ソフトウェア基礎論配布資料 (7)
π 計算

五十嵐 淳
京都大学 大学院情報学研究科知能情報学専攻
e-mail: igarashi@kuis.kyoto-u.ac.jp

平成 18 年 1 月 10 日

1 π 計算—特徴

mobile process の計算体系:

- 並列実行される**プロセス**(*process*) によるシステム記述
- 主要な計算ステップ: **通信路/チャネル**(*communication channel*) を介してのプロセス間通信
- 主要なデータ: 通信チャネルの名前 (cf. URL)
- 新しい名前の生成機構と動的に変化する名前の有効範囲による通信トポロジーの動的な変化

1.1 概要

- **0** … 何もしない・実行終了状態にあるプロセス
- $P_1 \mid P_2$ … プロセス P_1 と P_2 の並列実行
- $x![y].P$ … 通信チャネル x へ y を送信，送信後に P を実行
- $x?[z].P$ … 通信チャネル x からデータを受信，パラメータ z (有効範囲は P) をそれに束縛して P を実行
- **new** x **in** P … 新しい通信チャネルを生成し，その名前を x として P を実行
- $*P$ … P の無限コピー ($P \mid P \mid \cdots \mid P \mid \cdots$)

- $P_1 + P_2$ ··· 入出力プロセス P_1 か P_2 の，可能な通信のうち一方を実行 (両方可能でも，どちらか一方を非決定的に選択)

主要な計算規則:

$$x![y].P \mid x?[z].Q \longrightarrow P \mid [y/z]Q$$

($[y/z]$ は z を y で変数参照関係を保ちながら置き換える操作．) 非決定性:

$$\begin{array}{rcl} x![y].P_1 \mid x![w].P_2 \mid x?[z].P_3 & \longrightarrow & P_1 \mid x![w].P_2 \mid [y/z]P_3 \\ \downarrow & & \\ x![y].P_1 \mid P_2 \mid [w/z]P_3 & & \end{array}$$

new x **in** P について:

$$\begin{array}{rcl} (\textbf{new}\ x\ \textbf{in}\ x![y].P) \mid x?[z].Q & \not\longrightarrow & \textbf{new}\ x\ \textbf{in}\ P \mid [y/z]Q \\ (\textbf{new}\ x\ \textbf{in}\ \#^1 x![y].P) \mid x?[z].Q & \longrightarrow & (\textbf{new}\ x\ \textbf{in}\ P) \mid [y/z]Q \end{array}$$

また，**new** で束縛された名前が送受信対象になると有効範囲の移動が発生する．P に y が現われないとすると，

$$\begin{array}{rcl} (\textbf{new}\ y\ \textbf{in}\ x![y].P \mid y?[w].Q) \mid x?[z].z![v].R & \longrightarrow & P \mid (\textbf{new}\ y\ \textbf{in}\ y?[w].Q \mid y![v].R') \\ & \longrightarrow & P \mid (\textbf{new}\ y\ \textbf{in}\ [v/w]Q \mid R') \end{array}$$

1.2 例

「1 足す」サーバ: s でリクエストを受信して r に返事を送信.

$$\begin{array}{l} P \equiv *s?[n].r![n+1].\mathbf{0} \\ P \mid s![2].r?[x].Q \longrightarrow \cdots \longrightarrow ? \\ P \mid s![2].r?[x].Q \mid s![4].r?[y].R \longrightarrow \cdots \longrightarrow ? \end{array}$$

「1 足す」サーバ (改良版)

$$\begin{array}{l} P \equiv *s?[n,r].r![n+1].\mathbf{0} \\ P \mid (\textbf{new}\ r'\ \textbf{in}\ s![2,r'].r'?[x].Q) \longrightarrow \cdots \longrightarrow ?? \\ P \mid (\textbf{new}\ r_1\ \textbf{in}\ s![2,r_1].r_1?[x].Q) \mid (\textbf{new}\ r_2\ \textbf{in}\ s![4,r_2].r_2?[y].R) \longrightarrow \cdots \longrightarrow ?? \end{array}$$

点オブジェクト:

$$\begin{array}{rcl} P & \equiv & \textbf{new}\ \mathit{state}\ \textbf{in} \\ & & \quad \mathit{state}![0]. \mid \\ & & \quad *\mathit{state}?[n].(\mathit{get}?[r].r![n].\mathit{state}![n].\mathbf{0} + \mathit{set}?[n',r].r![].\mathit{state}![n'].\mathbf{0}) \\ \multicolumn{3}{l}{P \mid (\textbf{new}\ r_1\ \textbf{in}\ \mathit{get}![r_1].r_1?[n].Q_1) \mid (\textbf{new}\ r_2\ \textbf{in}\ \mathit{set}![3,r_2].r_2?[].Q_2)} \end{array}$$

名前の組の通信 (polyadic π 計算) の単一名通信による模倣:

$$\begin{array}{rcl} x![y_1,\ldots,y_n].P & \equiv & \textbf{new}\ w\ \textbf{in}\ x![w].w![y_1].\cdots.w![y_n].P \\ x?[z_1,\ldots,z_n].Q & \equiv & x?[v].v?[z_1].\cdots.v?[z_n].Q \end{array}$$

2 Polyadic π 計算の形式的定義

2.1 文法

環境 Γ は変数 (宣言) の並びとする．判断 $\Gamma \vdash \#^i x \in \mathbf{Ch}$, $\Gamma \vdash P \in \mathbf{Pr}$, $\Gamma \vdash G \in \mathbf{GPr}$ はそれぞれ「$\#^i x$ が Γ のもとで有効な変数参照である」「Γ のもとで P はプロセスである」「Γ のもとで G は入出力ガード付きプロセスである」ことを表し，以下の規則で定義される．

$$\Gamma, x \vdash \#^0 x \in \mathbf{Ch} \qquad \text{(VarRef0)}$$

$$\frac{\Gamma \vdash \#^i x \in \mathbf{Ch}}{\Gamma, x \vdash \#^{i+1} x \in \mathbf{Ch}} \qquad \text{(VarRef1)}$$

$$\frac{\Gamma \vdash \#^i x \in \mathbf{Ch} \qquad (x \not\equiv y)}{\Gamma, y \vdash \#^i x \in \mathbf{Ch}} \qquad \text{(VarRef2)}$$

$$\Gamma \vdash \mathbf{0} \in \mathbf{Pr} \qquad \text{(P-Nil)}$$

$$\frac{\Gamma \vdash P_1 \in \mathbf{Pr} \qquad \Gamma \vdash P_2 \in \mathbf{Pr}}{\Gamma \vdash P_1 \mid P_2 \in \mathbf{Pr}} \qquad \text{(P-Par)}$$

$$\frac{\Gamma, x \vdash P \in \mathbf{Pr}}{\Gamma \vdash \mathbf{new}\ x\ \mathbf{in}\ P \in \mathbf{Pr}} \qquad \text{(P-New)}$$

$$\frac{\Gamma \vdash P \in \mathbf{Pr}}{\Gamma \vdash *P \in \mathbf{Pr}} \qquad \text{(P-Rep)}$$

$$\frac{\Gamma \vdash G_1 \in \mathbf{GPr} \qquad \cdots \qquad \Gamma \vdash G_n \in \mathbf{GPr}}{\Gamma \vdash G_1 + \cdots + G_n \in \mathbf{Pr}} \qquad \text{(P-Choice)}$$

$$\frac{\Gamma \vdash \#^{i_0} x_0 \in \mathbf{Ch} \quad \cdots \quad \Gamma \vdash \#^{i_n} x_n \in \mathbf{Ch} \qquad \Gamma \vdash P \in \mathbf{Pr}}{\Gamma \vdash \#^{i_0} x_0 ![\#^{i_1} x_1, \ldots, \#^{i_n} y_n].P \in \mathbf{GPr}} \qquad \text{(G-Out)}$$

$$\frac{\Gamma \vdash \#^i x \in \mathbf{Ch} \qquad \Gamma, y_1, \ldots, y_n \vdash P \in \mathbf{Pr}}{\#^i x?[y_1, \ldots, y_n].P \in \mathbf{GPr}} \qquad \text{(G-In)}$$

2.2 簡約

- 通信を起こすプロセスが，必ずしも項の構造の中で近くにあるわけではない．

$$(x![y].P_1 \mid x![w].P_2) \mid x?[z].P_3 \longrightarrow (P_1 \mid x![w].P_2) \mid [y/z]P_3$$

- λ 計算のように局所的な計算のみを表現した簡約+ 通信するプロセスが「近く」に来る「配置換え」を許すようなプロセス間の等価関係 $\cong$:

$$(x![y].P_1 \mid x![w].P_2) \mid x?[z].P_3 \cong (x![y].P_1 \mid x?[z].P_3) \mid x![w].P_2$$

以下で，$x \Uparrow P$ は λ 計算でみたような，(**new** の有効範囲にない) 変数参照 $\#^i x$ の添字 i を 1 増加させる操作，$[y_1/z_1, \ldots, y_n/z_n]$ は (変数参照関係を保つ) 同時置換である．

2.2.1 定義: 構造的合同関係(*structural congruence*) $\Gamma \vdash P_1 \cong P_2$ を以下の規則で定義する．

$$\frac{\Gamma \vdash P \in \mathbf{Pr}}{\Gamma \vdash P \cong P} \quad \text{(SC-Refl)} \qquad \frac{\Gamma \vdash P \in \mathbf{Pr} \qquad \Gamma \vdash Q \in \mathbf{Pr} \qquad \Gamma \vdash R \in \mathbf{Pr}}{P \mid (Q \mid R) \cong (P \mid Q) \mid R} \quad \text{(SC-Assoc)}$$

$$\frac{\Gamma \vdash P \cong Q}{\Gamma \vdash Q \cong P} \quad \text{(SC-Symm)} \qquad \frac{\Gamma \vdash P \in \mathbf{Pr}}{*P \cong *P \mid P} \quad \text{(SC-Rep)}$$

$$\frac{\Gamma \vdash P \cong Q \qquad \Gamma \vdash Q \cong R}{\Gamma \vdash P \cong R} \quad \text{(SC-Trans)} \qquad \frac{\Gamma, x \vdash P \in \mathbf{Pr} \qquad \Gamma \vdash Q \in \mathbf{Pr}}{(\mathbf{new}\ x\ \mathbf{in}\ P) \mid Q \cong \mathbf{new}\ x\ \mathbf{in}\ (P \mid Q \Uparrow x)} \quad \text{(SC-New)}$$

$$\frac{\Gamma \vdash P \in \mathbf{Pr}}{\Gamma \vdash P \mid \mathbf{0} \cong P} \quad \text{(SC-Zero)} \qquad \frac{\Gamma \vdash P \cong P' \qquad Q \cong Q'}{\Gamma \vdash P \mid Q \cong P' \mid Q'} \quad \text{(SC-Par)}$$

$$\frac{\Gamma \vdash P \in \mathbf{Pr} \qquad \Gamma \vdash Q \in \mathbf{Pr}}{\Gamma \vdash P \mid Q \cong Q \mid P} \quad \text{(SC-Commut)} \qquad \frac{\Gamma, x \vdash P \cong Q}{\mathbf{new}\ x\ \mathbf{in}\ P \cong \mathbf{new}\ x\ \mathbf{in}\ Q} \quad \text{(SC-CNew)}$$

2.2.2 定義: 簡約関係 $\Gamma \vdash P \longrightarrow Q$ を以下の規則で定義する.

$$\frac{\begin{array}{c}\Gamma \vdash (G_1 + \cdots + G_n) \mid (G'_1 + \cdots + G'_m) \in \mathbf{Pr} \\ G_j \equiv \#^i x![\#^{i_1} z_1, \ldots, \#^{i_n} z_n].P \qquad G'_k \equiv \#^i x?[y_1, \ldots, y_n].Q\end{array}}{\Gamma \vdash (G_1 + \cdots + G_n) \mid (G'_1 + \cdots + G'_m) \longrightarrow P \mid [\#^{i_1} z_1/y_1, \ldots, \#^{i_n} z_n/y_n]Q} \quad \text{(R-Comm)}$$

$$\frac{\Gamma \vdash P \longrightarrow Q \qquad \Gamma \vdash R \in \mathbf{Pr}}{\Gamma \vdash P \mid R \longrightarrow Q \mid R} \quad \text{(R-Par)}$$

$$\frac{\Gamma, x \vdash P \longrightarrow Q}{\Gamma \vdash \mathbf{new}\ x\ \mathbf{in}\ P \longrightarrow \mathbf{new}\ x\ \mathbf{in}\ Q} \quad \text{(R-New)}$$

$$\frac{\Gamma \vdash P \cong P' \qquad \Gamma \vdash P' \longrightarrow Q' \qquad \Gamma \vdash Q' \cong Q}{\Gamma \vdash P \longrightarrow Q} \quad \text{(R-SP)}$$

3 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

3.1 型，型付構文，型判断，型付け規則

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

型判断: $\Gamma \vdash \#^i x : T$ と $\Gamma \vdash P$ ok
型付け規則:

$$\frac{}{\Gamma, x \in T \vdash \#^0 x \in T} \text{(T-Var)} \qquad \frac{\Gamma \vdash P \text{ ok}}{\Gamma \vdash *P \text{ ok}} \text{(T-Rep)}$$

$$\frac{\Gamma \vdash \#^n x \in T}{\Gamma, x \in T' \vdash \#^{n+1} x \in T} \text{(T-Varref1)} \qquad \frac{\Gamma \vdash G_1 \text{ ok} \quad \cdots \quad \Gamma \vdash G_n \text{ ok}}{\Gamma \vdash G_1 + \cdots + G_n \text{ ok}} \text{(T-Choice)}$$

$$\frac{\Gamma \vdash \#^n x \in T \qquad x \not\equiv y}{\Gamma, y \in T' \vdash \#^n x \in T} \text{(T-Varref2)}$$

$$\frac{}{\Gamma \vdash \mathbf{0} \text{ ok}} \text{(T-Nil)} \qquad \frac{\Gamma \vdash \#^i x \in [T_1, \ldots, T_n] \qquad \Gamma \vdash P \text{ ok} \quad \Gamma \vdash \#^{i_1} z_1 \in T_1 \quad \cdots \quad \Gamma \vdash \#^{i_n} z_n \in T_n}{\Gamma \vdash \#^i x![\#^{i_1} z_1, \ldots, \#^{i_n} z_n].P \text{ ok}} \text{(T-Out)}$$

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

$$\frac{\Gamma, x \in T \vdash P \text{ ok}}{\Gamma \vdash \mathbf{new}\ x \in T\ \mathbf{in}\ P \text{ ok}} \text{(T-New)} \qquad \frac{\Gamma \vdash \#^i x \in [T_1, \ldots, T_n] \quad \Gamma, y_1 \in T_1, \ldots, y_n \in T_n \vdash P \text{ ok}}{\Gamma \vdash \#^i x?[y_1, \ldots, y_n].P \text{ ok}} \text{(T-In)}$$

3.2 性質

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

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

$$P \cong \cdots + \#^i x![\#^{i_1} z_1, \ldots, \#^{i_n} z_n].P_1 + \cdots \mid \cdots + \#^i x?[y_1, \ldots, y_m].P_2 + \cdots \mid P_3$$

かつ $n \neq m$ であるような，$n, m, P_1, P_2, P_3, i, x, i_1, \ldots, i_n, z_1, \ldots, z_n, y_1, \ldots, y_m$ は存在しない．

4 展望

- ふたつのプロセスが「等しい」とは？
- 自然数など，チャネルの名前以外の基本データの導入
- link mobility から process mobility へ: λ 抽象したプロセスと，その送受信を可能にする「高階 π 計算」

- 場所 (site,location) の概念を導入した「分散 π 計算」
- 暗号プリミティブを追加した「暗号 π 計算」