Typage d'une version décorée du π-calcul

Julien Gabet
sous la direction d'Emmanuel Beffara

Institut de Mathématiques de Marseille

Mars-Juin 2018

- Processus mobiles : objets en interaction sur un réseau, actions non déterministes.
- Modèle habituel : π-calcul.
- Vérifier le comportement d'un objet du modèle : typage.
- Notre approche : annoter les termes pour guider l'exécution.

Le π-calcul

- $P, Q ::= 0 \;\; ; \;\; P|Q \;\; ; \;\; u(t).P \;\; ; \;\; \bar{u}(v).P \;\; ; \;\; \tau.P \;\; ; \;\; (\nu u)P$

Le π-calcul

- $P, Q ::= 0 \;\; ; \;\; P|Q \;\; ; \;\; u(t).P \;\; ; \;\; \bar{u}(v).P \;\; ; \;\; \tau.P \;\; ; \;\; (\nu u)P$
- Congruence structurelle :

$$
\begin{array}{rl}
P|0 \equiv P & P|Q \equiv Q|P \\
P|(Q|R) \equiv (P|Q)|R & (\nu u)(\nu v)P \equiv (\nu v)(\nu u)P \\
(\nu u)0 \equiv 0 & (\nu u)(P|Q) \equiv P|(\nu u)Q \quad \text{if } u \notin fn(P)
\end{array}
$$

Le π-calcul

- $P, Q ::= 0 \;;\; P|Q \;;\; u(t).P \;;\; \bar{u}(v).P \;;\; \tau.P \;;\; (\nu u)P$
- Congruence structurelle :

$$\begin{array}{cc} P|0 \equiv P & P|Q \equiv Q|P \\ P|(Q|R) \equiv (P|Q)|R & (\nu u)(\nu v)P \equiv (\nu v)(\nu u)P \\ (\nu u)0 \equiv 0 & (\nu u)(P|Q) \equiv P|(\nu u)Q \quad \text{if } u \notin fn(P) \end{array}$$

- Règles de réduction :

$$\frac{}{u(t).P|\bar{u}(v).Q \to P[v/t]|Q} \qquad \frac{}{\tau.P \to P}$$

$$\frac{P \to P'}{P|Q \to P'|Q} \qquad \frac{P \to P'}{(\nu u)P \to (\nu u)P'} \qquad \frac{P \equiv Q \to Q' \equiv P'}{P \to P'}$$

Exemple

Un terme simple pour voir le système de réduction :

$$\Big(u(t).P|Q\Big)\Big|\bar{u}(v).R$$

Exemple

Un terme simple pour voir le système de réduction :

$$\Big(u(t).P|Q\Big)\Big|\bar{u}(v).R \equiv \Big(Q|u(t).P\Big)\Big|\bar{u}(v).R$$

Exemple

Un terme simple pour voir le système de réduction :

$$\begin{aligned}\Big(u(t).P|Q\Big)\Big|\bar{u}(v).R &\equiv \Big(Q|u(t).P\Big)\Big|\bar{u}(v).R \\ &\equiv Q\Big|\Big(u(t).P|\bar{u}(v).R\Big)\end{aligned}$$

Exemple

Un terme simple pour voir le système de réduction :

$$\begin{aligned}\Big(u(t).P|Q\Big)\Big|\bar{u}(v).R &\equiv \Big(Q|u(t).P\Big)\Big|\bar{u}(v).R \\ &\equiv Q\Big|\Big(u(t).P|\bar{u}(v).R\Big) \\ &\to Q\Big|\Big(P[v/t]|R\Big)\end{aligned}$$

Exemple

Un exemple non confluent :

$$
\begin{array}{ccc}
\Big(u(t).P|\bar{u}(v).Q\Big)\Big|u(t).S & \equiv & u(t).P\Big|\Big(\bar{u}(v).Q|u(t).S\Big) \\
\downarrow & & \downarrow \\
\Big(P[v/t]|Q\Big)\Big|u(t).S & & u(t).P\Big|\Big(Q|S[v/t]\Big)
\end{array}
$$

Les termes annotés

Les termes annotés sont définis comme suit :

$$
\begin{array}{llr}
P, Q ::= & x \leftrightarrow y \ ; \ 0_x \ ; & \text{termes de base} \\
& P|_x Q \ ; \ P||_x Q \ ; & \text{parallèle et synchronisation} \\
& u_x(t).P \ ; \ \bar{u}_x(v).P \ ; & \text{préfixes d'action} \\
& \epsilon_x.P \ ; \ \lambda_x y.P \ ; & \text{préfixes de planification} \\
& (\nu u)P & \text{privatisation de nom}
\end{array}
$$

où $x \in fv(P) \cap fv(Q)$ pour les règles $|$ et $||$,
$x \notin fv(P)$ pour la règle ϵ, et $x, y \in fv(P)$ pour les autres règles.

Les termes annotés

Et où l'ensemble des variables libres d'un terme $fv(P)$ est défini par induction sur les termes :

$$
\begin{aligned}
fv(x \leftrightarrow y) &= \{x, y\} & fv(0_x) &= \{x\} \\
fv(P|_x Q) &= fv(P) \cup fv(Q) & fv(P||_x Q) &= (fv(P) \cup fv(Q)) \backslash \{x\} \\
fv(u_x(t).P) &= fv(P) & fv(\bar{u}_x(v).P) &= fv(P) \\
fv(\epsilon_x.P) &= fv(P) \cup \{x\} & fv(\lambda_x y.P) &= fv(P) \backslash \{y\} \\
fv((\nu u)P) &= fv(P)
\end{aligned}
$$

La réduction

- Règles de réduction :

$$\epsilon_x.P||_x 0_x \to P \qquad (P|_x Q)||_x \lambda_x y.R \to P||_x(Q[y/x]||_y R)$$

$$P||_x x \leftrightarrow y \to P[y/x] \qquad \lambda_x y.R||_x(P|_x Q) \to (R||_x P)||_y Q[y/x]$$

$$\bar{u}_x(v).P||_x u_x(t).Q \to P||_x Q[v/t]$$

La réduction

- Règles de réduction :

$$\epsilon_x.P||_x 0_x \to P \qquad (P|_x Q)||_x \lambda_x y.R \to P||_x(Q[y/x]||_y R)$$
$$P||_x x \leftrightarrow y \to P[y/x] \qquad \lambda_x y.R||_x(P|_x Q) \to (R||_x P)||_y Q[y/x]$$
$$\bar{u}_x(v).P||_x u_x(t).Q \to P||_x Q[v/t]$$

- Règles de remontée du $||$:
Si le contexte l'exige, on note P^y si le terme P contient y.
$(P^y|_x Q)||_y R \succ (P||_y R)|_x Q \qquad (P|_x Q^y)||_y R \succ P|_x(Q||_y R)$
$(\nu u)P||_x Q \succ (\nu u)(P||_x Q) \qquad$ si $u \notin fn(Q)$

La réduction

Il faut une congruence pour faire confluer $\succ$:

$$\begin{array}{ll}
(P^y|_x Q)|_y R \equiv (P^x|_y R)|_x Q & (\nu u)(\nu v)P \equiv (\nu v)(\nu u)P \\
P|_x(Q|_y R^x) \equiv Q|_y(P|_x R^y) & (\nu u)0_x \equiv 0_x \\
(P|_x Q^y)|_y R \equiv P|_x(Q^x|_y R) & (\nu u)P|_x Q \equiv (\nu u)(P|_x Q) \quad u \notin Q
\end{array}$$

Proposition

- *$\rightarrow$ est fortement confluent*
- *$\succ$ est confluent à $\equiv$ près.*

Confluence de $\rightarrow$ et $\succ$

Pour $\rightarrow$, seule la règle $x \leftrightarrow y$ interagit avec elle-même :

$$
\begin{tikzcd}
 & x \leftrightarrow y \|_x x \leftrightarrow z \arrow[dl] \arrow[dr] & \\
(x \leftrightarrow z)[y/x] \arrow[d, equal] & & (x \leftrightarrow y)[z/x] \arrow[d, equal] \\
y \leftrightarrow z & = & z \leftrightarrow y
\end{tikzcd}
$$

Confluence de $\to$ et $\succ$

Pour $\succ$, on regarde un cas (les autres sont similaires) :

$$\begin{tikzcd}[column sep=tiny]
& (P^y|_x Q)||_y(R^y|_z S) \arrow[dl, "\succ_{left}"'] \arrow[dr, "\succ_{right}"] & \\
\Big(P^y||_y(R^y|_z S)\Big)\Big|_x Q \arrow[d, "\succ"] & & \Big((P^y|_x Q)||_y R^y\Big)\Big|_z S \arrow[d, "\succ"] \\
\Big((P^y||_y R^y)|_z S\Big)\Big|_x Q & \equiv & \Big((P^y||_y R^y)|_x Q\Big)\Big|_z S
\end{tikzcd}$$

Confluence de $\rightarrow$ et $\succ$

Fermeture spécifique de $\equiv$ pour $\rightarrow$, avec $\succ$: donner un exemple

Le système de types : langage et règles

Préservation du type : proposition et un exemple (en 2 slides ?)

Terminaison de $\rightarrow$ et $\succ$ (+ un exemple ?)

Extension du système de réduction

Élimination des coupures

Conclusion

conclure ici : projection (on ne la présente pas vraiment ici, juste évoquée à l'oral éventuellement), limitations des choix faits.