並列分散システム論配布資料 (6)
π 計算: 型システムと遷移関係

京都大学 大学院情報学研究科 通信情報システム専攻
五十嵐 淳
e-mail: igarashi@kuis.kyoto-u.ac.jp

平成 25 年 11 月 18 日

1 型システム

目的: polyadic 通信におけるミスマッチ，つまり送受信されるデータの数 (arity) の不一致を防ぐ.

チャネル型: arity 情報 + どんな値を送受信するかの情報

1.1 型，型判断，型付け規則

型:

$$\begin{array}{lcll} T & ::= & b \mid [T_1, \ldots, T_n] & (n \geq 0) \\ \Gamma & ::= & \bullet \mid \Gamma, n : T & \end{array}$$

b は `int` などの (チャネル以外の) 基本的な値の型を表す**基底型** (*base type*) である.

型判断 (型付け関係): $\Gamma \vdash P$ ok

型付け規則:

$$\frac{\Gamma \vdash \pi_i.P_i \text{ ok} \quad (\text{for } i \in I)}{\Gamma \vdash \sum_{i \in I} \pi_i.P_i} \text{ (T-Sum)} \qquad \frac{\Gamma \vdash P \text{ ok}}{\Gamma \vdash !P \text{ ok}} \text{ (T-Rep)}$$

$$\frac{\Gamma \vdash P \text{ ok} \qquad \Gamma \vdash Q \text{ ok}}{\Gamma \vdash P \parallel Q \text{ ok}} \text{ (T-Par)}$$

$$\frac{\Gamma, a : [T_1, \ldots, T_n] \vdash P \text{ ok}}{\Gamma \vdash \mathsf{new}\, a\, P \text{ ok}} \text{ (T-New)} \qquad \frac{\Gamma \vdash P \text{ ok}}{\Gamma \vdash \tau.P \text{ ok}} \text{ (T-Tau)}$$

$$\frac{(n : [T_1, \ldots, T_n] \in \Gamma) \qquad \Gamma \vdash P \text{ ok} \quad (m_1 : T_1 \in \Gamma \quad \cdots \quad m_k : T_k \in \Gamma)}{\Gamma \vdash \overline{n}\langle m_1, \ldots, m_k \rangle.P \text{ ok}} \text{ (T-Out)}$$

$$\frac{(n : [T_1, \ldots, T_k] \in \Gamma) \quad (\{x_1, \ldots, x_k\} \cap dom(\Gamma) = \emptyset) \quad \Gamma, x_1 : T_1, \ldots, x_k : T_k \vdash P \text{ ok}}{\Gamma \vdash n(x_1, \ldots, x_k).P \text{ ok}} \text{ (T-In)}$$

1.2 性質

1.2.1 定理 [Type Preservation]: $\Gamma \vdash P$ ok かつ $P \longrightarrow P'$ ならば，$\Gamma \vdash P'$ ok である．

1.2.2 定理 [No Immediate Communication Error]: $\Gamma \vdash P$ ok ならば，

$$P \equiv \cdots + \overline{n}\langle m_1, \ldots, m_n \rangle.P_1 + \cdots \parallel \cdots + n(y_1, \ldots, y_k).P_2 + \cdots \parallel P_3$$

かつ $n \neq k$ であるような，$n, k, P_1, P_2, P_3, n, m_1, \ldots, m_n, y_1, \ldots, y_m$ は存在しない．

2 遷移関係

以下では，送受信される値がひとつだけの (純粋な)π 計算を考える．つまり，送信は $\overline{n}\langle m \rangle.P$, 受信は $n(x).P$ の形に限られる．

アクションの定義: アクションは基本的にプロセスの構文定義に用いられたアクション接頭辞であるが，$(\boldsymbol{\nu} a)$ で生成された名前が通信によって当初の有効範囲の外に飛び出す可能性を表現するために $(\boldsymbol{\nu} a)\overline{n}\langle a \rangle$ という形が加わっている．また，入力を表すアクションは (受信値を表すパラメータではなく) 実際に受信した値が m として含まれている．

$$\alpha, \beta, \ldots \in Act = \overline{n}\langle m \rangle \mid n(m) \mid (\boldsymbol{\nu} a)\overline{n}\langle a \rangle \mid \tau$$

2.1 定義 [π 計算のプロセス式から生成される LTS]: 並行プロセス式とプロセス定義 (の集合) から生成される LTS とは，

- $\mathcal{Q} = \mathcal{P}^{\pi}$
- $\mathcal{T}$ は以下の規則 (遷移規則と呼ぶ) で与えられる

ような LTS のことである．(規則に現れる $\mathsf{fn}(P)$ は P に自由に—$(\boldsymbol{\nu} a)$ の有効範囲になく—現れる名前の集合である．)

$$\frac{\pi_j = \overline{n}\langle m\rangle}{\sum_{i\in I}\pi_i.P_i \xrightarrow{\overline{n}\langle m\rangle} P_j}\ (\text{OUT-SUM}_\mathbf{t}) \qquad \frac{(\text{if } \alpha = (\boldsymbol{\nu} a)\overline{n}\langle a\rangle \text{ then } a \notin \mathsf{fn}(Q)) \quad P \xrightarrow{\alpha} P'}{P \parallel Q \xrightarrow{\alpha} P' \parallel Q}\ (\text{L-PAR}_\mathbf{t})$$

$$\frac{\pi_j = n(x)}{\sum_{i\in I}\pi_i.P_i \xrightarrow{n(m)} [m/x]P_j}\ (\text{IN-SUM}_\mathbf{t}) \qquad \frac{(\text{if } \alpha = (\boldsymbol{\nu} a)\overline{n}\langle a\rangle \text{ then } a \notin \mathsf{fn}(P)) \quad Q \xrightarrow{\alpha} Q'}{P \parallel Q \xrightarrow{\alpha} P \parallel Q'}\ (\text{R-PAR}_\mathbf{t})$$

$$\frac{\pi_j = \tau}{\sum_{i\in I}\pi_i.P_i \xrightarrow{\tau} P_j}\ (\text{TAU-SUM}_\mathbf{t}) \qquad \frac{P \xrightarrow{\alpha} P' \qquad (\text{if } a \text{ does not appear in } \alpha)}{\mathsf{new}\, a\, P \xrightarrow{\alpha} \mathsf{new}\, a\, P'}\ (\text{RES}_\mathbf{t})$$

$$\frac{P \xrightarrow{\overline{n}\langle m\rangle} P' \qquad Q \xrightarrow{n(m)} Q'}{P \parallel Q \xrightarrow{\tau} P' \parallel Q'}\ (\text{L-REACT}_\mathbf{t}) \qquad \frac{P \xrightarrow{\overline{n}\langle a\rangle} P'}{\mathsf{new}\, a\, P \xrightarrow{(\boldsymbol{\nu} a)\overline{n}\langle a\rangle} P'}\ (\text{OPEN}_\mathbf{t})$$

$$\frac{P \xrightarrow{n(m)} P' \qquad Q \xrightarrow{\overline{n}\langle m\rangle} Q'}{P \parallel Q \xrightarrow{\tau} P' \parallel Q'}\ (\text{R-REACT}_\mathbf{t}) \qquad \frac{P \xrightarrow{\alpha} P'}{!P \xrightarrow{\alpha} P' \parallel !P}\ (\text{REP-ACT}_\mathbf{t})$$

$$\frac{P \xrightarrow{(\boldsymbol{\nu} a)\overline{n}\langle a\rangle} P' \qquad Q \xrightarrow{n(a)} Q'}{P \parallel Q \xrightarrow{\tau} (\boldsymbol{\nu} a)(P' \parallel Q')}\ (\text{L-CLOSE}_\mathbf{t}) \qquad \frac{P \xrightarrow{\overline{n}\langle m\rangle} P' \qquad P \xrightarrow{n(m)} P''}{!P \xrightarrow{\tau} P' \parallel P'' \parallel !P}\ (\text{REP-REACT}_\mathbf{t})$$

$$\frac{P \xrightarrow{n(a)} P' \qquad Q \xrightarrow{(\boldsymbol{\nu} a)\overline{n}\langle a\rangle} Q'}{P \parallel Q \xrightarrow{\tau} (\boldsymbol{\nu} a)(P' \parallel Q')}\ (\text{R-CLOSE}_\mathbf{t}) \qquad \frac{P \xrightarrow{(\boldsymbol{\nu} a)\overline{n}\langle a\rangle} P' \qquad Q \xrightarrow{n(a)} P''}{!P \xrightarrow{\tau} (\boldsymbol{\nu} a)(P' \parallel P'') \parallel !P}\ (\text{REP-CLOSE}_\mathbf{t})$$

遷移関係を使うと，強双模倣性，$\sim$ などは CCS の場合と同様に定義でき，同様な性質が成立する．ただし，合同性については注意が必要である．

2.2 定理 [τ **遷移とリアクションの同値性**]: $P \longrightarrow P'$ ならば，その時に限り $P \xrightarrow{\tau}\!\!\equiv P'$

2.3 定理:

1. 構造的合同性は並行プロセス上の強双模倣である
2. $P \equiv Q$ ならば $P \sim Q$

2.4 Proposition [**Strong process congruence**]: $\sim$ は以下の意味で合同関係である．すなわち，もし $P \sim Q$ ならば

1. $\alpha.P + M \sim \alpha.Q + M$ (ただし α は $\overline{n}\langle m\rangle$ か τ である)
2. $\mathsf{new}\, a\, P \sim \mathsf{new}\, a\, Q$

3. $P \parallel R \sim Q \parallel R$

4. $R \parallel P \sim R \parallel Q$

5. $!P \sim !Q$

6. 任意の名前 a について $P[a/x] \sim Q[a/x]$ ならば，$n(x).P + M \sim n(x).Q + M$

3　今後の講義について

分散計算のモデル

[1] Matthew Hennessy and James Riely. Resource access control in systems of mobile agents (extended abstract). *Electronic Notes in Theoretical Computer Science*, 16(3), 1998.

[2] Matthew Hennessy and James Riely. Resource access control in systems of mobile agents. *Information and Computation*, 173:82–120, 2002.

[3] Luca Cardelli and Andrew D. Gordon. Mobile ambients. In *Proc. of FoSSaCS*, volume 1378 of *Springer LNCS*, pages 140–155, 1998.

[4] Luca Cardelli and Andrew D. Gordon. Mobible ambients. *Theoretical Computer Science*, 240(1):177–213, 2000.

暗号プロトコル・セキュリティ

[5] Matín Abadi and Andrew D. Gordon. Reasoning about cryptographic protocols in the Spi calculus. In *Proc. of CONCUR*, volume 1243 of *Springer LNCS*, pages 59–73, 1997.

[6] Matín Abadi and Andrew D. Gordon. A calculus for cryptographic protocols: The Spi calculus. In *Proc. of ACM Conference on Computer and Communications Security*, pages 36–47, 1997.

[7] Andrew D. Gordon and Alan Jeffrey. Authenticity by typing for security protocols. In *Proc. of IEEE Computer Security Foundations Workshop*, pages 145–159, 2001.