Specification analysis of concurrent programs

早川 眞雄 健 (Ken Hirose)
早川 明展 (Makoto Takahashi)

Abstract

A formal system $FL_{m,n}$ is proposed to analyse the specification 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 proposed 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 $\text{FL}_{m,n}$ 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 $\geq k$, which means "at least k out of $\ell$ objects $\{x_1, \ldots, x_\ell\}".$\langle x_1, \ldots, x_\ell \rangle_k$ denotes a set of the subsets of $\{x_1, \ldots, x_\ell\}$ whose cardinality $\geq k$, which means,"at most k out of $\ell$ objects $\{x_1, \ldots, x_\ell\}".$\langle x_1, \ldots, x_\ell \rangle_k \rightarrow Y$ means that the element of $\langle x_1, \ldots, x_\ell \rangle_k$ operates only on the element in $Y$,$\{x_1, \ldots, x_\ell\}_k \rightarrow Y$ means that the element in $Y$ can be operated only by the element in $\{x_1, \ldots, x_\ell\}_k$, and $X \rightarrow Y$ 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:

\[
\begin{align*}
\langle \text{ph1} \rangle_1 \rightarrow [\langle f5, f1 \rangle_2]_1 & \quad \langle \text{ph1}, \text{ph2} \rangle_1 \rightarrow \langle f1 \rangle_1 \\
\langle \text{ph2} \rangle_1 \rightarrow [\langle f1, f2 \rangle_2]_1 & \quad \langle \text{ph2}, \text{ph3} \rangle_1 \rightarrow \langle f2 \rangle_1 \\
\langle \text{ph3} \rangle_1 \rightarrow [\langle f2, f3 \rangle_2]_1 & \quad \langle \text{ph3}, \text{ph4} \rangle_1 \rightarrow \langle f3 \rangle_1 \\
\langle \text{ph4} \rangle_1 \rightarrow [\langle f3, f4 \rangle_2]_1 & \quad \langle \text{ph4}, \text{ph5} \rangle_1 \rightarrow \langle f4 \rangle_1 \\
\langle \text{ph5} \rangle_1 \rightarrow [\langle f4, f5 \rangle_2]_1 & \quad \langle \text{ph5}, \text{ph1} \rangle_1 \rightarrow \langle f5 \rangle_1
\end{align*}
\]

where $\text{ph}k$ ($k=1, \ldots, 5$) represents the philosopher $k$ and $\text{fi}$ ($i=1, \ldots, 5$) represents the folk $i$.

Then, for example, the conclusion $[\text{ph1, \ldots, ph5}]_2 \rightarrow [\langle f5, f1 \rangle_2, \ldots, \langle f4, f5 \rangle_2]_2$ is deducible from (*) in our system.

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

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

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

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

(1) Constant symbols,
   \[ p_1, \ldots, p_m \text{ (p-sort)}, \]
   \[ d_1, \ldots, d_n \text{ (d-sort)}. \]

(2) Function symbols,
   \[ [\ldots,]_k <\ldots,<_k \text{ ($k$-ary, } 0 \leq k \leq \ell, \ell \neq 0), \]
   \[ (\ldots,) \text{ (q-ary, } 1 \leq q), \]
   \[ ((\ldots,)) \text{ (r-ary, } 0 \leq r). \]

(3) Predicate symbols,
   \[ \rightarrow, \rightarrow, \rightarrow, \rightarrow, \rightarrow. \]

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

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

(ii) If $S_1, \ldots, S_\ell$ are p-terms (d-terms), then $[S_1, \ldots, S_\ell]_k$
    and $<S_1, \ldots, S_\ell>_k$ 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) $p_1, \ldots, p_m \ (d_1, \ldots, d_n)$ are p-A-terms (d-A-terms).

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

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

(vi) If $(\ldots)$ is a 0-ary function symbol, then $(\ldots)$ is a p-C-term and a d-C-term.
(vi) If \( u_1, \ldots, u_\ell \) (\( \tau_1, \ldots, \tau_\ell \)) are p-B-terms (d-B-terms), then
\[
((u_1, \ldots, u_\ell)) \cdot \((\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, \( \sigma \) for p-A-terms, \( \rho \) for d-A-terms, \( \mu \) for p-B-terms, \( \tau \) for d-B-terms, \( \alpha \) for p-C-terms and \( \beta \) for d-C-terms.

\[ S \rightarrow T, \; S \rightarrow T, \; S \rightarrow T, \; \mu \rightarrow \tau, \; \alpha \rightarrow \tau, \]
\[ \mu \rightarrow \beta \] and \( \alpha \rightarrow \beta \) are formulas.

Let \( X \) be a set, \( X_1, \ldots, X_\ell \) be subsets of \( P(X) \) and \( k \leq \ell \). We define \( {\langle X_1, \ldots, X_\ell \rangle}_k \) and \( [X_1, \ldots, X_\ell]_k \) as follows:
\[
{\langle X_1, \ldots, X_\ell \rangle}_k = \{ \bigcup_{i \in I} X_i \mid I \subseteq \{1, \ldots, \ell\}, \#I \leq k \text{ and } x_i \in X_i \text{ for every } i \in I \},
\]
\[
[X_1, \ldots, X_\ell]_k = \{ \bigcup_{i \in I} X_i \mid I \subseteq \{1, \ldots, \ell\}, \#I \leq k \text{ and } x_i \in X_i \text{ for every } i \in I \}.
\]
We define the canonical interpretation \( \gamma , - \) of terms as follows:

(i) If \( a \) is a constant symbol, then \( \gamma (a) = \{ a \} \) and \( \overline{a} = \{ a \} \).

(ii) \( \langle S_1, \ldots, S_\ell \rangle_k = \langle \overline{S_1}, \ldots, \overline{S_\ell} \rangle_k \) and \( [S_1, \ldots, S_\ell]_k = [\overline{S_1}, \ldots, \overline{S_\ell}]_k \).

The canonical interpretation \( \gamma \) of d-terms is similarly defined.

(iii) \( \langle \sigma_1, \ldots, \sigma_\ell \rangle_k = \{ \sigma_i \mid 1 \leq i \leq \ell \} \) , \( (\sigma_1, \ldots, \sigma_\ell) = (\overline{\sigma_1}, \ldots, \overline{\sigma_\ell}) \) and
\( \langle (u_1, \ldots, u_\ell) \rangle = \{ u_1, \ldots, u_\ell \} \). The canonical interpretation \( \gamma \) of d-A-terms, d-B-terms and d-C-terms are similarly defined.

If \( x \in \{ p_1, \ldots, p_m \} \) (\( y \in \{ d_1, \ldots, d_n \} \)), then we denote by \( \widehat{x} (\widehat{y}) \) one of the p-A-terms (d-A-terms) which satisfies \( \gamma (\widehat{x}) = x \) (\( \gamma (\widehat{y}) = y \)).

We denote by \( \alpha_1 \vdash \alpha_2 \) the p-C-term \( ((u_1^1, \ldots, u_\ell^1), (\tau_1, \ldots, \tau_\ell)) \) where \( \alpha_1 = (\langle u_1, \ldots, u_\ell \rangle) \) and \( \alpha_2 = (\langle \tau_1, \ldots, \tau_\ell \rangle) \). If \( \gamma (\sigma_1, \ldots, \sigma_\ell) \), then \( \gamma (\sigma) \) is the p-A-term \( \langle \sigma_1, \ldots, \sigma_\ell \rangle \). We denote by \( S_1 \times \cdots \times S_\ell \) one of the p-C-terms which satisfies \( \gamma (\overline{S_1} \times \cdots \times \overline{S_\ell}) = \gamma (\widehat{x} \times \cdots \times \widehat{x}) \) and by \( [S_1, \ldots, S_\ell]_k \) one of the p-C-terms which satisfies
\[
[S_1, \ldots, S_\ell]_k = \bigcup \{ [S_{j_1} \times \cdots \times S_{j_q}]_k \mid 1 \leq j_1 < j_2 < \cdots < j_q \leq \ell, \; q \leq k \}.
\]
\( \beta_{1} \rightarrow \beta_{2} \), \( \tau^{0}, T_{1} \cdots T_{k} \) and \( [T_{1}, \ldots, T_{k}]_{k} \) are similarly defined.

Let \( \Gamma_{1} = \{ S_{1} \rightarrow T_{1}, \ldots, S_{k} \rightarrow T_{k} \} \) and \( \Gamma_{2} = \{ S_{1}^{l} \rightarrow T_{1}^{l}, \ldots, S_{k}^{l} \rightarrow T_{k}^{l} \} \). We say that \( S \rightarrow T \) is deducible from \( \Gamma_{1} \) and \( \Gamma_{2} \)

\[(\Gamma_{1}, \Gamma_{2}, m, n, S \rightarrow T) \] if \( S \rightarrow T \) is provable from \( \Gamma_{1}, \Gamma_{2} \) and \( [S_{1}, \ldots, S_{k}]_{k} \rightarrow [T_{1}, \ldots, T_{k}]_{k} \) by the following inference rules.

\[ S \rightarrow T \]

\[ (A_{1}) \]

\[ (\sigma_{1}^{0}, \ldots, \sigma_{k}^{0}, \sigma_{1}^{l}, \ldots, \sigma_{k}^{l}) \rightarrow (\rho_{1}^{0}, \ldots, \rho_{k}^{0}, \rho_{1}^{l}, \ldots, \rho_{k}^{l}) \]

where \( \langle \sigma_{1}^{0}, \ldots, \sigma_{k}^{0}, \sigma_{1}^{l}, \ldots, \sigma_{k}^{l} \rangle \) and there exists a \( \tilde{\sigma} \in T' \) such that \( \tilde{\sigma} \in \tilde{\sigma}_{i} \) for every \( i \leq k \) and \( \tilde{\sigma} \in \tilde{\sigma}_{j}^{0} \) for every \( j \leq k \).

\[ (A_{2}) \]

\[ (\sigma_{1}, \ldots, \sigma_{i}, \ldots, \sigma_{j}, \ldots, \sigma_{k}^{0}, \sigma_{1}^{l}, \ldots, \sigma_{k}^{l}) \rightarrow (\rho_{1}, \ldots, \rho_{i}, \ldots, \rho_{j}, \ldots, \rho_{k}^{0}, \rho_{1}^{l}, \ldots, \rho_{k}^{l}) \]

\[ (\sigma_{1}, \ldots, \sigma_{i}^{l}, \ldots, \sigma_{j}^{l}, \sigma_{1}^{l}, \ldots, \sigma_{k}^{l}) \rightarrow (\rho_{1}, \ldots, \rho_{i}^{l}, \ldots, \rho_{j}^{l}, \rho_{1}^{l}, \ldots, \rho_{k}^{l}) \]

where \( \sigma_{i} = \sigma_{i}^{0} \), \( \sigma_{j} = \sigma_{j}^{l} \), \( \rho_{i} = \rho_{i}^{0} \) and \( \rho_{j} = \rho_{j}^{l} \).

\[ (B_{1}) \]

\[ S_{1}^{0} \rightarrow T_{1}^{0}, \ldots, S_{k}^{0} \rightarrow T_{k}^{0} \]

\[ (\sigma_{1}, \ldots, \sigma_{k}^{0}) \rightarrow T_{1}^{0} \cdots T_{k}^{0} \]

where \( \sigma_{i} \in T_{i}^{0} \) for every \( i \leq k' \) and \( S_{i} \rightarrow T_{i}^{0} \) are all different formulas.

\[ (B_{2}) \]

\[ \mu \rightarrow (\tau_{1}, \ldots, \tau_{i}, \ldots, \tau_{k}), \mu \rightarrow \tau_{i} \]

\[ (\mu_{i}, \ldots, \mu_{i-1}, \mu_{i+1}, \ldots, \mu_{k}) \rightarrow \tau \]

\[ (C_{1}) \]

\[ S_{1}^{0} \rightarrow T_{1}^{0}, \ldots, S_{k}^{0} \rightarrow T_{k}^{0} \]

\[ S_{1}^{0} \cdots S_{k}^{0} \rightarrow (\rho_{1}, \ldots, \rho_{k}) \]

where \( \rho_{i} \in T_{i}^{0} \) for every \( i \leq k' \) and \( S_{i} \rightarrow T_{i}^{0} \) are all different formulas.

\[ (C_{2}) \]

\[ (\mu_{1}, \ldots, \mu_{i}, \ldots, \mu_{k}) \rightarrow \tau, \mu_{i} \rightarrow \tau \]

\[ (\mu_{1}, \ldots, \mu_{i-1}, \mu_{i+1}, \ldots, \mu_{k}) \rightarrow \tau \]

\[ (D_{1}) \]

\[ (\mu_{1}, \ldots, \mu_{i}, \ldots, \mu_{k}) \rightarrow \beta, \mu_{i} \rightarrow (\mu) \]

\[ (\mu_{1}, \ldots, \mu_{i-1}, \mu_{i+1}, \ldots, \mu_{k}) \rightarrow \beta \]
3. Completeness theorem

In this section, we show that the completeness theorem for $\text{FL}_{m,n}$ 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:

\begin{align*}
    u^* &= \{(x, y) \epsilon u \mid y \neq \emptyset\}, \\
    \pi_1(u) &= \{x \mid (x, y) \epsilon u \text{ for some } y\}, \\
    \pi_2(u) &= \{y \mid (x, y) \epsilon 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') \epsilon u \text{ for some } y' \supseteq y\}.
\end{align*}
Let $P = \{p_1, \ldots, p_m\}$, $D = \{d_1, \ldots, d_n\}$ and $u$ be a nonempty subset of $P(D)^* \times P(D)$. We define the relation $u \models \phi (u \text{ satisfies } \phi)$ for every formula $\phi$ as follows:

(1) $u \models S \rightarrow T$ if and only if $S^+ = \phi$ or $\left[ \forall (x, y) \in u [x \in S \text{ implies } y \in T], \exists (x, y) \in u [x \in S \text{ and } y \in T] \right.$ and \left.$\forall (x, y), (x', y') \in u [x, x' \in S \text{ and } y, y' \in T \text{ imply } \left[ [x = x' \text{ and } y = y'] \text{ or } y = \phi \text{ or } y' = \phi \right]] \right]$. 

(2) $u \models S \rightarrow T$ if and only if $\forall y \in T^+ [A(u, y) \neq \phi \text{ implies } A(u, y) \in S]$. 

(3) $u \models (\sigma_1, \ldots, \sigma_k) \rightarrow (\rho_1, \ldots, \rho_k)$ if and only if $u \neq \{(\sigma_1, \sigma_1'), \ldots, (\sigma_k, \sigma_k')\}$. 

(4) $u \models (\sigma_1, \ldots, \sigma_k) \rightarrow (\beta)$ if and only if $\forall y_1, \ldots, y_k \in P(D) \left[ u^* = \{(\sigma_1, y_1'), \ldots, (\sigma_k, y_k') \text{ implies } (y_1, \ldots, y_k) \in \beta \right]$. 

(5) $u \models \alpha \rightarrow (\rho_1, \ldots, \rho_k)$ if and only if $\forall x_1, \ldots, x_k \in P(D)^* [u^* = \{(x_1, \rho_1'), \ldots, (x_k, \rho_k') \} \text{ implies } (x_1, \ldots, x_k) \in \alpha]$. 

(6) $u \models \alpha \rightarrow \beta$ if and only if $\pi_1^*(u^*) = \phi$ or $[\pi_1^*(u^*) \cap \overline{\alpha} \neq \phi \text{ and } \pi_2^*(u^*) \cap \overline{\beta} \neq \phi]$. 

(7) $u \models S \rightarrow T$ if and only if $\bigcup \pi_1^*(u^*) \in S^\dagger$ and $\bigcup \pi_2^*(u^*) \in T^\dagger$. 

Let $\Gamma_1 = \{S_1 \rightarrow T_1, \ldots, S_k \rightarrow T_k\}$ and $\Gamma_2 = \{S'_1 \rightarrow T'_1, \ldots, S'_l \rightarrow T'_l\}$. $u$ is said to be a (standard) model of $\Gamma_1$ and $\Gamma_2$ if and only if $u \models \phi$ for every $\phi \in \Gamma_1 \cup \Gamma_2$ and $\forall (x, y) \in u \exists i \leq k [x \in S_i \text{ and } y \in T_i]$. We write $\Gamma_1, \Gamma_2 \models \phi$ if every model of $\Gamma_1$ and $\Gamma_2$ satisfies $\phi$. 

- 7 -
We say that $\Gamma_1$ is normal if $\forall i \leq k [ S_i^+ \neq \emptyset$ and $\phi \epsilon T_i^+]$ and
$
\forall i,j \leq k [ i \neq j \text{ implies } S_i^+ / S_j^+ = \emptyset ].$ Also, we say that $\Gamma_1$ is good if $\Gamma_1$ is normal and $\forall i,j \leq k [ i \neq j \text{ implies } T_i^+ / T_j^+ = \emptyset ].$

Lemma 1. Suppose that $\Gamma_1$ is normal.

(i) $\forall u$: a model of $\Gamma_1$ and $\Gamma_2 [ \emptyset \neq \cup \pi_1(u^*) ]$ if and only if

$\forall (x_1, \ldots, x_k) \epsilon [\tilde{S}_1]_1 \times \cdots \times [\tilde{S}_k]_1 \forall (y_1, \ldots, y_k) \epsilon \tilde{T}_1 \times \cdots \times \tilde{T}_k$

$\emptyset = \emptyset \cup \{ x_i | 1 \leq i \leq k \} \text{ and } \{ i | x_i \neq \phi \} = \{ i | y_i \neq \phi \} \text{ imply } \exists j \subseteq \emptyset \exists y \epsilon \tilde{T}_j$

$\emptyset \subseteq \{ i | x_i \neq \phi \} \cup \{ j | y_j \neq \phi \} \subseteq \{ i | x_i \neq \phi \}$

$\forall x \epsilon \{ i | x_i \neq \phi \} - J \{ y \neq y_i \} \}$.

(ii) In (i), we can replace $\emptyset \neq \emptyset \cup \pi_1(u^*)$ by $\emptyset \neq \emptyset \cup \pi_2(u^*)$ and

$\emptyset = \emptyset \cup \{ x_i | 1 \leq i \leq k \} \text{ by } \emptyset = \emptyset \cup \{ y_i | 1 \leq i \leq k \}$.

Proof. $(\Rightarrow)$ Suppose that

$\exists (x_1, \ldots, x_k) \epsilon [\tilde{S}_1]_1 \times \cdots \times [\tilde{S}_k]_1 \exists (y_1, \ldots, y_k) \epsilon \tilde{T}_1 \times \cdots \times \tilde{T}_k$

$\emptyset = \emptyset \cup \{ x_i | 1 \leq i \leq k \}, \{ i | x_i \neq \phi \} = \{ i | y_i \neq \phi \} \text{ and } \forall x \subseteq \emptyset \exists y \epsilon \tilde{T}_j\quad J \subseteq \{ i | x_i \neq \phi \}$

$\forall x \epsilon \{ i | x_i \neq \phi \} - J \{ y \neq y_i \} \}$.

Without loss of generality, we can assume that

$\{ i | x_i \neq \phi \} = \{ 1, 2, \ldots, k' \}$. Pick $x_i^+ \epsilon \tilde{S}_i^+$ for $k' \leq i \leq k$. Let

$u = \{ (x_i, y_i) | 1 \leq i \leq k' \} \cup \{ (x_i^+, \phi) | k' < i \leq k \}$. Since $\Gamma_1$ is normal, $u \subseteq \Gamma_1$.

Suppose that $1 \leq j \leq l, y \epsilon \tilde{T}_j$ and $A(u, y) \neq \emptyset$. Let $J = \{ i | y \subseteq y_i \}$. Since $y \neq \phi$ and $A(u, y) \neq \emptyset$, $J \subseteq \{ i | x_i \neq \phi \}$ and $J \neq \emptyset$. It is clear that

$y \subseteq \emptyset \{ y_i | i \epsilon J \}$. Hence, by the assumption, $A(u, y) = \emptyset \{ x_i \ | \ y \neq y_i \} = \{ x_i \ | \ i \epsilon J \} \epsilon \tilde{S}_j$. So $u \subseteq \Gamma_2$. Hence $u$ is a model of $\Gamma_1$ and $\Gamma_2$ by the definition of $u$. $\pi_1(u^*) = \{ x_i, l \ | \ i \epsilon k' \} = \{ x_i, l \ | \ i \epsilon k \} = \emptyset$. But this contradicts our assumption that $\forall u$: a model of $\Gamma_1$ and $\Gamma_2 [ \emptyset \neq \emptyset \cup \pi_1(u^*) ]$.

- 8 -
(\_\_\_\_\_\_\_) Suppose that $\exists u: a$ model of $\Gamma_1$ and $\Gamma_2[\sigma = \bigcup \pi_1(u^*)]$. Without loss of generality, since $u$ is a model of $\Gamma_1$ and $\Gamma_2$, we can assume that $u^* = \{(x_1, y_1), \ldots, (x_k, y_k)\}$ and $(x_i, y_i) \in \tilde{S} \times \tilde{T}$ for every $i \leq k$. Let $x_i = y_i = \phi$ for $k' < i \leq k$. \bigcup \{x_i | 1 \leq i \leq k\} = \bigcup \{x_i | 1 \leq i \leq k'\} = \bigcup \{x_i | i \leq k'\} = \bigcup \{x_i | i \leq k\} = \bigcup \{x_i | i \leq k\}$ for $k' < i \leq k$. Hence, by our assumption, $\exists j \exists z \exists T_j \exists J \subseteq \{i | x_i \neq \phi\} [J \neq \phi, y \subseteq \bigcap \{y_i | i \in J\}$, $\bigcup \{x_i | i \in J\} \neq \tilde{S}_j$ and $\forall i \in \{i | x_i \neq \phi\} - J [y \not\subseteq y_i]$. Therefore $A(u, y) = \bigcup \{x_i | i \in J\} \neq \tilde{S}_j$. Since $J \neq \phi$, $A(u, y) \neq \phi$. Hence $u \not\in S_j \rightarrow T_j$. But this contradicts that $u$ is a model of $\Gamma_1$ and $\Gamma_2$. Therefore $\forall u: a$ model of $\Gamma_1$ and $\Gamma_2[\sigma = \bigcup \pi_1(u^*)]$.

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

It is easy to show that if $\phi \in \tilde{S}$, then there is a $S'$ such that $\tilde{S}' = \tilde{S} \setminus \{S_1', \ldots, S_k'\}_k$. So let $S_1'$ be one of the $p$-terms which satisfies $S_1' = \tilde{S} \setminus \{S_1, \ldots, S_k\}_k$ for every $S$ such that $\phi \in \tilde{S}$. $T_1$ is defined similarly.

Lemma 2. Suppose that $\Gamma_1$ satisfies $\forall i \leq k[\phi \in T_i]$, $\phi \in \tilde{S}$ and $\phi \in \tilde{T}$. $\Gamma_1, \Gamma_2 \models S \rightarrow T$ if and only if $\Gamma_1, \Gamma_2 \models S \rightarrow T$. $T$.

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

(\_\_\_\_\_\_\_) Suppose that $\Gamma_1, \Gamma_2 \models S \rightarrow T$. Let $u$ be a model of $\Gamma_1$ and $\Gamma_2$. Since $u \models S \rightarrow T$, $\bigcup \pi_1(u^*) \in \tilde{S}$. On the other hand, since $u \models \Gamma_1$, $\bigcup \pi_1(u^*) \in \{S_1, \ldots, S_k\}_k$. Hence $\bigcup \pi_1(u^*) \in \tilde{S} \cap \{S_1, \ldots, S_k\}_k = \tilde{S}_1$. It is similarly showed that $\bigcup \pi_2(u^*) \in \tilde{T}_1$. Therefore $\Gamma_1, \Gamma_2 \models S_1 \rightarrow T_1$.
Theorem (Completeness theorem). Suppose that $\Gamma_1$ is good.

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

Proof. We prove only hard direction. Suppose that $\Gamma_1, \Gamma_2 \models S \rightarrow T$.

Since $\Gamma_1$ is normal, $u = \{ (x_i, \phi) | 1 \leq i \leq k, x_i \in S_i^+ \}$ is a model of $\Gamma_1$ and $\Gamma_2$. Hence $\phi = \bigcup \pi_1(u^*) \in S$ and $\phi = \bigcup \pi_2(u^*) \in T$. Hence, by virtue of lemma 2, $\Gamma_1, \Gamma_2 \models S \rightarrow T_{\Gamma_1}$. We try to show that

$\Gamma_1, \Gamma_2 \models S \rightarrow T_{\Gamma_1}$. If we can show it, then $\Gamma_1, \Gamma_2 \models S \rightarrow T$ by the inference rule (F). For $x \in [S_1, \ldots, S_k]_k$ and $y \in [T_1, \ldots, T_k]_k$, let

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

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

Since $\Gamma_1, \Gamma_2 \models [S_1, \ldots, S_k]_k \rightarrow [T_1, \ldots, T_k]_k$, it is enough to show that $\Gamma_1, \Gamma_2 \models (\sigma_1, \ldots, \sigma_h) \rightarrow (\rho_1, \ldots, \rho_h)$ for every $(\sigma_1, \ldots, \sigma_h) \in F(x)$ and $(\rho_1, \ldots, \rho_h) \in F(y)$ where $x \not\in S_{\Gamma_1}$ and $y \not\in T_{\Gamma_1}$. Suppose that $x \not\in S_{\Gamma_1}$ and $(\sigma_1, \ldots, \sigma_h) \in F(x)$. Without loss of generality, we assume that $\sigma_i \in S_i^+$ for every $i \leq h$. Let $x_i = y_i = \phi$ for $h < i \leq k$ and $x_i = \sigma_i$ for $1 \leq i \leq h$. If there is an $i \leq h$ such that $\sigma_i = \phi$, then by the rule (B_1)

$$S_1 \rightarrow T_1, \ldots, S_h \rightarrow T_h$$

$$\sigma_1, \ldots, \sigma_h \rightarrow (\sigma_1, \ldots, \sigma_h)$$

Hence we assume that $\sigma_i \neq \phi$ for every $i \leq h$. Pick $y_i \in S_i^+$ for $1 \leq i \leq h$.

Then $\bigcup \{ x_i \mid 1 \leq i \leq k \} = \bigcup \{ y_i \mid 1 \leq i \leq h \} = S = x$ and $\{ i \mid x_i \neq \phi \} = \{ i \mid y_i \neq \phi \}$.

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

Therefore $\forall u : a$ model of $\Gamma_1$ and $\Gamma_2 \models [\bigcup \pi_1(u^*) \in \bigcup [S_i^+]_{\Gamma_1}]$. Hence, by lemma 1, $\exists y \in \bigcup S_j, y \in T_{\Gamma_1}^+, \exists J \subseteq \{ i \mid x_i \neq \phi \} \{ J \neq \phi, y \subseteq \bigcup \{ i \mid y_i \neq \phi \}, \bigcup \{ i \mid y_i \neq \phi \} \neq J \neq \bigcup \{ i \mid y_i \neq \phi \} \}$. Without loss of generality, we assume $J = \{ 1, 2, \ldots, m' \}$. Then $\langle x_1, \ldots, x_m, y \rangle = \{ i \mid x_i \mid 1 \leq i \leq m' \}$

$\bigcup \{ i \mid y_i \neq \phi \} \neq J \neq \bigcup \{ i \mid y_i \neq \phi \}$. Also, $y \in T_{\Gamma_1}^+, y \subseteq y_i$ for $1 \leq i \leq m'$ and $y \neq y_i$ for $m' < i \leq h$. Hence, by the rules (A_1) and (A_2),

- 10 -
Hence $\Gamma_1, \Gamma_2 \vdash (\sigma_1, \ldots, \sigma_h) \rightarrow (\hat{y}_1, \ldots, \hat{y}_h)$ for every $(y_1, \ldots, y_h) \in T_{1}^+ \times \cdots \times T_{h}^+$. Therefore, by the rules $(B_1)$, $(B_2)$ and $(A_2)$, $\Gamma_1, \Gamma_2 \vdash (\sigma_1, \ldots, \sigma_h) \rightarrow (())$. It is similarly proved that $\Gamma_1, \Gamma_2 \vdash (()) \rightarrow (\rho_1, \ldots, \rho_h)$.

Remark. If $\Gamma_1$ is not good, then let $\Gamma^* = \{S_1 \rightarrow [T_1, b_1 \, 2]_1, \ldots, S_k \rightarrow [T_k, b_k \, 2]_1\}$ where $b_1, \ldots, b_k$ are new constant symbols of $d$-sort. If $\Gamma_1$ is normal, then for every $T$, there is a $d$-term $T^*$ in $L_{m,n+k}$ such that $\Gamma_1, \Gamma_2 \vdash S \rightarrow T$ if and only if $\Gamma^*, \Gamma_2 \vdash S \rightarrow T^*$. If $\Gamma_1$ is normal, then $\Gamma^*$ is good. Hence, if $\Gamma_1$ is normal, then $\Gamma^*_1, \Gamma_2 \vdash S \rightarrow T$ if and only if $\Gamma^*_1, \Gamma_2 \vdash_{m,n+k} S \rightarrow T^*$.

Acknowledgement

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

"Process-Data Representation", Proc. 3rd US-Japan

"Specification technique for parallel processing;
process-data representation", AFIPS, Conference Proc.,

[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

[5] Aschcroft, E. and Manna, Z.,
"Formalization of Properties of Parallel Programs",