

Control Flow Analysis for the π -calculus

Samuel Mimram

MPRI

22 juin 2005

Objectifs

- π -calcul : modèle des programmes concurrents (e.g. un serveur qui communique des informations par des canaux)
- On veut prouver certaines propriétés de sécurité sur ces programmes (des informations secrètes ne sont pas divulguées)
- On veut le faire automatiquement¹ (\rightarrow par analyse de flot de contrôle)

¹On perd bien sûr la complétude.

Syntaxe du π -calcul

Termes :

$$P ::= 0 \mid \mu.P \mid P + P \mid P|P \mid (\nu x)P \\ \mid [x = y]P \mid !P$$

Préfixes :

$$\mu ::= \tau \mid x(y) \mid \bar{x}y$$

$x(y)$ sera aussi noté xy

Syntaxe du π -calcul

Termes :

$$P ::= 0 \mid \mu.P \mid P + P \mid P|P \mid (\nu x^\chi)P \\ \mid [x = y]P \mid !P$$

Préfixes :

$$\mu ::= \tau \mid x(y^\beta) \mid \bar{x}y \mid \bar{x}(y)$$

Lieurs :

- $\beta \in \mathcal{B}$: *binders*
- $\chi \in \mathcal{C}$: *channels*

Équivalence \equiv : congruence structurelle

- $(\nu x^\chi)(\nu y^{\chi'})P \equiv (\nu y^{\chi'})P$
(si $x \neq y$, sinon $(\nu x^\chi)P \equiv (\nu x^{\chi'})P$)
- $[x = x]P \equiv P$

Un exemple de réduction

$$\begin{aligned} \bar{a}b.0 \mid (\nu x)(\bar{a}x.0) \mid a(x).\bar{c}x.0 &\longrightarrow 0 \mid (\nu x)(\bar{a}x).0 \mid \bar{c}b.0 \\ &\longrightarrow \bar{a}b.0 \mid (\nu x)(0 \mid \bar{c}x.0) \end{aligned}$$

Un exemple de réduction

$$\begin{aligned} \bar{a}b.0 \mid (\nu x)(\bar{a}x.0) \mid a(x).\bar{c}x.0 &\longrightarrow 0 \mid (\nu x)(\bar{a}x).0 \mid \bar{c}b.0 \\ &\longrightarrow \bar{a}b.0 \mid (\nu x)(0 \mid \bar{c}x.0) \end{aligned}$$

La première peut se décomposer en

$$\frac{\bar{a}b.0 \xrightarrow{\bar{a}b} 0 \quad a(x).\bar{c}x.0 \xrightarrow{ab} \bar{c}b.0}{\bar{a}b.0 \mid a(x).\bar{c}x.0 \xrightarrow{\tau} \bar{c}b.0}$$

Un exemple de réduction

$$\begin{aligned} \bar{a}b.0 \mid (\nu x)(\bar{a}x.0) \mid a(x).\bar{c}x.0 &\longrightarrow 0 \mid (\nu x)(\bar{a}x).0 \mid \bar{c}b.0 \\ &\longrightarrow \bar{a}b.0 \mid (\nu x)(0 \mid \bar{c}x.0) \end{aligned}$$

La première peut se décomposer en

$$\frac{\bar{a}b.0 \xrightarrow{\bar{a}b} 0 \quad a(x).\bar{c}x.0 \xrightarrow{ab} \bar{c}b.0}{\bar{a}b.0 \mid a(x).\bar{c}x.0 \xrightarrow{\tau} \bar{c}b.0}$$

et seconde en

$$\frac{(\nu x)(\bar{a}x.0) \xrightarrow{\bar{a}(x)} 0 \quad a(x).\bar{c}x.0 \xrightarrow{ax} \bar{c}x.0}{(\nu x)(\bar{a}x.0) \mid a(x).\bar{c}x.0 \xrightarrow{\tau} (\nu x)(\bar{c}x.0)}$$

Sémantique du π -calcul

$$\frac{\mu \neq x(y)}{\mu.P \xrightarrow{\mu} P} \text{(Act)}$$

$$\frac{\text{bn}(\mu) \cap \text{fn}(P_2) = \emptyset \quad P \xrightarrow{\mu} Q \quad x \notin \text{fn}(\mu)}{(\nu x)P \xrightarrow{\mu} (\nu x)Q} \text{(Res)}$$

$$\frac{P_1 \xrightarrow{\bar{x}(y)} Q_1 \quad P_2 \xrightarrow{xy} Q_2 \quad y \notin \text{fn}(P_2)}{P_1|P_2 \xrightarrow{\tau} (\nu y)(Q_1|Q_2)} \text{(Close)}$$

$$\frac{}{x(y).P \xrightarrow{xw} P[w/y]} \text{(Ein)}$$

$$\frac{x \neq y \quad P \xrightarrow{\bar{x}y} Q}{(\nu y)P \xrightarrow{\bar{x}(y)} Q} \text{(Open)}$$

$$\frac{P_1 \xrightarrow{\bar{x}y} Q_1 \quad P_2 \xrightarrow{xy} Q_2}{P_1|P_2 \xrightarrow{\tau} Q_1|Q_2} \text{(Com)}$$

passage à \equiv , | et +

Sémantique du π -calcul

$$\frac{\mu \neq x(y^\beta)}{\mu.P \xrightarrow[\varepsilon]{\mu} P} \text{(Act)}$$

$$\text{bn}(\mu) \cap \text{fn}(P_2) = \emptyset$$

$$\frac{P \xrightarrow[\lambda]{\mu} Q \quad x \notin \text{fn}(\mu)}{(\nu x^\lambda)P \xrightarrow[\lambda]{\mu} (\nu x^\lambda)Q} \text{(Res)}$$

$$y \notin \text{fn}(P_2)$$

$$\frac{P_1 \xrightarrow[\lambda]{\bar{x}(y)} Q_1 \quad P_2 \xrightarrow[\lambda]{xy} Q_2}{P_1|P_2 \xrightarrow[\varepsilon]{\tau} (\nu y^\lambda)(Q_1|Q_2)} \text{(Close)}$$

$$\frac{}{x(y^\beta).P \xrightarrow[\lambda]{xw} P[w/y]} \text{(Ein)}$$

$$x \neq y$$

$$\frac{P \xrightarrow[\varepsilon]{\bar{x}y} Q}{(\nu y^\lambda)P \xrightarrow[\lambda]{\bar{x}(y)} Q} \text{(Open)}$$

$$\frac{P_1 \xrightarrow[\varepsilon]{\bar{x}y} Q_1 \quad P_2 \xrightarrow[\varepsilon]{xy} Q_2}{P_1|P_2 \xrightarrow[\varepsilon]{\tau} Q_1|Q_2} \text{(Com)}$$

passage à \equiv , | et + $\lambda \in \mathcal{C} \cup \{\varepsilon\}$

Un jugement de correction : la validation

$$(\rho, \kappa) \models_{\text{me}} P$$

- $\text{me} : \mathcal{N} \rightarrow (\mathcal{B} \cup \mathcal{C})$: environnement de marqueurs
 (un nom unique pour chaque canal)
- $\rho : \mathcal{B} \rightarrow \wp(\mathcal{C})$: environnement abstrait
 (canaux auquel un lieu peut être lié)
- $\kappa : \mathcal{C} \rightarrow \wp(\mathcal{C})$: environnement de canaux abstrait
 (canaux qui peuvent transiter par un canal)

Doit être correct (approximation)

Un exemple

$$P = a(x^{\beta_0}).(\nu b^{\chi_0})(\nu c^{\chi_1}) ((\bar{b}a.\bar{x}x.b(x^{\beta_1}).\bar{x}c + \bar{b}d.\bar{a}c) | b(x^{\beta_2}).\bar{b}x) | d(x^{\beta_3})$$

On a par exemple $(\rho, \kappa) \models_{\text{me}} P$ avec

- $\text{me} \begin{cases} a \mapsto \chi_2 \\ d \mapsto \chi_3 \end{cases}$
- $\rho \begin{cases} \beta_1, \beta_2 \mapsto \{\chi_0, \chi_1, \chi_2, \chi_3, \chi_4\} \\ \beta_0, \beta_3 \mapsto \{\chi_1, \chi_2, \chi_3, \chi_4\} \end{cases}$
- $\kappa \begin{cases} \chi_0 \mapsto \{\chi_0, \chi_1, \chi_2, \chi_3, \chi_4\} \\ \chi_{i,i>0} \mapsto \{\chi_1, \chi_2, \chi_3, \chi_4\} \end{cases}$

Définition de \models

$(\rho, \kappa) \models_{\text{me}}$	ssi
0	\top
$\tau.P$	$(\rho, \kappa) \models_{\text{me}} P$
$\bar{x}y.P$	$(\rho, \kappa) \models_{\text{me}} P$ et $\forall \chi \in \rho(\text{me}(x)), \rho(\text{me}(y)) \subseteq \kappa(\chi)$
$x(y^\beta).P$	$(\rho, \kappa) \models_{\text{me}[y \mapsto \beta]} P$ et $\forall \chi \in \rho(\text{me}(x)), \kappa(\chi) \subseteq \rho(\beta)$
$P_1 + P_2, P_1 P_2$	$(\rho, \kappa) \models_{\text{me}} P_1$ et $(\rho, \kappa) \models_{\text{me}} P_2$
$(\nu x^\chi)P$	$(\rho, \kappa) \models_{\text{me}[x \mapsto \chi]} P$
$[x = y]P$	$(\rho(\text{me}(x)) \cap \rho(\text{me}(y)) \neq \emptyset \vee \text{me}(x) = \text{me}(y))$ $\Rightarrow (\rho, \kappa) \models_{\text{me}} P$
$!P$	$(\rho, \kappa) \models_{\text{me}} P$

Existence de solutions

- On ordonne (ρ, κ) par \sqsubseteq qui est l'extension point à point de \subseteq
- L'ensemble des solutions est alors un treillis complet

Théorème

Pour tous m_e , P et $(\bar{\rho}, \bar{\kappa})$, l'ensemble

$$\{(\rho, \kappa) \mid (\rho, \kappa) \models_{m_e} P \wedge (\bar{\rho}, \bar{\kappa}) \sqsubseteq (\rho, \kappa)\}$$

est une famille de Moore.

- Il existe toujours une plus petite solution (avec $(\bar{\rho}, \bar{\kappa}) = (\perp, \perp)$)
- Il existe une procédure constructive, cubique en la taille du processus

Correction

Si $\text{me}[\text{fin}(P)] \subseteq \mathcal{C}$, $(\rho, \kappa) \models_{\text{me}} P$ et $P \xrightarrow[\lambda]{\mu} Q$ alors

si $\mu =$	alors
τ	$\lambda = \varepsilon$ et $(\rho, \kappa) \models_{\text{me}} Q$ et $\text{me}[\text{fin}(Q)] \subseteq \mathcal{C}$
$\bar{x}y$	$\lambda = \varepsilon$ et $(\rho, \kappa) \models_{\text{me}} Q$ et $\text{me}[\text{fin}(Q)] \subseteq \mathcal{C}$ et $\rho(\text{me}(y)) \subseteq \bigcap_{\chi' \in \rho(\text{me}(x))} \kappa(\chi')$
$\bar{x}(y)$	$\lambda = \chi$ (pour un $\chi \in \mathcal{C}$) et $(\rho, \kappa) \models_{\text{me}[y \mapsto \chi]} Q$ et $(\text{me}[y \mapsto \chi])[\text{fin}(Q)] \subseteq \mathcal{C}$ et $\rho(\chi) \subseteq \bigcap_{\chi' \in \rho(\text{me}(x))} \kappa(\chi')$
xy	si $\lambda = \varepsilon$, $\text{me}(y) \in \mathcal{C}$ et $\rho(\text{me}(y)) \subseteq \bigcap_{\chi' \in \rho(\text{me}(x))} \kappa(\chi')$ alors $(\rho, \kappa) \models_{\text{me}} Q$ et $\text{me}[\text{fin}(Q)] \subseteq \mathcal{C}$
xy	si $\lambda = \chi$, $\rho(\chi) \subseteq \bigcap_{\chi' \in \rho(\text{me}(x))} \kappa(\chi')$ et $y \notin \text{fn}(P)$ alors $(\rho, \kappa) \models_{\text{me}[y \mapsto \chi]} Q$ et $(\text{me}[y \mapsto \chi])[\text{fin}(Q)] \subseteq \mathcal{C}$

Preuve : par induction sur la dérivation de $P \xrightarrow[\lambda]{\mu} Q$.

Définition du problème

- Problème : on ne veut pas qu'un nom de canal secret (créé par un ν) transite par un canal public
- $\mathcal{S} \subseteq \mathcal{C}$: canaux secrets (\Rightarrow canaux publics : $\mathcal{P} = \mathcal{C} \setminus \mathcal{S}$)

Définition

Une paire (P, me) est dite admissible pour l'ensemble $\mathcal{S} \subseteq \mathcal{C}$ de canaux secrets ssi

$$\text{me}[\text{fin}(P)] \subseteq \mathcal{C} \quad \text{et} \quad \text{me}[\text{fin}(P)] \cap \mathcal{S} = \emptyset$$

$$(\Leftrightarrow \text{me}[\text{fin}(P)] \subseteq \mathcal{P})$$

Définition (Réduction censurée)

Avec \mathcal{P} , me_P et S donnés,

$$(P, \text{me}_P) \xrightarrow[\lambda]{\mu} (Q, \text{me}_Q)$$

est une réduction censurée ssi

$$\text{me}_Q = \begin{cases} \text{me}_P & \text{si } \lambda = \varepsilon \\ \text{me}_P[\text{obj}(\mu) \mapsto \chi] & \text{si } \lambda = \chi \end{cases}$$

et est défini dès que

① $P \xrightarrow[\chi]{\mu} Q$ et

② si $\mu = xy$ alors $\begin{cases} \text{me}_P(y) \in \mathcal{P} & \text{si } \lambda = \varepsilon \\ \lambda \in \mathcal{P} \text{ et } y \notin \text{fn}(P) & \text{si } \lambda = \chi. \end{cases}$

⇒ aucun nom secret ne peut être lu par une entrée libre

Les réductions censurées préservent l'admissibilité.

Théorème

Soient (P, me_P) un couple admissible pour \mathcal{S} et $(P, \text{me}_P) \xrightarrow[\lambda]{\mu} (Q, \text{me}_Q)$ telle que si $\mu = \bar{x}(y)$ alors $\lambda = \chi \in \mathcal{P}$. Alors (Q, me_Q) est admissible pour \mathcal{S} .

Processus sans fuite

Notre notion de sécurité :

Définition (Processus sans fuite)

Un processus P est dit sans fuite par rapport à S et me_P ssi si

$$(P, \text{me}_P) \Longrightarrow^* (Q, \text{me}_Q)$$

alors il n'y a aucune paire (R, me_R) telle que

$$(Q, \text{me}_Q) \xrightarrow[\chi]{\bar{x}(y)} (R, \text{me}_R)$$

avec $\chi \in S$.

Notion dynamique.

Processus confiné

Notion statique :

Définition (Processus confiné)

Soit (P, me) une paire admissible pour un \mathcal{S} donné. Un processus P est dit confiné par rapport à \mathcal{S} et me ssi il existe ρ et κ tels que

$$(\rho, \kappa) \models_{\text{me}} P$$

et

$$\kappa(\chi) = \begin{cases} \mathcal{C} & \text{si } \chi \in \mathcal{S} \\ \mathcal{P} & \text{si } \chi \in \mathcal{P} \end{cases}$$

Théorème (Subject reduction du confinement)

*Si P est confiné (par rapport à \mathcal{S} et me_P), $(P, \text{me}_P) \xrightarrow[\lambda]{\mu} (Q, \text{me}_Q)$
et $\text{me}_P[\text{fin}(P)] \subseteq \mathcal{P}$, alors Q est confiné (par rapport à \mathcal{S} et me_Q)
et $\text{me}_Q[\text{fin}(Q)] \subseteq \mathcal{P}$.*

\Rightarrow le confinement restera vrai après n'importe quelle réduction censurée

Théorème

Si P est confiné par rapport à \mathcal{S} et me_P alors P n'a pas de fuite par rapport à \mathcal{S} et me_P .

\Rightarrow le confinement est une notion statique qui permet de vérifier la sécurité

- Nous avons défini une notion de validation sémantique
- Il existe un moyen de calculer la plus petite solution qui valide un processus
- Nous avons défini une notion de sécurité dynamique
- Nous avons exhibé une notion statique qui correspond à la sécurité et qui est calculable grâce à la validation