Recherche de preuves en logique spatiale

Stage MIM_1 sous la direction de messieurs Daniel Hirschkoff et Étienne Lozes

Samuel Mimram

Un titre original long

Recherche de preuves dans un sous-ensemble d'une logique spatiale sur les π-algèbres :

- ***π-calcul, spatial*** : modèle pour s'intéresser à des problèmes liés à la concurrence dans les programmes
- ***logique*** : prouver de façon semi-automatique des propriétés sur les programmes (types, preuve interactive, . . .)
- ***sous-ensemble*** : tout ça est vite indécidable
- ***recherche de preuves*** : trouver un algorithme de décision

Le π-calcul

Les ***processus***

$$P, Q ::= 0 \quad | \quad b\,(x)\,.P \quad | \quad b\,\langle a\rangle\,.P \quad | \quad P|Q \quad | \quad \nu a.P$$

« communiquent » entre eux en s'échangeant des ***noms de canaux***. Les ***réductions*** peuvent être indéterministes :

$$a\,\langle b\rangle \;|\, a\,(x)\,.c\,(x) \quad \rightarrow \quad 0\,|\,c\,\langle b\rangle$$

$$a\,\langle b\rangle \;|\, a\,(x)\,.c\,\langle x\rangle \;|\, a\,(x)\,.d\,\langle x\rangle \quad \rightarrow \quad \begin{cases} c\,\langle b\rangle \;|\, a\,(x)\,.d\,\langle x\rangle \\ a\,(x)\,.c\,\langle x\rangle \;|\, d\,\langle b\rangle \end{cases}$$

La logique (Caires & Cardelli 2002)

- notions de base : validation ($P \models \mathcal{A}$), validité
- contient les opérateurs habituels ($\mathbf{F}$, $\wedge$, $\Rightarrow$) et des opérateurs pour parler de la ***structure*** des processus :
  - 0 : le processus est vide
  - $\mathcal{A} \mid \mathcal{B}$: le processus peut s'écrire $P \mid Q$ avec $P \models \mathcal{A}$ et $Q \models \mathcal{B}$
  - $\mathcal{A} \triangleright \mathcal{B}$: vérifié par tout processus P tel que pour tout $Q \models \mathcal{A}$ on ait $P \mid Q \models \mathcal{B}$
  - $\Diamond \mathcal{A}$: le processus peut se réduire en $P \models \mathcal{A}$
  - ...
- expressivité : environnement ($\triangleright$)
- validité $\Leftrightarrow$ MC : optique d'un ***prover***

Les séquents

- manipuler les opérateurs en préservant la validité
- sous la forme $\langle S \rangle \ \Gamma \vdash \Delta$ avec :
  - *contextes* : Γ (conjonction) et Δ (disjonction) contenant des couples $u : \mathcal{A}$ (propriétés)
  - S : *théorie de contraintes* ($u \doteq X_1 \mid \ldots \mid X_n$) ; inhabituel, permet de stocker des informations sur la ***structure*** des index :

$$\frac{\langle S, u \doteq \mathcal{X}|\mathcal{Y} \rangle \ \Gamma, \mathcal{X} : \mathcal{A}, \mathcal{Y} : \mathcal{B} \vdash \Delta}{\langle S \rangle \ \Gamma, u : \mathcal{A}|\mathcal{B} \vdash \Delta} \ (|\mathrm{L})$$

- adaptés au caractère classique de la logique

Règles traditionnelles

$$\frac{u \doteq_S v}{\langle S \rangle\ \Gamma, u : A \vdash v : A, \Delta}\ (\mathsf{Id})$$

$$\frac{}{\langle S \rangle\ \Gamma, u : \mathbf{F} \vdash \Delta}\ (\mathbf{F}\mathrm{L}) \qquad \frac{\langle S \rangle\ \Gamma \vdash \Delta}{\langle S \rangle\ \Gamma \vdash u : \mathbf{F}, \Delta}\ (\mathbf{F}\mathrm{R})$$

$$\frac{\langle S \rangle\ \Gamma, u : \mathcal{A}, u : \mathcal{B} \vdash \Delta}{\langle S \rangle\ \Gamma, u : \mathcal{A} \wedge \mathcal{B} \vdash \Delta}\ (\wedge\mathrm{L}) \qquad \frac{\langle S \rangle\ \Gamma \vdash u : \mathcal{A}, \Delta \quad \langle S \rangle\ \Gamma \vdash u : \mathcal{B}, \Delta}{\langle S \rangle\ \Gamma \vdash u : \mathcal{A} \wedge \mathcal{B}, \Delta}\ (\wedge\mathrm{R})$$

$$\frac{\langle S \rangle\ \Gamma \vdash u : \mathcal{A}, \Delta \quad \langle S \rangle\ \Gamma, u : \mathcal{B} \vdash \Delta}{\langle S \rangle\ \Gamma, u : \mathcal{A} \Rightarrow \mathcal{B} \vdash \Delta}\ (\Rightarrow\mathrm{L}) \qquad \frac{\langle S \rangle\ \Gamma, u : \mathcal{A} \vdash u : \mathcal{B}, \Delta}{\langle S \rangle\ \Gamma \vdash u : \mathcal{A} \Rightarrow \mathcal{B}, \Delta}\ (\Rightarrow\mathrm{R})$$

Un sous-ensemble décidable

- but : chercher un sous-ensemble de la logique pour lequel on puisse automatiquement décider de la validité des formules
- logique globalement indécidable : l'est avec $\mathbf{F}$, $\wedge$, $\Rightarrow$, 0, $|$, $\triangleright$, $b.$ et $\forall b$
- restriction à : $\mathbf{F}$, $\wedge$, $\Rightarrow$, 0, $|$ et $\triangleright$
- modèle possible : unions finies d'intervalles de $\mathbb{N}$ mais notre travail est facilement ***extensible*** à d'autres opérateurs
- reste à trouver un système de séquents ***correct*** et ***complet*** pour cette logique pour décrire un ***algorithme de décision***

Règles du système $\mathcal{S}_0$ (Caires & Cardelli)

$$\frac{\langle S\rangle\ \Gamma, u:\mathcal{A}, u:\mathcal{A} \vdash \Delta}{\langle S\rangle\ \Gamma, u:\mathcal{A} \vdash \Delta}\ (\mathsf{CL})$$

$$\frac{\langle S\rangle\ \Gamma \vdash u:\mathcal{A}, u:\mathcal{A}, \Delta}{\langle S\rangle\ \Gamma \vdash u:\mathcal{A}, \Delta}\ (\mathsf{CR})$$

[$\mathcal{X}$ *et* $\mathcal{Y}$ *non libres dans la conclusion*]

$$\frac{\langle S, u \doteq \mathcal{X}|\mathcal{Y}\rangle\ \Gamma, \mathcal{X}:\mathcal{A}, \mathcal{Y}:\mathcal{B} \vdash \Delta}{\langle S\rangle\ \Gamma, u:\mathcal{A}|\mathcal{B} \vdash \Delta}\ (|\mathrm{L})$$

$$\frac{\langle S\rangle\ \Gamma \vdash v:\mathcal{A}, \Delta \quad \langle S\rangle\ \Gamma \vdash t:\mathcal{B}, \Delta \quad u \doteq_S v|t}{\langle S\rangle\ \Gamma \vdash u:\mathcal{A}|\mathcal{B}, \Delta}\ (|\mathrm{R})$$

$$\frac{\langle S\rangle\ \Gamma \vdash t:\mathcal{A}, \Delta \quad \langle S\rangle\ \Gamma, t|u:\mathcal{B} \vdash \Delta}{\langle S\rangle\ \Gamma, u:\mathcal{A} \triangleright \mathcal{B} \vdash \Delta}\ (\triangleright\mathrm{L})$$

[$\mathcal{X}$ *non libre dans la conclusion*]

$$\frac{\langle S\rangle\ \Gamma, \mathcal{X}:\mathcal{A} \vdash v:\mathcal{B}, \Delta \quad v \doteq_S \mathcal{X}|u}{\langle S\rangle\ \Gamma \vdash u:\mathcal{A} \triangleright \mathcal{B}, \Delta}\ (\triangleright\mathrm{R})$$

Quelques idées importantes

- les règles de contraction sont « incorporées » aux règles avant lesquelles elles peuvent être indispensables : $(|\mathrm{R})$ et $(\triangleright\mathrm{L})$
- on introduit une notion de ***taille*** sur les processus et sur les formules : deux processus assez grands ($\sim_w$) sont ***indiscernables*** par une formule donnée
- permet de déterminer la ***granularité*** avec laquelle nous allons devoir observer une formule : $(|\mathrm{R})$
- permet de déterminer un ensemble *fini* de représentants de *tous* les processus : $(\triangleright\mathrm{L})$

Règles du système $\mathcal{S}_2$ (le nôtre)

$$\frac{[\sigma \text{ est la subsitution telle que } \forall i \in [\![1,n]\!], X_i \leftarrow X_i^1|X_i^2] \quad \langle \sigma(S), v \doteq X_1^1|\ldots|X_n^1, t \doteq X_1^2|\ldots|X_n^2\rangle\ \sigma(\Gamma), v:\mathcal{A}, t:\mathcal{B} \vdash \sigma(\Delta) \quad u \doteq_S X_1|\ldots|X_n}{\langle S\rangle\ \Gamma, u:\mathcal{A}|\mathcal{B} \vdash \Delta}\ (|\mathrm{L})$$

$$\frac{\langle S\rangle\ \Gamma \vdash v:\mathcal{A}, \Delta \quad \langle S\rangle\ \Gamma \vdash t:\mathcal{B}, \Delta}{\langle S\rangle\ \Gamma \vdash v \between t:\mathcal{A} \between \mathcal{B}, \Delta}\ (|\mathrm{R}')$$

$$\frac{\left\langle S, v_i \doteq \overline{v}_i^S, t_i \doteq \overline{t}_i^S \right\rangle\ \Gamma \vdash v_1 \between t_1 : \mathcal{A} \between \mathcal{B}, \ldots, v_n \between t_n : \mathcal{A} \between \mathcal{B}, \Delta \quad \text{avec } \{(v_i, t_i) \quad / \quad i \in [\![1,n]\!]\} = \widehat{u}^S}{\langle S\rangle\ \Gamma \vdash u : \mathcal{A}|\mathcal{B}, \Delta}\ (|\mathrm{R})$$

Règles du système $\mathcal{S}_2$ (suite)

$$[\textit{Avec } n = \|\mathcal{A} \triangleright \mathcal{B}\| \textit{ et } J \subseteq [\![1, n]\!]]$$

Pour tout $j \in J$ $\quad \langle S, t_1 \doteq Y_1, \ldots, t_j \doteq Y_1 | \ldots | Y_j, y_1 \doteq Y_1, \ldots, y_j \doteq Y_j \rangle \ \Gamma \vdash t_j : \mathcal{A}, y_1 : 0, \ldots, y_j : 0, \Delta$

Pour tout $j \in [\![1, n]\!] \setminus J$ $\quad \langle S, t_1 \doteq Y_1, \ldots, t_j \doteq Y_1 | \ldots | Y_j, y_1 \doteq Y_1, \ldots, y_j \doteq Y_j \rangle \ \Gamma, t_j : \mathcal{A} \vdash y_1 : 0, \ldots, y_j : 0, \Delta$

$$\left\langle S, \underbrace{v_j \doteq u | t_j, t_j \doteq Y_1 | \ldots | Y_j}_{\text{pour tout } j \in J}, y_1 \doteq Y_1, \ldots, y_n \doteq Y_n \right\rangle \ \Gamma, \underbrace{v_j : \mathcal{B}}_{j \in J} \vdash y_1 : 0, \ldots, y_n : 0, \Delta$$

$$\frac{\langle S \rangle \ \Gamma, u : \mathcal{A} \triangleright \mathcal{B} \vdash \Delta \qquad \left\langle S, v \doteq_S \overline{t}^S | \overline{u}^S, t = Y_1 | \ldots | Y_{\|\mathcal{A} \triangleright \mathcal{B}\|} \right\rangle \ \Gamma, t : \mathcal{A} \vdash v : \mathcal{B}, \Delta}{\langle S \rangle \ \Gamma \vdash u : \mathcal{A} \triangleright \mathcal{B}, \Delta} \ (\triangleright \mathrm{R})$$

$$\frac{S \Vdash u_1 \sim_{\|\mathcal{A}_1\|} v_1, \ldots, u_n \sim_{\|\mathcal{A}_n\|} v_n, Z \quad \text{avec } \{(u_i : \mathcal{A}_i, v_i : \mathcal{A}_i) \quad / \quad i \in [\![1, n]\!]\} \in \Gamma \times \Delta}{\langle S \rangle \ \Gamma \vdash \Delta, \widetilde{Z}} \ (\widetilde{\mathsf{Id}})$$

Exemple d'utilisation de la règle $(\mathbf{C}\mathrm{R})$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\langle\rangle\ X:A \vdash X:0, X:A, X:0}\,(\mathsf{Id})}{\langle\rangle\ \vdash X:\neg A, X:0, X:A, X:0}\,(\neg\mathrm{R})}{\langle\rangle\ \vdash X:\neg A, X:0, X:(A\vee 0)}\,(\vee\mathrm{R}) \quad \dfrac{\dfrac{}{\langle\rangle\ \vdash X:\neg A, X:0, 0:\neg A, 0:0}\,(0\mathrm{R})}{\langle\rangle\ \vdash X:\neg A, X:0, 0:(\neg A\vee 0)}\,(\vee\mathrm{R})}{\langle\rangle\ \vdash X:\neg A, X:0, X:(A\vee 0)\,|\,(\neg A\vee 0)}\,(|\mathrm{R})}{\langle\rangle\ \vdash X:\neg A\vee 0, X:(A\vee 0)\,|\,(\neg A\vee 0)}\,(\vee\mathrm{R}) \quad \dfrac{}{\langle\rangle\ \vdash 0}}{\langle\rangle\ \vdash X:(A\vee 0)\,|\,(\neg A\vee 0), X:(A\vee 0)\,|\,(\neg A\vee 0)}$$

$$\langle\rangle\ \vdash X:(A\vee 0)\,|\,(\neg A\vee 0)$$