修論の進捗状況

斉藤 新 [shin]

2001. 5. 18

1 Polymorphic Deadlock-free Process Calculus

1.1 syntax

ネストした tuple を扱うために、tuple 型を導入してチャネルは monadic なものだけに制限する。そのかわり tuple 型の値から各成分を取り出す構文を導入する。

多相型に関しては、Turner のように、existential な多相型を *CML* の多相型のかわりに用いる。明示的型付けをするため、受信チャネルは、型に関する引数を持つ。また送信チャネルは値と同時に型も送る。

Definition 1 (usage). Usage の syntax は以下の通り。v は usage 変数を表すメタ変数。

$$U, V, W, \ldots ::= 0 \mid v \mid O_a.U \mid I_a.U \mid (U_1 \| U_2) \mid U_1 \sqcap U_2 \mid \mu v.U \mid *U$$

Definition 2 (type). ネストした tuple を許すためにレコード型を用意してチャネル通信を monadic なものに限定する。

τ	(type)	::=	α	(type variable)
		$\mid$	$bool$	(boolean type)
		$\mid$	int	(integer type)
		$\mid$	$\{\tau_1, \ldots, \tau_n\} \quad (n \geq 0)$	(record type)
		$\mid$	$[\alpha_1, \ldots, \alpha_m; \tau]^t/U \quad (m \geq 0)$	(polymorphic channel type)

channel において各 α_i は相異なるとする。省略して $[\tilde{\alpha}; \tau]^t/U$ と書いたりする。$i = 0$ なら $[\tau]^t/U$ と書くこともある。

Definition 3 (process). ここでは通信を monadic なものに限定したかわりに、record value から値を取り出す構文を導入する。これもパターンを使って複雑なものにできるが、現在のところは単純な形にしておく。

P, Q	(process)	::=	$\mathbf{0} \mid G \mid (P \mid Q) \mid (\nu x : \tau)P$
			$\mid$ **if** v **then** P **else** $Q \mid F + G \mid *G$
			$\mid$ **match** $\{x_1 : \tau_1, \ldots, x_m : \tau_m\} = v$ **in** P
F, G	(guarded process)	::=	$x!^a[\tilde{\sigma}; v].P \mid x?^a[\tilde{\alpha}; y : \tau].P$
v	(value)	::=	$b \mid i \mid r \mid x$
b	(boolean)	::=	true $\mid$ false
i	(integer)	::=	$0 \mid 1 \mid \cdots$
r	(record)	::=	$\{v_1, \ldots, v_j\} \qquad (j \geq 0)$
x	(variable)	::=	$x, y, z, \ldots$

上の match 文において、レコードから値を取り出した後は v は使えない。各 x_i は相異なるとする。またとりあえず choice を入れてある。

Example 1. Pair の中身を入れ替える関数 *swap* の例。

$$\begin{array}{l}(\nu\, swap : [\alpha, \beta; \{\{\alpha, \beta\}, [\{\beta, \alpha\}]^u/O\}]^t/(*I \,\|\, O))(\\ \quad *swap?[\alpha, \beta; x : \{\{\alpha, \beta\}, [\{\beta, \alpha\}]^u/O\}]. \\ \qquad \textbf{match}\ \{p : \{\alpha, \beta\}, s : [\{\beta, \alpha\}]^u/O\} = x\ \textbf{in} \\ \qquad\quad \textbf{match}\ \{y : \alpha, z : \beta\} = p\ \textbf{in} \\ \qquad\qquad s![\{z, y\}].\mathbf{0} \\ \mid \\ \quad (\nu r : [\{bool, int\}]^u/(O \,\|\, I))(\\ \qquad swap!^{\mathbf{c}}[int, bool; \{\{3, \text{true}\}, r\}]. \\ \qquad\quad r?^{\mathbf{c}}[ans : \{bool, int\}].Q))\end{array}$$

1.2 Operational Semantics

Definition 4 (Structual Congruence). 後回し。

Definition 5 (reduction label). Reduction label は以下のとおり。

$$l ::= \varepsilon \mid x$$

ε は外部から観測できない通信による reduction を表す。

Definition 6 (reduction relation). reduction relation を LTS で表す。

$$x!^a[\tilde{\sigma}; v].P \mid x?^{a'}[\tilde{\alpha}; y : \tau].Q \xrightarrow{x} P \mid [\tilde{\sigma}/\tilde{\alpha}][v/y]Q \tag{R-Com}$$

$$\frac{P \xrightarrow{l} Q}{P \mid R \xrightarrow{l} Q \mid R} \tag{R-Par}$$

$$\frac{P \xrightarrow{l} P'}{P + Q \xrightarrow{l} P'} \tag{R-Sum}$$

$$\frac{P \mid *P \mid Q \xrightarrow{l} R}{*P \mid Q \xrightarrow{l} R} \tag{R-Rep}$$

$$\frac{P \xrightarrow{x} Q}{(\nu x)P \xrightarrow{\varepsilon} (\nu x)Q} \tag{R-New1}$$

$$\frac{P \xrightarrow{l} Q \qquad l \neq x}{(\nu x)P \xrightarrow{l} (\nu x)Q} \tag{R-New2}$$

$$\textbf{if}\ \text{true}\ \textbf{then}\ P\ \textbf{else}\ Q \xrightarrow{\varepsilon} P, \qquad \textbf{if}\ \text{false}\ \textbf{then}\ P\ \textbf{else}\ Q \xrightarrow{\varepsilon} Q \tag{R-If}$$

$$\textbf{match}\ \{x_1, \ldots, x_i\} = \{v_1, \ldots, v_i\}\ \textbf{in}\ P \xrightarrow{\varepsilon} [\tilde{v}/\tilde{x}]P \tag{R-Match}$$

$$\frac{P \equiv P' \qquad P' \xrightarrow{l} Q' \qquad Q' \equiv Q}{P \xrightarrow{l} Q} \tag{R-Cong}$$

Example 2. 例 1 のプロセス P の reduction は以下のように進む。

$$
\begin{aligned}
&P \equiv \\
&\quad (\nu\, swap : [\alpha,\beta;\{\{\alpha,\beta\},[\{\beta,\alpha\}]^u/O\}]^t/(*I \parallel O))(\\
&\qquad \underline{*swap?[\alpha,\beta;x:\{\{\alpha,\beta\},[\{\beta,\alpha\}]^u/O\}].} \\
&\qquad\quad \mathbf{match}\ \{p:\{\alpha,\beta\}, s:[\{\beta,\alpha\}]^u/O\} = x\ \mathbf{in} \\
&\qquad\qquad \mathbf{match}\ \{y:\alpha, z:\beta\} = p\ \mathbf{in} \\
&\qquad\qquad\quad s![\{z,y\}].\mathbf{0} \\
&\qquad\quad | \\
&\qquad\quad (\nu r : [\{bool,int\}]^u/(O \parallel I))(\\
&\qquad\qquad \underline{swap!^{\mathbf{c}}[int,bool;\{\{3,\mathrm{true}\},r\}].} \\
&\qquad\qquad\quad r?^{\mathbf{c}}[ans:\{bool,int\}].Q)) \\
&\to \\
&\quad (\nu\, swap:\tau)(\\
&\qquad *swap?[\alpha,\beta;x:\{\{\alpha,\beta\},[\{\beta,\alpha\}]^u/O\}]. \ldots \\
&\qquad | \\
&\qquad (\nu r:\tau')(\\
&\qquad\quad \underline{\mathbf{match}\ \{p:\{int,bool\}, s:[\{bool,int\}]^u/O\} = \{\{3,\mathrm{true}\},r\}\ \mathbf{in}} \\
&\qquad\qquad \mathbf{match}\ \{y:int, z:bool\} = p\ \mathbf{in} \\
&\qquad\qquad\quad s![\{z,y\}].\mathbf{0} \\
&\qquad\quad | \\
&\qquad\quad r?^{\mathbf{c}}[ans:\{bool,int\}].Q)) \\
&\to \\
&\quad (\nu\, swap:\tau)(\\
&\qquad *swap?[\alpha,\beta;x:\{\{\alpha,\beta\},[\{\beta,\alpha\}]^u/O\}]. \ldots \\
&\qquad | \\
&\qquad (\nu r:\tau')(\\
&\qquad\quad \underline{\mathbf{match}\ \{y:int, z:bool\} = \{3,\mathrm{true}\}\ \mathbf{in}} \\
&\qquad\qquad r![\{z,y\}].\mathbf{0} \\
&\qquad\quad | \\
&\qquad\quad r?^{\mathbf{c}}[ans:\{bool,int\}].Q)) \\
&\to \\
&\quad (\nu\, swap:\tau)(\\
&\qquad *swap?[\alpha,\beta;x:\{\{\alpha,\beta\},[\{\beta,\alpha\}]^u/O\}]. \ldots \\
&\qquad | \\
&\qquad (\nu r:\tau')(\\
&\qquad\quad \underline{r![\{\mathrm{true},3\}]}.\mathbf{0} \\
&\qquad\quad | \\
&\qquad\quad \underline{r?^{\mathbf{c}}[ans:\{bool,int\}]}.Q)) \\
&\to \\
&\quad (\nu\, swap:\tau)(\\
&\qquad *swap?[\alpha,\beta;x:\{\{\alpha,\beta\},[\{\beta,\alpha\}]^u/O\}]. \ldots \\
&\qquad | \\
&\qquad [\{\mathrm{true},3\}/ans]\,Q)
\end{aligned}
$$

2 Type System

型判定式は

1. プロセス P が型環境 Γ と time tag 関係 $\mathcal{T}$ のもとで正しく型付けされる

$$\Gamma;\mathcal{T} \vdash P$$

2. 値 v が型環境 Γ のもとで型 τ を持つ

$$\Gamma \vdash_T v : \tau$$

の 2 種類からなる。

推論規則についても match 文と多相型に関して改良する。型環境 Γ とは

$$\Gamma ::= \emptyset \mid \Gamma, x:\tau$$

で定義されるもののうち、もしあれば $\Gamma(\mathrm{true}) = bool$, $\Gamma(\mathrm{false}) = bool$, $\Gamma(i) = int$ となっているもの。

2.1 Typing rules

Definition 7 (型に関する加算).

$$
\begin{aligned}
bool + bool &\triangleq bool \\
int + int &\triangleq int \\
\{\tau_1,\tau_2,\ldots,\tau_n\} + \{\tau'_1,\tau'_2,\ldots,\tau'_n\} &\triangleq \{\tau_1+\tau'_1,\ldots,\tau_n+\tau'_n\} \\
[\tilde{\alpha};\tau]^t/U_1 + [\tilde{\alpha};\tau]^t/U_2 &\triangleq [\tilde{\alpha};\tau]^t/(U_1 \parallel U_2)
\end{aligned}
$$

Definition 8 (型の無限コピー).

$$
\begin{aligned}
*bool &\triangleq bool \\
*int &\triangleq int \\
\{\tau_1,\tau_2,\ldots,\tau_n\} &\triangleq \{\tau_1,*\tau_2,\ldots,*\tau_n\} \\
*([\alpha;\tau]^t/U) &\triangleq [\alpha;\tau]^t/*U
\end{aligned}
$$

Definition 9 (レコードに関する型環境の展開).

$$
\begin{aligned}
flat(\{v_1,\ldots,v_n\}:\{\tau_1,\ldots,\tau_n\}) &\triangleq flat(v_1:\tau_1) + \cdots + flat(v_n:\tau_n) \\
flat(x:\tau) &\triangleq x:\tau \qquad \text{(otherwise)}
\end{aligned}
$$

これを用いると、

$$flat(\{\{3,\mathrm{true}\},r\}:\{\{int,bool\},[\{bool,int\}]/O\}) = 3:int, \mathrm{true}:bool, r:[\{bool,int\}]/O$$

のように展開できる。

Definition 10 (Typing rules for values). 右辺に現れる型を決定するために最低限必要な型環境が左辺に現れる。

$$x:\tau \vdash_T x:\tau \qquad \text{(TV-Var)}$$

$$\emptyset \vdash_T i : int \qquad \text{(TV-Int)}$$

$$\emptyset \vdash_T b : bool \qquad \text{(TV-Bool)}$$

$$\frac{\Gamma_i \vdash_T v_i:\tau_i \qquad (1 \le i \le n)}{\Gamma_1 + \cdots + \Gamma_n \vdash_T \{v_1,v_2,\ldots,v_n\}:\{\tau_1,\tau_2,\ldots,\tau_n\}} \qquad \text{(TV-Rec)}$$

Definition 11 (Typing rules for processes). 型判定は図 1 のようになる。

Example 3 (推論の例). 前回の例のプログラムについて、以下のように推論できる (time tag については省略)。

$$\dfrac{\dfrac{\dfrac{\Gamma, ans:\{bool,int\} \vdash Q}{\Gamma, r:[\{bool,int\}]/0, ans:\{bool,int\} \vdash Q}\ \text{(T-Weak)}}{\Gamma, r:[\{bool,int\}]/I.0 \vdash r?^{\mathbf{c}}[ans:\{bool,int\}].Q}\ \text{(T-In)}}{swap:[\alpha,\beta;\{\{\alpha,\beta\},[\{\beta,\alpha\}]/O\}]/0, \Gamma, r:[\{bool,int\}]/I.0 \vdash r?^{\mathbf{c}}[ans:\{bool,int\}].Q}\ \text{(T-Weak)}$$

$$\emptyset; \mathcal{T} \vdash \mathbf{0} \qquad \text{(T-Zero)}$$

$$\frac{\begin{array}{c}\Gamma, x : [\tilde{\alpha}; \tau]^t/U; \mathcal{T} \vdash P \qquad \sigma = [\tilde{\delta}/\tilde{\alpha}]\tau \\ a \subseteq a' \qquad t\mathcal{T}(v : \sigma + \Gamma) \qquad ob(v : \sigma + \Gamma) \implies \mathbf{c} \subseteq a'\end{array}}{x : [\tilde{\alpha}; \tau]^t/O_{a'}.U + flat(v : \sigma) + \Gamma; \mathcal{T} \vdash x!^a[\tilde{\delta}; v].P} \qquad \text{(T-Out)}$$

$$\frac{\begin{array}{c}\tilde{\alpha} \notin ftv(\Gamma) \qquad \Gamma, x : [\tilde{\alpha}; \tau]^t/U, y : \tau'; \mathcal{T} \vdash P \qquad \tau \leq \tau' \\ a \subseteq a' \qquad t\mathcal{T}\Gamma \qquad ob(\Gamma) \implies \mathbf{c} \subseteq a'\end{array}}{\Gamma, x : [\tilde{\alpha}; \tau]^t/I_{a'}U; \mathcal{T} \vdash x?^a[\tilde{\alpha}; y].P} \qquad \text{(T-In)}$$

$$\frac{\Gamma_1 \vdash_T v : \{\tau_1, \ldots, \tau_i\} \qquad \Gamma_2, \tilde{x} : \tilde{\tau}; \mathcal{T} \vdash P}{\Gamma_1 + \Gamma_2; \mathcal{T} \vdash \mathbf{match}\ \{x_1 : \tau_1, \ldots, x_i : \tau_i\} = v\ \mathbf{in}\ P} \qquad \text{(T-Match)}$$

$$\frac{\Gamma_i; \mathcal{T} \vdash P_i \quad (i = 1, 2)}{\Gamma_1 + \Gamma_2; \mathcal{T} \vdash P_1 \mid P_2} \qquad \text{(T-Par)}$$

$$\frac{\Gamma_i; \mathcal{T} \vdash P_i \quad (i = 1, 2)}{\Gamma_1 \sqcap \Gamma_2; \mathcal{T} \vdash \mathbf{if}\ v\ \mathbf{then}\ P_1\ \mathbf{else}\ P_2} \qquad \text{(T-If)}$$

$$\frac{\Gamma, x : [\tilde{\alpha}; \tau]^t/U; \mathcal{T} \vdash P \qquad rel(U)}{\Gamma; \mathcal{T} \vdash (\nu x : [\tilde{\alpha}; \tau]^t/U)P} \qquad \text{(T-New)}$$

$$\frac{\Gamma_i; \mathcal{T} \vdash P_i \quad (i = 1, 2)}{\Gamma_1 \sqcap \Gamma_2; \mathcal{T} \vdash P_1 + P_2} \qquad \text{(T-Choice)}$$

$$\frac{\Gamma; \mathcal{T} \vdash P}{*\Gamma; \mathcal{T} \vdash *P} \qquad \text{(T-Rep)}$$

$$\frac{\Gamma; \mathcal{T} \vdash P \qquad noob(\tau)}{\Gamma, x : \tau; \mathcal{T} \vdash P} \qquad \text{(T-Weak)}$$

図 1: Typing Rules

これを $\mathcal{I}_1$ とおいて、

$$\frac{\mathcal{I}_1 \quad \{\{int, bool\}, [\{bool, int\}]/O\} = [int/\alpha, bool/\beta]\{\{\alpha, \beta\}, [\{\beta, \alpha\}]/O\}}{\begin{array}{c}swap : [\alpha, \beta; \{\{\alpha, \beta\}, [\{\beta, \alpha\}]/O\}]/O.0 + (\Gamma, r : [\{bool, int\}]/I.0) \\ + flat(\{\{3, \text{true}\}, r\} : \{\{int, bool\}, [\{bool, int\}]/O\}) \\ \vdash swap!^{\mathbf{c}}[int, bool; \{\{3, \text{true}\}, r\}].r?^{\mathbf{c}}[ans : \{bool, int\}].Q\end{array}}$$

すなわち

$$\frac{\begin{array}{c}\mathcal{I}_1 \quad \{\{int, bool\}, [\{bool, int\}]/O\} = [int/\alpha, bool/\beta]\{\{\alpha, \beta\}, [\{\beta, \alpha\}]/O\} \\ swap : [\alpha, \beta; \{\{\alpha, \beta\}, [\{\beta, \alpha\}]/O\}]/O.0, \Gamma, r : [\{bool, int\}]/(O \parallel I.0) \\ \vdash swap!^{\mathbf{c}}[int, bool; \{\{3, \text{true}\}, r\}].r?^{\mathbf{c}}[ans : \{bool, int\}].Q \quad rel(O \parallel I.0)\end{array}}{\begin{array}{c}swap : [\alpha, \beta; \{\{\alpha, \beta\}, [\{\beta, \alpha\}]/O\}]/O.0, \Gamma \\ \vdash (\nu r : \tau) swap!^{\mathbf{c}}[int, bool; \{\{3, \text{true}\}, r\}].r?^{\mathbf{c}}[ans : \{bool, int\}].Q\end{array}}$$

となる (これを $\mathcal{I}_2$ とおく)。一方、

$$\frac{\dfrac{\dfrac{\dfr

Definition 12 (Syntax-directed typing rule (抜粋)).

$$\emptyset;\ \mathcal{T} \vdash_S \mathbf{0} \tag{ST-Zero}$$

$$\frac{\begin{array}{c}\Gamma;\ \mathcal{T} \vdash_S P \qquad \sigma = [\tilde{\delta}/\tilde{\alpha}]\tau \\ \Gamma(x) = [\tilde{\alpha};\tau]^t/U \quad \text{or} \quad x \notin dom(\Gamma) \wedge U = 0 \\ a \subseteq a' \qquad t\mathcal{T}(v : \sigma + \Gamma \setminus \{x\}) \qquad ob(v : \sigma + \Gamma \setminus \{x\}) \implies \mathbf{c} \subseteq a'\end{array}}{x : [\tilde{\alpha};\tau]^t/O_{a'}.U + flat(v : \sigma) + \Gamma \setminus \{x\};\ \mathcal{T} \vdash_S x!^a[\tilde{\delta}; v].P} \tag{ST-Out}$$

$$\frac{\begin{array}{c}\tilde{\alpha} \notin ftv(\Gamma \setminus \{x, y\}) \qquad \Gamma;\ \mathcal{T} \vdash_S P \\ \tau \leq \Gamma(y) \wedge y \in dom(\Gamma) \quad \text{or} \quad noob(\tau) \wedge y \notin dom(\Gamma) \\ \Gamma(x) = [\tilde{\alpha};\tau]^t/U \quad \text{or} \quad (x \notin dom(\Gamma) \wedge U = 0) \\ a \subseteq a' \qquad t\mathcal{T}\Gamma \setminus \{x, y\} \qquad ob(\Gamma \setminus \{x, y\}) \implies \mathbf{c} \subseteq a'\end{array}}{\Gamma \setminus \{x, y\}, x : [\tilde{\alpha};\tau]^t/I_{a'}U;\ \mathcal{T} \vdash_S x?^a[\tilde{\alpha}; y].P} \tag{ST-In}$$

$$\frac{\begin{array}{c}\Gamma_1 \vdash_T v : \{\tau_1, \ldots, \tau_i\} \qquad \Gamma_2;\ \mathcal{T} \vdash_S P \\ \Gamma_2(x_i) = \tau_i \wedge x_i \in dom(\Gamma_2) \quad \text{or} \quad noob(\tau_i) \wedge x_i \notin dom(\Gamma_2)\end{array}}{\Gamma_1 + \Gamma_2 \setminus \{\tilde{x}\}; \mathcal{T} \vdash \mathbf{match}\ \{x_1 : \tau_1, \ldots, x_i : \tau_i\} = v\ \mathbf{in}\ P} \tag{ST-Match}$$

$$\frac{\Gamma_i;\ \mathcal{T} \vdash_S P_i \quad (i = 1, 2)}{\Gamma_1 + \Gamma_2;\ \mathcal{T} \vdash_S P_1 \mid P_2} \tag{ST-Par}$$

$$\frac{\Gamma_i;\ \mathcal{T} \vdash_S P_i \quad (i = 1, 2)}{\Gamma_1 \sqcap \Gamma_2;\ \mathcal{T} \vdash_S \mathbf{if}\ v\ \mathbf{then}\ P_1\ \mathbf{else}\ P_2} \tag{ST-If}$$

$$\frac{\begin{array}{c}\Gamma;\ \mathcal{T} \vdash_S P \\ (\Gamma(x) = [\tilde{\alpha};\tau]^t/U \wedge rel(U)) \vee x \notin dom(\Gamma)\end{array}}{\Gamma \setminus \{x\};\ \mathcal{T} \vdash_S (\nu x : [\tilde{\alpha};\tau]^t/U)P} \tag{ST-New}$$

$$\frac{\Gamma_i;\ \mathcal{T} \vdash_S P_i \quad (i = 1, 2)}{\Gamma_1 \sqcap \Gamma_2;\ \mathcal{T} \vdash_S P_1 + P_2} \tag{ST-Choice}$$

$$\frac{\Gamma;\ \mathcal{T} \vdash_S P}{*\Gamma;\ \mathcal{T} \vdash_S *P} \tag{ST-Rep}$$

Theorem 3 (Correctness of syntax-derected rules).

1. $\Gamma;\ \mathcal{T} \vdash P$ ならばある Γ' が存在して $\Gamma';\ \mathcal{T} \vdash_S P$ かつ $\Gamma = \Gamma', x_1 : \tau_1, \ldots, x_n : \tau_n$ が成り立つ。(そしてさらに $noob(\tau_i)$ が成り立つ)
2. $\Gamma;\ \mathcal{T} \vdash_S P$ が成り立てば $\Gamma;\ \mathcal{T} \vdash P$ が成り立つ。