Le Pi-calcul

Maser 2 GLSD 2015-2016

Matière: VSM

plan

- CCS avec passage de valeur : Syntaxe, exemples
- Pi-calcul: motivation, application, syntaxe, exemples, sémantique

CCS avec passage de valeur
Valued-CCS

- Enrichissement du CCS avec la possibilité de faire **un échange d'informations** entre les processus durant leurs communications

- Des **données (valeurs)** peuvent être échangées via les ports

- Ces valeurs peuvent être **scalaires** ou des **vecteurs**

Valued-CCS: Syntaxe

- Le préfixe α a une syntaxe plus enrichie:

$$\alpha ::= \overline{a}(x) | a(x) | \tau$$

Tel que :

- $\overline{a}(x)$: signifie l'envoi de la valeur x via le port a
- $a(x)$: signifie la réception de la valeur x sur le port *a*

Ici, on a deux ensembles disjoints :
- A pour les noms des ports
- et X pour les noms des valeurs

Exemples

$$C \stackrel{\text{def}}{=} in(x).C'(x)$$

$$C'(x) \stackrel{\text{def}}{=} \overline{out}(x).C$$

$$C \stackrel{\text{def}}{=} in(x).\overline{out}(x).C$$

$$A \stackrel{\text{def}}{=} in(x).in(y).\overline{out}(x).\overline{out}(y).A$$

$$B \stackrel{\text{def}}{=} in_1(x).\overline{out_1}(x).B + in_2(x).\overline{out_2}(x).B$$

$$(\overline{a}5.P' \mid a(x).R')\backslash a$$

Pi-calcul: Motivation

- Un formalisme pour les **systèmes dynamiques**.
- Pratiquement: pour les systèmes où les **liens** de communications sont **dynamiques**
- Les **noms des ports** de communications peuvent **changer** durant le **déroulement** du systèmes
- Les **processus** (dits **agents**) peuvent **échanger** leurs **ports** de communication, comme ils échangent des valeurs entre eux.

Exemple d’une application

- Pour prouver des propriétés de correction des protocoles (par exemple le protocole PLMN ou **Public Land Mobile Network** pour le GSM)

« *Journal of Formal Aspects of Computing* » 1992

An algebraic verification of a mobile network

Pi-calcul : Syntaxe

- **Principe de base** : les noms des valeurs et les noms des ports appartiennent à **un même ensemble** qu'on appelle N (pour Names):

N = A Union X

A: les noms des ports

X: les noms des valeurs

Exemples

$$Q \equiv b(y).b(z).\overline{y}z.\mathbf{0};$$

$$(P' \mid \overline{a}5.\mathbf{0} \mid a(x).R')$$

$$(P' \mid \overline{a}5.\mathbf{0} \mid a(x).R')\backslash a$$

$$(\overline{b}a.\overline{b}5.P' \mid b(y).b(z).\overline{y}z.\mathbf{0} \mid a(x).R')\backslash a \backslash b$$

Pi-calcul: Syntaxe

Prefixes	α	$::=$	$\overline{a}x$	Output
			$a(x)$	Input
			τ	Silent
Agents	P	$::=$	$\mathbf{0}$	Nil
			$\alpha\,.\,P$	Prefix
			$P + P$	Sum
			$P \mid P$	Parallel
			$\texttt{if}\ x = y\ \texttt{then}\ P$	Match
			$\texttt{if}\ x \neq y\ \texttt{then}\ P$	Mismatch
			$(\boldsymbol{\nu} x)P$	Restriction
			$A(y_1, \ldots, y_n)$	Identifier
Definitions			$A(x_1, \ldots, x_n) \stackrel{\mathrm{def}}{=} P$	(where $i \neq j \Rightarrow x_i \neq x_j$)

Table 1: The syntax of the π-calculus.

Occurrences libres et liées

- Pour un nom *x* il est lié ssi

- Soit il est sous la porté d'un préfixe d'entrée

  Exemple : dans ***a(x)***, *x* est lié

- Soit il est sous la porte d'une restriction

  Exemple : dans $\boldsymbol{v(x)}$, x est lié

Sinon, il est libre

Substitution et α-conversion

- Lors d'une substitution dans un terme, on ne peut que substituer **les noms non liés**.

- Pour éviter que des noms libres seront capturés par des lieurs **il faut effectuer un re-nomage** des noms liés.

- Ce re-nomage des noms liés est dit une **α-conversion**.

SOS du Pi-calcul

TAU-ACT : $\dfrac{-}{\tau.P \xrightarrow{\tau} P}$

OUTPUT-ACT : $\dfrac{-}{\overline{x}y.P \xrightarrow{\overline{x}y} P}$

INPUT-ACT : $\dfrac{-}{x(z).P \xrightarrow{x(w)} P\{w/z\}}$ $w \notin \mathrm{fn}((z)P)$

SUM : $\dfrac{P \xrightarrow{\alpha} P'}{P + Q \xrightarrow{\alpha} P'}$

MATCH : $\dfrac{P \xrightarrow{\alpha} P'}{[x=x]P \xrightarrow{\alpha} P'}$

IDE : $\dfrac{P\{\widetilde{y}/\widetilde{x}\} \xrightarrow{\alpha} P'}{A(\widetilde{y}) \xrightarrow{\alpha} P'}$ $A(\widetilde{x}) \stackrel{\mathrm{def}}{=} P$

SOS du Pi-calcul

$$\text{PAR}: \quad \frac{P \xrightarrow{\alpha} P'}{P \mid Q \xrightarrow{\alpha} P' \mid Q} \quad \mathrm{bn}(\alpha) \cap \mathrm{fn}(Q) = \emptyset$$

$$\text{COM}: \quad \frac{P \xrightarrow{\overline{x}y} P' \quad Q \xrightarrow{x(z)} Q'}{P \mid Q \xrightarrow{\tau} P' \mid Q'\{y/z\}} \qquad \text{CLOSE}: \quad \frac{P \xrightarrow{\overline{x}(w)} P' \quad Q \xrightarrow{x(w)} Q'}{P \mid Q \xrightarrow{\tau} \nu(w)(P' \mid Q')}$$

$$\text{RES}: \quad \frac{P \xrightarrow{\alpha} P'}{\nu(y)P \xrightarrow{\alpha} \nu(y)P'} \quad y \notin \mathrm{n}(\alpha) \qquad \text{OPEN}: \quad \frac{P \xrightarrow{\overline{x}y} P'}{\nu(y)P \xrightarrow{\overline{x}(w)} P'\{w/y\}} \quad \begin{array}{l} y \neq x \\ w \notin \mathrm{fn}(\nu(y)P') \end{array}$$

Sémantique ?

$$a(x)\,.\,\overline{c}x \mid \overline{a}b \quad \xrightarrow{\tau}$$

$$(\boldsymbol{\nu} b)(a(x)\,.\,\overline{c}x \mid \overline{a}b) \quad \xrightarrow{\tau}$$

$$a(x)\,.\,P \mid (\boldsymbol{\nu} b)\overline{a}b\,.\,Q \quad \xrightarrow{\tau}$$

$$((\boldsymbol{\nu} b)a(x)\,.\,P) \mid \overline{a}b\,.\,Q$$

$(a(x)\,.\,(\boldsymbol{\nu} b)\overline{x}b\,.\,\overline{c}y\,.\,\mathbf{0})$ **[y<-x, c<-b]**