Title	Specification analysis of concurrent programs(LOGIC AND THE FOUNDATIONS OF MATHEMATICS)
Author(s)	Hirose, Ken; Takahashi, Makoto
Citation	数理解析研究所講究録 (1984), 516: 111-122
Issue Date	1984-03
URL	http://hdl.handle.net/2433/98385
Right	
Type	Departmental Bulletin Paper
Textversion	publisher

数理解析研究所講究録
516巻 1984年 111-122

Specification analysis of concurrent programs

早大理工 廣瀬 健 (Ken Hirose)
早大理工 高橋 真 (Makoto Takahashi)

Abstract

A formal system $FL_{m,n}$ is proposed to analyse the specificatio of concurrent programs. The completeness theorem is also proved for this system.

1. Introduction

In [1] and [2], one of the authors and his colleagues propose a new specification technique called Process-Data Representation (PDR). PDR aims at the improved reliability and modifiability in software system, 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 terms of the formulas 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 propose a formal system $FL_{m,n}$ as a tool for analysing the specification described in the forcing logic.

Following notations are used in this paper:
$\langle x_1,\ldots,x_\ell\rangle_k$ denotes a set of the subsets of $\{x_1,\ldots,x_\ell\}$ whose cardinality $\geqq k$, which means " at least k out of ℓ objects $\{x_1,\ldots,x_\ell\}$". $[x_1,\ldots,x_\ell]_k$ denotes a set of the subsets of $\{x_1,\ldots,x_\ell\}$ whose cardinality $\geqq k$, which means," at most k out of ℓ objects $\{x_1,\ldots,x_\ell\}$". $\langle x_1,\ldots,x_\ell\rangle_k \rightarrowtail Y$ means that the element of $\langle x_1,\ldots,x_\ell\rangle_k$ operates only on the element in Y, $[x_1,\ldots,x_\ell]_k \twoheadrightarrow Y$ means that the element in Y can be operated only by the element in $[x_1,\ldots,x_\ell]_k$, and $X \Longrightarrow Y$ means that the element of X operates on the element of Y. For example, the specification of the conditions in the dining philosophers problem can be described as follows:

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

where phk $(k=1,\ldots,5)$ represents the philosopher k and fi $(i=1,\ldots,5)$ represents the folk i.
Then, for example, the conclusion

$$[ph1,\ldots,ph5]_2 \rightarrowtail [\langle f5,f1\rangle_2,\ldots,\langle f4,f5\rangle_2]_2$$

is deducible from (*) in our system.

In section 2, we shall present the system $FL_{m,n}$ and, in section 3, we shall prove the completeness theorem for $FL_{m,n}$.

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

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

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

The language $L_{m,n}$ consists of

(1) Constant symbols,

$$p_1,\dots,p_m \text{ (p-sort)},$$
$$d_1,\dots,d_n \text{ (d-sort)}.$$

(2) Function symbols,

$$[\ ,\dots,]_k\ ,<\ ,\dots,\ >_k \quad (\ell\text{-ary},\ 0 \leqq k \leqq \ell, \ell \neq 0),$$
$$(\ ,\dots,\ ) \quad (q\text{-ary},\ 1 \leqq q),$$
$$((\ ,\dots,\ )) \ (r\text{-ary},\ 0 \leqq r).$$

(3) Predicate symbols,

$$\rightarrowtail\ ,\ \twoheadrightarrow\ ,\ \longrightarrow\ ,\ \not\longrightarrow\ ,\ \Longrightarrow\ .$$

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

(i) $p_1,\dots,p_m$ ($d_1,\dots,d_n$) are p-terms (d-terms).

(ii) If $S_1,\dots,S_\ell$ are p-terms (d-terms) , then $[S_1,\dots,S_\ell]_k$ and $<S_1,\dots,S_\ell>_k$ are p-terms (d-terms).

We define the p-A-terms, p-B-terms and p-C-terms (respectively d-A-terms, d-B-terms and d-C-terms) as follows:

(iii) $p_1,\dots,p_m$($d_1,\dots,d_n$) are p-A-terms (d-A-terms).

(iv) If $\sigma_1,\dots,\sigma_\ell$ ($\rho_1,\dots,\rho_\ell$) are p-A-terms (d-A-terms), then $<\sigma_1,\dots,\sigma_\ell>_\ell$ ($<\rho_1,\dots,\rho_\ell>_\ell$) is a p-A-term (d-A-term).

(v) If $\sigma_1,\dots,\sigma_\ell$ ($\rho_1,\dots,\rho_\ell$) are p-A-terms (d-A-terms), then $(\sigma_1,\dots,\sigma_\ell)$ ($(\rho_1,\dots,\rho_\ell)$) is a p-B-term (d-B-term).

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

(vii) If $\mu_1,\ldots,\mu_\ell$ ($\tau_1,\ldots,\tau_\ell$) are p-B-terms (d-B-terms), then $((\mu_1,\ldots,\mu_\ell))$ ($((\tau_1,\ldots,\tau_\ell))$) is a p-C-term (d-C-term).

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, τ for d-B-terms, α for p-C-terms and β for d-C-terms.

$S \rightarrowtail T$, $S \twoheadrightarrow T$, $S \dashrightarrow T$, $\mu \not\rightarrow \tau$, $\alpha \longrightarrow \tau$, $\mu \longrightarrow \beta$ and $\alpha \dashrightarrow \beta$ are formulas.

Let X be a set, $X_1,\ldots,X_\ell$ be subsets of $P(X)$ and $k \leqq \ell$. We define $\langle X_1,\ldots,X_\ell\rangle_k$ and $[X_1,\ldots,X_\ell]_k$ as follows:

$\langle X_1,\ldots,X_\ell\rangle_k = \{\bigcup_{i\in I} x_i \mid I\subset\{1,\ldots,\ell\}, \#I \geqq k \text{ and } x_i \in X_i \text{ for every } i\in I\}$,

$[X_1,\ldots,X_\ell]_k = \{\bigcup_{i\in I} x_i \mid I\subset\{1,\ldots,\ell\}, \#I \leqq k \text{ and } x_i \in X_i \text{ for every } i\in I\}$.

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

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

(ii) $\widetilde{\langle S_1,\ldots,S_\ell\rangle_k} = \langle\tilde{S}_1,\ldots,\tilde{S}_\ell\rangle_k$ and $\widetilde{[S_1,\ldots,S_\ell]_k} = [\tilde{S}_1,\ldots,\tilde{S}_\ell]_k$.

The canonical interpretation $\sim$ of d-terms is similarly defined.

(iii) $\overline{\langle\sigma_1,\ldots,\sigma_\ell\rangle_\ell} = \bigcup\{\sigma_i \mid 1\leqq i \leqq \ell\}$, $\overline{(\sigma_1,\ldots,\sigma_\ell)} = (\bar{\sigma}_1,\ldots,\bar{\sigma}_\ell)$ and $\overline{((\mu_1,\ldots,\mu_\ell))} = \{\mu_1,\ldots,\mu_\ell\}$. The canonical interpretation $-$ of d-A-terms, d-B-terms and d-C-terms are similarly defined.

If $x\subset\{p_1,\ldots,p_m\}$ ($y\subset\{d_1,\ldots,d_n\}$), then we denote by $\hat{x}$ ($\hat{y}$) one of the p-A-terms (d-A-terms) which satisfies $\bar{\hat{x}} = x$ ($\bar{\hat{y}} = y$). We denote by $\alpha_1{}^\frown\alpha_2$ the p-C-term $((\mu_1^1,\ldots,\mu_k^1,\mu_1^2,\ldots,\mu_\ell^2))$ where $\alpha_1 = ((\mu_1^1,\ldots,\mu_k^1))$ and $\alpha_2 = ((\mu_1^2,\ldots,\mu_\ell^2))$. If $\mu=(\sigma_1,\ldots,\sigma_\ell)$, then μ° is the p-A-term $\langle\sigma_1,\ldots,\sigma_\ell\rangle_\ell$. We denote by $S_1 * \cdots * S_\ell$ one of the p-C-terms which satisfies $\overline{S_1 * \cdots * S_\ell} = S_1^+ \times\cdots\times S_\ell^+$ and by $\widetilde{[S_1,\ldots,S_\ell]_k}$ one of the p-C-terms which satisfies

$\widetilde{[S_1,\ldots,S_\ell]_k} = \bigcup\{S_{j_1} * \cdots * S_{j_q} \mid 1\leqq j_1 < j_2 < \cdots < j_q \leqq \ell,\ q\leqq k\}$.

$\beta_1 \frown \beta_2$, τ° , $T_1 * \cdots * T_\ell$ and $\overset{\vee}{[T_1,\ldots,T_\ell]}_k$ are similarly defined.

Let $\Gamma_1 = \{S_1 \rightarrowtail T_1, \ldots, S_\ell \rightarrowtail T_\ell\}$ 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 $\overset{\vee}{[S_1,\ldots,S_\ell]}_\ell \Longrightarrow \overset{\vee}{[T_1,\ldots,T_\ell]}_\ell$ by the following inference rules.

$$(A_1)\ \frac{S \twoheadrightarrow T}{(\sigma_1^0,\ldots,\sigma_{\ell'}^0,\sigma_1,\ldots,\sigma_{k'}) \not\longrightarrow (\rho_1^0,\ldots,\rho_{\ell'}^0,\rho_1,\ldots,\rho_{k'})}$$

where $\overline{\langle\sigma_1,\ldots,\sigma_k\rangle_k} \notin \tilde{S}$ and there exists a $\bar{\rho} \varepsilon \tilde{T}$ such that $\bar{\rho} \varepsilon \tilde{\rho}_i$ for every $i \leqq k$ and $\bar{\rho} \notin \tilde{\rho}_j^0$ for every $j \leqq \ell'$.

$$(A_2)\ \frac{(\sigma_1,\ldots,\sigma_i,\ldots,\sigma_j,\ldots,\sigma_{k'}) \not\longrightarrow (\rho_1,\ldots,\rho_i,\ldots,\rho_j,\ldots,\rho_{k'})}{(\sigma_1,\ldots,\sigma'_j,\ldots,\sigma'_i,\ldots,\sigma_{k'}) \not\longrightarrow (\rho_1,\ldots,\rho'_j,\ldots,\rho'_i,\ldots,\rho_{k'})}$$

where $\bar{\sigma}_i = \bar{\sigma}'_i$, $\bar{\sigma}_j = \bar{\sigma}'_j$, $\bar{\rho}_i = \bar{\rho}'_i$ and $\bar{\rho}_j = \bar{\rho}'_j$.

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

where $\bar{\sigma}_i \varepsilon \tilde{S}_i^0$ for every $i \leqq k'$ and $S_i^0 \rightarrowtail T_i^0 (i \leqq k')$ are all different formulas.

$$(B_2)\ \frac{\mu \longrightarrow ((\tau_1,\ldots,\tau_i,\ldots,\tau_{\ell'}))\ ,\ \mu \not\longrightarrow \tau_i}{\mu \longrightarrow ((\tau_1,\ldots,\tau_{i-1},\tau_{i+1},\ldots,\tau_{\ell'}))}$$

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

where $\bar{\rho}_i \varepsilon \tilde{T}_i^0$ for every $i \leqq k'$ and $S_i^0 \rightarrowtail T_i^0 (i \leqq k')$ are all different formulas.

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

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

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

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

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

$$(E_2)\ \frac{((\mu_1,\ldots,\mu_{\ell'})) \Longrightarrow ((\tau_1,\ldots,\tau_{k'}))}{[\mu_1^\circ,\ldots,\mu_{\ell'}^\circ]_1 \Longrightarrow [\tau_1^\circ,\ldots,\tau_{k'}^\circ]_1}$$

where $\ell', k' \leqq 1$.

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

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

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

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

3. Completeness theorem

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

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:

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

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

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

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

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

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

Let $P=\{p_1,\ldots,p_m\}$, $D=\{d_1,\ldots,d_n\}$ and u be a nonempty subset of $\mathcal{P}(P)^+ \times \mathcal{P}(D)$. 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

$$S^+=\phi \text{ or } \left[\begin{array}{l} \forall (x,y)\varepsilon u[x\varepsilon S \text{ implies } y\varepsilon T], \\ \exists (x,y)\varepsilon u[x\varepsilon S \text{ and } y\varepsilon T] \text{ and} \\ \forall (x,y),(x',y')\varepsilon u[x,x'\varepsilon S \text{ and } y,y'\varepsilon T \text{ imply} \\ \qquad\qquad [[x=x' \text{ and } y=y'] \text{ or } y=\phi \text{ or } y'=\phi]] \end{array}\right].$$

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

$\forall y\varepsilon T^+[\ A(u,y)\neq\phi$ implies $A(u,y)\varepsilon S\ ]$.

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

$u^*\neq\{(\bar{\sigma}_1,\bar{\rho}_1),\ldots,(\bar{\sigma}_k,\bar{\rho}_k)\}$.

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

$$\forall y_1,\ldots,y_k\varepsilon \mathcal{P}(D)^+[u^*=\{(\bar{\sigma}_1,y_1),\ldots,(\bar{\sigma}_k,y_k) \text{ implies } (y_1,\ldots,y_k)\varepsilon\bar{\beta}].$$

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

$$\forall x_1,\ldots,x_k\varepsilon \mathcal{P}(P)^+[u^*=\{(x_1,\bar{\rho}_1),\ldots,(x_k,\bar{\rho}_k)\} \text{ implies } (x_1,\ldots,x_k)\varepsilon\bar{\alpha}].$$

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

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

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

$\bigcup\pi_1(u^*)\varepsilon\tilde{S}$ and $\bigcup\pi_2(u^*)\varepsilon\tilde{T}$.

Let $\Gamma_1=\{S_1 \rightarrowtail T_1,\ldots,S_k \rightarrowtail T_k\}$ and $\Gamma_2=\{S_1' \twoheadrightarrow T_1',\ldots, S_\ell' \twoheadrightarrow T_\ell'\}$. u is said to be a (standard) model of Γ_1 and Γ_2 if and only if $u \models \Phi$ for every $\Phi\varepsilon\Gamma_1\cup\Gamma_2$ and $\forall(x,y)\varepsilon u\ \exists\, i \leqq k\ [x\varepsilon\tilde{S}_i$ and $y\varepsilon\tilde{T}_i\ ]$. We write $\Gamma_1,\Gamma_2 \models \Phi$ if every model of Γ_1 and Γ_2 satisfies Φ.

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

Lemma 1. Suppose that Γ_1 is normal.

(i) $\forall u$: a model of Γ_1 and Γ_2 $[\ \bar{\sigma} \neq \bigcup \pi_1(u^*)]$ if and only if

$\forall (x_1,\ldots,x_k)\varepsilon[\widetilde{S_1}]_1 \times \cdots \times [\widetilde{S_k}]_1 \forall (y_1,\ldots,y_k)\varepsilon \widetilde{T}_1 \times \cdots \times \widetilde{T}_k$ $[\bar{\sigma} = \bigcup\{x_i \mid 1 \leqq i \leqq k\}$ and $\{i \mid x_i \neq \phi\} = \{i \mid y_i \neq \phi\}$ imply $\exists j \leqq \ell \exists y \varepsilon \widetilde{T}_j'^+$ $\exists J \subseteqq \{i \mid x_i \neq \phi\}[\ J \neq \phi,\ y \subseteqq \bigcap\{y_i \mid i \varepsilon J\},\ \bigcup\{x_i \mid i \varepsilon J\} \notin \widetilde{S}_j'$ and $\forall i \varepsilon \{i \mid x_i \neq \phi\} - J[\ y \nsubseteq y_i]]]$.

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

Proof. ($\Longrightarrow$) Suppose that

$\exists (x_1,\ldots,x_k)\varepsilon[\widetilde{S_1}]_1 \times \cdots \times [\widetilde{S_k}]_1 \exists (y_1,\ldots,y_k)\varepsilon \widetilde{T}_1 \times \cdots \times \widetilde{T}_k$ $[\sigma = \bigcup\{x_i \mid 1 \leqq i \leqq k\}, \{i \mid x_i \neq \phi\} = \{i \mid y_i \neq \phi\}$ and $\forall j \leqq \ell \forall y \varepsilon \widetilde{T}_j'^+ \forall J \subseteqq \{i \mid x_i \neq \phi\}$ $[J \neq \phi,\ y \subseteqq \bigcap\{y_i \mid i \varepsilon J\}$ and $\forall i \varepsilon \{i \mid x_i \neq \phi\} - J[y \nsubseteq y_i]$ imply $\bigcup\{x_i \mid i \varepsilon J\} \varepsilon \widetilde{S}_j']]$.

Without loss of generality, we can assume that $\{i \mid x_i \neq \phi\} = \{1,2,\ldots,k'\}$. Pick $x_i' \varepsilon \widetilde{S}_i^+$ for $k' < i \leqq k$. Let $u = \{(x_i,y_i) \mid 1 \leqq i \leqq k'\} \cup \{(x_i',\phi) \mid k' < i \leqq k\}$. Since Γ_1 is normal, $u \models \Gamma_1$. Suppose that $1 \leqq j \leqq \ell, y \varepsilon \widetilde{T}_j'^+$ and $A(u,y) \neq \phi$. Let $J = \{i \mid y \subseteqq y_i\}$. Since $y \neq \phi$ and $A(u,y) \neq \phi$, $J \subseteqq \{i \mid x_i \neq \phi\}$ and $J \neq \phi$. It is clear that $y \subseteqq \bigcap\{y_i \mid i \varepsilon J\}$. Hence, by the assumption, $A(u,y) = \bigcup\{x_i \mid y \subseteqq y_i\} = \bigcup\{x_i \mid i \varepsilon J\} \varepsilon \widetilde{S}_j'$. So $u \models \Gamma_2$. Hence u is a model of Γ_1 and Γ_2 by the definition of u. $\bigcup \pi_1(u^*) = \bigcup\{x_i \mid 1 \leqq i \leqq k'\} = \bigcup\{x_i \mid 1 \leqq i \leqq k\} = \sigma$. But this contradicts our assumption that $\forall u$:a model of Γ_1 and Γ_2 $[\bar{\sigma} \neq \bigcup \pi_1(u^*)]$.

($\Leftarrow$) Suppose that $\exists u$:a model of Γ_1 and $\Gamma_2[\bar{\sigma}=\bigcup\pi_1(u^*)]$. Without loss of generality, since u is a model of Γ_1 and Γ_2, we can assume that $u^*=\{(x_1,y_1),\ldots,(x_{k'},y_{k'})\}$ and $(x_i,y_i)\varepsilon\widetilde{S_i}\times\widetilde{T_i}$ for every $i\leqq k'$. Let $x_i=y_i=\phi$ for $k'<i\leqq k$. $\bigcup\{x_i|1\leqq i\leqq k\}=\bigcup\{x_i|1\leqq i\leqq k'\}=\bigcup\pi_1(u^*)=\bar{\sigma}$ and $\{i|x_i\neq\phi\}=\{i|y_i\neq\phi\}$. Hence, by our assumption, $\exists j\leqq \ell\exists y\varepsilon\widetilde{T_j'}{}^{+}\exists J\subseteq\{i|x_i\neq\phi\}[J\neq\phi, y\subseteq\bigcap\{y_i|i\varepsilon J\}$, $\bigcup\{x_i|i\varepsilon J\}\not\varepsilon\widetilde{S_j'}$ and $\forall i\varepsilon\{i|x_i\neq\phi\}-J[y\not\subseteq y_i]]$. Therefore $A(u,y)=\bigcup\{x_i|i\varepsilon J\}\not\varepsilon\widetilde{S_j'}$. Since $J\neq\phi$, $A(u,y)\neq\phi$. Hence $u\not\models S_j'\longrightarrow\!\!\!\!\!\rightarrow T_j'$. But this contradicts that u is a model of $\Gamma_1$and Γ_2. Therefore $\forall u$:a model of $\Gamma_1$and $\Gamma_2[\bar{\sigma}=\bigcup\pi_1(u^*)]$.

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

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

Lemma 2. Suppose that Γ_1 satisfies $\forall i\leqq k[\phi\varepsilon T_i]$, $\phi\varepsilon\widetilde{S}$ and $\phi\varepsilon\widetilde{T}$. $\Gamma_1,\Gamma_2\models S\Longrightarrow T$ if and only if $\Gamma_1,\Gamma_2\models S_{\Gamma_1}\Longrightarrow T_{\Gamma_1}$.

Proof. ($\Leftarrow$) It follows easily from $\widetilde{S_{\Gamma_1}}\subseteq\widetilde{S}$ and $\widetilde{T_{\Gamma_1}}\subseteq\widetilde{T}$.

($\Rightarrow$) Suppose that $\Gamma_1,\Gamma_2\models S\Longrightarrow T$. Let u be a model of Γ_1 and Γ_2. Since $u\models S\Longrightarrow T$, $\bigcup\pi_1(u^*)\varepsilon\widetilde{S}$. On the other hand, since $u\models\Gamma_1$, $\bigcup\pi_1(u^*)\varepsilon\widetilde{[S_1,\ldots,S_k]_k}$. Hence $\bigcup\pi_1(u^*)\varepsilon\widetilde{S}\cap\widetilde{[S_1,\ldots,S_k]_k}=\widetilde{S_{\Gamma_1}}$. It is similarly showed that $\bigcup\pi_2(u^*)\varepsilon\widetilde{T_{\Gamma_1}}$. 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. We prove only hard direction. Suppose that $\Gamma_1, \Gamma_2 \models S \Longrightarrow T$. Since Γ_1 is normal, $u=\{(x_i,\phi) \mid 1 \leq i \leq k,\ x_i \in \widetilde{S}_i^+\}$ is a model of Γ_1 and Γ_2. Hence $\phi = \bigcup \pi_1(u^*) \in \widetilde{S}$ and $\phi = \bigcup \pi_2(u^*) \in \widetilde{T}$. 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 $x \in [\widetilde{S_1, \ldots, S_k}]_k$ and $y \in [\widetilde{T_1, \ldots, T_k}]_k$, let

$F(x) = \{(\sigma_1, \ldots, \sigma_h) \mid \overline{(\sigma_1, \ldots, \sigma_h)} \in \overline{[\widetilde{S_1, \ldots, S_k}]_k},\ x = \bigcup\{\overline{\sigma}_i \mid 1 \leq i \leq h\} \text{ and } h \leq k\}$,

$F(y) = \{(\rho_1, \ldots, \rho_h) \mid \overline{(\rho_1, \ldots, \rho_h)} \in \overline{[\widetilde{T_1, \ldots, T_k}]_k},\ y = \bigcup\{\overline{\rho}_i \mid 1 \leq i \leq h\} \text{ and } h \leq k\}$.

Since $\Gamma_1, \Gamma_2 \vdash [\widetilde{S_1, \ldots, S_k}]_k \Longrightarrow [\widetilde{T_1, \ldots, T_k}]_k$, 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 $x \notin \widetilde{S}_{\Gamma_1}$ and $y \notin \widetilde{T}_{\Gamma_1}$. Suppose that $x \notin \widetilde{S}_{\Gamma_1}$ and $(\sigma_1, \ldots, \sigma_h) \in F(x)$. Without loss of generality, we assume that $\overline{\sigma}_i \in \widetilde{S}_i$ for every $i \leq h$. Let $x_i = y_i = \phi$ for $h \leq i \leq k$ and $x_i = \overline{\sigma}_i$ for $1 \leq i \leq h$. If there is an $i \leq h$ such that $\widetilde{T}_i^+ = \phi$, 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 $\widetilde{T}_i^+ \neq \phi$ for every $i \leq h$. Pick $y_i \in \widetilde{T}_i^+$ for $1 \leq i \leq h$. Then $\bigcup\{x_i \mid 1 \leq i \leq k\} = \bigcup\{x_i \mid 1 \leq i \leq h\} = \hat{\overline{x}} = x$ and $\{i \mid x_i \neq \phi\} = \{i \mid y_i \neq \phi\}$. Since $\Gamma_1, \Gamma_2 \models S_{\Gamma_1} \Longrightarrow T_{\Gamma_1}$, $\forall u$:a model of Γ_1 and Γ_2 $[\bigcup \pi_1(u^*) \in \widetilde{S}_{\Gamma_1}]$. Therefore $\forall u$:a model of Γ_1 and $\Gamma_2 [\bigcup \pi_1(u^*) \neq \hat{\overline{x}}]$. Hence, by lemma 1, $\exists j \leq \ell\, \exists y \in \widetilde{T}_j^{\prime +}\, \exists J \subseteq \{i \mid x_i \neq \phi\}[\ J \neq \phi,\ y \subseteq \bigcap\{y_i \mid i \in J\},\ \bigcup\{x_i \mid i \in J\} \notin \widetilde{S}_j^{\prime}$ and $\forall i \in \{i \mid x_i \neq \phi\} - J[y \not\subseteq y_i]]$. Without loss of generality, we assume $J = \{1, 2, \ldots, m'\}$. Then $\overline{\langle x_1, \ldots, x_{m'} \rangle_{m'}} = \bigcup\{x_i \mid 1 \leq i \leq m'\} = \bigcup\{x_i \mid i \in J\} \notin \widetilde{S}_j^{\prime}$. Also, $y \in \widetilde{T}_j^{\prime +}$, $y \subseteq y_i$ for $1 \leq i \leq m'$ and $y \not\subseteq y_i$ for $m' < i \leq h$. Hence, by the rules (A_1) and (A_2),

$$\dfrac{\dfrac{S'_j \longrightarrow\!\!\!\!\rightarrow T'_j}{(\hat{x}_{m'+1},\ldots,\hat{x}_h,\hat{x}_1,\ldots,\hat{x}_{m'}) \not\longrightarrow (\hat{y}_{m'+1},\ldots,\hat{y}_h,\hat{y}_1,\ldots,\hat{y}_{m'})}}{\vdots}$$

$$\dfrac{\overline{(\hat{x}_1,\ldots,\hat{x}_h) \not\longrightarrow (\hat{y}_1,\ldots,\hat{y}_h)}}{(\sigma_1,\ldots,\sigma_h) \not\longrightarrow (\hat{y}_1,\ldots,\hat{y}_h)} \quad .$$

Hence $\Gamma_1,\Gamma_2 \vdash (\sigma_1,\ldots,\sigma_h) \not\longrightarrow (\hat{y}_1,\ldots,\hat{y}_h)$ for every $(y_1,\ldots,y_h) \varepsilon \tilde{T}_1^+ \times \cdots \times \tilde{T}_h^+$. 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 $\Gamma_1,\Gamma_2 \vdash ((\ )) \text{———} (\rho_1,\ldots,\rho_h)$.

Remark. If Γ_1 is not good, then let $\Gamma_1^* = \{S_1 \rightarrowtail [<T_1,b_1>_2]_1, \ldots, S_k \rightarrowtail [<T_k,b_k>_2]_1\}$ where $b_1,\ldots,b_k$ are new constant symbols of d-sort. If Γ_1 is normal, 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 $\Gamma_1^*,\Gamma_2 \models S \Longrightarrow T^*$. If Γ_1 is normal, then Γ_1^* is good. Hence, if Γ_1 is normal, then $\Gamma_1,\Gamma_2 \models S \Longrightarrow T$ if and only if $\Gamma_1^*,\Gamma_2 \vdash_{m,n+k} S \longrightarrow T^*$.

Acknowledgement

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

Reference

[1] Hirose,K., Saito,N., Doi,N., et al., "Process-Data Representation", Proc. 3rd US-Japan Computer Conference, pp 225-230, 1978.

[2] Hirose,K., Saito,N., Doi,N., et al., "Specification technique for parallel processing; process-data representation", AFIPS, Conference Proc., vol. 50, pp 407-413, 1981.

[3] Hirose,K. and Takahashi,M., "A Formal System for Specification Analysis of Concurrent Programs", Publ. RIMS, Kyoto Univ., vol 19, pp 911-926, 1983.

[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., No. 16, Springer Verlag, Berlin, 1974.

[5] Aschcroft,E. and Manna,Z., "Formalization of Properties of Parallel Programs", Stanford AI Memo, No. AIM-110, 1970.