Une bisimulation ouverte pour le spi calcul

Sébastien Briais

Faculté Informatique et Communication
École Polytechnique Fédérale de Lausanne

LIP-ENS Lyon
1er Juin 2007
Lyon, FRANCE

Plan

Plan

Syntaxe

- Ensemble dénombrable de noms : canaux de communication, données, ...

Syntaxe

- Ensemble dénombrable de noms : canaux de communication, données, ...
- Processus

$$P, Q \quad ::=$$

Syntaxe

- Ensemble dénombrable de noms : canaux de communication, données, ...
- Processus

$$P, Q \quad ::= \quad \mathbf{0}$$

Syntaxe

- Ensemble dénombrable de noms : canaux de communication, données, ...
- Processus

$$P, Q \quad ::= \quad \mathbf{0} \mid a(x).P \mid \overline{a}\langle b \rangle.P$$

Syntaxe

- Ensemble dénombrable de noms : canaux de communication, données, ...
- Processus

$$\begin{array}{rcl} P, Q & ::= & \mathbf{0} \mid a(x).P \mid \overline{a}\langle b\rangle.P \\ & \mid & [a=b]P \end{array}$$

Syntaxe

- Ensemble dénombrable de noms : canaux de communication, données, ...
- Processus

$$\begin{array}{rcl} P, Q & ::= & \mathbf{0} \mid a(x).P \mid \overline{a}\langle b\rangle.P \\ & \mid & [a{=}b]P \mid (\nu x)\, P \end{array}$$

Syntaxe

- Ensemble dénombrable de noms : canaux de communication, données, ...
- Processus

$$\begin{array}{rcl} P, Q & ::= & \mathbf{0} \mid a(x).P \mid \overline{a}\langle b\rangle.P \\ & \mid & [a=b]P \mid (\nu x)\, P \\ & \mid & P \| Q \end{array}$$

Syntaxe

- Ensemble dénombrable de noms : canaux de communication, données, ...
- Processus

$$\begin{array}{rcl} P, Q & ::= & \mathbf{0} \mid a(x).P \mid \overline{a}\langle b\rangle.P \\ & \mid & [a{=}b]P \mid (\nu x)\, P \\ & \mid & P \| Q \mid P + Q \end{array}$$

Syntaxe

- Ensemble dénombrable de noms : canaux de communication, données, ...
- Processus

$$\begin{array}{rcl} P, Q & ::= & \mathbf{0} \mid a(x).P \mid \overline{a}\langle b\rangle.P \\ & \mid & [a{=}b]P \mid (\nu x)\, P \\ & \mid & P \| Q \mid P + Q \mid\, !\, P \end{array}$$

Syntaxe

- Ensemble dénombrable de noms : canaux de communication, données, ...
- Processus

$$\begin{array}{rcl} P, Q & ::= & \mathbf{0} \mid a(x).P \mid \overline{a}\langle b\rangle.P \\ & \mid & [a=b]P \mid (\nu x)\, P \\ & \mid & P \| Q \mid P + Q \mid !\, P \end{array}$$

- Agents

$$A \quad ::= \quad P$$

Syntaxe

- Ensemble dénombrable de noms : canaux de communication, données, ...
- Processus

$$\begin{array}{rcl} P, Q & ::= & \mathbf{0} \mid a(x).P \mid \overline{a}\langle b\rangle.P \\ & \mid & [a=b]P \mid (\nu x)\, P \\ & \mid & P \| Q \mid P + Q \mid !\, P \end{array}$$

- Agents

$$\begin{array}{rcl} A & ::= & P \\ & \mid & (x)P \end{array}$$

Syntaxe

- Ensemble dénombrable de noms : canaux de communication, données, ...
- Processus

$$\begin{array}{rcl} P, Q & ::= & \mathbf{0} \mid a(x).P \mid \overline{a}\langle b\rangle.P \\ & \mid & [a{=}b]P \mid (\nu x)\, P \\ & \mid & P \| Q \mid P + Q \mid\, !\, P \end{array}$$

- Agents

$$\begin{array}{rcll} A & ::= & P & \\ & \mid & (x)P & \\ & \mid & (\nu \tilde{z})\, \langle y\rangle P & \text{avec } \{\tilde{z}\} \subseteq \{y\} \end{array}$$

On a donc $\tilde{z} = \epsilon$ ou $\tilde{z} = y$.

Composition des agents et des processus

- Restriction :

$$(\nu x)\, P \quad := \quad (\nu x)\, P$$

Composition des agents et des processus

- Restriction :

$$\begin{aligned} (\nu x)\, P &:= (\nu x)\, P \\ (\nu x)\, ((y)P) &:= (y)(\nu x)\, P \qquad \text{si } y \neq x \end{aligned}$$

Composition des agents et des processus

- Restriction :

$$
\begin{array}{rcll}
(\nu x)\, P & := & (\nu x)\, P & \\
(\nu x)\, ((y)P) & := & (y)(\nu x)\, P & \text{si } y \neq x \\
(\nu x)\, ((\nu \tilde{z})\, \langle y \rangle P) & := & (\nu \tilde{z})\, \langle y \rangle (\nu x)\, P & \text{si } y \notin \{\tilde{z}\} \text{ et } x \neq y \\
(\nu x)\, ((\nu \tilde{z})\, \langle y \rangle P) & := & (\nu x \tilde{z})\, \langle y \rangle P & \text{si } y \notin \{\tilde{z}\} \text{ et } x = y
\end{array}
$$

Composition des agents et des processus

- Restriction :

$$
\begin{array}{rcll}
(\nu x)\, P & := & (\nu x)\, P & \\
(\nu x)\, ((y)P) & := & (y)(\nu x)\, P & \text{si } y \neq x \\
(\nu x)\, ((\nu \tilde{z})\, \langle y \rangle P) & := & (\nu \tilde{z})\, \langle y \rangle (\nu x)\, P & \text{si } y \notin \{\tilde{z}\} \text{ et } x \neq y \\
(\nu x)\, ((\nu \tilde{z})\, \langle y \rangle P) & := & (\nu x \tilde{z})\, \langle y \rangle P & \text{si } y \notin \{\tilde{z}\} \text{ et } x = y
\end{array}
$$

- Composition parallèle :

Composition des agents et des processus

- Restriction :

$$
\begin{array}{rcll}
(\nu x)\, P & := & (\nu x)\, P & \\
(\nu x)\, ((y)P) & := & (y)(\nu x)\, P & \text{si } y \neq x \\
(\nu x)\, ((\nu \tilde{z})\, \langle y \rangle P) & := & (\nu \tilde{z})\, \langle y \rangle (\nu x)\, P & \text{si } y \notin \{\tilde{z}\} \text{ et } x \neq y \\
(\nu x)\, ((\nu \tilde{z})\, \langle y \rangle P) & := & (\nu x \tilde{z})\, \langle y \rangle P & \text{si } y \notin \{\tilde{z}\} \text{ et } x = y
\end{array}
$$

- Composition parallèle :

$$
((x)P) \| Q \quad := \quad (x)(P \| Q) \qquad \text{si } x \notin \text{fn}(Q)
$$

Composition des agents et des processus

- Restriction :

$$
\begin{array}{rcll}
(\nu x)\, P & := & (\nu x)\, P & \\
(\nu x)\, ((y)P) & := & (y)(\nu x)\, P & \text{si } y \neq x \\
(\nu x)\, ((\nu \tilde{z})\, \langle y \rangle P) & := & (\nu \tilde{z})\, \langle y \rangle (\nu x)\, P & \text{si } y \notin \{\tilde{z}\} \text{ et } x \neq y \\
(\nu x)\, ((\nu \tilde{z})\, \langle y \rangle P) & := & (\nu x \tilde{z})\, \langle y \rangle P & \text{si } y \notin \{\tilde{z}\} \text{ et } x = y
\end{array}
$$

- Composition parallèle :

$$
\begin{array}{rcll}
((x)P) \| Q & := & (x)(P \| Q) & \text{si } x \notin \mathrm{fn}(Q) \\
((\nu \tilde{z})\, \langle y \rangle P) \| Q & := & (\nu \tilde{z})\, \langle y \rangle (P \| Q) & \text{si } \{\tilde{z}\} \cap \mathrm{fn}(Q) = \emptyset
\end{array}
$$

Composition des agents et des processus

- Restriction :

$$
\begin{array}{rcll}
(\boldsymbol{\nu} x)\, P & := & (\nu x)\, P & \\
(\boldsymbol{\nu} x)\, ((y)P) & := & (y)(\nu x)\, P & \text{si } y \neq x \\
(\boldsymbol{\nu} x)\, ((\nu \tilde{z})\, \langle y \rangle P) & := & (\nu \tilde{z})\, \langle y \rangle (\nu x)\, P & \text{si } y \notin \{\tilde{z}\} \text{ et } x \neq y \\
(\boldsymbol{\nu} x)\, ((\nu \tilde{z})\, \langle y \rangle P) & := & (\nu x \tilde{z})\, \langle y \rangle P & \text{si } y \notin \{\tilde{z}\} \text{ et } x = y
\end{array}
$$

- Composition parallèle :

$$
\begin{array}{rcll}
((x)P) \| Q & := & (x)(P \| Q) & \text{si } x \notin \mathrm{fn}(Q) \\
((\nu \tilde{z})\, \langle y \rangle P) \| Q & := & (\nu \tilde{z})\, \langle y \rangle (P \| Q) & \text{si } \{\tilde{z}\} \cap \mathrm{fn}(Q) = \emptyset
\end{array}
$$

  + les version symétriques

Intéraction entre agents

- Pseudo-application :
  Étant données

Intéraction entre agents

- Pseudo-application :
  Étant données une abstraction $F = (x)P$

Intéraction entre agents

- Pseudo-application :
  Étant données une abstraction $F = (x)P$ et une concrétion $C = (\nu \tilde{z})\langle y \rangle Q$ (avec $\tilde{z} \cap \mathrm{fn}(P) = \emptyset$),

Intéraction entre agents

- Pseudo-application :
  Étant données une abstraction $F = (x)P$ et une concrétion $C = (\nu \tilde{z})\langle y \rangle Q$ (avec $\tilde{z} \cap \mathrm{fn}(P) = \emptyset$), on définit :

$$F \bullet C := (\nu \tilde{z})\,(P\{^{y}/_{x}\} \| Q)$$

Intéraction entre agents

- Pseudo-application :
  Étant données une abstraction $F = (x)P$ et une concrétion $C = (\nu \tilde{z})\langle y \rangle Q$ (avec $\tilde{z} \cap \mathrm{fn}(P) = \emptyset$), on définit :

$$F \bullet C := (\nu \tilde{z})\,(P\{^{y}/_{x}\} \| Q)$$

  et la version symétrique $C \bullet F$.

Système de transition

$$\textsc{Input}\ \frac{}{a(x).P \xrightarrow{a} (x)P}$$

Système de transition

$$\textsc{Input}\ \frac{}{a(x).P \xrightarrow{a} (x)P} \qquad \textsc{Output}\ \frac{}{\overline{a}\langle z\rangle.P \xrightarrow{\overline{a}} \langle z\rangle P}$$

Système de transition

$$\textsc{Input}\ \frac{}{a(x).P \xrightarrow{a} (x)P} \qquad \textsc{Output}\ \frac{}{\overline{a}\langle z\rangle.P \xrightarrow{\overline{a}} \langle z\rangle P}$$

$$\textsc{Close-L}\ \frac{P \xrightarrow{a} F \qquad Q \xrightarrow{\overline{a}} C}{P \| Q \xrightarrow{\tau} F \bullet C}$$

Système de transition

$$\textsc{Input}\ \frac{}{a(x).P \xrightarrow{a} (x)P} \qquad \textsc{Output}\ \frac{}{\overline{a}\langle z\rangle.P \xrightarrow{\overline{a}} \langle z\rangle P}$$

$$\textsc{Close-l}\ \frac{P \xrightarrow{a} F \qquad Q \xrightarrow{\overline{a}} C}{P \| Q \xrightarrow{\tau} F \bullet C} \qquad \textsc{Res}\ \frac{P \xrightarrow{\mu} A}{(\nu z)\, P \xrightarrow{\mu} (\nu z)\, A}\ z \notin \mathrm{n}(\mu)$$

Système de transition

$$\textsc{Input}\ \frac{}{a(x).P \xrightarrow{a} (x)P} \qquad \textsc{Output}\ \frac{}{\overline{a}\langle z\rangle.P \xrightarrow{\overline{a}} \langle z\rangle P}$$

$$\textsc{Close-L}\ \frac{P \xrightarrow{a} F \qquad Q \xrightarrow{\overline{a}} C}{P \| Q \xrightarrow{\tau} F \bullet C} \qquad \textsc{Res}\ \frac{P \xrightarrow{\mu} A}{(\nu z)\, P \xrightarrow{\mu} (\nu z)\, A}\ z \notin \mathrm{n}(\mu)$$

$$\textsc{IfThen}\ \frac{P \xrightarrow{\mu} P'}{[a=a]P \xrightarrow{\mu} P'}$$

Système de transition

$$\textsc{Input}\ \frac{}{a(x).P \xrightarrow{a} (x)P} \qquad \textsc{Output}\ \frac{}{\overline{a}\langle z\rangle.P \xrightarrow{\overline{a}} \langle z\rangle P}$$

$$\textsc{Close-L}\ \frac{P \xrightarrow{a} F \qquad Q \xrightarrow{\overline{a}} C}{P\|Q \xrightarrow{\tau} F \bullet C} \qquad \textsc{Res}\ \frac{P \xrightarrow{\mu} A}{(\nu z)\,P \xrightarrow{\mu} (\nu z)\,A}\ z \notin \mathrm{n}(\mu)$$

$$\textsc{IfThen}\ \frac{P \xrightarrow{\mu} P'}{[a=a]P \xrightarrow{\mu} P'} \qquad \textsc{Par-L}\ \frac{P \xrightarrow{\mu} A}{P\|Q \xrightarrow{\mu} A\|Q}$$

Système de transition

$$\textsc{Input}\ \frac{}{a(x).P \xrightarrow{a} (x)P} \qquad \textsc{Output}\ \frac{}{\overline{a}\langle z\rangle.P \xrightarrow{\overline{a}} \langle z\rangle P}$$

$$\textsc{Close-L}\ \frac{P \xrightarrow{a} F \qquad Q \xrightarrow{\overline{a}} C}{P \| Q \xrightarrow{\tau} F \bullet C} \qquad \textsc{Res}\ \frac{P \xrightarrow{\mu} A}{(\nu z)\, P \xrightarrow{\mu} (\nu z)\, A}\ z \notin \mathrm{n}(\mu)$$

$$\textsc{IfThen}\ \frac{P \xrightarrow{\mu} P'}{[a=a]P \xrightarrow{\mu} P'} \qquad \textsc{Par-L}\ \frac{P \xrightarrow{\mu} A}{P \| Q \xrightarrow{\mu} A \| Q} \qquad \textsc{Sum-L}\ \frac{P \xrightarrow{\mu} A}{P + Q \xrightarrow{\mu} A}$$

Système de transition

$$\textsc{Input}\ \frac{}{a(x).P \xrightarrow{a} (x)P} \qquad \textsc{Output}\ \frac{}{\overline{a}\langle z\rangle.P \xrightarrow{\overline{a}} \langle z\rangle P}$$

$$\textsc{Close-l}\ \frac{P \xrightarrow{a} F \qquad Q \xrightarrow{\overline{a}} C}{P\|Q \xrightarrow{\tau} F \bullet C} \qquad \textsc{Res}\ \frac{P \xrightarrow{\mu} A}{(\nu z)\,P \xrightarrow{\mu} (\nu z)\,A}\ z \notin \mathrm{n}(\mu)$$

$$\textsc{IfThen}\ \frac{P \xrightarrow{\mu} P'}{[a=a]P \xrightarrow{\mu} P'} \qquad \textsc{Par-l}\ \frac{P \xrightarrow{\mu} A}{P\|Q \xrightarrow{\mu} A\|Q} \qquad \textsc{Sum-l}\ \frac{P \xrightarrow{\mu} A}{P + Q \xrightarrow{\mu} A}$$

$$\textsc{Rep-act}\ \frac{P \xrightarrow{\mu} A}{!\,P \xrightarrow{\mu} A\|!\,P} \qquad \textsc{Rep-close}\ \frac{P \xrightarrow{a} F \qquad P \xrightarrow{\overline{a}} C}{!\,P \xrightarrow{\tau} F \bullet C\|!\,P}$$

Système de transition

$$\textsc{Input}\ \frac{}{a(x).P \xrightarrow{a} (x)P} \qquad \textsc{Output}\ \frac{}{\overline{a}\langle z\rangle.P \xrightarrow{\overline{a}} \langle z\rangle P}$$

$$\textsc{Close-l}\ \frac{P \xrightarrow{a} F \qquad Q \xrightarrow{\overline{a}} C}{P\|Q \xrightarrow{\tau} F \bullet C} \qquad \textsc{Res}\ \frac{P \xrightarrow{\mu} A}{(\nu z)\,P \xrightarrow{\mu} (\nu z)\,A}\ z \notin \mathrm{n}(\mu)$$

$$\textsc{IfThen}\ \frac{P \xrightarrow{\mu} P'}{[a{=}a]P \xrightarrow{\mu} P'} \qquad \textsc{Par-l}\ \frac{P \xrightarrow{\mu} A}{P\|Q \xrightarrow{\mu} A\|Q} \qquad \textsc{Sum-l}\ \frac{P \xrightarrow{\mu} A}{P + Q \xrightarrow{\mu} A}$$

$$\textsc{Rep-act}\ \frac{P \xrightarrow{\mu} A}{!\,P \xrightarrow{\mu} A\|!\,P} \qquad \textsc{Rep-close}\ \frac{P \xrightarrow{a} F \qquad P \xrightarrow{\overline{a}} C}{!\,P \xrightarrow{\tau} F \bullet C\|!\,P}$$

+ Close-r, Par-r, Sum-r et Alpha.

Bisimulation précoce et tardive

- $\mathcal{R}$ est une simulation précoce si pour tout $(P, Q) \in \mathcal{R}$

Bisimulation précoce et tardive

- $\mathcal{R}$ est une simulation précoce si pour tout $(P, Q) \in \mathcal{R}$
  - si $P \xrightarrow{\tau} P'$ alors il existe Q' tel que $Q \xrightarrow{\tau} Q'$ et $(P', Q') \in \mathcal{R}$

Bisimulation précoce et tardive

- $\mathcal{R}$ est une simulation précoce si pour tout $(P, Q) \in \mathcal{R}$
  - si $P \xrightarrow{\tau} P'$ alors il existe Q' tel que $Q \xrightarrow{\tau} Q'$ et $(P', Q') \in \mathcal{R}$
  - si $P \xrightarrow{\overline{a}} (\nu \tilde{z}) \langle y \rangle P'$ alors il existe Q' tel que $Q \xrightarrow{\overline{a}} (\nu \tilde{z}) \langle y \rangle Q'$ et $(P', Q') \in \mathcal{R}$

Bisimulation précoce et tardive

- $\mathcal{R}$ est une simulation précoce si pour tout $(P, Q) \in \mathcal{R}$
  - si $P \xrightarrow{\tau} P'$ alors il existe Q' tel que $Q \xrightarrow{\tau} Q'$ et $(P', Q') \in \mathcal{R}$
  - si $P \xrightarrow{\overline{a}} (\nu \tilde{z}) \langle y \rangle P'$ alors il existe Q' tel que $Q \xrightarrow{\overline{a}} (\nu \tilde{z}) \langle y \rangle Q'$ et $(P', Q') \in \mathcal{R}$
  - si $P \xrightarrow{a} (x)P'$ alors pour tout nom y, il existe Q' tel que $Q \xrightarrow{a} (x)Q'$ et $(P'\{^y/_x\}, Q'\{^y/_x\}) \in \mathcal{R}$

Bisimulation précoce et tardive

- $\mathcal{R}$ est une simulation précoce si pour tout $(P, Q) \in \mathcal{R}$
  - si $P \xrightarrow{\tau} P'$ alors il existe Q' tel que $Q \xrightarrow{\tau} Q'$ et $(P', Q') \in \mathcal{R}$
  - si $P \xrightarrow{\overline{a}} (\nu \tilde{z}) \langle y \rangle P'$ alors il existe Q' tel que $Q \xrightarrow{\overline{a}} (\nu \tilde{z}) \langle y \rangle Q'$ et $(P', Q') \in \mathcal{R}$
  - si $P \xrightarrow{a} (x)P'$ alors pour tout nom y, il existe Q' tel que $Q \xrightarrow{a} (x)Q'$ et $(P'\{^y/_x\}, Q'\{^y/_x\}) \in \mathcal{R}$
- $\mathcal{R}$ est une bisimulation précoce si de plus $\mathcal{R}$ est symétrique.

Bisimulation précoce et tardive

- $\mathcal{R}$ est une simulation précoce si pour tout $(P, Q) \in \mathcal{R}$
  - si $P \xrightarrow{\tau} P'$ alors il existe Q' tel que $Q \xrightarrow{\tau} Q'$ et $(P', Q') \in \mathcal{R}$
  - si $P \xrightarrow{\overline{a}} (\nu \tilde{z}) \langle y \rangle P'$ alors il existe Q' tel que $Q \xrightarrow{\overline{a}} (\nu \tilde{z}) \langle y \rangle Q'$ et $(P', Q') \in \mathcal{R}$
  - si $P \xrightarrow{a} (x)P'$ alors pour tout nom y, il existe Q' tel que $Q \xrightarrow{a} (x)Q'$ et $(P'\{^y/_x\}, Q'\{^y/_x\}) \in \mathcal{R}$
- $\mathcal{R}$ est une bisimulation précoce si de plus $\mathcal{R}$ est symétrique.
- $\mathcal{R}$ est une simulation tardive si pour tout $(P, Q) \in \mathcal{R}$

Bisimulation précoce et tardive

- $\mathcal{R}$ est une simulation précoce si pour tout $(P, Q) \in \mathcal{R}$
  - si $P \xrightarrow{\tau} P'$ alors il existe Q' tel que $Q \xrightarrow{\tau} Q'$ et $(P', Q') \in \mathcal{R}$
  - si $P \xrightarrow{\overline{a}} (\nu \tilde{z}) \langle y \rangle P'$ alors il existe Q' tel que $Q \xrightarrow{\overline{a}} (\nu \tilde{z}) \langle y \rangle Q'$ et $(P', Q') \in \mathcal{R}$
  - si $P \xrightarrow{a} (x)P'$ alors pour tout nom y, il existe Q' tel que $Q \xrightarrow{a} (x)Q'$ et $(P'\{^{y}/_{x}\}, Q'\{^{y}/_{x}\}) \in \mathcal{R}$
- $\mathcal{R}$ est une bisimulation précoce si de plus $\mathcal{R}$ est symétrique.
- $\mathcal{R}$ est une simulation tardive si pour tout $(P, Q) \in \mathcal{R}$
  - si $P \xrightarrow{\tau} P'$ alors ...

Bisimulation précoce et tardive

- $\mathcal{R}$ est une simulation précoce si pour tout $(P, Q) \in \mathcal{R}$
  - si $P \xrightarrow{\tau} P'$ alors il existe Q' tel que $Q \xrightarrow{\tau} Q'$ et $(P', Q') \in \mathcal{R}$
  - si $P \xrightarrow{\overline{a}} (\nu \tilde{z}) \langle y \rangle P'$ alors il existe Q' tel que $Q \xrightarrow{\overline{a}} (\nu \tilde{z}) \langle y \rangle Q'$ et $(P', Q') \in \mathcal{R}$
  - si $P \xrightarrow{a} (x)P'$ alors pour tout nom y, il existe Q' tel que $Q \xrightarrow{a} (x)Q'$ et $(P'\{^{y}/_{x}\}, Q'\{^{y}/_{x}\}) \in \mathcal{R}$
- $\mathcal{R}$ est une bisimulation précoce si de plus $\mathcal{R}$ est symétrique.
- $\mathcal{R}$ est une simulation tardive si pour tout $(P, Q) \in \mathcal{R}$
  - si $P \xrightarrow{\tau} P'$ alors ...
  - si $P \xrightarrow{\overline{a}} (\nu \tilde{z}) \langle y \rangle P'$ alors ...

Bisimulation précoce et tardive

- $\mathcal{R}$ est une simulation précoce si pour tout $(P, Q) \in \mathcal{R}$
  - si $P \xrightarrow{\tau} P'$ alors il existe Q' tel que $Q \xrightarrow{\tau} Q'$ et $(P', Q') \in \mathcal{R}$
  - si $P \xrightarrow{\overline{a}} (\nu \tilde{z}) \langle y \rangle P'$ alors il existe Q' tel que $Q \xrightarrow{\overline{a}} (\nu \tilde{z}) \langle y \rangle Q'$ et $(P', Q') \in \mathcal{R}$
  - si $P \xrightarrow{a} (x)P'$ alors pour tout nom y, il existe Q' tel que $Q \xrightarrow{a} (x)Q'$ et $(P'\{^y/_x\}, Q'\{^y/_x\}) \in \mathcal{R}$
- $\mathcal{R}$ est une bisimulation précoce si de plus $\mathcal{R}$ est symétrique.
- $\mathcal{R}$ est une simulation tardive si pour tout $(P, Q) \in \mathcal{R}$
  - si $P \xrightarrow{\tau} P'$ alors ...
  - si $P \xrightarrow{\overline{a}} (\nu \tilde{z}) \langle y \rangle P'$ alors ...
  - si $P \xrightarrow{a} (x)P'$ alors il existe Q' tel que $Q \xrightarrow{a} (x)Q'$ et pour tout nom y on a $(P'\{^y/_x\}, Q'\{^y/_x\}) \in \mathcal{R}$

Bisimulation précoce et tardive

- $\mathcal{R}$ est une simulation précoce si pour tout $(P, Q) \in \mathcal{R}$
  - si $P \xrightarrow{\tau} P'$ alors il existe Q' tel que $Q \xrightarrow{\tau} Q'$ et $(P', Q') \in \mathcal{R}$
  - si $P \xrightarrow{\overline{a}} (\nu \tilde{z}) \langle y \rangle P'$ alors il existe Q' tel que $Q \xrightarrow{\overline{a}} (\nu \tilde{z}) \langle y \rangle Q'$ et $(P', Q') \in \mathcal{R}$
  - si $P \xrightarrow{a} (x)P'$ alors pour tout nom y, il existe Q' tel que $Q \xrightarrow{a} (x)Q'$ et $(P'\{^y/_x\}, Q'\{^y/_x\}) \in \mathcal{R}$
- $\mathcal{R}$ est une bisimulation précoce si de plus $\mathcal{R}$ est symétrique.
- $\mathcal{R}$ est une simulation tardive si pour tout $(P, Q) \in \mathcal{R}$
  - si $P \xrightarrow{\tau} P'$ alors ...
  - si $P \xrightarrow{\overline{a}} (\nu \tilde{z}) \langle y \rangle P'$ alors ...
  - si $P \xrightarrow{a} (x)P'$ alors il existe Q' tel que $Q \xrightarrow{a} (x)Q'$ et pour tout nom y on a $(P'\{^y/_x\}, Q'\{^y/_x\}) \in \mathcal{R}$
- Bisimilarités : $\sim_e$, $\sim_l$

Bisimulation ouverte

- $\sim_e$ et $\sim_l$ ne sont pas des congruences

Bisimulation ouverte

- $\sim_e$ et $\sim_l$ ne sont pas des congruences
- car elles ne sont pas préservées par la réception :

$$P := x(z).\mathbf{0} \,\|\, \overline{y}\langle z\rangle.\mathbf{0}$$
$$Q := x(z).\overline{y}\langle z\rangle.\mathbf{0} + \overline{y}\langle z\rangle.x(z).\mathbf{0}$$

Bisimulation ouverte

- $\sim_e$ et $\sim_l$ ne sont pas des congruences
- car elles ne sont pas préservées par la réception :

$$P := x(z).\mathbf{0} \,\|\, \overline{y}\langle z\rangle.\mathbf{0}$$
$$Q := x(z).\overline{y}\langle z\rangle.\mathbf{0} + \overline{y}\langle z\rangle.x(z).\mathbf{0}$$

et $C[\cdot] = a(y).[\cdot]$

Bisimulation ouverte

- $\sim_e$ et $\sim_l$ ne sont pas des congruences
- car elles ne sont pas préservées par la réception :

$$P := x(z).\mathbf{0} \,\|\, \overline{y}\langle z\rangle.\mathbf{0}$$
$$Q := x(z).\overline{y}\langle z\rangle.\mathbf{0} + \overline{y}\langle z\rangle.x(z).\mathbf{0}$$

  et $C[\cdot] = a(y).[\cdot]$
- Congruence précoce : $P \sim_e^c Q \iff P\sigma \sim_e Q\sigma$ pour toute substitution σ.

Bisimulation ouverte

- $\sim_e$ et $\sim_l$ ne sont pas des congruences
- car elles ne sont pas préservées par la réception :

$$P := x(z).\mathbf{0} \,\|\, \overline{y}\langle z\rangle.\mathbf{0}$$
$$Q := x(z).\overline{y}\langle z\rangle.\mathbf{0} + \overline{y}\langle z\rangle.x(z).\mathbf{0}$$

  et $C[\cdot] = a(y).[\cdot]$
- Congruence précoce : $P \sim_e^c Q \iff P\sigma \sim_e Q\sigma$ pour toute substitution σ.
- Dans la (bi)simulation ouverte, la quantification sur les substitutions est rentrée à l'intérieur de la définition.

Bisimulation ouverte

- $\sim_e$ et $\sim_l$ ne sont pas des congruences
- car elles ne sont pas préservées par la réception :

$$P := x(z).\mathbf{0} \,\|\, \overline{y}\langle z\rangle.\mathbf{0}$$
$$Q := x(z).\overline{y}\langle z\rangle.\mathbf{0} + \overline{y}\langle z\rangle.x(z).\mathbf{0}$$

  et $C[\cdot] = a(y).[\cdot]$
- Congruence précoce : $P \sim_e^c Q \iff P\sigma \sim_e Q\sigma$ pour toute substitution σ.
- Dans la (bi)simulation ouverte, la quantification sur les substitutions est rentrée à l'intérieur de la définition.
- $\mathcal{R}$ est une simulation ouverte si pour tout $(P, Q) \in \mathcal{R}$

Bisimulation ouverte

- $\sim_e$ et $\sim_l$ ne sont pas des congruences
- car elles ne sont pas préservées par la réception :

$$P := x(z).\mathbf{0} \,\|\, \overline{y}\langle z\rangle.\mathbf{0}$$
$$Q := x(z).\overline{y}\langle z\rangle.\mathbf{0} + \overline{y}\langle z\rangle.x(z).\mathbf{0}$$

  et $C[\cdot] = a(y).[\cdot]$
- Congruence précoce : $P \sim_e^c Q \iff P\sigma \sim_e Q\sigma$ pour toute substitution σ.
- Dans la (bi)simulation ouverte, la quantification sur les substitutions est rentrée à l'intérieur de la définition.
- $\mathcal{R}$ est une simulation ouverte si pour tout $(P, Q) \in \mathcal{R}$ et tout σ

Bisimulation ouverte

- $\sim_e$ et $\sim_l$ ne sont pas des congruences
- car elles ne sont pas préservées par la réception :

$$P := x(z).\mathbf{0} \,\|\, \overline{y}\langle z\rangle.\mathbf{0}$$
$$Q := x(z).\overline{y}\langle z\rangle.\mathbf{0} + \overline{y}\langle z\rangle.x(z).\mathbf{0}$$

  et $C[\cdot] = a(y).[\cdot]$
- Congruence précoce : $P \sim_e^c Q \iff P\sigma \sim_e Q\sigma$ pour toute substitution σ.
- Dans la (bi)simulation ouverte, la quantification sur les substitutions est rentrée à l'intérieur de la définition.
- $\mathcal{R}$ est une simulation ouverte si pour tout $(P, Q) \in \mathcal{R}$ et tout σ
  - si $P\sigma \xrightarrow{\tau} P'$ alors il existe Q' tel que $Q\sigma \xrightarrow{\tau} Q'$ et $(P', Q') \in \mathcal{R}$

Bisimulation ouverte

- $\sim_e$ et $\sim_l$ ne sont pas des congruences
- car elles ne sont pas préservées par la réception :

$$P := x(z).\mathbf{0} \,\|\, \overline{y}\langle z\rangle.\mathbf{0}$$
$$Q := x(z).\overline{y}\langle z\rangle.\mathbf{0} + \overline{y}\langle z\rangle.x(z).\mathbf{0}$$

  et $C[\cdot] = a(y).[\cdot]$
- Congruence précoce : $P \sim_e^c Q \iff P\sigma \sim_e Q\sigma$ pour toute substitution σ.
- Dans la (bi)simulation ouverte, la quantification sur les substitutions est rentrée à l'intérieur de la définition.
- $\mathcal{R}$ est une simulation ouverte si pour tout $(P, Q) \in \mathcal{R}$ et tout σ
  - si $P\sigma \xrightarrow{\tau} P'$ alors il existe Q' tel que $Q\sigma \xrightarrow{\tau} Q'$ et $(P', Q') \in \mathcal{R}$
  - si $P\sigma \xrightarrow{\overline{a}} (\nu\tilde{z})\langle y\rangle P'$ alors il existe Q' tel que $Q\sigma \xrightarrow{\overline{a}} (\nu\tilde{z})\langle y\rangle Q'$ et $(P', Q') \in \mathcal{R}$

Bisimulation ouverte

- $\sim_e$ et $\sim_l$ ne sont pas des congruences
- car elles ne sont pas préservées par la réception :

$$P := x(z).\mathbf{0} \,\|\, \overline{y}\langle z\rangle.\mathbf{0}$$
$$Q := x(z).\overline{y}\langle z\rangle.\mathbf{0} + \overline{y}\langle z\rangle.x(z).\mathbf{0}$$

  et $C[\cdot] = a(y).[\cdot]$
- Congruence précoce : $P \sim_e^c Q \iff P\sigma \sim_e Q\sigma$ pour toute substitution σ.
- Dans la (bi)simulation ouverte, la quantification sur les substitutions est rentrée à l'intérieur de la définition.
- $\mathcal{R}$ est une simulation ouverte si pour tout $(P, Q) \in \mathcal{R}$ et tout σ
  - si $P\sigma \xrightarrow{\tau} P'$ alors il existe Q' tel que $Q\sigma \xrightarrow{\tau} Q'$ et $(P', Q') \in \mathcal{R}$
  - si $P\sigma \xrightarrow{\overline{a}} (\nu\tilde{z})\langle y\rangle P'$ alors il existe Q' tel que $Q\sigma \xrightarrow{\overline{a}} (\nu\tilde{z})\langle y\rangle Q'$ et $(P', Q') \in \mathcal{R}$
  - si $P\sigma \xrightarrow{a} (x)P'$ alors il existe Q' tel que $Q\sigma \xrightarrow{a} (x)Q'$ et $(P', Q') \in \mathcal{R}$

Bisimulation ouverte

- En fait, certaines substitutions ne devraient pas être considérées

Bisimulation ouverte

- En fait, certaines substitutions ne devraient pas être considérées

$$P := c(x).(\nu k)\,\overline{c}\langle k\rangle.[x=k]\overline{c}\langle c\rangle.\mathbf{0}$$
$$Q := c(x).(\nu k)\,\overline{c}\langle k\rangle.\mathbf{0}$$

Bisimulation ouverte

- En fait, certaines substitutions ne devraient pas être considérées

$$[x = k]\overline{c}\langle c\rangle.\mathbf{0}$$
$$\mathbf{0}$$

- $\{^{k}/_{x}\}$ ne sera pas une substitution à considérer

Bisimulation ouverte

- En fait, certaines substitutions ne devraient pas être considérées

$$[x = k]\overline{c}\langle c\rangle.\mathbf{0}$$
$$\mathbf{0}$$

- $\{^{k}/_{x}\}$ ne sera pas une substitution à considérer
- σ devrait "respecter" l'inégalité $x \neq k$

Bisimulation ouverte

- En fait, certaines substitutions ne devraient pas être considérées

$$[x = k]\overline{c}\langle c\rangle.\mathbf{0}$$
$$\mathbf{0}$$

- $\{^{k}/_{x}\}$ ne sera pas une substitution à considérer
- σ devrait "respecter" l'inégalité $x \neq k$
- $\mathcal{R}$ est une simulation ouverte si pour tout $(D, P, Q) \in \mathcal{R}$ et tout σ

Bisimulation ouverte

- En fait, certaines substitutions ne devraient pas être considérées

$$[x = k]\overline{c}\langle c\rangle.\mathbf{0}$$
$$\mathbf{0}$$

- $\{^{k}/_{x}\}$ ne sera pas une substitution à considérer
- σ devrait "respecter" l'inégalité $x \neq k$
- $\mathcal{R}$ est une simulation ouverte si pour tout $(D, P, Q) \in \mathcal{R}$ et tout $\sigma \triangleright D$

Bisimulation ouverte

- En fait, certaines substitutions ne devraient pas être considérées

$$[x = k]\overline{c}\langle c\rangle.\mathbf{0}$$
$$\mathbf{0}$$

- $\{^{k}/_{x}\}$ ne sera pas une substitution à considérer
- σ devrait "respecter" l'inégalité $x \neq k$
- $\mathcal{R}$ est une simulation ouverte si pour tout $(D, P, Q) \in \mathcal{R}$ et tout $\sigma \triangleright D$
  - si $P\sigma \xrightarrow{\tau} P'$ alors il existe Q' tel que $Q\sigma \xrightarrow{\tau} Q'$ et $(D\sigma, P', Q') \in \mathcal{R}$

Bisimulation ouverte

- En fait, certaines substitutions ne devraient pas être considérées

$$[x = k]\overline{c}\langle c\rangle.\mathbf{0}$$
$$\mathbf{0}$$

- $\{^{k}/_{x}\}$ ne sera pas une substitution à considérer
- σ devrait "respecter" l'inégalité $x \neq k$
- $\mathcal{R}$ est une simulation ouverte si pour tout $(D, P, Q) \in \mathcal{R}$ et tout $\sigma \triangleright D$
  - si $P\sigma \xrightarrow{\tau} P'$ alors il existe Q' tel que $Q\sigma \xrightarrow{\tau} Q'$ et $(D\sigma, P', Q') \in \mathcal{R}$
  - si $P\sigma \xrightarrow{a} (x)P'$ alors il existe Q' tel que $Q\sigma \xrightarrow{a} (x)Q'$ et $(D\sigma, P', Q') \in \mathcal{R}$

Bisimulation ouverte

- En fait, certaines substitutions ne devraient pas être considérées

$$[x = k]\overline{c}\langle c\rangle.\mathbf{0}$$
$$\mathbf{0}$$

- $\{^{k}/_{x}\}$ ne sera pas une substitution à considérer
- σ devrait "respecter" l'inégalité $x \neq k$
- $\mathcal{R}$ est une simulation ouverte si pour tout $(D, P, Q) \in \mathcal{R}$ et tout $\sigma \triangleright D$
  - si $P\sigma \xrightarrow{\tau} P'$ alors il existe Q' tel que $Q\sigma \xrightarrow{\tau} Q'$ et $(D\sigma, P', Q') \in \mathcal{R}$
  - si $P\sigma \xrightarrow{a} (x)P'$ alors il existe Q' tel que $Q\sigma \xrightarrow{a} (x)Q'$ et $(D\sigma, P', Q') \in \mathcal{R}$
  - si $P\sigma \xrightarrow{\overline{a}} (\nu\tilde{z})\langle y\rangle P'$ alors il existe Q' tel que $Q\sigma \xrightarrow{\overline{a}} (\nu\tilde{z})\langle y\rangle Q'$ et $(D\sigma, P', Q') \in \mathcal{R}$

Bisimulation ouverte

- En fait, certaines substitutions ne devraient pas être considérées

$$[x = k]\overline{c}\langle c\rangle.\mathbf{0}$$
$$\mathbf{0}$$

- $\{^{k}/_{x}\}$ ne sera pas une substitution à considérer
- σ devrait "respecter" l'inégalité $x \neq k$
- $\mathcal{R}$ est une simulation ouverte si pour tout $(D, P, Q) \in \mathcal{R}$ et tout $\sigma \triangleright D$
  - si $P\sigma \xrightarrow{\tau} P'$ alors il existe Q' tel que $Q\sigma \xrightarrow{\tau} Q'$ et $(D\sigma, P', Q') \in \mathcal{R}$
  - si $P\sigma \xrightarrow{a} (x)P'$ alors il existe Q' tel que $Q\sigma \xrightarrow{a} (x)Q'$ et $(D\sigma, P', Q') \in \mathcal{R}$
  - si $P\sigma \xrightarrow{\overline{a}} (\nu\tilde{z})\langle y\rangle P'$ alors il existe Q' tel que $Q\sigma \xrightarrow{\overline{a}} (\nu\tilde{z})\langle y\rangle Q'$ et $(D\sigma \cup \{\tilde{z}\} \otimes (\mathsf{fn}(P\sigma, Q\sigma) \cup \mathsf{n}(D\sigma)), P', Q') \in \mathcal{R}$

Bisimulation ouverte (quelques propriétés)

- La quantification sur toutes les substitutions confèrent un côté paresseux à la bisimulation ouverte :

Bisimulation ouverte (quelques propriétés)

- La quantification sur toutes les substitutions confèrent un côté paresseux à la bisimulation ouverte :

$$P := c(x).(\tau + \tau.\tau)$$
$$Q := c(x).(\tau + \tau.\tau + \tau.[x = a]\tau)$$

Bisimulation ouverte (quelques propriétés)

- La quantification sur toutes les substitutions confèrent un côté paresseux à la bisimulation ouverte :

$$P := c(x).(\tau + \tau.\tau)$$
$$Q := c(x).(\tau + \tau.\tau + \tau.[x = a]\tau)$$

- La bisimulation ouverte est une congruence

Bisimulation ouverte (quelques propriétés)

- La quantification sur toutes les substitutions confèrent un côté paresseux à la bisimulation ouverte :

$$P := c(x).(\tau + \tau.\tau)$$
$$Q := c(x).(\tau + \tau.\tau + \tau.[x = a]\tau)$$

- La bisimulation ouverte est une congruence
- Elle est “facilement” implémentable (MWB, ABC) via une version symbolique

Plan

Le spi calcul

Le spi calcul

- Modélisation et étude des protocoles cryptographiques

Le spi calcul

- Modélisation et étude des protocoles cryptographiques
- Messages

$$M, N \quad ::= \quad x \mid (M\,.\,N) \mid \mathrm{Enc}^{\mathrm{S}}_{N} M$$

Le spi calcul

- Modélisation et étude des protocoles cryptographiques
- Messages

$$M, N \quad ::= \quad x \mid (M \,.\, N) \mid \mathrm{Enc}^{\mathrm{s}}_{N} M$$

- Expressions

$$\begin{aligned} E, F \quad ::= \quad & x \mid (E \,.\, F) \mid \mathrm{Enc}^{\mathrm{s}}_{F} E \\ \mid \quad & \pi_1 (E) \mid \pi_2 (E) \mid \mathrm{Dec}^{\mathrm{s}}_{F} E \end{aligned}$$

Le spi calcul

- Modélisation et étude des protocoles cryptographiques
- Messages

$$M, N \quad ::= \quad x \mid (M \,.\, N) \mid \mathrm{Enc}^{\mathrm{s}}_{N} M$$

- Expressions

$$\begin{aligned} E, F \quad ::= \quad & x \mid (E \,.\, F) \mid \mathrm{Enc}^{\mathrm{s}}_{F} E \\ \mid \quad & \pi_1(E) \mid \pi_2(E) \mid \mathrm{Dec}^{\mathrm{s}}_{F} E \end{aligned}$$

- Gardes

$$\phi \quad ::= \quad [E = F] \mid [E : \boldsymbol{N}]$$

Syntaxe

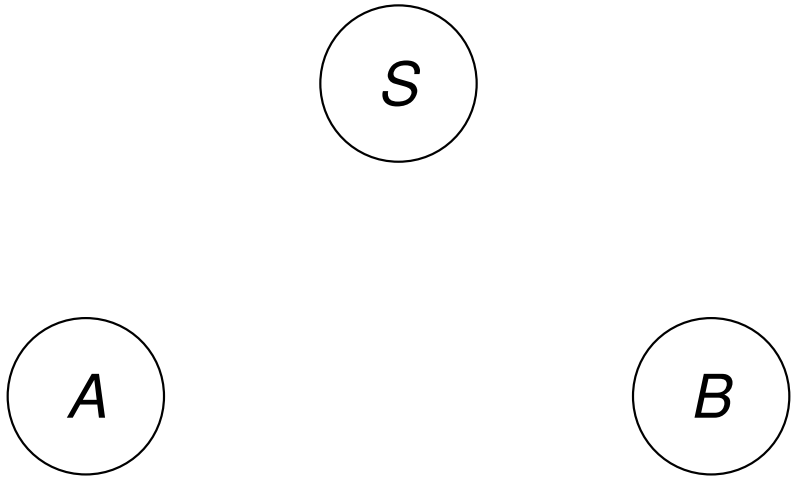
- Processus

$$\begin{array}{rcl} P, Q & ::= & \mathbf{0} \mid E(x).P \mid \overline{E}\langle F\rangle.P \\ & \mid & \phi P \mid (\nu x)\, P \\ & \mid & P \| Q \mid P + Q \mid !\, P \end{array}$$

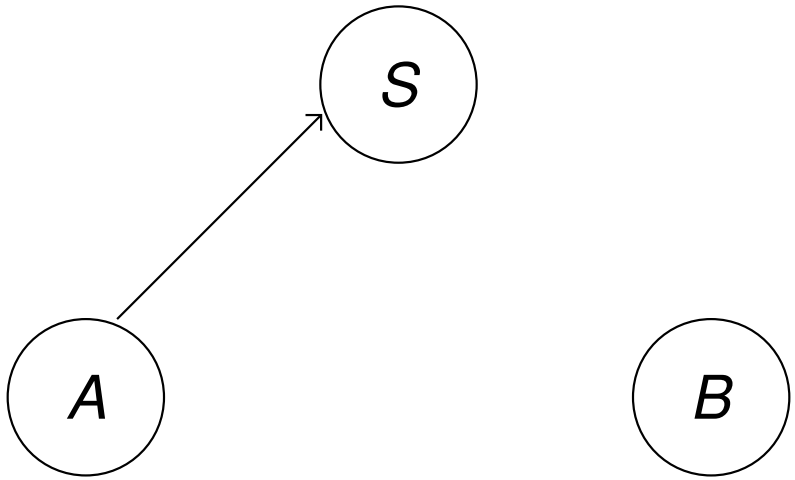
- Agents

$$\begin{array}{rcl} A & ::= & P \\ & \mid & (x)P \\ & \mid & (\nu \tilde{z})\, \langle M\rangle P \quad \text{avec } \{\tilde{z}\} \subseteq \mathrm{n}(M) \end{array}$$

Le protocole “wide-mouthed frog”

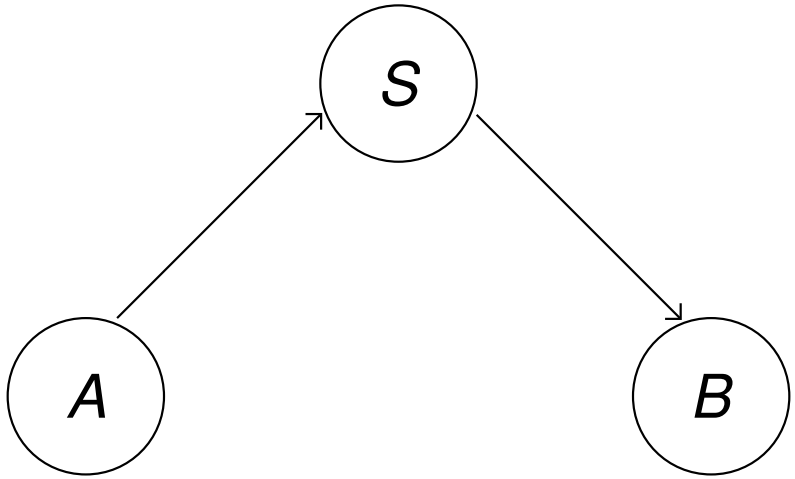


Le protocole “wide-mouthed frog”



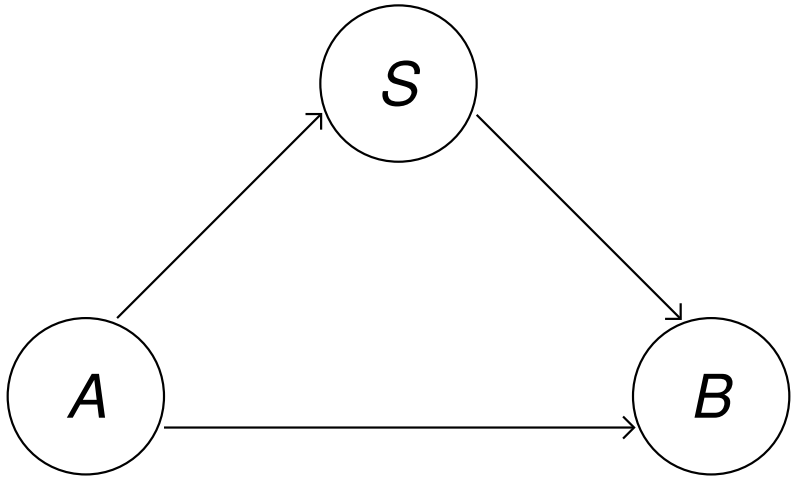
1. $A \rightarrow S : (A\,.\,\mathrm{Enc}^{s}_{k_{AS}}(B\,.\,k_{AB}))$

Le protocole “wide-mouthed frog”



1. $A \rightarrow S : (A \,.\, \mathrm{Enc}^{\mathrm{S}}_{k_{AS}}(B \,.\, k_{AB}))$
2. $S \rightarrow B : \mathrm{Enc}^{\mathrm{S}}_{k_{BS}}((A \,.\, B) \,.\, k_{AB})$

Le protocole “wide-mouthed frog”



1. $A \longrightarrow S : (A\,.\,\mathrm{Enc}^{\mathrm{S}}_{k_{AS}}(B\,.\,k_{AB}))$
2. $S \longrightarrow B : \mathrm{Enc}^{\mathrm{S}}_{k_{BS}}((A\,.\,B)\,.\,k_{AB})$
3. $A \longrightarrow B : \mathrm{Enc}^{\mathrm{S}}_{k_{AB}} m$

.. en spi calcul

$$
\begin{aligned}
&(\nu k_{AS}, k_{BS}) \\
&\quad (\nu k_{AB})\, \overline{S}\langle (A\,.\,\mathrm{Enc}^{\mathrm{S}}_{k_{AS}}(B\,.\,k_{AB}))\rangle.\overline{B}\langle \mathrm{Enc}^{\mathrm{S}}_{k_{AB}} m\rangle.\,\mathbf{0} \\
&\quad \| B(x_1).\phi_1 B(x_2).\phi_2\,\mathbf{0} \\
&\quad \| S(x_0).\phi_0 \overline{B}\langle \mathrm{Enc}^{\mathrm{S}}_{k_{BS}}((A\,.\,B)\,.\,\pi_2\left(\mathrm{Dec}^{\mathrm{S}}_{k_{AS}}\pi_2\,(x_0)\right))\rangle.\,\mathbf{0}
\end{aligned}
$$

.. en spi calcul

$$
\begin{array}{l}
(\nu k_{AS}, k_{BS}) \\
\quad (\nu k_{AB})\, \overline{S}\langle (A\,.\,\mathrm{Enc}^{\mathrm{S}}_{k_{AS}}(B\,.\,k_{AB}))\rangle.\overline{B}\langle \mathrm{Enc}^{\mathrm{S}}_{k_{AB}} m\rangle.\,\mathbf{0} \\
\quad \| B(x_1).\phi_1 B(x_2).\phi_2\, \mathbf{0} \\
\quad \| S(x_0).\phi_0 \overline{B}\langle \mathrm{Enc}^{\mathrm{S}}_{k_{BS}}((A\,.\,B)\,.\,\pi_2\left(\mathrm{Dec}^{\mathrm{S}}_{k_{AS}}\pi_2\,(x_0)\right))\rangle.\,\mathbf{0}
\end{array}
$$

$$
\begin{array}{lcl}
\phi_0 & = & [B = \pi_1\left(\mathrm{Dec}^{\mathrm{S}}_{k_{AS}}\pi_2\,(x_0)\right)] \wedge [A = \pi_1\,(x_0)] \\
\phi_1 & = & [B = \pi_1\left(\pi_2\left(\mathrm{Dec}^{\mathrm{S}}_{k_{BS}} x_1\right)\right)] \wedge [A = \pi_1\left(\mathrm{Dec}^{\mathrm{S}}_{k_{BS}} x_1\right)] \\
\phi_2 & = & [\mathrm{Dec}^{\mathrm{S}}_{\pi_2\left(\pi_2\left(\mathrm{Dec}^{\mathrm{S}}_{k_{BS}} x_1\right)\right)} x_2 : \boldsymbol{M}]
\end{array}
$$

Composition des agents et des processus

- Restriction :

$$
\begin{array}{rcll}
(\boldsymbol{\nu} x)\, P & := & (\nu x)\, P & \\
(\boldsymbol{\nu} x)\, ((y)P) & := & (y)(\nu x)\, P & \text{si } y \neq x \\
(\boldsymbol{\nu} x)\, ((\nu \tilde{z})\, \langle M \rangle P) & := & (\nu \tilde{z})\, \langle M \rangle (\nu x)\, P & \text{si } y \notin \{\tilde{z}\} \text{ et } x \notin \mathrm{n}(M) \\
(\boldsymbol{\nu} x)\, ((\nu \tilde{z})\, \langle M \rangle P) & := & (\nu x \tilde{z})\, \langle M \rangle P & \text{si } y \notin \{\tilde{z}\} \text{ et } x \in \mathrm{n}(M)
\end{array}
$$

- Composition parallèle :

$$
\begin{array}{rcll}
((x)P) \| Q & := & (x)(P \| Q) & \text{si } x \notin \mathrm{fn}(Q) \\
((\nu \tilde{z})\, \langle M \rangle P) \| Q & := & (\nu \tilde{z})\, \langle M \rangle (P \| Q) & \text{si } \{\tilde{z}\} \cap \mathrm{fn}(Q) = \emptyset
\end{array}
$$

  + les version symétriques

Intéraction entre agents

- Pseudo-application :
  Étant données une abstraction $F = (x)P$ et une concrétion $C = (\nu \tilde{z})\,\langle M \rangle Q$ (avec $\tilde{z} \cap \mathrm{fn}(P) = \emptyset$), on définit :

$$F \bullet C := (\nu \tilde{z})\,(P\{^{M}/_{x}\} \| Q)$$

  et la version symétrique $C \bullet F$.

Evaluation des expressions et des gardes

$$
\begin{array}{rcll}
\mathbf{e}_c(a) & := & a & \\
\mathbf{e}_c(\mathrm{Enc}^s_F E) & := & \mathrm{Enc}^s_N M & \text{si } \mathbf{e}_c(E) = M \in \boldsymbol{M} \text{ et } \mathbf{e}_c(F) = N \in \boldsymbol{M} \\
\mathbf{e}_c(\mathrm{Dec}^s_F E) & := & M & \text{si } \mathbf{e}_c(E) = \mathrm{Enc}^s_N M \in \boldsymbol{M} \text{ et } \mathbf{e}_c(F) = N \in \boldsymbol{M} \\
\mathbf{e}_c(E) & := & \bot & \text{dans les autres cas}
\end{array}
$$

Evaluation des expressions et des gardes

$$
\begin{array}{rcll}
\mathbf{e}_c(a) & := & a & \\
\mathbf{e}_c(\mathrm{Enc}^s_F E) & := & \mathrm{Enc}^s_N M & \text{si } \mathbf{e}_c(E) = M \in \boldsymbol{M} \text{ et } \mathbf{e}_c(F) = N \in \boldsymbol{M} \\
\mathbf{e}_c(\mathrm{Dec}^s_F E) & := & M & \text{si } \mathbf{e}_c(E) = \mathrm{Enc}^s_N M \in \boldsymbol{M} \text{ et } \mathbf{e}_c(F) = N \in \boldsymbol{M} \\
\mathbf{e}_c(E) & := & \bot & \text{dans les autres cas}
\end{array}
$$

$$
\begin{array}{rcll}
\mathbf{e}([E = F]) & := & \textbf{true} & \text{si } \mathbf{e}_c(E) = \mathbf{e}_c(F) = M \in \boldsymbol{M} \\
\mathbf{e}([E : \boldsymbol{N}]) & := & \textbf{true} & \text{si } \mathbf{e}_c(E) = a \in \boldsymbol{N} \\
\mathbf{e}(\phi) & := & \textbf{false} & \text{dans les autres cas}
\end{array}
$$

Système de transition

$$\textsc{Input}\ \frac{\mathbf{e}_c(E) = a \in \boldsymbol{N}}{E(x).P \xrightarrow{a} (x)P} \qquad \textsc{Output}\ \frac{\mathbf{e}_c(E) = a \in \boldsymbol{N} \qquad \mathbf{e}_c(F) = M \in \boldsymbol{M}}{\overline{E}\langle F\rangle.P \xrightarrow{\bar{a}} \langle M\rangle P}$$

$$\textsc{IfThen}\ \frac{P \xrightarrow{\mu} P'}{\phi P \xrightarrow{\mu} P'}\ \mathbf{e}(\phi) = \mathbf{true}$$

+ Close, Par, Res, Sum, Rep- et Alpha.

Bisimulation du pi en spi

Bisimulation du pi en spi

- Elles sont trop fines :

$$P(M) := (\nu k)\, \overline{c}\langle \mathrm{Enc}^{\mathrm{S}}_k M \rangle . \mathbf{0}$$

Bisimulation du pi en spi

- Elles sont trop fines :

$$P(M) := (\nu k)\, \overline{c}\langle \mathrm{Enc}^{\mathrm{S}}_k M \rangle . \mathbf{0}$$

- On aimerait identifier $P(M)$ et $P(N)$ quelque soit M et N (autrement dit le message M reste secret)

Bisimulation du pi en spi

- Elles sont trop fines :

$$P(M) := (\nu k)\, \overline{c}\langle \mathrm{Enc}^{\mathrm{s}}_k M \rangle . \mathbf{0}$$

- On aimerait identifier $P(M)$ et $P(N)$ quelque soit M et N (autrement dit le message M reste secret)
- Mais les bisimulations du pi calcul distinguent ces deux processus dès que $M \neq N$.

Bisimulation du pi en spi

- Elles sont trop fines :

$$P(M) := (\nu k)\, \overline{c}\langle \mathrm{Enc}^{\mathrm{s}}_{k} M \rangle . \mathbf{0}$$

- On aimerait identifier $P(M)$ et $P(N)$ quelque soit M et N (autrement dit le message M reste secret)
- Mais les bisimulations du pi calcul distinguent ces deux processus dès que $M \neq N$.
- Il faut ajouter une notion d'indistingabilité...

Les haies pour représenter la connaissance

- Une haie h est une partie finie de $\boldsymbol{M} \times \boldsymbol{M}$

Les haies pour représenter la connaissance

- Une haie h est une partie finie de $\boldsymbol{M} \times \boldsymbol{M}$
- La synthèse $\mathcal{S}(h)$

$$\textsc{Syn-Inc}\ \frac{(M, N) \in h}{(M, N) \in \mathcal{S}(h)}$$

$$\textsc{Syn-Enc-s}\ \frac{(M_1, N_1) \in \mathcal{S}(h) \qquad (M_2, N_2) \in \mathcal{S}(h)}{(\mathrm{Enc}^{\mathrm{s}}_{M_2} M_1, \mathrm{Enc}^{\mathrm{s}}_{N_2} N_1) \in \mathcal{S}(h)}$$

$$\textsc{Syn-Pair}\ \frac{(M_1, N_1) \in \mathcal{S}(h) \qquad (M_2, N_2) \in \mathcal{S}(h)}{((M_1 \,.\, M_2), (N_1 \,.\, N_2)) \in \mathcal{S}(h)}$$

L'analyse

- L'analyse $\mathcal{A}(h)$ est la plus petite haie qui contient h et qui est stable par $\mathrm{analz}(\cdot)$

$$\textsc{Ana-Inc}\ \frac{(M,N) \in h}{(M,N) \in \mathrm{analz}(h)}$$

$$\textsc{Ana-Dec-s}\ \frac{(\mathrm{Enc}^{s}_{M_2} M_1, \mathrm{Enc}^{s}_{N_2} N_1) \in \mathrm{analz}(h) \qquad (M_2,N_2) \in \mathcal{S}(h)}{(M_1,N_1) \in \mathrm{analz}(h)}$$

$$\textsc{Ana-Fst}\ \frac{((M_1 \,.\, M_2),(N_1 \,.\, N_2)) \in \mathrm{analz}(h)}{(M_1,N_1) \in \mathrm{analz}(h)}$$

$$\textsc{Ana-Snd}\ \frac{((M_1 \,.\, M_2),(N_1 \,.\, N_2)) \in \mathrm{analz}(h)}{(M_2,N_2) \in \mathrm{analz}(h)}$$

Les éléments irréductibles et la consistance

- $\mathcal{I}(h)$ est la plus petite haie telle que $\mathcal{S}(\mathcal{I}(h)) = \mathcal{S}(\mathcal{A}(h))$.

Les éléments irréductibles et la consistance

- $\mathcal{I}(h)$ est la plus petite haie telle que $\mathcal{S}(\mathcal{I}(h)) = \mathcal{S}(\mathcal{A}(h))$.
- Une haie h est consistante si elle ne contient pas de contradictions :

Les éléments irréductibles et la consistance

- $\mathcal{I}(h)$ est la plus petite haie telle que $\mathcal{S}(\mathcal{I}(h)) = \mathcal{S}(\mathcal{A}(h))$.
- Une haie h est consistante si elle ne contient pas de contradictions :
  Pour tout $(M, N) \in h$
  - $M \in \boldsymbol{N} \iff N \in \boldsymbol{N}$

Les éléments irréductibles et la consistance

- $\mathcal{I}(h)$ est la plus petite haie telle que $\mathcal{S}(\mathcal{I}(h)) = \mathcal{S}(\mathcal{A}(h))$.
- Une haie h est consistante si elle ne contient pas de contradictions :
  Pour tout $(M, N) \in h$
  - $M \in \boldsymbol{N} \iff N \in \boldsymbol{N}$
  - pour tout $(M', N') \in h : M = M' \iff N = N'$

Les éléments irréductibles et la consistance

- $\mathcal{I}(h)$ est la plus petite haie telle que $\mathcal{S}(\mathcal{I}(h)) = \mathcal{S}(\mathcal{A}(h))$.
- Une haie h est consistante si elle ne contient pas de contradictions :
  Pour tout $(M, N) \in h$
  - $M \in \boldsymbol{N} \iff N \in \boldsymbol{N}$
  - pour tout $(M', N') \in h : M = M' \iff N = N'$
  - $M \neq (M_1 \,.\, M_2)$ et $N \neq (N_1 \,.\, N_2)$

Les éléments irréductibles et la consistance

- $\mathcal{I}(h)$ est la plus petite haie telle que $\mathcal{S}(\mathcal{I}(h)) = \mathcal{S}(\mathcal{A}(h))$.
- Une haie h est consistante si elle ne contient pas de contradictions :
  Pour tout $(M, N) \in h$
  - $M \in \boldsymbol{N} \iff N \in \boldsymbol{N}$
  - pour tout $(M', N') \in h : M = M' \iff N = N'$
  - $M \neq (M_1 \,.\, M_2)$ et $N \neq (N_1 \,.\, N_2)$
  - si $M = \mathrm{Enc}^{\mathrm{s}}_{M_2} M_1$ alors $(M_2, N_2) \notin \mathcal{S}(h)$
  - si $N = \mathrm{Enc}^{\mathrm{s}}_{N_2} N_1$ alors $(M_2, N_2) \notin \mathcal{S}(h)$

Les éléments irréductibles et la consistance

- $\mathcal{I}(h)$ est la plus petite haie telle que $\mathcal{S}(\mathcal{I}(h)) = \mathcal{S}(\mathcal{A}(h))$.
- Une haie h est consistante si elle ne contient pas de contradictions :
  Pour tout $(M, N) \in h$
  - $M \in \boldsymbol{N} \iff N \in \boldsymbol{N}$
  - pour tout $(M', N') \in h : M = M' \iff N = N'$
  - $M \neq (M_1 \,.\, M_2)$ et $N \neq (N_1 \,.\, N_2)$
  - si $M = \mathrm{Enc}^{\mathrm{s}}_{M_2} M_1$ alors $(M_2, N_2) \notin \mathcal{S}(h)$
  - si $N = \mathrm{Enc}^{\mathrm{s}}_{N_2} N_1$ alors $(M_2, N_2) \notin \mathcal{S}(h)$
- Une haie consistante est irréductible.

La bisimulation tardive à haie

- Une relation “symmétrique” $\mathcal{R}$ est une bisimulation tardive à haie si pour tout $(h, P, Q) \in \mathcal{R}$,

La bisimulation tardive à haie

- Une relation “symmétrique” $\mathcal{R}$ est une bisimulation tardive à haie si pour tout $(h, P, Q) \in \mathcal{R}$,
  - $\text{fn}(P) \subseteq \pi_1(h)$ et $\text{fn}(Q) \subseteq \pi_2(h)$

La bisimulation tardive à haie

- Une relation “symmétrique” $\mathcal{R}$ est une bisimulation tardive à haie si pour tout $(h, P, Q) \in \mathcal{R}$,
  - $\text{fn}(P) \subseteq \pi_1(h)$ et $\text{fn}(Q) \subseteq \pi_2(h)$
  - h est consistante

La bisimulation tardive à haie

- Une relation “symmétrique” $\mathcal{R}$ est une bisimulation tardive à haie si pour tout $(h, P, Q) \in \mathcal{R}$,
  - $\text{fn}(P) \subseteq \pi_1(h)$ et $\text{fn}(Q) \subseteq \pi_2(h)$
  - h est consistante
  - si $P \xrightarrow{\tau} P'$ alors $Q \xrightarrow{\tau} Q'$ et $(h, P', Q') \in \mathcal{R}$

La bisimulation tardive à haie

- Une relation “symmétrique” $\mathcal{R}$ est une bisimulation tardive à haie si pour tout $(h, P, Q) \in \mathcal{R}$,
  - $\mathrm{fn}(P) \subseteq \pi_1(h)$ et $\mathrm{fn}(Q) \subseteq \pi_2(h)$
  - h est consistante
  - si $P \xrightarrow{\tau} P'$ alors $Q \xrightarrow{\tau} Q'$ et $(h, P', Q') \in \mathcal{R}$
  - si $P \xrightarrow{\overline{a}} (\nu \tilde{c}) \langle M \rangle P'$ et $a \in \pi_1(\mathcal{S}(h))$ alors

La bisimulation tardive à haie

- Une relation “symmétrique” $\mathcal{R}$ est une bisimulation tardive à haie si pour tout $(h, P, Q) \in \mathcal{R}$,
  - $\text{fn}(P) \subseteq \pi_1(h)$ et $\text{fn}(Q) \subseteq \pi_2(h)$
  - h est consistante
  - si $P \xrightarrow{\tau} P'$ alors $Q \xrightarrow{\tau} Q'$ et $(h, P', Q') \in \mathcal{R}$
  - si $P \xrightarrow{\bar{a}} (\nu \tilde{c}) \langle M \rangle P'$ et $a \in \pi_1(\mathcal{S}(h))$ alors $Q \xrightarrow{\bar{b}} (\nu \tilde{d}) \langle N \rangle Q'$ avec $(a, b) \in \mathcal{S}(h)$

La bisimulation tardive à haie

- Une relation “symmétrique” $\mathcal{R}$ est une bisimulation tardive à haie si pour tout $(h, P, Q) \in \mathcal{R}$,
  - $\mathrm{fn}(P) \subseteq \pi_1(h)$ et $\mathrm{fn}(Q) \subseteq \pi_2(h)$
  - h est consistante
  - si $P \xrightarrow{\tau} P'$ alors $Q \xrightarrow{\tau} Q'$ et $(h, P', Q') \in \mathcal{R}$
  - si $P \xrightarrow{\overline{a}} (\nu \tilde{c}) \langle M \rangle P'$ et $a \in \pi_1(\mathcal{S}(h))$ alors $Q \xrightarrow{\overline{b}} (\nu \tilde{d}) \langle N \rangle Q'$ avec $(a, b) \in \mathcal{S}(h)$ et $(\mathcal{I}(h \cup \{(M, N)\}), P', Q') \in \mathcal{R}$

La bisimulation tardive à haie

- Une relation “symmétrique” $\mathcal{R}$ est une bisimulation tardive à haie si pour tout $(h, P, Q) \in \mathcal{R}$,
  - $\text{fn}(P) \subseteq \pi_1(h)$ et $\text{fn}(Q) \subseteq \pi_2(h)$
  - h est consistante
  - si $P \xrightarrow{\tau} P'$ alors $Q \xrightarrow{\tau} Q'$ et $(h, P', Q') \in \mathcal{R}$
  - si $P \xrightarrow{\overline{a}} (\nu \tilde{c}) \langle M \rangle P'$ et $a \in \pi_1(\mathcal{S}(h))$ alors $Q \xrightarrow{\overline{b}} (\nu \tilde{d}) \langle N \rangle Q'$ avec $(a, b) \in \mathcal{S}(h)$ et $(\mathcal{I}(h \cup \{(M, N)\}), P', Q') \in \mathcal{R}$
  - si $P \xrightarrow{a} (x)P'$ et $a \in \pi_1(\mathcal{S}(h))$ alors

La bisimulation tardive à haie

- Une relation “symmétrique” $\mathcal{R}$ est une bisimulation tardive à haie si pour tout $(h, P, Q) \in \mathcal{R}$,
  - $\text{fn}(P) \subseteq \pi_1(h)$ et $\text{fn}(Q) \subseteq \pi_2(h)$
  - h est consistante
  - si $P \xrightarrow{\tau} P'$ alors $Q \xrightarrow{\tau} Q'$ et $(h, P', Q') \in \mathcal{R}$
  - si $P \xrightarrow{\overline{a}} (\nu \tilde{c}) \langle M \rangle P'$ et $a \in \pi_1(\mathcal{S}(h))$ alors $Q \xrightarrow{\overline{b}} (\nu \tilde{d}) \langle N \rangle Q'$ avec $(a, b) \in \mathcal{S}(h)$ et $(\mathcal{I}(h \cup \{(M, N)\}), P', Q') \in \mathcal{R}$
  - si $P \xrightarrow{a} (x)P'$ et $a \in \pi_1(\mathcal{S}(h))$ alors $Q \xrightarrow{b} (x)Q'$ avec $(a, b) \in \mathcal{S}(h)$

La bisimulation tardive à haie

- Une relation “symmétrique” $\mathcal{R}$ est une bisimulation tardive à haie si pour tout $(h, P, Q) \in \mathcal{R}$,
  - $\text{fn}(P) \subseteq \pi_1(h)$ et $\text{fn}(Q) \subseteq \pi_2(h)$
  - h est consistante
  - si $P \xrightarrow{\tau} P'$ alors $Q \xrightarrow{\tau} Q'$ et $(h, P', Q') \in \mathcal{R}$
  - si $P \xrightarrow{\bar{a}} (\nu \tilde{c}) \langle M \rangle P'$ et $a \in \pi_1(\mathcal{S}(h))$ alors $Q \xrightarrow{\bar{b}} (\nu \tilde{d}) \langle N \rangle Q'$ avec $(a, b) \in \mathcal{S}(h)$ et $(\mathcal{I}(h \cup \{(M, N)\}), P', Q') \in \mathcal{R}$
  - si $P \xrightarrow{a} (x)P'$ et $a \in \pi_1(\mathcal{S}(h))$ alors $Q \xrightarrow{b} (x)Q'$ avec $(a, b) \in \mathcal{S}(h)$ et pour tout $(M, N) \in \mathcal{S}(h)$ on a $(h, P'\{^M/_x\}, Q'\{^N/_x\}) \in \mathcal{R}$

La bisimulation tardive à haie

- Une relation “symmétrique” $\mathcal{R}$ est une bisimulation tardive à haie si pour tout $(h, P, Q) \in \mathcal{R}$,
  - $\text{fn}(P) \subseteq \pi_1(h)$ et $\text{fn}(Q) \subseteq \pi_2(h)$
  - h est consistante
  - si $P \xrightarrow{\tau} P'$ alors $Q \xrightarrow{\tau} Q'$ et $(h, P', Q') \in \mathcal{R}$
  - si $P \xrightarrow{\overline{a}} (\nu \tilde{c}) \langle M \rangle P'$ et $a \in \pi_1(\mathcal{S}(h))$ alors $Q \xrightarrow{\overline{b}} (\nu \tilde{d}) \langle N \rangle Q'$ avec $(a, b) \in \mathcal{S}(h)$ et $(\mathcal{I}(h \cup \{(M, N)\}), P', Q') \in \mathcal{R}$
  - si $P \xrightarrow{a} (x)P'$ et $a \in \pi_1(\mathcal{S}(h))$ alors $Q \xrightarrow{b} (x)Q'$ avec $(a, b) \in \mathcal{S}(h)$ et pour tout $(M, N) \in \mathcal{S}(h \cup B)$ on a $(h \cup B, P'\{^M/_x\}, Q'\{^N/_x\}) \in \mathcal{R}$

Plan

À propos des substitutions admissibles

- Dans le pi calcul, les distinctions sont suffisantes pour restreindre l'ensemble des substitutions ... mais pas dans le spi

À propos des substitutions admissibles

- Dans le pi calcul, les distinctions sont suffisantes pour restreindre l'ensemble des substitutions ... mais pas dans le spi
- Plutôt que d'interdire la fusion de termes via des distinctions, on va caractériser quels noms sont "substituables" et par quels termes on peut les remplacer.

À propos des substitutions admissibles

- Dans le pi calcul, les distinctions sont suffisantes pour restreindre l'ensemble des substitutions ... mais pas dans le spi
- Plutôt que d'interdire la fusion de termes via des distinctions, on va caractériser quels noms sont "substituables" et par quels termes on peut les remplacer.
- Pour $P := c(x).(\nu k)\,\overline{c}\langle k\rangle.[x=k]\overline{c}\langle c\rangle.\,\mathbf{0}$

À propos des substitutions admissibles

- Dans le pi calcul, les distinctions sont suffisantes pour restreindre l'ensemble des substitutions ... mais pas dans le spi
- Plutôt que d'interdire la fusion de termes via des distinctions, on va caractériser quels noms sont "substituables" et par quels termes on peut les remplacer.
- Pour $P := c(x).(\nu k)\,\overline{c}\langle k\rangle.[x=k]\overline{c}\langle c\rangle.\,\mathbf{0}$
  x : nom "substituable" (variable) par toutes les valeurs que peut construire l'observateur au moment où x est reçu (par P)

À propos des substitutions admissibles

- Dans le pi calcul, les distinctions sont suffisantes pour restreindre l'ensemble des substitutions ... mais pas dans le spi
- Plutôt que d'interdire la fusion de termes via des distinctions, on va caractériser quels noms sont "substituables" et par quels termes on peut les remplacer.
- Pour $P := c(x).(\nu k)\,\overline{c}\langle k\rangle.[x=k]\overline{c}\langle c\rangle.\,\mathbf{0}$
  x : nom "substituable" (variable) par toutes les valeurs que peut construire l'observateur au moment où x est reçu (par P)
  k : nom "non substituable" (constante)

À propos des substitutions admissibles

- Dans le pi calcul, les distinctions sont suffisantes pour restreindre l'ensemble des substitutions ... mais pas dans le spi
- Plutôt que d'interdire la fusion de termes via des distinctions, on va caractériser quels noms sont "substituables" et par quels termes on peut les remplacer.
- Pour $P := c(x).(\nu k)\,\overline{c}\langle k\rangle.[x=k]\overline{c}\langle c\rangle.\,\mathbf{0}$
  x : nom "substituable" (variable) par toutes les valeurs que peut construire l'observateur au moment où x est reçu (par P)
  k : nom "non substituable" (constante)
- K-open bisimulation

Représentation de l'environnement

- Un environnement est maintenant un triplet $e = (h, v, \prec)$

Représentation de l'environnement

- Un environnement est maintenant un triplet $e = (h, v, \prec)$
  - h : haie contenant les connaissances accumulées par l'environnement

Représentation de l'environnement

- Un environnement est maintenant un triplet $e = (h, v, \prec)$
  - h : haie contenant les connaissances accumulées par l'environnement
  - v : variables dont les valeurs sont données par l'environnement

Représentation de l'environnement

- Un environnement est maintenant un triplet $e = (h, v, \prec)$
  - h : haie contenant les connaissances accumulées par l'environnement
  - v : variables dont les valeurs sont données par l'environnement
  - $\prec$: historique de la construction de la connaissance

Représentation de l'environnement

- Un environnement est maintenant un triplet $e = (h, v, \prec)$
  - h : haie contenant les connaissances accumulées par l'environnement
  - v : variables dont les valeurs sont données par l'environnement
  - $\prec$: historique de la construction de la connaissance
- On définit l'ensemble des paires de substitutions (σ, ρ) qui respectent un environnement e.

Représentation de l'environnement

- Un environnement est maintenant un triplet $e = (h, v, \prec)$
  - h : haie contenant les connaissances accumulées par l'environnement
  - v : variables dont les valeurs sont données par l'environnement
  - $\prec$: historique de la construction de la connaissance
- On définit l'ensemble des paires de substitutions (σ, ρ) qui respectent un environnement e.
- ... ainsi que l'environnement mis à jour $e^{(\sigma,\rho)}$ qui reflètent les choix de (σ, ρ)

Bisimulation ouverte en spi

- Une relation “symétrique” $\mathcal{R}$ est une bisimulation ouverte à haie si pour tout $(e, P, Q) \in \mathcal{R}$ et $(\sigma, \rho) \triangleright e$,

Bisimulation ouverte en spi

- Une relation “symétrique” $\mathcal{R}$ est une bisimulation ouverte à haie si pour tout $(e, P, Q) \in \mathcal{R}$ et $(\sigma, \rho) \triangleright e$,
  - e contient les noms libres de P et Q

Bisimulation ouverte en spi

- Une relation “symétrique” $\mathcal{R}$ est une bisimulation ouverte à haie si pour tout $(e, P, Q) \in \mathcal{R}$ et $(\sigma, \rho) \triangleright e$,
  - e contient les noms libres de P et Q
  - e est consistant

Bisimulation ouverte en spi

- Une relation “symétrique” $\mathcal{R}$ est une bisimulation ouverte à haie si pour tout $(e, P, Q) \in \mathcal{R}$ et $(\sigma, \rho) \triangleright e$,
  - e contient les noms libres de P et Q
  - e est consistant
  - si $P\sigma \xrightarrow{\tau} P'$ alors $Q\rho \xrightarrow{\tau} Q'$ et $(e^{(\sigma,\rho)}, P', Q') \in \mathcal{R}$

Bisimulation ouverte en spi

- Une relation “symétrique” $\mathcal{R}$ est une bisimulation ouverte à haie si pour tout $(e, P, Q) \in \mathcal{R}$ et $(\sigma, \rho) \triangleright e$,
  - e contient les noms libres de P et Q
  - e est consistant
  - si $P\sigma \xrightarrow{\tau} P'$ alors $Q\rho \xrightarrow{\tau} Q'$ et $(e^{(\sigma,\rho)}, P', Q') \in \mathcal{R}$
  - si $P\sigma \xrightarrow{a} (x)P'$ et $a \in \pi_1(\mathcal{S}(e^{(\sigma,\rho)}))$ alors

Bisimulation ouverte en spi

- Une relation “symétrique” $\mathcal{R}$ est une bisimulation ouverte à haie si pour tout $(e, P, Q) \in \mathcal{R}$ et $(\sigma, \rho) \triangleright e$,
  - e contient les noms libres de P et Q
  - e est consistant
  - si $P\sigma \xrightarrow{\tau} P'$ alors $Q\rho \xrightarrow{\tau} Q'$ et $(e^{(\sigma,\rho)}, P', Q') \in \mathcal{R}$
  - si $P\sigma \xrightarrow{a} (x)P'$ et $a \in \pi_1(\mathcal{S}(e^{(\sigma,\rho)}))$ alors $Q\rho \xrightarrow{b} (x)Q'$ avec $(a, b) \in \mathcal{S}(e^{(\sigma,\rho)})$ et $(e^{(\sigma,\rho)} +_v (x, y), P', Q') \in \mathcal{R}$

Bisimulation ouverte en spi

- Une relation “symétrique” $\mathcal{R}$ est une bisimulation ouverte à haie si pour tout $(e, P, Q) \in \mathcal{R}$ et $(\sigma, \rho) \triangleright e$,
  - e contient les noms libres de P et Q
  - e est consistant
  - si $P\sigma \xrightarrow{\tau} P'$ alors $Q\rho \xrightarrow{\tau} Q'$ et $(e^{(\sigma,\rho)}, P', Q') \in \mathcal{R}$
  - si $P\sigma \xrightarrow{a} (x)P'$ et $a \in \pi_1(\mathcal{S}(e^{(\sigma,\rho)}))$ alors $Q\rho \xrightarrow{b} (x)Q'$ avec $(a, b) \in \mathcal{S}(e^{(\sigma,\rho)})$ et $(e^{(\sigma,\rho)} +_v (x, y), P', Q') \in \mathcal{R}$
  - si $P\sigma \xrightarrow{\bar{a}} (\nu\tilde{c}) \langle M \rangle P'$ et $a \in \pi_1(\mathcal{S}(e^{(\sigma,\rho)}))$ alors

Bisimulation ouverte en spi

- Une relation “symétrique” $\mathcal{R}$ est une bisimulation ouverte à haie si pour tout $(e, P, Q) \in \mathcal{R}$ et $(\sigma, \rho) \triangleright e$,
  - e contient les noms libres de P et Q
  - e est consistant
  - si $P\sigma \xrightarrow{\tau} P'$ alors $Q\rho \xrightarrow{\tau} Q'$ et $(e^{(\sigma,\rho)}, P', Q') \in \mathcal{R}$
  - si $P\sigma \xrightarrow{a} (x)P'$ et $a \in \pi_1(\mathcal{S}(e^{(\sigma,\rho)}))$ alors $Q\rho \xrightarrow{b} (x)Q'$ avec $(a, b) \in \mathcal{S}(e^{(\sigma,\rho)})$ et $(e^{(\sigma,\rho)} +_v (x, y), P', Q') \in \mathcal{R}$
  - si $P\sigma \xrightarrow{\bar{a}} (\nu\tilde{c})\langle M\rangle P'$ et $a \in \pi_1(\mathcal{S}(e^{(\sigma,\rho)}))$ alors $Q\rho \xrightarrow{\bar{b}} (\nu\tilde{d})\langle N\rangle Q'$ avec $(a, b) \in \mathcal{S}(e^{(\sigma,\rho)})$ et $(e^{(\sigma,\rho)} +_c (M, N), P', Q') \in \mathcal{R}$

Un problème de typage

- $P = a(x).\overline{x}\langle M\rangle.\overline{a}\langle \mathrm{Dec}_k^s x\rangle.\mathbf{0}$

Un problème de typage

- $P = a(x).\overline{x}\langle M\rangle.\overline{a}\langle \mathrm{Dec}^{s}_{k}\, x\rangle.\,\mathbf{0}$
- Avec la définition précédente, la dernière transition sera examinée car les substitutions de la forme $\{^{\mathrm{Enc}^{s}_{k}\, N}/_{x}\}$ ne sont pas interdites.

Un problème de typage

- $P = a(x).\overline{x}\langle M\rangle.\overline{a}\langle \mathrm{Dec}^{\mathrm{s}}_k x\rangle.\,\mathbf{0}$
- Avec la définition précédente, la dernière transition sera examinée car les substitutions de la forme $\{^{\mathrm{Enc}^{\mathrm{s}}_k N}/_x\}$ ne sont pas interdites.
- Mais comme x a été utilisé comme canal auparavant, x ne peut pas prendre d'autres valeurs qu'un nom de canal.

Un problème de typage

- $P = a(x).\overline{x}\langle M\rangle.\overline{a}\langle \mathrm{Dec}^{s}_{k} x\rangle.\,\mathbf{0}$
- Avec la définition précédente, la dernière transition sera examinée car les substitutions de la forme $\{^{\mathrm{Enc}^{s}_{k} N}/_{x}\}$ ne sont pas interdites.
- Mais comme x a été utilisé comme canal auparavant, x ne peut pas prendre d'autres valeurs qu'un nom de canal.
- On modifie donc les définitions précédentes pour prendre en compte les noms "substituables" qui ne peuvent prendre comme valeur que des noms de canaux.

Un problème de typage

- $P = a(x).\overline{x}\langle M\rangle.\overline{a}\langle \mathrm{Dec}^{s}_{k} x\rangle.\,\mathbf{0}$
- Avec la définition précédente, la dernière transition sera examinée car les substitutions de la forme $\{^{\mathrm{Enc}^{s}_{k} N}/_{x}\}$ ne sont pas interdites.
- Mais comme x a été utilisé comme canal auparavant, x ne peut pas prendre d'autres valeurs qu'un nom de canal.
- On modifie donc les définitions précédentes pour prendre en compte les noms "substituables" qui ne peuvent prendre comme valeur que des noms de canaux.
- On modifie aussi le système de transitions pour collecter les noms dont le fait d'être un simple nom a permis de dériver la transition.

Un problème de typage

- $P = a(x).\overline{x}\langle M\rangle.\overline{a}\langle \mathrm{Dec}_k^s x\rangle.\mathbf{0}$
- Avec la définition précédente, la dernière transition sera examinée car les substitutions de la forme $\{^{\mathrm{Enc}_k^s N}/_x\}$ ne sont pas interdites.
- Mais comme x a été utilisé comme canal auparavant, x ne peut pas prendre d'autres valeurs qu'un nom de canal.
- On modifie donc les définitions précédentes pour prendre en compte les noms "substituables" qui ne peuvent prendre comme valeur que des noms de canaux.
- On modifie aussi le système de transitions pour collecter les noms dont le fait d'être un simple nom a permis de dériver la transition.
- Au final, un environnement peut être vu comme une séquence $h_0(x_1, y_1)h_1(x_2, y_2)\cdots(x_n, y_n)h_n$ avec $h_1 \subseteq h_2 \subseteq \cdots \subseteq h_n$ et certains couples (x_i, y_i) sont marquées comme ne pouvant prendre comme valeur que des noms de canaux.

Conclusion

- On a généralisé la notion de bisimulation ouverte (paresseuse) au cas du spi calcul.

Conclusion

- On a généralisé la notion de bisimulation ouverte (paresseuse) au cas du spi calcul.
  - Cette définition est correcte.

Conclusion

- On a généralisé la notion de bisimulation ouverte (paresseuse) au cas du spi calcul.
  - Cette définition est correcte.
  - C'est une extension de la bisimulation ouverte de Sangiorgi.

Conclusion

- On a généralisé la notion de bisimulation ouverte (paresseuse) au cas du spi calcul.
  - Cette définition est correcte.
  - C'est une extension de la bisimulation ouverte de Sangiorgi.
  - Une variante de cette bisimulation possède de bonnes propriétés de congruence (Alwen Tiu, 2007).

Conclusion

- On a généralisé la notion de bisimulation ouverte (paresseuse) au cas du spi calcul.
  - Cette définition est correcte.
  - C'est une extension de la bisimulation ouverte de Sangiorgi.
  - Une variante de cette bisimulation possède de bonnes propriétés de congruence (Alwen Tiu, 2007).
- On a proposé une version symbolique de cette bisimulation ouverte.

Conclusion

- On a généralisé la notion de bisimulation ouverte (paresseuse) au cas du spi calcul.
  - Cette définition est correcte.
  - C'est une extension de la bisimulation ouverte de Sangiorgi.
  - Une variante de cette bisimulation possède de bonnes propriétés de congruence (Alwen Tiu, 2007).
- On a proposé une version symbolique de cette bisimulation ouverte.
  - ... qu'on a prouvé correcte et complète.

Conclusion

- On a généralisé la notion de bisimulation ouverte (paresseuse) au cas du spi calcul.
  - Cette définition est correcte.
  - C'est une extension de la bisimulation ouverte de Sangiorgi.
  - Une variante de cette bisimulation possède de bonnes propriétés de congruence (Alwen Tiu, 2007).
- On a proposé une version symbolique de cette bisimulation ouverte.
  - ... qu'on a prouvé correcte et complète.
  - Certains algorithmes restent à formaliser.

Conclusion

- On a généralisé la notion de bisimulation ouverte (paresseuse) au cas du spi calcul.
  - Cette définition est correcte.
  - C'est une extension de la bisimulation ouverte de Sangiorgi.
  - Une variante de cette bisimulation possède de bonnes propriétés de congruence (Alwen Tiu, 2007).
- On a proposé une version symbolique de cette bisimulation ouverte.
  - ... qu'on a prouvé correcte et complète.
  - Certains algorithmes restent à formaliser.
  - Idéalement, on aimerait pouvoir extraire un outil d'une formalisation Coq...

Merci !

Merci !
Questions ?