)

構造規則

始式：

$$\frac{}{(F,\Gamma_1/F,\Delta_1),\tilde{\Gamma}\Rightarrow(\Gamma_0/\Delta_0)}\qquad\frac{}{\tilde{\Gamma}\Rightarrow(F,\Gamma_0/F,\Delta_0)}$$

増：

$$\frac{(\Gamma_1/\Delta_1)...(\Gamma_n/\Delta_n)\Rightarrow(\Gamma_0/\Delta_0)}{(\Gamma'_1/\Delta'_1)...(\Gamma'_n/\Delta'_n)\Rightarrow(\Gamma'_0/\Delta'_0)}$$

但し $\forall i \in \{0,1,...,n\}.\ \{\Gamma_i\} \subset \{\Gamma_i'\} \& \{\Delta_i\} \subset \{\Delta_i'\}$

換：

$$\frac{(\Gamma_1/\Delta_1)...(\Gamma_n/\Delta_n) \Rightarrow (\Gamma_0/\Delta_0)}{(\Gamma_{\sigma(1)}/\Delta_{\sigma(1)})...(\Gamma_{\sigma(n)}/\Delta_{\sigma(n)}) \Rightarrow (\Gamma_0/\Delta_0)}$$

但し σ は {0,1,...,n} 上の置換。

転：

$$\frac{(\Gamma_2,\Gamma_1/\Delta_2,\Delta_1) \Rightarrow (\Gamma_3,\Gamma_0/\Delta_3,\Delta_0)}{(\Gamma_3,\Gamma_1/\Delta_3,\Delta_1) \Rightarrow (\Gamma_2,\Gamma_0/\Delta_2,\Delta_0)}$$

論理規則

1：

$$\frac{}{(1/[a]F),\tilde{\Gamma} \Rightarrow (\Gamma/\Delta)} \qquad \frac{\tilde{\Gamma} \Rightarrow (\Gamma/\Delta)}{(1/),\tilde{\Gamma} \Rightarrow (\Gamma/\Delta)}$$

¬：

$$\frac{(F,\Gamma_1/\Delta_1),\tilde{\Gamma} \Rightarrow (\Gamma_0/\Delta_0)}{(\Gamma_1/\neg F,\Delta_1),\tilde{\Gamma} \Rightarrow (\Gamma_0/\Delta_0)} \qquad \frac{\tilde{\Gamma} \Rightarrow (F,\Gamma_0/\Delta_0)}{\tilde{\Gamma} \Rightarrow (\Gamma_0/F,\Delta_0)}$$

$$\frac{(\Gamma_1/F,\Delta_1),\tilde{\Gamma} \Rightarrow (\Gamma_0/\Delta_0)}{(\neg F,\Gamma_1/\Delta_1),\tilde{\Gamma} \Rightarrow (\Gamma_0/\Delta_0)} \qquad \frac{\tilde{\Gamma} \Rightarrow (\Gamma_0/F,\Delta_0)}{\tilde{\Gamma} \Rightarrow (\neg F,\Gamma_0/\Delta_0)}$$

∧：

$$\frac{(\Gamma_1/F,\Delta_1),\tilde{\Gamma} \Rightarrow (\Gamma_0/\Delta_0) \qquad (\Gamma_1/G,\Delta_1),\tilde{\Gamma} \Rightarrow (\Gamma_0/\Delta_0)}{(\Gamma_1/F \wedge G,\Delta_1),\tilde{\Gamma} \Rightarrow (\Gamma_0/\Delta_0)}$$

$$\frac{\tilde{\Gamma} \Rightarrow (\Gamma_0/F,\Delta_0) \qquad \tilde{\Gamma} \Rightarrow (\Gamma_0/G,\Delta_0)}{\tilde{\Gamma} \Rightarrow (\Gamma_0/F \wedge G,\Delta_0)}$$

$$\frac{(F,\Gamma_1/\Delta_1),\tilde{\Gamma} \Rightarrow (\Gamma_0/\Delta_0)}{(F \wedge G,\Gamma_1/\Delta_1),\tilde{\Gamma} \Rightarrow (\Gamma_0/\Delta_0)} \qquad \frac{(F,\Gamma_1/\Delta_1),\tilde{\Gamma} \Rightarrow (\Gamma_0/\Delta_0)}{(G \wedge F,\Gamma_1/\Delta_1),\tilde{\Gamma} \Rightarrow (\Gamma_0/\Delta_0)}$$

$$\frac{\tilde{\Gamma} \Rightarrow (F,\Gamma_0/\Delta_0)}{\tilde{\Gamma} \Rightarrow (F,\wedge G,\Gamma_0/\Delta_0)} \qquad \frac{\tilde{\Gamma} \Rightarrow (F,\Gamma_0/\Delta_0)}{\tilde{\Gamma} \Rightarrow (G \wedge F,\Gamma_0/\Delta_0)}$$

$\multimap$：

$$\frac{(F/),\tilde{\Gamma} \Rightarrow (/G)}{\tilde{\Gamma} \Rightarrow (/F \multimap G)} \qquad \frac{\tilde{\Gamma} \Rightarrow (/F) \qquad (G/),\tilde{\Gamma}' \Rightarrow (\Gamma_0/\Delta_0)}{(F \multimap G/),\tilde{\Gamma},\tilde{\Gamma}' \Rightarrow (\Gamma_0/\Delta_0)}$$

$*$：

$$\frac{\tilde{\Gamma} \Rightarrow (/F) \qquad \tilde{\Gamma}' \Rightarrow (/G)}{\tilde{\Gamma},\tilde{\Gamma}' \Rightarrow (/F * G)} \qquad \frac{(F/)(G/),\tilde{\Gamma} \Rightarrow (\Gamma_0/\Delta_0)}{(F * G/),\tilde{\Gamma} \Rightarrow (\Gamma_0/\Delta_0)}$$

[−]：

$$\frac{(\Gamma_1/F),\tilde{\Gamma} \Rightarrow (\Gamma_0/)}{([a]\Gamma_1/[a]F),\tilde{\Gamma} \Rightarrow ([a]\Gamma_0/)}$$

$$\frac{(\Gamma_1/F),(\Gamma_2/G),\tilde{\Gamma} \Rightarrow (\Gamma_0/)}{([a]\Gamma_1/[a]F),([\bar{a}]\Gamma_2/[\bar{a}]G),\tilde{\Gamma} \Rightarrow ([\tau]\Gamma_0/)}$$

$$\frac{(\Gamma_i^a/),\tilde{\Gamma} - (\Gamma_i/\Delta_i) \Rightarrow (\Gamma_0/F) \quad (\text{全ての } i \in \{1,2,...,n\} \text{ に対して})}{\tilde{\Gamma} \Rightarrow ([a]\Gamma_0/[a]F)}$$

但し $\tilde{\Gamma} = (\Gamma_1/\Delta_1)...(\Gamma_n/\Delta_n)$ 、$a \neq \tau$

$$\frac{(\Gamma_i^a/), (\Gamma_j^a/), \tilde{\Gamma} - (\Gamma_i/\Delta_i) - (\Gamma_j/\Delta_j) \Rightarrow (\Gamma_0/F) \quad (\text{全ての } i,j \in \{1,2,...,n\}\ (i \neq j) \text{ に対して}) \quad (\Gamma_i^\tau/), \tilde{\Gamma} - (\Gamma_i/\Delta_i) \Rightarrow (\Gamma_0/F) \quad (\text{全ての } i \in \{1,2,...,n\} \text{ に対して})}{\tilde{\Gamma} \Rightarrow ([\tau]\Gamma_0/[\tau]F)}$$

但し $\tilde{\Gamma} = (\Gamma_1/\Delta_1)...(\Gamma_n/\Delta_n)$

切断

$$\frac{(F, \Gamma_1/\Delta_1), \tilde{\Gamma} \Rightarrow (\Gamma_0/\Delta_0) \qquad (\Gamma_1/F, \Delta_1), \tilde{\Gamma} \Rightarrow (\Gamma_0/\Delta_0)}{(\Gamma_1/\Delta_1), \tilde{\Gamma} \Rightarrow (\Gamma_0/\Delta_0)}$$

$$\frac{(\Gamma_1/\Delta_1), \tilde{\Gamma} \Rightarrow (F, \Gamma_0/\Delta_0) \qquad (\Gamma_1/\Delta_1), \tilde{\Gamma} \Rightarrow (\Gamma_0/F, \Delta_0)}{(\Gamma_1/\Delta_1), \tilde{\Gamma} \Rightarrow (\Gamma_0/\Delta_0)}$$

$$\frac{\tilde{\Gamma} \Rightarrow (F, \Gamma_1/\Delta_1) \qquad (\Gamma_1/\Delta_1), \tilde{\Gamma}' \Rightarrow (\Gamma_0/F, \Delta_0)}{\tilde{\Gamma}, \tilde{\Gamma}' \Rightarrow (\Gamma_0/\Delta_0)}$$

この推論規則で式 $\tilde{\Gamma} \Rightarrow (\Gamma/\Delta)$ が導出されることを $\vdash \tilde{\Gamma} \Rightarrow (\Gamma/\Delta)$ と書く。論理式 F に対して、$\vdash \Rightarrow (/F)$ を単に $\vdash F$ と書く。

予想 7.3 ある式が証明可能ならば、切断規則を使わないで証明可能である。

補題 7.4 (健全性)

$$\vdash (\Gamma_1/\Delta_1)(\Gamma_2/\Delta_2)...(\Gamma_n/\Delta_n) \Rightarrow (\Gamma_0/\Delta_0)$$

ならば、以下を充たすプロセス $P_1, ..., P_n$ はない。

$$\forall F \in \Gamma_0.\ P_1 * ... * P_n \models F) \& \forall F \in \Gamma_i.\ P_1 * ... * P_n \not\models F$$
$$\forall i \in 1,2,...,n.\ (\forall F \in \Gamma_i.\ P_i \models F) \& \forall F \in \Gamma_i.\ P_i \not\models F$$

定理 7.5 (健全性) $\vdash F \Longrightarrow \models F$

予想 7.6 (完全性) $\models F \Longrightarrow \vdash F$

更に、この論理体系の証明探査手続によって証明不能であることが示された場合には、それと同時に反例構成が成されることが予想される。

参考文献

[S] Stirling, S: 'Modal and Temporal Logics', in Abramsky, S. et.al. eds: *Handbook of Logic in Computer Science*, vol. 2, pp477 - 563, Oxford Science Publications, 1993.

[M] Milner, R.: *Communication and concurrency*, Prentice-Hall International Computer Science Series archive, Prentice-Hall, Inc. 1989.