The System $FL_{m,n}$ for Specification Analysis and its Completeness Theorem

KEN HIROSE*, MAKOTO TAKAHASHI* and SHINICHI YAMADA*

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

1. Introduction

In [1] and [2], one of the authors and his colleagues proposed a new specification technique called Process-Data Representation (PDR).

PDR aim is to improve reliability and modifiability of software systems, especially involving concurrent processing, by giving a precise specification of their whole computational processes.

In PDR, concurrent interactions between processes and data are specified by describing the constraint conditions imposed on them in the Forcing Logic (FL).

A formal system should be formulated not only to provide a compact description of the system specification but also to make it possible to derive certain useful conclusions from the given specification. To fill this requirement, we proposed a formal system in [3] as a tool for analyzing the specification described in the Forcing Logic and proved its soundness theorem.

In this paper, we present a formal system $FL_{m,n}$ by introducing into the former system in [3] some modifications which facilitate its completeness proof. The formal system $FL_{m,n}$ is delineated in Section 2 and the completeness theorem for $FL_{m,n}$ is proved in Section 3.

In brief, this completeness result implies that any proposition is (mechanically) deducible from a given (consistent) specification in $FL_{m,n}$ if and only if it is true (in the standard model of the specification).

In parallel with the modification and the completeness proof, several versions of automated theorem provers (ATP) for $FL_{m,n}$ were also implemented in both Prolog and micro-Prolog by making use of difference reduction as its problem solving strategy [6, 7. Chap. 9], part of which is described in [8]. In the appendix, sample specification and proof figure is shown for the dining philosophers problem to illustrate the usage of $FL_{m,n}$.

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

*Waseda University

2. The formal system $FL_{m,n}$

In this section, we define the language $L_{m,n}$ and inference rules for the formal system $FL_{m,n}$.

2.1 Language $L_{m,n}$

The language $L_{m,n}$ has as symbols the following.

2.1.1 Symbols

(1) Constant symbols,
$p_1, \ldots, p_m$ (p-sort),
$d_1, \ldots, d_n$ (d-sort).

(2) Function symbols,
$[, \ldots,]_k$, $\langle, \ldots, \rangle_k$ (l-ary, $0 \leq k \leq l$, $l \neq 0$),
$(, \ldots,)$ (q-ary, $1 \leq q$),
$((, \ldots,))$ (r-ary, $0 \leq r$).

(3) Predicate symbols,
$\rightarrowtail$, $\twoheadrightarrow$, $\longrightarrow$, $\not\rightarrow$, $\Longrightarrow$.

Remarks

(1) Informally, constant symbols of p-sort denote concurrent processes under consideration, and constant symbols of d-sort denote data available to the processes.

(2) Informally, $\langle X_1, \ldots, X_l \rangle_k$ denotes a set of the subsets of $\{X_1, \ldots, X_l\}$ whose cardinality $\geq k$, which means "at least k objects out of l objects $\{X_1, \ldots, X_l\}$". $[X_1, \ldots, X_l]_k$ denotes a set of the subsets of $\{X_1, \ldots, X_l\}$ whose cardinality $\leq k$, which means "at most k objects out of l objects $\{X_1, \ldots, X_l\}$". $(X_1, \ldots, X_q)$ denotes the set of objects designated by atomic terms (p-A-terms or d-A-terms), and $((Y_1, \ldots, Y_q))$ denotes the set of objects designated by p-B-terms or d-B-terms.

(3) $\langle X_1, \ldots, X_l \rangle_k \rightarrowtail Y$ means that the element in $\langle X_1, \ldots, X_l \rangle_k$ operates only on the element in Y, $[X_1, \ldots, X_l]_k \twoheadrightarrow Y$ means that the element in Y can be operated only by the element in $[X_1, \ldots, X_l]_k$, and $X \Longrightarrow Y$ means that the elements in X operates on the element in Y.

2.1.2 Terms

We inductively define the p-terms and d-terms as follows:

(i) $p_1, \ldots, p_m$ are p-terms, and $d_1, \ldots, d_n$ are d-terms;

(ii) If $S_1, \ldots, S_l$ are p-terms, then $[S_1, \ldots, S_l]_k$ are $\langle S_1, \ldots, S_l\rangle_k$ are p-terms, and if $T_1, \ldots, T_l$ are d-terms, then $[T_1, \ldots, T_l]_k$ and $\langle t_1, \ldots, T_l\rangle_k$ are p-terms.

Next, we define the p-A-terms, p-B-terms and p-C-terms; and d-A-terms, d-B-terms and d-C-terms as follows:

(iii) $p_1, \ldots, p_m$ are p-A-terms, and $d_1, \ldots, d_n$ are d-A-terms;

(iv) If $\sigma_1, \ldots, \sigma_l$ are p-A-terms, then $\langle\sigma_1, \ldots, \sigma_l\rangle_l$ is a p-A-term, and if $\rho_1, \ldots, \rho_l$ are d-A-terms, then $\langle\rho_1, \ldots, \rho_l\rangle_l$ is a d-A-term.

(v) If $\sigma_1, \ldots, \sigma_l$ are p-A-terms, then $(\sigma_1, \ldots, \sigma_l)$ is a p-B-term, and if $\rho_1, \ldots, \rho_l$ are d-A-terms, then $(\rho_1, \ldots, \rho_l)$ is a d-B-term.

(vi) If (( )) is a 0-ary function symbol, then (( )) is a p-C-term and a d-C-term.

(vii) If $\mu_1, \ldots, \mu_l$ are p-B-terms, then $((\mu_1, \ldots, \mu_l))$ is a p-C-term, and if $\tau_1, \ldots, \tau_l$ are d-B-terms, then $((r_1, \ldots, r_l))$ is d-C-term.

Remarks

(1) Generally, p-terms and d-terms are used to describe a specification. $p_1, \ldots, p_m$ denote processes and $d_1, \ldots, d_n$ denote data. $\langle S_1, \ldots, S_l\rangle_k$ reads "at least k objects out of $\{S_1, \ldots, S_l\}$" and $[S_1, \ldots, S_l]_k$ reads "at most k objects out of $\{S_1, \ldots, S_l\}$".

(2) p-A-terms, p-B-terms and p-C-terms (d-A-terms, d-B-terms and d-C-terms, respectively) are mainly used in the proof procedure of $FL_{m,n}$. p-A-terms and d-A-terms are atomic terms. p-B-terms and d-B-terms are the sequence of atomic terms denoting the set of the sets denoted by p-A-terms (or d-A-terms). And p-C-terms and d-C-terms are the sequence of p-B-terms and d-B-terms, respectively.

2.1.3 Formulas

In the following we use S for p-terms, T for d-terms, σ for p-A-terms, ρ for d-A-terms, μ for p-B-terms, r for d-B-terms, α for p-C-terms and β for d-C-terms.

$$S \rightarrowtail T, \quad S \twoheadrightarrow T,$$
$$S \Longrightarrow T, \quad \mu \not\rightarrow \tau,$$
$$\alpha \longrightarrow \tau, \quad \mu \longrightarrow \beta,$$
$$\alpha \Longrightarrow \beta$$

are formulas.

Remarks

$S \rightarrowtail T$ reads "the element in S operates only on the element in T".

$S \twoheadrightarrow T$ reads "the element in T can be operated only by the element in S".

$S \Longrightarrow T$ reads "the element in S operates on the element in T".

$\alpha \longrightarrow \tau$, $\mu \longrightarrow \beta$, and $\mu \not\rightarrow \tau$ are used in the proof procedure of $FL_{m,n}$.

2.3 Canonical Interpretation

Let X be a set, $X_1, \ldots, X_l$ be subsets of $\rho(X)$ and $k \leq l$.

We define $\langle X_1, \ldots, X_l\rangle_k$ and $[X_1, \ldots, X_l]_k$ as follows:

$$\langle X_1, \ldots, X_l\rangle_k = \{\cup_{i\in I} x_i \mid I \subseteq \{1, \ldots, l\},\ \#I \geq k \text{ and } x_i \in X_i \text{ for every } i \in I\},$$

$$[X_1, \ldots, X_l]_k = \{\cup_{i\in I} x_i \mid I \subseteq \{1, \ldots, l\},\ \#I \leq k \text{ and } x_i \in X_i \text{ for every } i \in I\}.$$

We define the canonical interpretation $\sim$ of p-term and d-terms, and the canonical interpretation of p-A-terms, p-B-terms, and p-C-terms (and d-A-terms, d-B-terms, and d-C-term, respectively) as follows:

(i) If a is a constant symbol, then $\tilde{a} = \{\{a\}\}$ and $\bar{a} = \{a\}$.

(ii) $\langle S_1, \ldots, S_l\rangle_k = \langle \tilde{S}_1, \ldots, \tilde{S}_l\rangle_k$ and $[S_1, \ldots, S_l]_k = [\tilde{S}_1, \ldots, \tilde{S}_l]_k$. The canonical interpretation $\sim$ of d-terms is similarly defined.

(iii) $\overline{\langle\sigma_1, \ldots, \sigma_l\rangle_l} = \cup\{\overline{\sigma_i} \mid 1 \leq i \leq l\}$, $\overline{(\sigma_1, \ldots, \sigma_l)} = (\overline{\sigma_1}, \ldots, \overline{\sigma_l})$ and $\overline{((\mu_1, \ldots, \mu_l))} = \{\overline{\mu_1}, \ldots, \overline{\mu_l}\}$.

The canonical interpretation of d-A-terms, d-B-terms and d-C-terms are similarly defined.

2.4 Deducibility

If $x \subseteq \{p_1, \ldots, p_m\}$ $(y \subseteq \{d_1, \ldots, d_n\})$, then we denote by $\hat{x}(\hat{y})$ one of the p-A-terms (d-A-terms) which satisfies $\tilde{\hat{x}} = x(\tilde{\hat{y}} = y)$. We denote by $\alpha_1 \frown \alpha_2$ the p-C-term $((\mu_1^1, \ldots, \mu_k^1, \mu_1^2, \ldots, \mu_l^2))$ where $\alpha_1 = ((\mu_1^1, \ldots, \mu_k^1))$ and $\alpha_2 = ((\mu_1^2, \ldots, \mu_l^2))$.

If $\mu = (\sigma_1, \ldots, \sigma_l)$, then μ^0 is the p-A-term $\langle\sigma_1, \ldots, \sigma_l\rangle_l$.

We denote by $S_1 * \cdots * S_l$ one of the p-C-terms which satisfies $\widetilde{S_1 * \cdots * S_l} = \tilde{S}_1^+ \times \cdots \times \tilde{S}_l^+$ and by $[S_1, \ldots, S_l]_k^\vee$ one of the p-C-terms which satisfies

$$\overline{[S_1, \ldots, S_l]_k^\vee} = \cup\{\overline{[S_{j_1} * \cdots * S_{j_q}]} \mid 1 \leq j_1 < j_2 < \cdots < j_q \leq l,\ q \leq k\}.$$

$\beta_1 \frown \beta_2$, τ^0, $T_1 * \cdots * T_l$ and $[T_1, \ldots, T_l]_k^\vee$ are similarly defined. Let

$$\Gamma_1 = \{S_1 \rightarrowtail T_1, \ldots, S_l \rightarrowtail T_l\}$$

and

$$\Gamma_2 = \{S_1' \twoheadrightarrow T_1', \ldots, S_k' \twoheadrightarrow T_k'\}.$$

We say that $S \Longrightarrow T$ is deducible from Γ_1 and Γ_2 ($\Gamma_1, \Gamma_2 \vdash_{m,n} S \Longrightarrow T$) if $S \Longrightarrow T$ is provable from Γ_1, Γ_2 and a formula $[S_1, \ldots, S_l]_l^\vee \Longrightarrow [T_1, \ldots, T_l]_l^\vee$ by the following inference rules.

Remarks

When no confusion appears possible, we shall write $\vdash$ in place of $\vdash_{m,n}$.

2.5 Inference Rules

$$(A_1)\quad \frac{S \to T}{(\sigma_1^0, \cdots, \sigma_{l'}^0, \sigma_1, \cdots, \sigma_{k'}) \not\to (\rho_1^0, \cdots, \rho_{l'}^0, \rho_1, \cdots, \rho_{k'})}$$

where $\overline{\langle \sigma_1, \cdots, \sigma_k \rangle_k} \notin S$ and there exists a $\bar{\rho} \in \bar{T}$ such that $\bar{\rho} \subseteq \overline{\rho_i}$ for every $i \leq k$ and $\bar{\rho} \not\subseteq \overline{\rho_j^0}$ for every $j \leq l'$.

$$(A_2)\quad \frac{(\sigma_1, \cdots, \sigma_i, \cdots, \sigma_j, \cdots, \sigma_{k'}) \not\to (\rho_1, \cdots, \rho_i, \cdots, \rho_j, \cdots, \rho_{k'})}{(\sigma_1, \cdots, \rho_j', \cdots, \sigma_i', \cdots, \sigma_{k'}) \not\to (\rho_1, \cdots, \rho_j', \cdots, \rho_i', \cdots, \rho_{k'})}$$

where $\overline{\sigma_i} = \overline{\sigma_i'}$, $\overline{\sigma_j} = \overline{\sigma_j'}$, $\overline{\rho_i} = \overline{\rho_i'}$ and $\overline{\rho_j} = \overline{\rho_j'}$.

$$(B_1)\quad \frac{S_1^0 \rightarrowtail T_1^0, \cdots, S_{k'}^0 \rightarrowtail T_{k'}^0}{(\sigma_1, \cdots, \sigma_{k'}) \rightarrowtail T_1^0 * \cdots * T_{k'}^0}$$

where $\overline{\sigma_i} \in S_i^0$ for every $i \leq k'$ and $S_i^0 \rightarrowtail T_i^0 (i \leq k')$ are all different formulas.

$$(B_2)\quad \frac{\mu \to ((\tau_1, \cdots, \tau_i, \cdots\cdots, \tau_{l'})), \mu \not\to \tau_i}{\mu \to ((\tau_1, \cdots, \tau_{i-1}, \tau_{i+1}, \cdots, \tau_{l'}))}$$

$$(C_1)\quad \frac{S_1^0 \rightarrowtail T_1^0, \cdots, S_{k'}^0 \rightarrowtail T_{k'}^0}{S_1^0 * \cdots * S_{k'}^0 \to (\rho_1, \cdots, \rho_{k'})}$$

where $\overline{\rho_i} \in \vdash T_i^0$ for every $i \leq k'$ and $S_i^0 \rightarrowtail T_i^0 (i \leq k')$ are all different formulas.

$$(C_2)\quad \frac{((\mu_1, \cdots, \mu_i, \cdots, \mu_{k'})) \to \tau, \mu_i \not\to \tau}{((\mu_1, \cdots, \mu_{i-1}, \mu_{i+1}, \cdots, \mu_{k'})) \to \tau}$$

$$(D_1)\quad \frac{((\mu_1, \cdots, \mu_i, \cdots, \mu_{k'})) \Longrightarrow \beta, \mu_i \to (( ))}{((\mu_1, \cdots, \mu_{i-1}, \mu_{i+1}, \cdots, \mu_{k'})) \Longrightarrow \beta}$$

$$(D_2)\quad \frac{\alpha \Longrightarrow ((\tau_1, \cdots, \tau_i, \cdots, \tau_{k'})), (( )) \to \tau_i}{\alpha \Longrightarrow ((\tau_1, \cdots, \tau_{i-1}, \tau_{i+1}, \cdots, \tau_{k'}))}$$

$$(E_1)\quad \frac{\alpha \Longrightarrow \beta}{\alpha' \Longrightarrow \beta'}$$

where $\bar{\alpha} = \overline{\alpha'}$ and $\beta = \overline{\beta'}$.

$$(E_2)\quad \frac{((\mu_1, \cdots, \mu_{l'})) \Longrightarrow ((\tau_1, \cdots, \tau_{k'}))}{[\mu_1^0, \cdots, \mu_l^0]_l \Longrightarrow [\tau_1^0, \cdots, \tau_k^0]_l}$$

where $l', k' \geq 1$.

$$(E_3)\quad \frac{\alpha \Longrightarrow \beta}{[p_1]_0 \Longrightarrow [d_1]_0}$$

where $\alpha = (( ))$ or $\beta = (( ))$.

$$(F)\quad \frac{S \Longrightarrow T}{S' \Longrightarrow T'}$$

where $\bar{S} \subseteq \bar{S}'$ and $\bar{T} \subseteq \bar{T}'$.

3. Completeness Theorem

In this section, we prove the completeness theorem for $FL_{m,n}$ after defining standard models.

3.1 Standard Model

Let X, Y be sets, u be a subset of $P(X) \times P(Y)$ and y be a subset of Y. We define u^*, $\pi_1(u)$, $\pi_2(u)$, $\pi_{*1}(u)$, $\pi_{*2}(u)$, and $A(u, y)$ as follows:

$u^* = \{(x, y) \in u \mid y \neq \phi\}$,

$\pi_1(u) = \{x \mid (x, y) \in u \text{ for some } y\}$,

$\pi_2(u) = \{y \mid (x, y) \in u \text{ for some } x\}$,

$\pi_1^*(u) = \{(x_1, \ldots, x_k) \mid \{x_1, \ldots, x_k\} = \pi_1(u), k = \#\pi_1(u)\}$,

$\pi_2^*(u) = \{(y_1, \ldots, y_k) \mid \{y_1, \ldots, y_k\} = \pi_2(u), k = \#\pi_2(u)\}$,

$A(u, y) = \cup \{x \mid (x, y') \in u \text{ for some } y' \supset y\}$.

Let $P = \{p_1, \ldots, p_m\}$, $D = \{d_1, \ldots, d_n\}$ and u be a nonempty subset of $\rho(\rho(P)^+ \times P(D))$. We define the relation $u \models \Phi$ (u satisfies Φ) for every formula Φ as follows:

(1) $u \models S \rightarrowtail T$ if and only if

$\bar{S}^+ = \phi$ or

$$\left[\begin{array}{l} \forall (x, y) \in u [x \in \bar{S} \text{ implies } y \in \bar{T}], \\ \exists (x, y) \in u [x \in \bar{S} \text{ and } y \in \bar{T}] \text{ and} \\ \forall (x, y), (x', y') \in u [x, x' \in \bar{S} \text{ and } y, y' \in \bar{T} \text{ imply} \\ \quad [[x = x' \text{ and } y = y'] \text{ or } y = \phi \text{ or } y' = \phi]] \end{array}\right]$$

(2) $u \models S \to T$ if and only if

$\forall y \in \bar{T}^+ \mid A(u, y) \neq \phi$ implies $A(u, y) \in \bar{S}]$.

(3) $u \models (\sigma_1, \ldots, \sigma_k) \not\to (\rho_1, \ldots, \rho_k)$ if and only if

$u^* \neq \{(\overline{\sigma_1}, \overline{\rho_1}), \ldots, (\overline{\sigma_k}, \overline{\rho_k})\}$.

(4) $u \models (\sigma_1, \ldots, \sigma_k) \longrightarrow \beta$ if and only if

$\forall y_1, \ldots, y_k \in P(D)^+ [u^* = \{(\overline{\sigma_1}, y_1), \ldots, (\overline{\sigma_k}, y_k)\}$ implies $(y_1, \ldots, y_k) \in \bar{\beta}]$.

(5) $u \models \alpha \longrightarrow (\rho_1, \ldots, \rho_k)$ if and only if

$\forall x_1, \ldots, x_k \in \rho(P)^+ [u^* = \{(x_1, \overline{\rho_1}), \ldots, (x_k, \overline{\rho_k})\}$ implies $(x_1, \ldots, x_k) \in \bar{\alpha}]$.

(6) $u \models \alpha \Longrightarrow \beta$ if and only if

$\pi_1(u^*) = \phi$ or $[\pi_1^*(u^*) \cap \leftrightarrow \bar{\alpha} \neq \phi$ and $\pi_2^*(u^*) \cap \bar{\beta} \neq \phi]$.

(7) $u \models S \Longrightarrow T$ if and only if

$\cup \pi_1(u^*) \in \bar{S}$ and $\cup \pi_2(u^*) \in \bar{T}$.

Let

$$\Gamma_1 = \{S_1 \rightarrowtail T_1, \ldots, S_k \rightarrowtail T_k\}$$

and

$$\Gamma_2 = \{S_1' \twoheadrightarrow T_1', \ldots, S_l' \twoheadrightarrow T_l'\}.$$

u is said to be a (standard) model of Γ_1 and Γ_2 if and

only if $u \models \Phi$ for every $\Phi \in \Gamma_1 \cup \Gamma_2$ and $\forall (x, y) \in u \exists i \leq k [x \in \tilde{S}_i$ and $y \in \tilde{T}_i]$. We write $\Gamma_1, \Gamma_2 \models \Phi$ if every model of Γ_1 and Γ_2 satisfies Φ.

3.2 A Proof of the Completeness Theorem

We say that Γ_1 is normal if $\forall i \leq k [\tilde{S}_i^+ \neq \phi$ and $\phi \in \tilde{T}_i]$ and $\forall i, j \leq k [i \neq j$ implies $\tilde{S}_i^+ \cap \tilde{S}_j^+ = \phi]$. Also, we say that Γ_1 is good if Γ_1 is normal and $\forall i, j \leq k [i \neq j$ implies $\tilde{T}_i^+ \cap \tilde{T}_j^+ = \phi]$.

Remark

If Γ_1 is normal but not good, then let

$$\Gamma_1^* = \{S_1 \rightarrowtail [\langle T_1, b_1 \rangle_2]_1, \ldots, S_k \rightarrowtail [\langle T_k, b_k \rangle_2]_1\}$$

where $b_1, \ldots, b_k$ are new constant symbols of d-sort. Then for every T, there is a d-term T^* in $L_{m,n+k}$ such that $\Gamma_1, \Gamma_2 \models S \Longrightarrow T$ if and only if $\Gamma_1^*, \Gamma_2 \models S \Longrightarrow T^*$. Moreover, if Γ_1 is normal, then Γ_1^* is good. Hence, $\Gamma_1, \Gamma_2 \models S \Longrightarrow T$ if and only if $\Gamma_1^*, \Gamma_2 \vdash_{m,n+k} S \Longrightarrow T^*$.

Lemma 1

Suppose that Γ_1 is normal.

(i) $\forall u$: a model of Γ_1 and $\Gamma_2[\bar{\sigma} \neq \cup \pi_1(u^*)]$ if and only if

$\forall (x_1, \ldots, x_k) \in \widetilde{[S_1]}_1 \times \cdots \times \widetilde{[S_k]}_1 \forall (y_1, \ldots, y_k) \in \tilde{T}_1 \times \cdots \times \tilde{T}_k [\bar{\sigma} = \cup \{x_i \mid 1 \leq i \leq k\}$ and $\{i \mid x_i \neq \phi\} = \{i \mid y_i \neq \phi\}$ imply $\exists j \leq l \exists y \in \tilde{T}_j'^+ \exists J \subseteq \{i \mid x_i \neq \phi\} [J \neq \phi, y \subseteq \cap \{y_i \mid i \in J\}, \cup \{x_i \mid i \in J\} \notin S_j'$ and $\forall i \in \{i \mid x_i \neq \phi\} - J [y \not\subseteq y_i]]]$.

(ii) In (i), we can replace $\bar{\sigma} \neq \cup \pi_1(u^*)$ by $\bar{\rho} \neq \cup \pi_2(u^*)$ and $\bar{\sigma} = \cup \{x_i \mid 1 \leq i \leq k\}$ by $\rho = \cup \{y_i \mid 1 \leq i \leq k\}$.

Proof. (i) ($\Rightarrow$) Suppose that the negation of the right hand side holds, i.e., $\exists (x_1, \ldots, x_k) \in \widetilde{[S_1]}_1 \times \cdots \times \widetilde{[S_k]}_1 \exists (y_1, \ldots, y_k) \in \tilde{T}_1 \times \cdots \times \tilde{T}_k [\bar{\sigma} = \cup \{x_i \mid 1 \leq i \leq k\}, \{i \mid x_i \neq \phi\} = \{i \mid y_i \neq \phi\}$ and $\forall j \leq l \forall y \in \tilde{T}_j'^+ \forall J \subseteq \{i \mid x_i \neq \phi\} [J \neq \phi, y \subseteq \cap \{y_i \mid i \in J\}$ and $\forall i \in \{i \mid x_i \neq \phi\} - J [y \not\subseteq y_i]$ imply $\cup \{x_i \mid i \in J\} \in S_j']]$.

Without loss of generality, we can assume that $\{i \mid x_i \neq \phi\} = \{1, 2, \ldots, k'\}$. Pick $x_i' \in \tilde{S}_i'^+$ for $k' < i \leq k$, and let $u = \{(x_i, y_i) \mid 1 \leq i \leq k'\} \cup \{(x_i', \phi) \mid k' < i \leq k\}$. $u \models \Gamma_1$, since Γ_1 is normal.

Suppose that $1 \leq j \leq l$, $y \in \widetilde{T_j'}^+$ and $A(u, y) \neq \phi$, and let $J = \{i \mid y \subseteq y_i\}$. Then, $J \subseteq \{i \mid x_i \neq \phi\}$ and $J \neq \phi$, since $y \neq \phi$ and $A(u, y) \neq \phi$.

It is clear that $y \subseteq \cap \{y_i \mid i \in J\}$. Hence, by the assumption, $A(u, y) = \cup \{x_i \mid y \subseteq y_i\} = \cup \{x_i \mid i \in J\} \in \tilde{S}_j'$. So $u \models \Gamma_2$. Hence u is a model of Γ_1 and Γ_2 by the definition of u, and $\cup \pi_1(u^*) = \cup \{x_i \mid 1 \leq i \leq k'\} = \cup \{x_i \mid 1 \leq i \leq k\} = \bar{\sigma}$. But this contradicts our assumption that $\forall u$: a model of Γ_1 and $\Gamma_2[\bar{\sigma} \neq \cup \pi_1(u^*)]$.

($\Leftarrow$) Suppose that $\exists u$: a model of Γ_1 and $\Gamma_2[\bar{\sigma} = \cup \pi_1(u^*)]$.

Without loss of generality, we can assume that $u^* = \{(x_1, y_1), \ldots, (x_{k'}, y_{k'})\}$ and $(x_i, y_i) \in \tilde{S}_i \times \tilde{T}_i$ for every $i \leq k'$.

Let $x_i = y_i = \phi$ for $k' < i \leq k$. Then, $\cup \{x_i \mid 1 \leq i \leq k\} = \cup \{x_i \mid 1 \leq i \leq k'\} = \cup \pi_1(u^*) = \bar{\sigma}$ and $\{i \mid x_i \neq \phi\} = \{i \mid y_i \neq \phi\}$.

Hence, by our assumption, $\exists j \leq l \exists y \in \widetilde{T_j'}^+ \exists J \subseteq \{i \mid x_i \neq \phi\} [J \neq \phi, y \subseteq \cap \{y_i \mid i \in J\}, \cup \{x_i \mid i \in J\} \notin \tilde{S}_j'^+$ and $\forall i \in \{i \mid x_i \neq \phi\} - J [y \not\subseteq y_i]]$. Therefore $A(u, y) = \cup \{x_i \mid i \in J\} \notin \tilde{S}_j'^+$.

Since $J \neq \phi$, $A(u, y) \neq \phi$, $u \not\models S_j' \twoheadrightarrow T_j'$. But this contradicts that u is a model of Γ_1 and Γ_2. Therefore $\forall u$: a model of Γ_1 and $\Gamma_2[\sigma = \cup \pi_1(u^*)]$.

(ii) The proof of (ii) is similar to that of (i).

Remark

It is easy to show that if $\phi \in \tilde{S}$, then there is a S' such that $\tilde{S}' = \tilde{S} \cap [S_1, \ldots, S_k]_k$. So let S_{Γ_1} be one of the p-terms which satisfies $\tilde{S}_{\Gamma_1} = \tilde{S} \cap [S_1, \ldots, S_k]_k$ for every S such that $\phi \in \tilde{S}$. T_{Γ_1} is defined similarly.

Lemma 2

Suppose that Γ_1 satisfies $\forall i \leq k [\phi \in \tilde{T}_i]$, $\phi \in \tilde{S}$ and $\phi \in \tilde{T}$. $\Gamma_1, \Gamma_2 \models S \Longrightarrow T$ if and only if $\Gamma_1, \Gamma_2 \models S_{\Gamma_1} \Longrightarrow T_{\Gamma_1}$.

Proof. ($\Rightarrow$) It follows easily from $\tilde{S}_{\Gamma_1} \subseteq \tilde{S}$ and $\tilde{T}_{\Gamma_1} \subseteq \tilde{T}$.

($\Leftarrow$) Suppose that $\Gamma_1, \Gamma_1 \models S \Longrightarrow T$. Let u be a model of Γ_1 and Γ_2. Then, $\cup \pi_1(u^*) \in \tilde{S}$, since $u \models S \Longrightarrow T$. On the other hand, $\cup \pi_1(u^*) \in [S_1, \ldots, S_k]_k$, since $u \models \Gamma_1$. Hence $\cup \pi_1(u^*) \in \tilde{S} \cap [S_1, \ldots, S_k]_k = \tilde{S}_{\Gamma_1}$. It is similarly shown that $\cup \pi_2(u^*) \in \tilde{T}_{\Gamma_1}$. Therefore

$$\Gamma_1, \Gamma_2 \models S_{\Gamma_1} \Longrightarrow T_{\Gamma_1}.$$

Theorem (Completeness theorem).

Suppose that Γ_1 is good.

$\Gamma_1, \Gamma_2 \vdash S \Longrightarrow T$ if and only if $\Gamma_1, \Gamma_2 \models S \Longrightarrow T$.

Proof (soundness).

It is enough to show that for every inference rule, if u satisfies upper formulas of a rule and is a model of Γ_1 and Γ_2, then u satisfies a lower formulas of a rule.

(A_1) Suppose that $u \not\models (\sigma_1^0, \ldots, \sigma_l^0, \sigma_1, \ldots, \sigma_{k'}) \rightarrow\!\!\!\!\!+ (\rho_1^0, \ldots, \rho_{l'}^0, \rho_1, \ldots, \rho_{k'})$.

Then $u^* = \{(\sigma_j^0, \rho_j^0) \mid 1 \leq j \leq l'\} \cup \{(\sigma_i, \rho_i) \mid 1 \leq i \leq k'\}$.

By the conditions of (A_1), there is a $\bar{p} \in \tilde{T}$ such that $\bar{p} \subseteq \overline{\rho_i}$ for every $i \leq k'$ and $\bar{p} \not\subseteq \overline{\rho_j^0}$ for every $j \leq l'$.

Hence $A(u, \bar{p}) = \cup \{\sigma_i \mid 1 \geq i \geq k'\} = \langle \sigma_1, \ldots, \sigma_{k'} \rangle_{k'} \notin \tilde{S}$. Therefore $A(u, \bar{p}) \notin \tilde{S}$.

But this contradicts that $u \models S \twoheadrightarrow T$, since $A(u, \rho) \neq \phi$.

(A_2) Clear.

(B_1) Suppose that $u \not\models (\sigma_1, \ldots, \sigma_{k'}) \longrightarrow T_1^0 * \cdots * T_{k'}^0$. Then

$$\exists y_1, \ldots, y_{k'} \in P(D)^+ [u^* = \{(\overline{\sigma_1}, y_1), \ldots, (\overline{\sigma_{k'}}, y_{k'})\}$$

and

$$(y_1, \ldots, y_{k'}) \notin \widetilde{T_1^0 * \cdots * T_{k'}^0} = \widetilde{T}_1'^{0+} \times \cdots \times \widetilde{T}_{k'}'^{0+}].$$

Therefore $\exists i \leq k' [\overline{\sigma_i} \in \tilde{S}_i^0]$ and $y_i \notin \tilde{T}_i'^{0+}$. But this contradicts $u \models S_i^0 \rightarrowtail T_i^0$.

(B_2) Clear.

(C_1) Suppose that

$$u \not\models S_1^0 * \cdots * S_k^0 \longrightarrow (\rho_1, \ldots, \rho_{k'}).$$

Then

$$\exists x_1, \ldots, x_{k'} \in \rho(P)^+ [u^* = \{(x_1, \overline{\rho_1}), \ldots, (x_{k'}, \rho_{k'})\}$$

and

$$(x_1, \ldots, x_{k'}) \notin \widetilde{S_1^0 * \cdots * S_k^0} = \tilde{S}_1'^{0+} \times \cdots \times \tilde{S}_k'^{0+}].$$

Therefore $\exists j \leq l [x_i \notin \tilde{S}_j'^{0+}$ and $\overline{\rho_i} \in \tilde{T}_j'^0]$. Then $\exists j \leq l [x_i \in \tilde{S}_j$

and $\overline{p_i} \in \tilde{T}_j]$, since u is a model of Γ_1 and Γ_2. Hence $\tilde{T}_i^0 = \tilde{T}_j$ and $\tilde{S}_i^0 = \tilde{S}_j$, since Γ_1 is normal and $\overline{p_i} \in \tilde{T}_i^{0+} \cap \tilde{T}_j^+$. But this contradicts that $x_i \notin \tilde{S}_i^{0+}$ and $x_i \in \tilde{S}_j$.

(C_2) Clear.

(D_1) Suppose that $u \not\models ((\mu_1, \ldots, \mu_{i-1}, \mu_{i+1}, \ldots, \mu_{l'})) \Longrightarrow \beta$, Let $\mu_i = (\sigma_1, \ldots, \sigma_{k'})$. Since $u \models ((\mu_1, \ldots, \mu_i, \ldots, \mu_{l'})) \Longrightarrow \beta$, $\pi_1(u) \neq \phi$ and $\overline{\mu_i} \in \pi_1^*(u^*)$. Then $\exists y_1, \ldots, y_{k'} \in P(D)^+ [u^* = \{(\overline{\sigma_1}, y_1), \ldots, (\overline{\sigma_{k'}}, y_{k'})\}]$. But this contradicts that $u \models \mu_i \longrightarrow (( ))$.

(D_2) The proof is similar to that of (D_1).

(E_1), (E_3) and (F) Clear.

(E_2) Suppose that $u \not\models [\mu_1^0, \ldots, \mu_{l'}^0]_{l'} \Longrightarrow [\tau_1^0, \ldots, \tau_{k'}^0]_{l'}$. Then

$$\cup \pi_1(u^*) \notin [\mu_1^0, \overbrace{\ldots}, \mu_{l'}^0]_{l'} \text{ or } \cup \pi_2(u^*) \notin [\tau_1^0, \overbrace{\ldots}, \tau_{k'}^0]_{l'}.$$

Hence $\cup \pi_1(u^*) \neq \phi$. Since

$$u \models ((\mu_1, \ldots, \mu_{l'})) \Longrightarrow ((\tau_1, \ldots, \tau_{k'}))$$

and

$$\pi_1(u^*) \neq \phi,\ \pi_1^*(u^*) \cap \{\overline{\mu_1}, \ldots, \overline{\mu_{l'}}\} \neq \phi$$

and

$$\pi_2^*(u^*) \cap \{\overline{\tau_1}, \ldots, \overline{\tau_{k'}}\} \neq \phi.$$

We have $\exists x_1, \ldots, x_{m'}, y_1, \ldots, y_{n'} [(x_1, \ldots, x_{m'}) \in \pi_1^*(u^*) \cap \{\overline{\mu_1}, \ldots, \overline{\mu_{l'}}\}$ and $(y_1, \ldots, y_{n'}) \in \pi_2^*(u^*) \cap \{\overline{\tau_1}, \ldots, \overline{\tau_{k'}}\}]$.

Therefore $\pi_1(u^*) = \{x_1, \ldots, x_m\}$ and $\pi_2(u^*) = \{y_1, \ldots, y_{n'}\}$.

Hence $\cup \pi_1(u^*) = \cup \{x_i | 1 \leq i \leq m'\} \in \{\mu_1^0, \ldots, \overbrace{\mu_{l'}^0}\} \subseteq [\mu_1^0, \overbrace{\ldots}, \mu_{l'}^0]_{l'}$ and $\cup \pi_2(u^*) = \cup \{y_i | 1 \leq i \leq n'\} \in [\tau_1^0, \ldots, \tau_{k'}^0]_{l'}$. But this is a contradiction.

(completeness)

Suppose that $\Gamma_1, \Gamma_2 \models S \Longrightarrow T$.

Since Γ_1 is normal, $u = \{(x_i, \phi) | 1 \leq i \leq k, x_i \in \tilde{S}_i^+\}$ is a model of Γ_1 and Γ_2.

Hence $\phi = \cup \pi_1(u^*) \in \tilde{S}$ and $\phi = \cup \pi_2(u^*) \in \tilde{T}$.

Hence, by virtue of lemma 2, $\Gamma_1, \Gamma_2 \models S_{\Gamma_1} \Longrightarrow T_{\Gamma_1}$.

We try to show that $\Gamma_1, \Gamma_2 \vdash S_{\Gamma_1} \Longrightarrow T_{\Gamma_1}$. If we can show it, then $\Gamma_1, \Gamma_2 \vdash S \Longrightarrow T$ by the inference rule (F).

For $x \in [S_1, \overbrace{\ldots}, S_k]_k$ and $y \in [T_1, \overbrace{\ldots}, T_k]_k$, let

$$F(x) = \{(\sigma_1, \ldots, \sigma_h) | \overbrace{(\sigma_1, \ldots, \sigma_h)} \in [S_1, \ldots, S_k]_k^\vee,\ x = \cup \{\overline{\sigma_i} | 1 \leq i \leq h\} \text{ and } h \leq k\},$$

$$F(y) = \{(\rho_1, \ldots, \rho_h) | \overbrace{(\rho_1, \ldots, \rho_h)} \in [T_1, \ldots, T_k]_k^\vee,\ y = \cup \{\overline{\rho_i} | 1 \leq i \leq h\} \text{ and } h \leq k\}.$$

Since $\Gamma_1, \Gamma_2 \vdash [S_1, \ldots, S_k]_k^\vee \Longrightarrow [T_1, \ldots, T_k]_k^\vee$, it is enough to show that

$$\Gamma_1, \Gamma_2 \vdash (\sigma_1, \ldots, \sigma_h) \longrightarrow (( ))$$

and

$\Gamma_1, \Gamma_2 \vdash (( )) \longrightarrow (\rho_1, \ldots, \rho_h)$ for every $(\sigma_1, \ldots, \sigma_h) \in F(x)$ and $(\rho_1, \ldots, \rho_h) \in F(y)$ where $x \notin \tilde{S}_{\Gamma_1}$ and $y \notin \tilde{T}_{\Gamma_1}$.

Suppose that $x \notin \tilde{S}_{\Gamma_1}$ and $(\sigma_1, \ldots, \sigma_h) \in F(x)$. Without loss of generality, we assume that $\overline{\sigma_i} \in \overline{S_i}$ for every $i \leq h$.

Let $x_1 = y_1 = \phi$ for $h < i \leq k$ and $x_i = \overline{\sigma_i}$ for $1 \leq i \leq h$.

If there is an $i \leq h$ such that $\tilde{T}_i^+ = \phi$, then by the rule (B_1)

$$\frac{S_1 \rightarrowtail T_1, \ldots, S_h \rightarrowtail T_h}{(\sigma_1, \ldots, \sigma_h) \longrightarrow (( ))}.$$

Hence we assume that $\tilde{T}_i^+ \neq \phi$ for every $i \leq h$.

Pick $y_i \in \tilde{T}_i^+$ for $1 \leq i \leq h$. Then $\cup \{x_i | 1 \leq i \leq k\} = \cup \{x_i | 1 \leq i \leq h\} = x = x^{\vee\vee}$ and $\{i | x_i \neq \phi\} = \{i | y_i \neq \phi\}$.

Since Γ_1, $\Gamma_2 \models S_{\Gamma_1} \Longrightarrow T_{\Gamma_1}$, $\forall u$: a model of Γ_1 and $\Gamma_2[\cup \pi_1(u^*) \in S_{\Gamma_1}]$.

Therefore $\forall u$: a model of Γ_1 and $\Gamma_2[\cup \pi_1(u^*) \neq \overbrace{x^\vee}]$.

Hence, by lemma 1, $\exists j \leq l \exists y \in \widetilde{T_j'}^+ \exists J \subseteq \{i | x_i \neq \phi\} [J \neq \phi, y \subseteq \cap \{y_i | i \in J\}, \cup \{x_i | i \in J\} \notin \widetilde{S_j'}^+$ and $\forall i \in \{i | x_i \neq \phi\} - J[y \not\subseteq y_i]]$.

Without loss of generality, we assume $J = \{1, 2, \ldots, m'\}$.

Then $\overbrace{\langle \hat{x}_1, \ldots, \hat{x}_{m'} \rangle}_{m'} = \cup \{\bar{\hat{x}}_i | 1 \leq i \leq m' = \cup \{x_i | i \in J\} \notin \widetilde{S_j'}$. Also, $\bar{\hat{y}} \in \widetilde{T_j'}^+$, $\bar{\hat{y}} \subseteq \bar{\hat{y}}_i$ for $1 \leq i \leq m'$ and $\bar{\hat{y}} \notin \bar{\hat{y}}_i$ for $m' < i \leq h$.

Hence, by the rules (A_1) and (A_2),

$$\frac{S_j' \twoheadrightarrow T_j'}{(\hat{x}_{m'+1}, \ldots, \hat{x}_h, \hat{x}_1, \ldots, \hat{x}_{m'}) \not\rightarrow (\hat{y}_{m'+1}, \ldots, \hat{y}_h, \hat{y}_1, \ldots, \hat{y}_{m'})}$$

$$\vdots$$

$$\frac{\overline{(\hat{x}_1, \cdots, \hat{x}_h) \not\rightarrow (\hat{y}_1, \cdots, \hat{y}_h)}}{(\hat{\sigma}_1, \cdots, \hat{\sigma}_h) \not\rightarrow (\hat{y}_1, \cdots, \hat{y}_y)}.$$

Hence $\Gamma_1, \Gamma_2 \vdash (\sigma_1, \ldots, \sigma_h) \not\rightarrow (\hat{y}_1, \ldots, \hat{y}_h)$ for every $(y_1, \ldots, y_h) \in \tilde{T}_1^+ \times \cdots \times \tilde{T}_h^+$.

Therefore, by the rules (B_1), (B_2) and (A_2), $\Gamma_1, \Gamma_2 \vdash (\sigma_1, \ldots, \sigma_h) \longrightarrow (( ))$.

It is similarly proved that

$$\Gamma_1, \Gamma_2 \vdash (( )) \longrightarrow (\rho_1, \ldots, \rho_h)$$

Appendix

(1) Problem

In the dining philosophers problem, five philosophers ph1, . . . , ph5 are sitting at a round table and spend their time eating and thinking. In the middle of the table, there is a large, continually replenished bowl of spaghetti, from which they can help themselves when they are hungry. There are only five forks $f1, \ldots, f5$ on the table, one between each philosopher's place (Figure). The spagetti however is so long and tangled that every philosopher requires two forks to eat it, and, furthermore, the only forks a philosopher can use are those on his immediate right and his immediate left. The problem is to find whether five philosophers can cooperate with each other for continually eating and thinking without a deadlock or starvation.

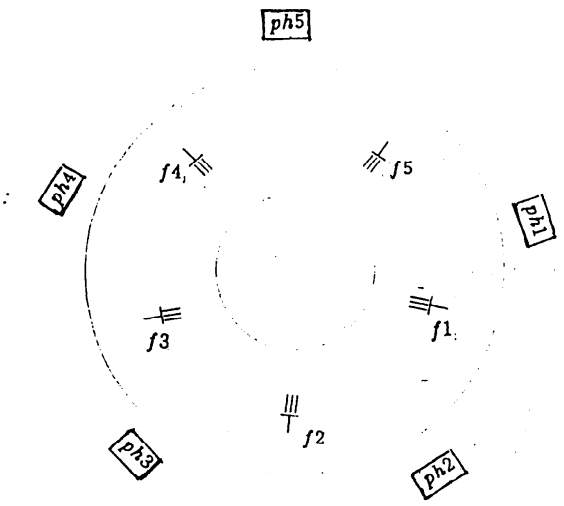

Figure Dining Philosopher

(2) Formulation in $FL_{m,n}$

When formulating the problem in $FL_{m,n}$ five philosophers ph1, . . . , ph5 will represent the processes concurrently using the data available to them, which are five forks $f1, \ldots, f5$. Hence, $m=n=5$, and ph1, . . . , ph5 are constant symbols of p-sort and $f_1, \ldots, f5$ are constant symbols of d-sort. One of the constraint conditions is that every philosopher is allowed to use only forks on his immediate right and left. For instance, a philosopher ph1 is allowed to use only two forks $f1$ and $f5$. Hence, in all possible situations, at least one philosopher ph1 uses at most a pair of fork $f1$ and $f5$, which will be written in $FL_{5,5}$ as:

$$\langle \text{ph1} \rangle_1 \rightarrowtail [\langle f1, f5 \rangle_2]_1.$$

This constraint condition can be similarly written down for each philosopher, totality of which forms the axiom Γ_1. Another constraint condition is that a fork between each philosopher's place can be used by both of the adjacent philosophers. For instance, fork $f1$ can be used by at most one of the two philosophers ph1 and ph2 in all possible situations, which will be written in $FL_{5,5}$ as:

$$[\text{ph1}, \text{ph2}]_1 \twoheadrightarrow \langle f1 \rangle_1$$

The totality of these constrains written for all forks forms the axiom Γ_2. In addition, it is an obvious premise in the problem that at most five philosophers use at most five pairs of forks in all possible situation. This general premise is represented in $FL_{5,5}$ by the formula:

$$[\text{ph1}, \ldots, \text{ph5}]_5^{\vee} \Longrightarrow [\langle f5, f1 \rangle_2, \ldots, \langle f4, f5 \rangle_2]_5^{\vee},$$

which is generated and used within the proof procedure of $FL_{m,n}$. Under the axiom Γ_1 and Γ_2, we would like to prove that at most two philosophers use the respective pair of forks allowed to them in all possible situations, which is written in $FL_{5,5}$ as:

$$[\text{ph1}, \ldots, \text{ph5}]_2 \Longrightarrow [\langle f5, f1 \rangle_2, \langle f1, f2 \rangle_2, \ldots, \langle f4, f5 \rangle_2]_2.$$

If this formula is provable from the axiom Γ_1 and Γ_2, then it is true, by our completeness theorem. In this case, this problem has an affirmative solution and five philosophers can continually keep eating and thinking.

(3) Specification in $FL_{m,n}$

In summary, the specification of the dining philosophers problem is described in $FL_{5,5}$ as follows:

$$\begin{aligned}
&\langle \text{ph1} \rangle_1 \rightarrowtail [\langle f5, f1 \rangle_2]_1 \ldots (P_1),\\
&\langle \text{ph2} \rangle_1 \rightarrowtail [\langle f1, f2 \rangle_2]_1 \ldots (P_2),\\
\Gamma_1:\ &\langle \text{ph3} \rangle_1 \rightarrowtail [\langle f2, f3 \rangle_2]_1 \ldots (P_3),\\
&\langle \text{ph4} \rangle_1 \rightarrowtail [\langle f3, f4 \rangle_2]_1 \ldots (P_4),\\
&\langle \text{ph5} \rangle_1 \rightarrowtail [\langle f4, f5 \rangle_2]_1 \ldots (P_5).\\
&[\text{ph1}, \text{ph2}]_1 \twoheadrightarrow \langle f1 \rangle_1 \ldots (Q_1),\\
&[\text{ph2}, \text{ph3}]_1 \twoheadrightarrow \langle f2 \rangle_1 \ldots (Q_2),\\
\Gamma_2:\ &[\text{ph3}, \text{ph4}]_1 \twoheadrightarrow \langle f3 \rangle_1 \ldots (Q_3),\\
&[\text{ph4}, \text{ph5}]_1 \twoheadrightarrow \langle f4 \rangle_1 \ldots (Q_4),\\
&[\text{ph5}, \text{ph1}]_1 \twoheadrightarrow \langle f5 \rangle_1 \ldots (Q_5),
\end{aligned}$$

(4) Sample Proof

In the following we give a proof figure (also see [8]) which shows

$$\{P_1, P_2, P_3, P_4, P_5\}, \{Q_1, Q_2, Q_3, Q_4, Q_5\} \vdash_{5,5}$$

$$[\text{ph1}, \text{ph2}, \text{ph3}, \text{ph4}, \text{ph5}]_2 \Longrightarrow$$

$$[\langle f5, f1 \rangle_2, \langle f1, f2 \rangle_2, \langle f2, f3 \rangle_2, \langle f3, f4 \rangle_2, \langle f4, f5 \rangle_2]_2.$$

For the sake of simplicity, we denote d-A-terms

$\langle f5, f1 \rangle_2, \langle f1, f2 \rangle_2, \langle f2, f3 \rangle_2, \langle f3, f4 \rangle_2, \langle f4, f5 \rangle_2$ by $t1, t2, t3, t4, t5$.

Let $1 \leq k \leq 5$ and $1 \leq i, i_1, \ldots, i_k \leq 5$.

We abbreviate some formulas as follws:

$\varphi_{i_1}, \cdots, i_k \equiv (phi_1, \cdots, phi_k) \not\longrightarrow (ti_1, \cdots, ti_k)$

$\psi_{i_1}, \cdots, i_k \equiv (phi_1, \cdots, phi_k) \longrightarrow (((ti_1, \cdots, ti_k)))$

$\theta_{i_1}, \cdots, i_k \equiv (phi_1, \cdots, phi_k) \longrightarrow ((\ ))$

$\xi_{i_1}, \cdots, i_k \equiv (((phi_1, \cdots, phi_k))) \longrightarrow (ti_1, \cdots, ti_k)$

$\eta_{i_1}, \cdots, i_k \equiv ((\ )) \longrightarrow (ti_1, \cdots, ti_k)$

$$\dfrac{\dfrac{\dfrac{|ph1, \cdots, ph5|^{\vee}_{5} \Longrightarrow [t1, \cdots, t5|^{\vee}_{5}\ \Delta_1}{|ph1, \cdots, ph5|^{\vee}_{4} \Longrightarrow [t1, \cdots, t5|^{\vee}_{5}}(D_1)\ \Delta_2}{[ph1, \cdots, ph5|^{\vee}_{3}(((ph1, ph2, ph3, ph5), \cdots, (ph2, ph3, ph4, ph5))) \Longrightarrow [t1, \cdots, t5]^{\vee}_{5}}(D_1)\ \theta_{1,2,3,5}\ \theta_{1,2,4,5}\ \theta_{1,3,4,5}\ \theta_{2,3,4,5}}{[ph1, \cdots, ph5]^{\vee}_{3} \Longrightarrow [t1, \cdots, t5]^{\vee}_{5}}(D_1)$$

Fig. 1

$$\dfrac{\dfrac{|ph1, \cdots, ph5|^{\vee}_{3} \Longrightarrow [t1, \cdots, t5]^{\vee}_{5}\ \Delta_3}{[ph1, \cdots, ph5]^{\vee}_{2}(((ph1, ph2, ph4), (ph1, ph2, ph5), \cdots, (ph3, ph4, ph5))) \Longrightarrow [t1, \cdots, t5]^{\vee}_{5}}(D_1)\ \theta_{1,2,4}\ \theta_{1,2,5}\ \theta_{3,4,5}}{[ph_1, \cdots, ph5]^{\vee}_{2} \Longrightarrow [t1, \cdots, t5]^{\vee}_{5}}(D_2)$$

Fig. 2

$$\dfrac{\dfrac{\dfrac{[ph1, \cdots, ph5]^{\vee}_{2} \Longrightarrow [t1, \cdots, t5]^{\vee}_{5}\ \Sigma_1}{[ph1, \cdots ph5]^{\vee}_{2} \Longrightarrow [t1, \cdots t5]^{\vee}_{4}}(D_2)\ \Sigma_2}{[ph1, \cdots, ph5]^{\vee}_{2} \Longrightarrow [t1, \cdots, t5]^{\vee}_{3}(((t1, t2, t3, t5), \cdots, (t2, t3, t4, t5)))}(D_2)\ \eta_{1,2,3,5}\ \eta_{1,2,4,5}\ \eta_{1,3,4,5}\ \eta_{2,3,4,5}}{[ph1, \cdots, ph5]^{\vee}_{2} \Longrightarrow [t1, \cdots, t5]^{\vee}_{3}}(D_2)$$

Fig. 3

$$\dfrac{[ph1, \cdots, ph5]^{\vee}_{2} \Longrightarrow [t1, \cdots, t5]^{\vee}_{2}\ \eta_{1,2,3}\ \eta_{1,2,4}\ \eta_{1,2,5}\ \eta_{1,3,4} \cdots \eta_{3,4,5}}{[ph1, \cdots, ph5]^{\vee}_{2} \Longrightarrow [t1, \cdots, t5]^{\vee}_{2}}(D_2)$$

$$\dfrac{}{[ph1, \cdots, ph5]^{\vee}_{2} \Longrightarrow [t1, \cdots, t5]^{\vee}_{2}}(E_2, F)$$

Fig. 4

where Δ_1, Δ_2, Δ_3 are as follows;

Δ_1:
$$\dfrac{\dfrac{\dfrac{Q_1}{\phi_{3,4,5,1,2}}(A_1)}{\phi_{1,2,3,4,5}}(A_2)\dfrac{P_1, P_2, P_3, P_4, P_5}{\psi_{1,2,3,4,5}}(B_1)}{\theta_{1,2,3,4,5}}(B_2)$$

Δ_2:
$$\dfrac{\dfrac{\dfrac{Q_1}{\phi_{3,4,1,2}}(A_1)}{\phi_{1,2,3,4,}}(A_2)\dfrac{P_1, P_2, P_3, P_4}{\psi_{1,2,3,4}}(B_1)}{\theta_{1,2,3,4}}(B_2)$$

Δ_3:
$$\dfrac{\dfrac{\dfrac{Q_1}{\phi_{3,1,2}}(A_1)}{\phi_{1,2,3}}(A_2)\dfrac{P_1, P_2, P_3}{\psi_{1,2,3}}(C_1)}{\theta_{1,2,3}}(C_2)$$

and Σ_1, Σ_2 are also as follows;

Σ_1:
$$\dfrac{\dfrac{\dfrac{Q_1}{\phi_{3,4,5,1,2}}(A_1)}{\phi_{1,2,3,4,5}}(A_2)\dfrac{P_1, P_2, P_3, P_4, P_5}{\xi_{1,2,3,4}}(C_2)}{\eta_{1,2,3,4,5}}(C_2)$$

Σ_2:
$$\dfrac{\dfrac{\dfrac{Q_1}{\phi_{3,4,1,2}}(C_1)}{\phi_{1,2,3,4}}(A_2)\dfrac{P_1, P_2, P_3, P_4}{\xi_{1,2,3,4}}(C_2)}{\eta_{1,2,3,4}}(C_2)$$

Remarks

In the proof figure, ═══(X) denotes the repeated applications of rule X.

Acknowledgement

The authors are grateful to Prof. N. Saito, Prof. N. Doi and Prof. S. Takasu for their advice and comments in completing this paper.

Reference

1. HIROSE, K., SAITO, N., DOI, N. *et al.* Process-data Representation, *Proc. 3rd US-Japan Computer Conference*, (1978), 225-230.
2. HIROSE, K., SAITO, N., DOI, N. *et al.* Specification technique for parallel processing; process-data representation, *AFIPS, Conference Proc.*, **50** (1981), 407-413.
3. HIROSE, K. and TAKAHASHI, M. A Formal System for Specification Analysis of Concurrent Programs, *Publ. RIMS, Kyoto Univ.*, **19** (1983), 911-926.
4. CAMBELL, R. H. and HABERMANN, A. N. The Specification of Process Synchronization by Path Expressions, *Proc. of International Symposium on Operating System, Lecture Note in Comp.* Sci. **16**, Springer Verlag, Berlin, (1974).
5. ASCHCROFT, E. and MANNA, Z. Formalization of Properties of Parallel Programs, *Stanford AI Memo*, AIM-110 (1970).
6. CLARK, K. L. and MCCABE, F. G. micro-PROLOG: Programming in Logic, Prentice-Hall (1984).
7. KOWALSKI, R. A. Logic for Problem Solving, North-Holland (1979).
8. HIROSE, K., TAKAHASHI, M. and YAMADA, S. The system $FL_{m,n}$ for specification analysis and an automatic theorem prover for $FL_{m,n}$, *Bulletin of Center for Informatics, Waseda Univ.*, **3** (to appear).

(Received June 21, 1985; revised November 25, 1986)