

# A Formal System for Specification Analysis of Concurrent Programs

By

Ken HIROSE\* and Makoto TAKAHASHI\*

## Abstract

A formal system  $FL_{m,n}$  is proposed to analyze the specification of concurrent programs. The soundness theorem for  $FL_{m,n}$  is also proved.

## § 1. Introduction

In order to have reliable and modifiable software system, it should be very important to give a precise specification of the whole computational processes. It is especially difficult to describe a detailed specification of a concurrent program.

In [1] and [2], one of the authors and his colleagues proposed a new specification technique called Process-Data Representation (PDR). The process data interactions in PDR are specified mainly by using formulas in the forcing logic (FL) which intends to describe constraint conditions for concurrent processing.

The formal logic for the specification description should express the essential properties of the target system. That is, we should choose several fundamental concepts in the target system and embed them in the predicate logic. Since the introduction of many concepts might make it difficult to define the formal system, it is necessary to carefully introduce only a few concepts which maximize readability.

There may be several fundamental concepts, for example, those relating to the number of objects, forcing, prohibition, constraint, priority for some actions and so forth. In the forcing logic, the concept concerning the number of objects involved in some activities was introduced.

---

Received March 4, 1983.

\* Department of Mathematics, School of Science and Engineering, Waseda University, Shinjuku, Tokyo 160, Japan.

Furthermore, for specification analysis, we should need a formal system which will enable us to conclude some situations from given specifications.

In the present paper, we propose a formal system  $FL_{m,n}$  to analyse specifications described by formulas in the forcing logic. The following notations are used:

$\langle x_1, \dots, x_n \rangle_k$  is a set of the subsets of  $\{x_1, \dots, x_n\}$  whose cardinality  $\geq k$ ,  
 $[x_1, \dots, x_n]_k$  is a set of the subsets of  $\{x_1, \dots, x_n\}$  whose cardinality  $\leq k$

and intuitively

$\langle x_1, \dots, x_n \rangle_k \rightarrow Y$  means “the element of  $\langle x_1, \dots, x_n \rangle_k$  (at least  $k$  out of  $n$  objects  $\{x_1, \dots, x_n\}$ ) should do the operation to only the element of  $Y$ ”,  $[x_1, \dots, x_n]_k \rightarrow Y$  means “the element of  $Y$  may be done the operation only by the element of  $[x_1, \dots, x_n]_k$  (at most  $k$  out of  $n$  objects  $\{x_1, \dots, x_n\}$ ) and  $X \Rightarrow Y$  means “the element of  $X$  do the operation to the element of  $Y$ ”. Then, for example, the specification of the conditions in the dining philosophers problem can be described as follows:

$$(*) \quad \left\{ \begin{array}{l} \langle ph1 \rangle_1 \rightarrow [\langle f5, f1 \rangle_2]_1 \\ \langle ph2 \rangle_1 \rightarrow [\langle f1, f2 \rangle_2]_1 \\ \langle ph3 \rangle_1 \rightarrow [\langle f2, f3 \rangle_2]_1 \\ \langle ph4 \rangle_1 \rightarrow [\langle f3, f4 \rangle_2]_1 \\ \langle ph5 \rangle_1 \rightarrow [\langle f4, f5 \rangle_2]_1 \\ [ph1, ph2]_1 \rightarrow \langle f1 \rangle_1 \\ [ph2, ph3]_1 \rightarrow \langle f2 \rangle_1 \\ [ph3, ph4]_1 \rightarrow \langle f3 \rangle_1 \\ [ph4, ph5]_1 \rightarrow \langle f4 \rangle_1 \\ [ph5, ph1]_1 \rightarrow \langle f5 \rangle_1 \end{array} \right.$$

where  $phk$  ( $k=1, \dots, 5$ ) represents the philosopher  $k$  and  $fi$  ( $i=1, \dots, 5$ ) represents the folk  $i$ .

And  $[ph1, \dots, ph5]_2 \Rightarrow [\langle f5, f1 \rangle_2, \dots, \langle f4, f5 \rangle_2]_2$  is deducible from (\*) in our system, as shown in Fig. 2.1 — Fig. 2.4.

In Section 2, we shall present the system  $FL_{m,n}$  and give some examples of the proof figures in  $FL_{m,n}$ . Also, in Section 3, we shall prove the soundness theorem for  $FL_{m,n}$ . We believe our definition of  $FL_{m,n}$  will lead to prove the completeness theorem, however, we do not succeed the proof yet.<sup>†</sup>

<sup>†</sup> The completeness theorem has been proved with slight modifications of the system since submission of the paper.

For the simplicity, the system  $FL_{m,n}$  treat with the predicates  $*\rightarrow*$ ,  $*\rightarrow*$ ,  $*\rightarrow$ ,  $*\rightarrow$ ,  $\rightarrow*$  and  $*\Rightarrow*$  only. However, it is easy to extend the system to a formal system containing the ordinary predicate logic.

In the following lines, for a set  $X$ , we denote the power set of  $X$  by  $\mathcal{P}(X)$ , the cardinality of  $X$  by  $|X|$  and  $X - \{\phi\}$  by  $X^+$ .

## §2. The Formal System $FL_{m,n}$

In this section, we shall define the two-sorted language  $\mathcal{L}_{m,n}$  and twelve deduction rules for the formal system  $FL_{m,n}$ .

The language  $\mathcal{L}_{m,n}$  consists of

1) Constant symbols,

$$p_1, \dots, p_m \text{ (} p\text{-sort),}$$

$$d_1, \dots, d_n \text{ (} d\text{-sort).}$$

2) Function symbols,

$$[*_1, \dots, *_k]_k, \langle *_1, \dots, *_k \rangle_k \text{ (} \ell\text{-ary, } k \leq \ell).$$

3) Predicate symbols,

$$*\rightarrow*, *\rightarrow*, *\rightarrow, *\rightarrow, \rightarrow*, *\Rightarrow*.$$

We define the  $p$ -terms (respectively  $d$ -terms) inductively as follows:

- i)  $p_1, \dots, p_m(d_1, \dots, d_n)$  are  $p$ -terms ( $d$ -terms).
- ii) If  $S_1, \dots, S_l$  are  $p$ -terms ( $d$ -terms), then  $[S_1, \dots, S_l]_k$  and  $\langle S_1, \dots, S_l \rangle_k$  are  $p$ -terms ( $d$ -terms).

If  $S$  is a  $p$ -term and  $T$  is a  $d$ -term, then  $S \rightarrow T$ ,  $S \rightarrow T$ ,  $S \rightarrow$ ,  $S \rightarrow$ ,  $\rightarrow T$  and  $S \Rightarrow T$  are formulas. A sequence  $\Gamma_1; \Gamma_2; \Delta; S \Rightarrow T$  is called a sequent where

$$\Gamma_1 \subseteq \{S \rightarrow T \mid S \text{ is a } p\text{-term and } T \text{ is a } d\text{-term}\},$$

$$\Gamma_2 \subseteq \{S \rightarrow T \mid S \text{ is a } p\text{-term and } T \text{ is a } d\text{-term}\},$$

$$\Delta \subseteq \{S \rightarrow \mid S \text{ is a } p\text{-term}\} \cup \{S \rightarrow \mid S \text{ is a } p\text{-term}\} \\ \cup \{\rightarrow T \mid T \text{ is a } d\text{-term}\}.$$

Let  $X$  be a set,  $X_1, \dots, X_l$  be subsets of  $\mathcal{P}(X)$  and  $k \leq \ell$ . We define  $\langle X_1, \dots, X_l \rangle_k$  and  $[X_1, \dots, X_l]_k$  as follows:

$$\langle X_1, \dots, X_l \rangle_k = \left\{ \bigcup_{i \in I} x_i \mid I \subseteq \{1, \dots, l\}, |I| \geq k, x_i \in X_i \text{ for every } i \in I \right\},$$

$$[X_1, \dots, X_l]_k = \left\{ \bigcup_{i \in I} x_i \mid I \subseteq \{1, \dots, l\}, |I| \leq k, x_i \in X_i \text{ for every } i \in I \right\}.$$

We define the canonical interpretation  $\sim$  of  $p$ -terms inductively as follows:

- i)  $p = \{\{p\}\}$  for every constant symbol  $p$  of the  $p$ -sort.  
 ii) If  $S_1, \dots, S_i$  are  $p$ -terms, then

$$\langle \overline{S_1, \dots, S_i} \rangle_k = \langle \tilde{S}_1, \dots, \tilde{S}_i \rangle_k,$$

$$[\overline{S_1, \dots, S_i}]_k = [\tilde{S}_1, \dots, \tilde{S}_i]_k.$$

The definition of the canonical interpretation  $\sim$  of  $d$ -terms is the same as  $p$ -terms.

Now we define the deduction rules  $A_1)$ – $A_4)$ ,  $B_1)$ – $B_4)$ ,  $C_1)$ – $C_3)$  and  $D$ . Every deduction rule consists of two sequents called the upper sequent and the under sequent.

$$\Lambda_1) \frac{\Gamma_1^0 \cup \{S_1 \multimap T_1, \dots, S_i \multimap T_i\}; \Gamma_2^0 \cup \{S \multimap T\}; \Delta; \varphi}{\tilde{\Gamma}_1^0 \cup \{S_1 \multimap T_1, \dots, S_i \multimap T_i\}; \tilde{\Gamma}_2^0 \cup \{S \multimap T\}; \Delta \cup \{S_0 \multimap\}; \varphi}$$

where ①  $\langle \tilde{S}_0, \tilde{S}' \rangle_2 \cap \tilde{S}_0^+ = \phi$  for every  $S' \multimap T' \in \Gamma_1^0$ .

②  $\tilde{S} \cap \tilde{S}_0^+ = \phi,$

③  $\forall \langle y_1, \dots, y_i \rangle \in \tilde{T}_1 \times \dots \times \tilde{T}_i, \exists y \in \tilde{T}^+ [y \subseteq \cap \{y_i | y_i \neq \phi\}].$

$$\Lambda_2) \frac{\Gamma_1^0 \cup \{S_1 \multimap T_1, \dots, S_i \multimap T_i\}; \Gamma_2^0 \cup \{S \multimap T\}; \Delta; \varphi}{\tilde{\Gamma}_1^0 \cup \{S_1 \multimap T_1, \dots, S_i \multimap T_i\}; \tilde{\Gamma}_2^0 \cup \{S \multimap T\}; \Delta \cup \{S_0 \multimap\}; \varphi}$$

where ①  $\cup \tilde{S}_0 \cap \cup \tilde{S}' = \phi$  for every  $S' \multimap T' \in \Gamma_1^0$ .

②  $\langle \tilde{S}, \tilde{S}_0 \rangle_2 \cap \tilde{S}^+ = \phi,$

③  $\forall \langle y_1, \dots, y_i \rangle \in \tilde{T}_1 \times \dots \times \tilde{T}_i, \exists y \in \tilde{T}^+ [y \subseteq \cap \{y_i | y_i \neq \phi\}].$

$$\Lambda_3) \frac{\Gamma_1; \Gamma_2; \Delta \cup \{S_1 \multimap \dots, S_i \multimap\}; \varphi}{\tilde{\Gamma}_1; \tilde{\Gamma}_2; \Delta \cup \{S \multimap\}; \varphi}$$

where  $\forall x \in \tilde{S}^+ \exists x' \in [\tilde{S}_1, \dots, \tilde{S}_i]^+ [x' \subseteq x].$

$$\Lambda_4) \frac{\Gamma_1^0 \cup \{S_1 \multimap T_1, \dots, S_i \multimap T_i\}; \Gamma_2; \Delta; \varphi}{\tilde{\Gamma}_1^0 \cup \{S_1 \multimap T_1, \dots, S_i \multimap T_i\}; \tilde{\Gamma}_2; \Delta \cup \{S_0 \multimap\}; \varphi}$$

where ①  $\langle \tilde{S}_0, \tilde{S}' \rangle_2 \cap \tilde{S}_0^+ = \phi$  for every  $S' \multimap T' \in \Gamma_1^0$ ,

②  $[\tilde{S}_1, \dots, \tilde{S}_i]_i \cap \tilde{S}_0^+ = \phi.$

$$B_1) \frac{\Gamma_1^0 \cup \{S\} \multimap T_1^1, \dots, S_i^1 \multimap T_i^1\}; \Gamma_2^0 \cup \{S_1^2 \multimap T_1^2, \dots, S_i^2 \multimap T_i^2\}; \Delta; \varphi}{\Gamma_1^0 \cup \{S\} \multimap T_1^1, \dots, S_i^1 \multimap T_i^1\}; \Gamma_2^0 \cup \{S_1^2 \multimap T_1^2, \dots, S_i^2 \multimap T_i^2\}; \Delta; \varphi}$$

$$\frac{S_i^2 \multimap T_i^2; \Delta; \varphi}{S_i^2 \multimap T_i^2; \Delta \cup \{\multimap T_0\}; \varphi}$$

where ①  $\langle \tilde{T}_0, \tilde{T}'^+ \rangle_2 \cap \tilde{T}_0^+ = \phi$  for every  $S' \multimap T' \in \Gamma_1^0$ ,

② there exists a natural number  $k$  such that

i)  $0 < k \leq /,$

- ii)  $[\tilde{T}'_1, \dots, \tilde{T}'_i]_{k-1} \cap \tilde{T}'_0 = \phi$ ,  
 iii)  $\langle \langle \tilde{S}'_1, \dots, \tilde{S}'_k \rangle_2, \tilde{S}'_i \rangle_2 \cap \tilde{S}'_i = \phi \quad (i=1, \dots, k')$ ,  
 iv)  $\forall \langle y_1, \dots, y_i \rangle \in \tilde{T}'_1 \times \dots \times \tilde{T}'_i [|\{i | y_i \neq \phi\}| \leq k$   
 $\Rightarrow \exists y \in [\tilde{T}'_1, \dots, \tilde{T}'_i]' [y \subseteq \cap \{y_i | y_i \neq \phi\}]]$ .

$$B_2) \frac{\Gamma_1^0 \cup \{S_1 \longrightarrow T_1, \dots, S_i \longrightarrow T_i\}; \Gamma_2; \Delta; \varphi}{\Gamma_1^0 \cup \{S_1 \longrightarrow T_1, \dots, S_i \longrightarrow T_i\}; \Gamma_2; \Delta \cup \{ \longrightarrow T_0 \}; \varphi}$$

where ①  $\langle \tilde{T}'_0, \tilde{T}'_i \rangle_2 \cap \tilde{T}'_0 = \phi$  for every  $S' \longrightarrow T' \in \Gamma_1^0$ ,

$$\textcircled{2} [\tilde{T}'_1, \dots, \tilde{T}'_i] \cap T_0 = \phi.$$

$$B_3) \frac{\Gamma_1^0 \cup \{S_1 \longrightarrow T_1, \dots, S_i \longrightarrow T_i\}; \Gamma_2; \Delta \cup \{ \longrightarrow T \}; \varphi}{\Gamma_1^0 \cup \{S_1 \longrightarrow T_1, \dots, S_i \longrightarrow T_i\}; \Gamma_2; \Delta \cup \{ \longrightarrow T, \longrightarrow T_0 \}; \varphi}$$

where ①  $\langle \tilde{T}'_0, \tilde{T}'_i \rangle_2 \cap \tilde{T}'_0 = \phi$  for every  $S' \longrightarrow T' \in \Gamma_1^0$ ,

$$\textcircled{2} \forall \langle y_1, \dots, y_i \rangle \in \tilde{T}'_1 \times \dots \times \tilde{T}'_i \forall I \subseteq \{1, \dots, i\} [\bigcup_{i \in I} y_i \in \tilde{T}'_0$$
  
 $\Rightarrow \exists I' \subseteq I [I' \neq \phi \text{ and } \bigcup_{i \in I'} y_i \in \tilde{T}']]$ .

$$B_4) \frac{\Gamma_1; \Gamma_2; \Delta \cup \{ \longrightarrow T_1, \dots, \longrightarrow T_i \}; \varphi}{\Gamma_1; \Gamma_2; \Delta \cup \{ \longrightarrow [T_1, \dots, T_i]_1 \}; \varphi}$$

$$C_1) \frac{\Gamma_1; \Gamma_2; \Delta \cup \{S \longrightarrow\}; [S_1, \dots, S_i, S']_1 \Longrightarrow T}{\Gamma_1; \Gamma_2; \Delta \cup \{S \longrightarrow\}; [S_1, \dots, S_i]_1 \Longrightarrow T}$$

where  $\tilde{S} = \tilde{S}'$ .

$$C_2) \frac{\Gamma_1; \Gamma_2; \Delta \cup \{S \longrightarrow\}; [S_1, \dots, S_i, S']_1 \Longrightarrow T}{\Gamma_1; \Gamma_2; \Delta \cup \{S \longrightarrow\}; [S_1, \dots, S_i]_1 \Longrightarrow T}$$

where  $\tilde{S} = \tilde{S}'$ .

$$C_3) \frac{\Gamma_1; \Gamma_2; \Delta \cup \{ \longrightarrow T \}; S \Longrightarrow [T_1, \dots, T_i, T']_1}{\Gamma_1; \Gamma_2; \Delta \cup \{ \longrightarrow T \}; S \Longrightarrow [T_1, \dots, T_i]_1}$$

where  $\tilde{T} = \tilde{T}'$ .

$$D) \frac{\Gamma_1; \Gamma_2; \Delta; S' \Longrightarrow T'}{\Gamma_1; \Gamma_2; \Delta; S \Longrightarrow T}$$

where  $\tilde{S} = \tilde{S}'$  and  $\tilde{T} = \tilde{T}'$ .

Let  $\pi, \pi'$  be sequents.  $\pi'$  is said to be an immediate consequence of  $\pi$ , if there is a deduction rule such that  $\pi$  is the upper sequent and  $\pi'$  is the under sequent.  $\pi'$  is deducible from  $\pi$  ( $\pi \vdash \pi'$ ), if there is a sequence  $\pi_0, \dots, \pi_i$  of sequents such that  $\pi_0 = \pi$ ,  $\pi_i = \pi'$  and  $\pi_{i+1}$  is an immediate consequence of  $\pi_i$  for  $i=0, \dots, i-1$ . We say that  $S \Rightarrow T$  is provable from  $\Gamma_1, \Gamma_2$  ( $\Gamma_1, \Gamma_2 \vdash S \Rightarrow T$ ), if  $\Gamma_1; \Gamma_2;; [p_1, \dots, p_m]_m \Rightarrow [d_1, \dots, d_n]_n \vdash \Gamma_1; \Gamma_2; \Delta; S \Rightarrow T$  for some  $\Delta$ .

In the following we shall give an example of proofs in the formal system  $FL_{3,3}$  (the cigarette-smokers' problem). We show that

$$\left\{ \begin{array}{l} \langle H_1 \rangle_1 \longrightarrow [\langle P, T \rangle_2]_1 \\ \langle H_2 \rangle_1 \longrightarrow [\langle T, M \rangle_2]_1 \\ \langle H_3 \rangle_1 \longrightarrow [\langle M, P \rangle_2]_1 \end{array} \right\}, \left\{ \begin{array}{l} [H_1, H_2]_1 \longrightarrow \langle T \rangle_1 \\ [H_2, H_3]_1 \longrightarrow \langle M \rangle_1 \\ [H_3, H_1]_1 \longrightarrow \langle P \rangle_1 \end{array} \right\} \vdash \\ [H_1, H_2, H_3]_1 \Longrightarrow [\langle P, T \rangle_2, \langle T, M \rangle_2, \langle M, P \rangle_2]_1.$$

Let

$$\Gamma_1 = \left\{ \begin{array}{l} \langle H_1 \rangle_1 \longrightarrow [\langle P, T \rangle_2]_1 \\ \langle H_2 \rangle_1 \longrightarrow [\langle T, M \rangle_2]_1 \\ \langle H_3 \rangle_1 \longrightarrow [\langle M, P \rangle_2]_1 \end{array} \right\}, \quad \Gamma_2 = \left\{ \begin{array}{l} [H_1, H_2]_1 \longrightarrow \langle T \rangle_1 \\ [H_2, H_3]_1 \longrightarrow \langle M \rangle_1 \\ [H_3, H_1]_1 \longrightarrow \langle P \rangle_1 \end{array} \right\}$$

and  $\varphi$  denotes the formula  $[H_1, H_2, H_3]_3 \Rightarrow [P, T, M]_3$ .

One of its proof is as follows:

$$\left\{ \begin{array}{l} \langle H_1 \rangle_1 \longrightarrow [\langle P, T \rangle_2]_1 \\ \langle H_2 \rangle_1 \longrightarrow [\langle T, M \rangle_2]_1 \\ \langle H_3 \rangle_1 \longrightarrow [\langle M, P \rangle_2]_1 \end{array} \right\} ; \left\{ \begin{array}{l} [H_1, H_2]_1 \longrightarrow \langle T \rangle_1 \\ [H_2, H_3]_1 \longrightarrow \langle M \rangle_1 \\ [H_3, H_1]_1 \longrightarrow \langle P \rangle_1 \end{array} \right\} ; ; \\ [H_1, H_2, H_3]_3 \Longrightarrow [P, T, M]_3 \quad (A_2)$$

$$\left\{ \begin{array}{l} \langle H_1 \rangle_1 \longrightarrow [\langle P, T \rangle_2]_1 \\ \langle H_2 \rangle_1 \longrightarrow [\langle T, M \rangle_2]_1 \\ \langle H_3 \rangle_1 \longrightarrow [\langle M, P \rangle_2]_1 \end{array} \right\} ; \left\{ \begin{array}{l} [H_1, H_2]_1 \longrightarrow \langle T \rangle_1 \\ [H_2, H_3]_1 \longrightarrow \langle M \rangle_1 \\ [H_3, H_1]_1 \longrightarrow \langle P \rangle_1 \end{array} \right\} ; \\ \{ \langle H_1, H_2 \rangle_2 \longrightarrow \} ; \varphi \quad (A_2)$$

$$\left\{ \begin{array}{l} \langle H_1 \rangle_1 \longrightarrow [\langle P, T \rangle_2]_1 \\ \langle H_2 \rangle_1 \longrightarrow [\langle T, M \rangle_2]_1 \\ \langle H_3 \rangle_1 \longrightarrow [\langle M, P \rangle_2]_1 \end{array} \right\} ; \left\{ \begin{array}{l} [H_1, H_2]_1 \longrightarrow \langle T \rangle_1 \\ [H_2, H_3]_1 \longrightarrow \langle M \rangle_1 \\ [H_3, H_1]_1 \longrightarrow \langle P \rangle_1 \end{array} \right\} ; \\ \left\{ \begin{array}{l} \langle H_1, H_2 \rangle_2 \longrightarrow \\ \langle H_2, H_3 \rangle_2 \longrightarrow \end{array} \right\} ; \varphi \quad (A_2)$$

$$\Gamma_1 \quad ; \quad \Gamma_2 \quad ; \left\{ \begin{array}{l} \langle H_1, H_2 \rangle_2 \longrightarrow \\ \langle H_2, H_3 \rangle_2 \longrightarrow \\ \langle H_3, H_1 \rangle_2 \longrightarrow \end{array} \right\} ; \varphi \quad (A_3)$$

$$\Gamma_1 ; \Gamma_2 ; \{ [\langle H_1, H_2 \rangle_2, \langle H_2, H_3 \rangle_2, \langle H_3, H_1 \rangle_2]_1 \longrightarrow \} ; \varphi \quad (A_3)$$

$$\Gamma_1 ; \Gamma_2 ; \{ \langle H_1, H_2, H_3 \rangle_2 \longrightarrow \} ; [H_1, H_2, H_3]_3 \Longrightarrow [P, T, M]_3 \quad (D)$$

$$\Gamma_1 ; \Gamma_2 ; \{ \langle H_1, H_2, H_3 \rangle_2 \longrightarrow \} ; [H_1, H_2, H_3, \langle H_1, H_2, H_3 \rangle_2]_1 \\ \Longrightarrow [P, T, M]_3 \quad (C_2)$$

$$\left\{ \begin{array}{l} \langle H_1 \rangle_1 \longrightarrow [\langle P, T \rangle_2] \\ \langle H_2 \rangle_1 \longrightarrow [\langle T, M \rangle_2] \\ \langle H_3 \rangle_1 \longrightarrow [\langle M, P \rangle_2] \end{array} \right\} ; \Gamma_2 ; \{ \langle H_1, H_2, H_3 \rangle_2 \longrightarrow \} ; \\ [H_1, H_2, H_3]_1 \Longrightarrow [P, T, M]_3 \quad (B_2)$$

$$\left\{ \begin{array}{l} \langle H_1 \rangle_1 \longrightarrow [\langle P, T \rangle_2] \\ \langle H_2 \rangle_1 \longrightarrow [\langle T, M \rangle_2] \\ \langle H_3 \rangle_1 \longrightarrow [\langle M, P \rangle_2] \end{array} \right\} ; \left\{ \begin{array}{l} [H_1, H_2]_1 \longrightarrow \langle T \rangle_1 \\ [H_2, H_3]_1 \longrightarrow \langle M \rangle_1 \\ [H_3, H_1]_1 \longrightarrow \langle P \rangle_1 \end{array} \right\} ; \\ \left\{ \begin{array}{l} \langle H_1, H_2, H_3 \rangle_2 \longrightarrow \\ \longrightarrow [T, M, P]_1 \end{array} \right\} ; [H_1, H_2, H_3] \Longrightarrow [P, T, M] \quad (B_1)$$

$$\Gamma_1 ; \Gamma_2 ; \left\{ \begin{array}{l} \langle H_1, H_2, H_3 \rangle_2 \longrightarrow \\ \longrightarrow [T, M, P]_1 \\ \longrightarrow \langle T, M, P \rangle_3 \end{array} \right\} ; [H_1, H_2, H_3]_1 \Longrightarrow [P, T, M]_3 \quad (D)$$

$$\Gamma_1 ; \Gamma_2 ; \left\{ \begin{array}{l} \langle H_1, H_2, H_3 \rangle_2 \longrightarrow \\ \longrightarrow [T, M, P]_1 \\ \longrightarrow \langle T, M, P \rangle_3 \end{array} \right\} ; [H_1, H_2, H_3]_1 \Longrightarrow \\ [P, T, M]_1, \langle P, T, M \rangle_2 \quad (C_3)$$

$$\Gamma_1 ; \Gamma_2 ; \left\{ \begin{array}{l} \langle H_1, H_2, H_3 \rangle_2 \longrightarrow \\ \longrightarrow [T, M, P]_1 \\ \longrightarrow \langle T, M, P \rangle_3 \end{array} \right\} ; [H_1, H_2, H_3]_1 \Longrightarrow \\ [\langle P, T, M \rangle_2]_1 \quad (D)$$

$$\Gamma_1 ; \Gamma_2 ; \left\{ \begin{array}{l} \langle H_1, H_2, H_3 \rangle_2 \longrightarrow \\ \longrightarrow [T, M, P]_1 \\ \longrightarrow \langle T, M, P \rangle_3 \end{array} \right\} ; \\ [H_1, H_2, H_3] \Longrightarrow [\langle P, T \rangle_2, \langle T, M \rangle_2, \langle M, P \rangle_2, \langle P, T, M \rangle_3]_1 \quad (C_3)$$

$$\left\{ \begin{array}{l} \langle H_1 \rangle_1 \longrightarrow [\langle P, T \rangle_2]_1 \\ \langle H_2 \rangle_1 \longrightarrow [\langle T, M \rangle_2]_1 \\ \langle H_3 \rangle_1 \longrightarrow [\langle M, P \rangle_2]_1 \end{array} \right\} ; \left\{ \begin{array}{l} [H_1, H_2]_1 \longrightarrow \langle T \rangle_1 \\ [H_2, H_3]_1 \longrightarrow \langle M \rangle_1 \\ [H_3, H_1]_1 \longrightarrow \langle P \rangle_1 \end{array} \right\} ; \\ \left\{ \begin{array}{l} \langle H_1, H_2, H_3 \rangle_2 \longrightarrow \\ \longrightarrow [T, M, P]_1 \\ \longrightarrow \langle T, M, P \rangle_3 \end{array} \right\} ; [H_1, H_2, H_3]_1 \Longrightarrow \\ [\langle P, T \rangle_2, \langle T, M \rangle_2, \langle M, P \rangle_2]_1$$

The above proof is so complicated that we try to abbreviate the deduction rules. We abbreviate A<sub>1</sub>)–D) to the following

$A'_1), \dots, D')$ .

$$A_1) \frac{S_1 \succ \rightarrow T_1, \dots, S_i \succ \rightarrow T_i, S \longrightarrow T}{S_0 \longrightarrow}$$

$$A_2) \frac{S_1 \succ \rightarrow T_1, \dots, S_i \longrightarrow T_i, S \longrightarrow T}{S_0 \longrightarrow}$$

$$A_3) \frac{S_1 \longrightarrow, \dots, S_i \longrightarrow}{S \longrightarrow}$$

$$B_1) \frac{S_1^1 \succ \rightarrow T_1^1, \dots, S_i^1 \succ \rightarrow T_i^1, S_1^2 \longrightarrow T_1^2, \dots, S_i^2 \longrightarrow T_i^2}{\succ \rightarrow T_0}$$

$$B_2) \frac{S_1 \succ \rightarrow T_1, \dots, S_i \succ \rightarrow T_i}{\succ \rightarrow T_0}$$

$$B_3) \frac{S_1 \succ \rightarrow T_1, \dots, S_i \succ \rightarrow T_i, \succ \rightarrow T}{\succ \rightarrow T_0}$$

$$B_4) \frac{\succ \rightarrow T_1, \dots, \succ \rightarrow T_i}{\succ \rightarrow [T_1, \dots, T_i]_1}$$

$$C_1) \frac{S \longrightarrow, [S_1, \dots, S_i, S']_1 \Longrightarrow T}{[S_1, \dots, S_i]_1 \Longrightarrow T}$$

$$C_2) \frac{S \longrightarrow, [S_1, \dots, S_i, S']_1 \Longrightarrow T}{[S_1, \dots, S_i]_1 \Longrightarrow T}$$

$$C_3) \frac{\succ \rightarrow T, S \Longrightarrow [T_1, \dots, T_i, T']_1}{S \Longrightarrow [T_1, \dots, T_i]_1}$$

$$D) \frac{S' \Longrightarrow T'}{S \Longrightarrow T}$$

By using above rules  $A'_1)$ – $D')$ , we obtain the following proof figures of

$$\left\{ \begin{array}{l} \langle H_1 \rangle_1 \succ \rightarrow [ \langle P, T \rangle_2 ]_1 \\ \langle H_2 \rangle_1 \succ \rightarrow [ \langle T, M \rangle_2 ]_1 \\ \langle H_3 \rangle_1 \succ \rightarrow [ \langle M, P \rangle_2 ]_1 \end{array} \right\}, \left\{ \begin{array}{l} [H_1, H_2]_1 \longrightarrow \langle T \rangle_1 \\ [H_2, H_3]_1 \longrightarrow \langle M \rangle_1 \\ [H_3, H_1]_1 \longrightarrow \langle P \rangle_1 \end{array} \right\}$$

$$\vdash [H_1, H_2, H_3]_1 \Longrightarrow [T, M, P]_1$$

(cigarette-smokers' example)

and

$$\left\{ \begin{array}{l} \langle ph1 \rangle_1 \succ \rightarrow [ \langle f5, f1 \rangle_2 ]_1 \\ \langle ph2 \rangle_1 \succ \rightarrow [ \langle f1, f2 \rangle_2 ]_1 \\ \langle ph3 \rangle_1 \succ \rightarrow [ \langle f2, f3 \rangle_2 ]_1 \\ \langle ph4 \rangle_1 \succ \rightarrow [ \langle f3, f4 \rangle_2 ]_1 \\ \langle ph5 \rangle_1 \succ \rightarrow [ \langle f4, f5 \rangle_2 ]_1 \end{array} \right\}, \left\{ \begin{array}{l} [ph5, ph1]_1 \longrightarrow \langle f1 \rangle_1 \\ [ph1, ph2]_1 \longrightarrow \langle f2 \rangle_1 \\ [ph2, ph3]_1 \longrightarrow \langle f3 \rangle_1 \\ [ph3, ph4]_1 \longrightarrow \langle f4 \rangle_1 \\ [ph4, ph5]_1 \longrightarrow \langle f5 \rangle_1 \end{array} \right\}$$

$$\vdash [ph1, \dots, ph5]_2 \Longrightarrow [ \langle f5, f1 \rangle_2, \dots, \langle f4, f5 \rangle_2 ]_2$$

(dining philosophers' example).



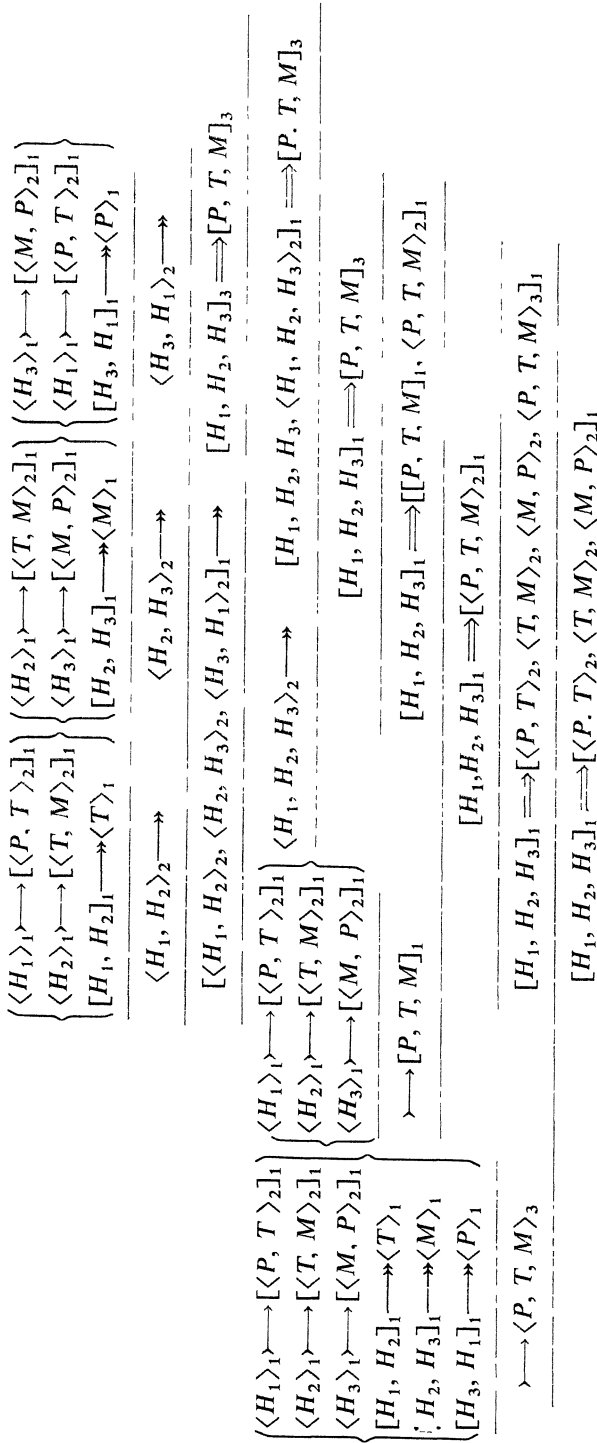


Fig. 1.

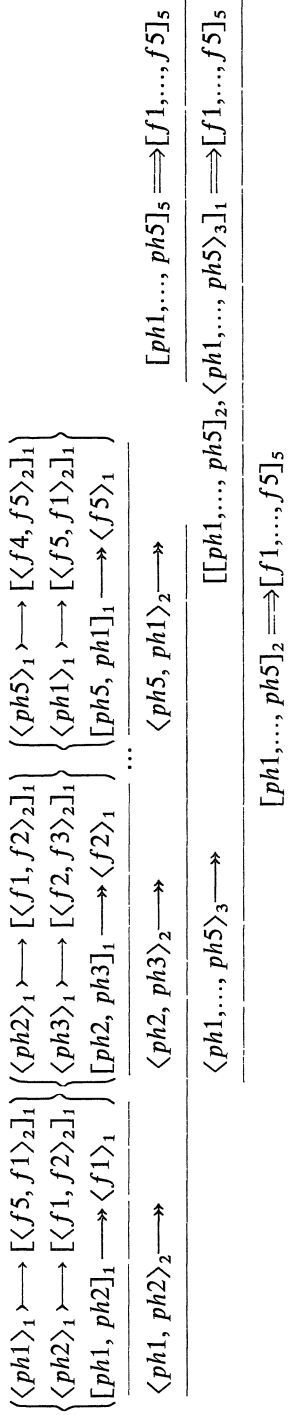


Fig. 2.1.



Fig. 2.1.

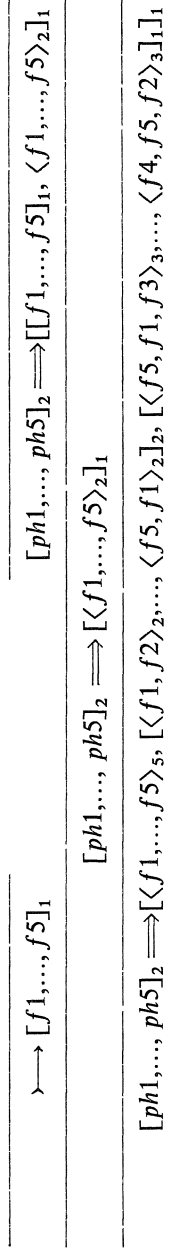


Fig. 2.2.

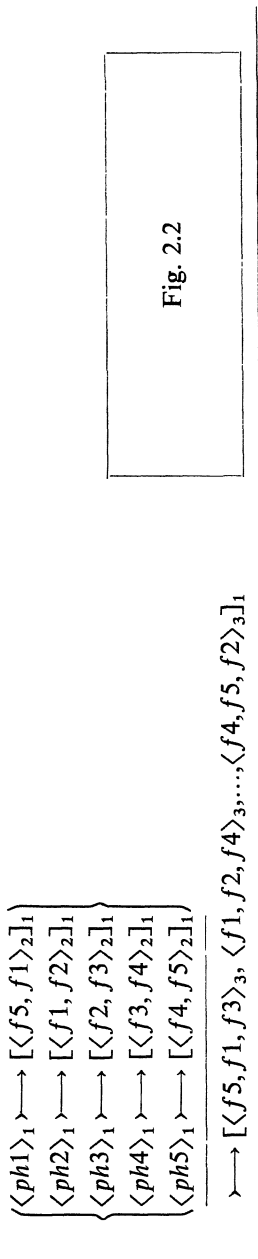


Fig. 2.3.

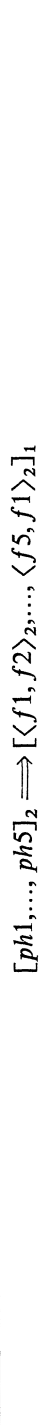
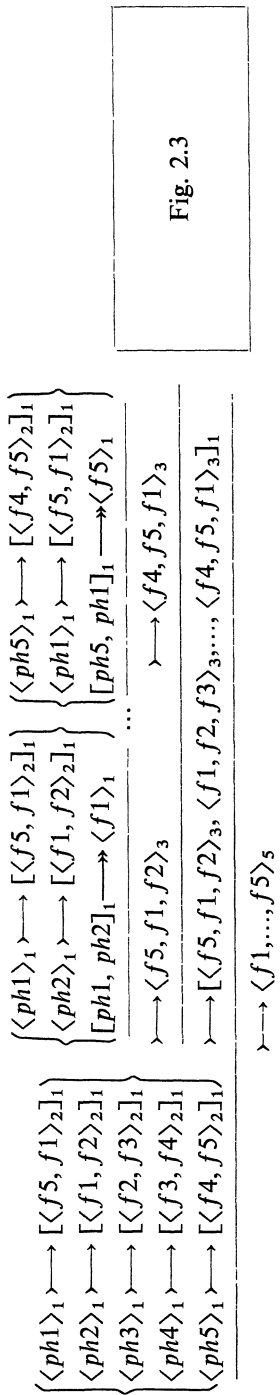


Fig. 2.4.

If we add the following deduction rule E) to  $FL_{m,n}$ , then we can make short proofs in  $FL_{m,n}$ .

$$\text{E) } \frac{\{S_1 \rangle \longrightarrow T_1, \dots, S_i \rangle \longrightarrow T_i\}; \Gamma_2; \Delta; t(S_1, \dots, S_i) \Longrightarrow T}{\{S_1 \rangle \longrightarrow T_1, \dots, S_i \rangle \longrightarrow T_i\}; \Gamma_2; \Delta; t(S_1, \dots, S_i) \Longrightarrow t(T_1, \dots, T_i)},$$

where ①  $\cup \tilde{S}_i \cap \cup \tilde{S}_j = \phi$  ( $i, j = 1, \dots, \ell, i \neq j$ ),

- ②  $t(S_1, \dots, S_i)$  is a  $p$ -term which is constructed from  $S_1, \dots, S_i$  only using function symbols and  $t(T_1, \dots, T_i)$  is the  $d$ -term which is constructed from  $t(S_1, \dots, S_i)$  replacing  $S_1, \dots, S_i$  to  $T_1, \dots, T_i$ .

For example, by using the rule (E), one of such proof figures of

$$\left\{ \begin{array}{l} \langle ph1 \rangle_1 \rangle \longrightarrow [\langle f5, f1 \rangle_2]_1 \\ \langle ph2 \rangle_1 \rangle \longrightarrow [\langle f1, f2 \rangle_2]_1 \\ \langle ph3 \rangle_1 \rangle \longrightarrow [\langle f2, f3 \rangle_2]_1 \\ \langle ph4 \rangle_1 \rangle \longrightarrow [\langle f3, f4 \rangle_2]_1 \\ \langle ph5 \rangle_1 \rangle \longrightarrow [\langle f4, f5 \rangle_2]_1 \end{array} \right\}, \left\{ \begin{array}{l} [ph5, ph1]_1 \longrightarrow \langle f1 \rangle_1 \\ [ph1, ph2]_1 \longrightarrow \langle f2 \rangle_1 \\ [ph2, ph3]_1 \longrightarrow \langle f3 \rangle_1 \\ [ph3, ph4]_1 \longrightarrow \langle f4 \rangle_1 \\ [ph4, ph5]_1 \longrightarrow \langle f5 \rangle_1 \end{array} \right\}$$

$$\vdash [ph1, \dots, ph5]_2 \Longrightarrow [\langle f5, f1 \rangle_2, \dots, \langle f4, f5 \rangle_2]_2$$

is as follows:

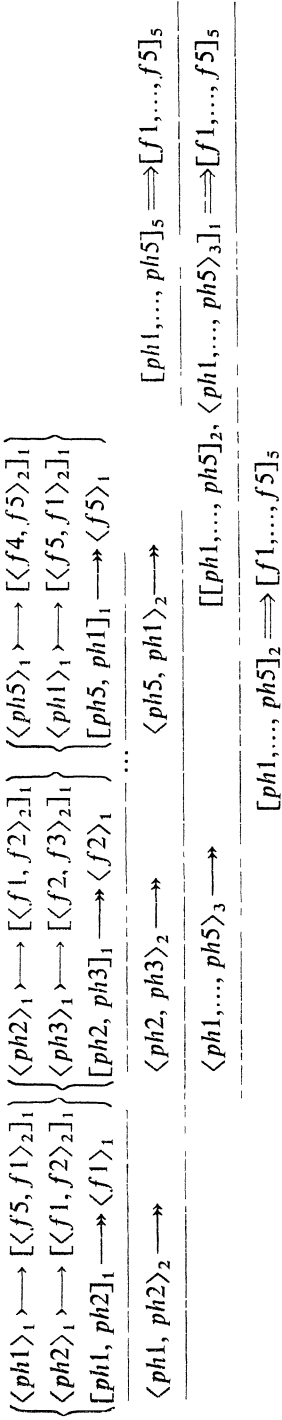


Fig. 3.1.

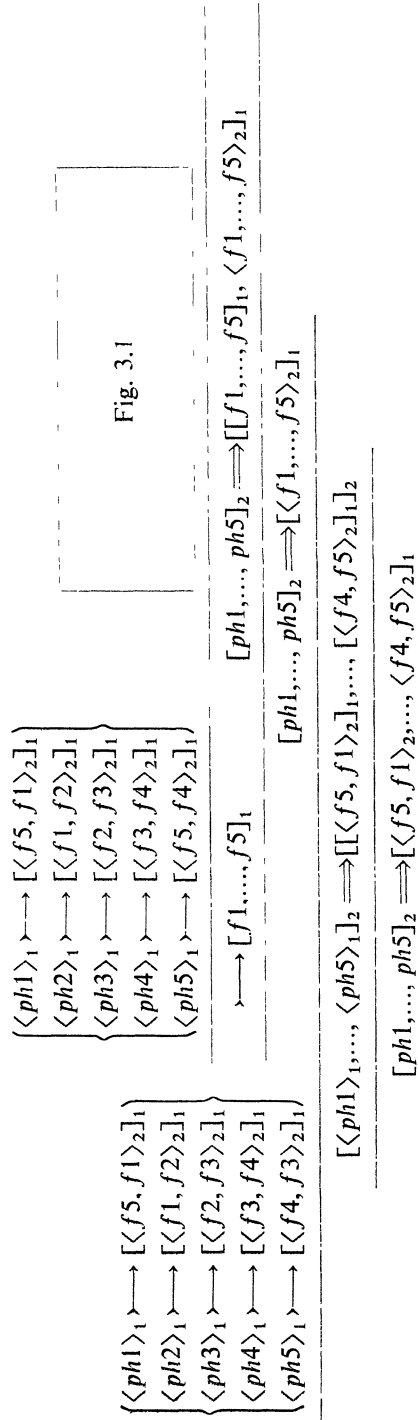


Fig. 3.2.

### §3. Soundness Theorem

In this section, we shall show the soundness theorem for  $FL_{m,n}$  after defining a standard model of a sequent. Let  $X, Y$  be sets,  $u$  be a subset of  $P(X) \times P(Y)$ ,  $X'$  be a subset of  $\mathcal{P}(X)$  and  $y_0$  be a subset of  $Y$ . We define  $\bar{u}, u^*, \pi_1(u), \pi_2(u)$  and  $A(u, y_0)$  as follows:

$$\begin{aligned}\bar{u} &= \cup \{x \times y \mid (x, y) \in u\}, \\ u^* &= \{(x, y) \in u \mid y \neq \phi\}, \\ \pi_1(u) &= \cup \{x \mid (x, y) \in u\}, \\ \pi_2(u) &= \cup \{y \mid (x, y) \in u\}, \\ A(u, y_0) &= \cup \{x \mid (x, y') \in u \text{ for some } y' \supset y_0\}.\end{aligned}$$

Let  $P = \{p_1, \dots, p_m\}, D = \{d_1, \dots, d_n\}$  and  $U$  be a nonempty subset of  $\mathcal{P}(\mathcal{P}(P)^+ \times \mathcal{P}(D))$ . We define the relation  $U \models \varphi$  for every formula  $\varphi$  as follows:

- i)  $U \models S \rightarrow T$  iff  $\forall u \in U \forall (x, y) \in u [x \in \tilde{S} \implies y \in \tilde{T}]$   
and  $\forall u \in U \exists !^*(x, y) \in u [x \in \tilde{S} \text{ and } y \in \tilde{T}]$ .
- ii)  $U \models S \rightarrow T$  iff  $\forall u \in U \forall y \in \tilde{T}^+ [A(u, y) \in \tilde{S} \text{ or } A(u, y) = \phi]$ ,  
and  $\forall u \in U [\forall y \in \tilde{T}^+ [A(u, y) = \phi] \implies \phi \in \tilde{S}]$ .
- iii)  $U \models S \rightarrow$  iff  $\forall u \in U [\pi_1(u^*) \notin \tilde{S}^+]$ .
- iv)  $U \models S \rightarrow$  iff  $\forall u \in U \forall x \in \tilde{S}^+ [x \not\subseteq \pi_1(u^*)]$ .
- v)  $U \models \rightarrow T$  iff  $\forall u \in U \forall v \subseteq u [\pi_2(v^*) \notin \tilde{T}^+]$ .
- vi)  $U \models S \implies T$  iff  $\forall u \in U [\pi_1(u^*) \in \tilde{S} \text{ and } \pi_2(u^*) \in \tilde{T}]$ .

$U$  is said to be a (standard) model of a sequent  $\Gamma_1; \Gamma_2; \Delta; S \Rightarrow T$  iff  $U \models \varphi$  for every  $\varphi \in \Gamma_1 \cup \Gamma_2 \cup \Delta \cup \{S \Rightarrow T\}$  and  $\forall u \in U \forall (x, y) \in u \exists !^1 S \rightarrow T \in \Gamma_1 [x \in \tilde{S} \text{ and } y \in \tilde{T}]$ .

#### Theorem (Soundness theorem).

Let  $\pi, \pi'$  be sequents. If  $\pi \vdash \pi'$  then for every model  $U$  of  $\pi$ ,  $U$  is also a model of  $\pi'$ .

*Proof.* It is enough to show that for every deduction rule, if  $U$  is a model of the upper sequent, then  $U$  is also a model of the under sequent.

A<sub>1</sub>) Suppose that  $U \models \Gamma_1^0 \cup \{S_1 \rightarrow T_1, \dots, S_l \rightarrow T_l\}; \Gamma_2^0 \cup \{S \rightarrow T\}; \Delta \cup \{S_0 \rightarrow\}; \varphi$ .

\*  $\exists !$  means that "there uniquely exists ...".

Since  $U \models \Gamma_1^0 \cup \{S_1 \mapsto T_1, \dots, S_l \mapsto T_l\}; \Gamma_2^0 \cup \{S \mapsto T\}; \Delta; \varphi, U \not\models S_0 \rightarrow$ . Hence there is a  $u \in U$  such that  $\pi_1(u^*) \in \tilde{S}_0^+$ . Let  $u^* = \{(x_1, y_1), \dots, (x_k, y_k)\}$ . By the condition ① of A<sub>1</sub>) and the definition of standard models, for every  $(x, y) \in u^*$  there is a unique  $i$  such that  $(x, y) \in \tilde{S}_i \times \tilde{T}_i$ . By the condition ③ of A<sub>1</sub>), there is a  $y \in \tilde{T}^+$  such that  $y \subseteq \bigwedge_{i=1}^k y_i$ . Since  $y \subseteq \bigwedge_{i=1}^k y_i$  implies that  $\pi_1(u^*) \subseteq A(u, y)$ ,  $\pi_1(u^*) = A(u, y) \neq \phi$ .  $y \in \tilde{T}^+, U \not\models S \mapsto T$  and  $A(u, y) \neq \phi$  imply  $A(u, y) \in \tilde{S}$ . Hence  $\pi_1(u^*) \in \tilde{S}_0 \cap \tilde{S}$ . But this contradicts the condition ② of A<sub>1</sub>).

A<sub>2</sub>) Suppose that  $U \not\models \Gamma_1^0 \cup \{S_1 \mapsto T_1, \dots, S_l \mapsto T_l\}; \Gamma_2^0 \cup \{S \mapsto T\}; \Delta \cup \{S \mapsto\}; \varphi$ . Since  $U \models \Gamma_1^0 \cup \{S_1 \mapsto T_1, \dots, S_l \mapsto T_l\}; \Gamma_2^0 \cup \{S \mapsto T\}; \Delta; \varphi, U \not\models S \mapsto$ . Hence there are  $u \in U$  and  $x \in \tilde{S}_0^+$  such that  $x \subseteq \pi_1(u^*)$ . Let  $u_0 = \{(x', y') \mid x' \cap x \neq \phi\} = \{(x_1, y_1), \dots, (x_k, y_k)\}$ . By the condition ① of A<sub>2</sub>), and the definition of standard models, for every  $(x', y') \in u_0$ , there is a unique  $i$  such that  $(x', y') \in \tilde{S}_i \times \tilde{T}_i$ . By the condition ③ of A<sub>2</sub>), there is a  $y \in \tilde{T}^+$  such that  $y \subseteq \bigwedge_{i=1}^k y_i$ . Since  $y \subseteq \bigwedge_{i=1}^k y_i$  implies that  $\pi_1(u^*) \subseteq A(u, y)$ ,  $x \subseteq A(u, y)$ . Hence  $A(u, y) \in \tilde{S}$  by  $U \models S \mapsto T$  and  $A(u, y) \supseteq x \neq \phi$ . So  $A(u, y) \in \langle \tilde{S}, \tilde{S}_0 \rangle_2 \cap \tilde{S}$ . But this contradicts the condition ② of A<sub>2</sub>).

A<sub>3</sub>) Suppose that  $U \not\models \Gamma_1; \Gamma_2; \Delta \cup \{S \mapsto\}; \varphi$ . Since  $U \models \Gamma_1; \Gamma_2; \Delta; \varphi, U \not\models S \mapsto$ . Hence there are  $u \in U$  and  $x \in \tilde{S}^+$  such that  $x \subseteq \pi_1(u^*)$ . By the condition of A<sub>3</sub>), there is an  $x' \in [\tilde{S}_1, \dots, \tilde{S}_l]_1$  such that  $x' \subseteq x$ . Hence  $x' \subseteq \pi_1(u^*)$ . Since  $U \models S_i \mapsto$  for  $i=1, \dots, l$ ,  $x' \notin S_i^+$  for  $i=1, \dots, l$ . Hence  $x' \notin [\tilde{S}_1, \dots, \tilde{S}_l]_1$ . But this is contradiction.

A<sub>4</sub>) Clear

B<sub>1</sub>) Suppose that  $U \not\models \Gamma_1^0 \cup \{S_1^1 \mapsto T_1^1, \dots, S_l^1 \mapsto T_l^1\}; \Gamma_2^0 \cup \{S_1^2 \mapsto T_1^2, \dots, S_l^2 \mapsto T_l^2\}; \Delta \cup \{\mapsto T_0\}; \varphi$ . Since  $U \models \Gamma_1^0 \cup \{S_1^1 \mapsto T_1^1, \dots, S_l^1 \mapsto T_l^1\}; \Gamma_2^0 \cup \{S_1^2 \mapsto T_1^2, \dots, S_l^2 \mapsto T_l^2\}; \Delta; \varphi, U \not\models \mapsto T_0$ . Hence there are  $u \in U$  and  $v \subset u$  such that  $\pi_2(v^*) \in \tilde{T}_0^+$ . Let  $v^* = \{(x_1, y_1), \dots, (x_k, y_k)\}$ . By the condition ① of B<sub>1</sub>) and the definition of standard models, for every  $(x', y') \in v^*$  there is a unique  $i$  such that  $(x', y') \in \tilde{S}_i \times \tilde{T}_i$ . Let  $k$  be a natural number which satisfies the condition ② of B<sub>1</sub>). If  $k' < k$ , then  $\pi_2(v^*) \in [\tilde{T}_1^1, \dots, \tilde{T}_l^1]_{k-1}$ . Hence  $\pi_2(v^*) \in [\tilde{T}_1^1, \dots, \tilde{T}_l^1]_{k-1} \cap \tilde{T}_0^+$ . But this contradicts the condition ii) of ② of B<sub>1</sub>). Hence  $k' \geq k$ . By the condition iv) of ② of B<sub>1</sub>), there is a  $y \in [\tilde{T}_1^2, \dots, \tilde{T}_l^2]_1^+$  such that  $y \subseteq \bigwedge_{i=1}^k y_i$ . Hence  $\bigcup_{i=1}^k x_i \subseteq A(u, y)$ . So  $A(u, y) \neq \phi$ . This implies  $A(u, y) \in [\tilde{S}_1^2, \dots, \tilde{S}_l^2]_1$  by  $U \models S_1^2 \mapsto T_1^2, \dots, U \models S_l^2 \mapsto T_l^2$ . Since  $\bigcup_{i=1}^k x_i \in \langle \tilde{S}_1^1, \dots, \tilde{S}_l^1 \rangle_k$ ,  $A(u, y) \in \langle \langle \tilde{S}_1^1, \dots, \tilde{S}_l^1 \rangle_k, [\tilde{S}_1^2, \dots, \tilde{S}_l^2]_1 \rangle_2 \cap [\tilde{S}_1^2, \dots, \tilde{S}_l^2]_1$ . But this contradicts the condition iii) of ② of B<sub>1</sub>).

B<sub>2</sub>) Suppose that  $U \not\models \Gamma_1^0 \cup \{S_1 \mapsto T_1, \dots, S_l \mapsto T_l\}; \Gamma_2; \Delta \cup \{\mapsto T_0\}; \varphi$ . Since

$U \models \Gamma_1^0 \cup \{S_1 \rightarrow T_1, \dots, S_i \rightarrow T_i\}; \Gamma_2; \Delta; \varphi, U \models \rightarrow T_0$ . Hence there are  $u \in U$  and  $v \subseteq u$  such that  $\pi_2(v^*) \in \tilde{T}_0^+$ . Let  $v^* = \{(x_1, y_1), \dots, (x_k, y_k)\}$ . By the same argument as  $A_1$ ),  $\bigcup_{i=1}^k y_i \in [\tilde{T}_1, \dots, \tilde{T}_i]_i$ . Hence  $\pi_2(v^*) = \bigcup_{i=1}^k y_i \in [\tilde{T}_1, \dots, \tilde{T}_i]_i \cap \tilde{T}_0^+$ . But this contradicts the condition ② of  $B_1$ ).

$B_3$ ) Suppose that  $U \not\models \Gamma_1^0 \cup \{S_1 \rightarrow T_1, \dots, S_i \rightarrow T_i\}; \Gamma_2; \Delta \cup \{\rightarrow T, \rightarrow T_0\}; \varphi$ . Since  $U \models \Gamma_1^0 \cup \{S_1 \rightarrow T_1, \dots, S_i \rightarrow T_i\}; \Gamma_2; \Delta \cup \{\rightarrow T\}; \varphi, U \not\models \rightarrow T_0$ . Hence there are  $u \in U$  and  $v \subseteq u$  such that  $\pi_2(v^*) \in \tilde{T}^+$ . Let  $v^* = \{(x_1, y_1), \dots, (x_k, y_k)\}$ . By the same argument of  $B_1$ ) and the condition ② of  $B_3$ ), there is a nonempty set  $I' \subset \{1, \dots, k\}$  such that  $\bigcup_{i \in I'} y_i \in \tilde{T}$ . Hence  $\pi_2(v^*) \supseteq \bigcup_{i \in I'} y_i \in \tilde{T}$ . But this contradicts  $U \models \rightarrow T$ .

$B_4$ ) Clear.

$C_1$ ) Suppose that  $U \not\models \Gamma_1; \Gamma_2; \Delta \cup \{S \rightarrow\}; [S_1, \dots, S_i]_1 \Rightarrow T$ . Since  $U \models \Gamma_1; \Gamma_2; \Delta \cup \{S \rightarrow\}; [S_1, \dots, S_i, S']_1 \Rightarrow T$ , there is a  $u \in U$  such that  $\pi_1(u^*) \in \tilde{S}'^+$ . By the condition  $\tilde{S} = \tilde{S}'$ ,  $\pi_1(u^*) \in \tilde{S}^+$ . But this contradicts  $U \models S \rightarrow$ .

$C_2$ ),  $C_3$ ) We can show by the same argument as  $C_1$ ).

$D$ ) Clear.

### Acknowledgement

The authors are grateful to Prof. N. Saito, Prof. N. Doi and Prof. S. Takasu for their discussions.

### References

- [1] Hirose, K. et al., Process-Data Representation, *Proc. 3rd US-Japan Computer Conference*, (1978), 225-230.
- [2] Hirose, K. et al., Specification technique for parallel processing: process-data representation, *AFIPS, Conference Proc.*, **50**, (1981), 407-413.
- [3] Campbell, R. H. and Habermann, A. H., The Specification of Process Synchronization by Path Expressions, *Proc. of International Symposium on Operating System*, Lecture Notes in Comp. Sci., No. 16, Springer Verlag, Berlin (1974).
- [4] Aschcroft, E. and Manna, Z., Formalization of Properties of Parallel Programs, Stanford AI Memo, No. AIM-110, 1970.