Protocoles personnalisés en logique de séparation : ressources fantômes et invariants dans la logique Iris

Jacques-Henri Jourdan[1]

[1]CNRS, LMF, ENS Paris-Saclay, Université Paris-Saclay, France

8 avril 2021 – Collège de France

Iris, une logique de séparation expressive

Une logique de séparation d'ordre supérieur indépendante du langage avec des fondements simples pour vérifier des programmes concurrents à grain fin en Coq.

Iris, une logique de séparation expressive

Une logique de séparation d'ordre supérieur indépendante du langage avec des fondements simples pour vérifier des programmes concurrents à grain fin en Coq.

Logique de séparation d'ordre supérieur : permet un haut degré de polymorphisme, pour prouver modulairement des programmes complexes.

Voir les cours :

- 21/11/2018 : *Polymorphisme à tous les étages ! Du système F au calcul des constructions*
- 15/04/2021 : *Logiques pour les langages fonctionnels et l'ordre supérieur*

Iris, une logique de séparation expressive

Une logique de séparation d'ordre supérieur indépendante du langage avec des fondements simples pour vérifier des programmes concurrents à grain fin en Coq.

Programmes concurrents à grain fin : programmes parallèles qui utilisent des primitives bas-niveau pour communiquer entre fils d'exécutions.

Exemple : instructions atomiques en mémoire partagée.

Iris, une logique de séparation expressive

Une logique de séparation d'ordre supérieur indépendante du langage avec des fondements simples pour vérifier des programmes concurrents à grain fin en Coq.

Indépendante du langage : la même logique peut être utilisée sur une large variété de langages de programmation avec des paradigmes de concurrence très différents.

Exemple : parallélisme à mémoire partagée, calcul distribué avec canaux de communication, mémoire faiblement cohérente, ...

Iris, une logique de séparation expressive

Une logique de séparation d'ordre supérieur indépendante du langage avec des fondements simples pour vérifier des programmes concurrents à grain fin en Coq.

Fondements simples : les règles de raisonnements sont « simples » et en « petit nombre ».

Quelques concepts unificateurs permettent d'exprimer de nombreux modes de raisonnement.

Iris, une logique de séparation expressive

Une logique de séparation d'ordre supérieur indépendante du langage avec des fondements simples pour vérifier des programmes concurrents à grain fin en Coq.

En Coq : permet de vérifier formellement les preuves, avec un haut niveau de garanties.

Iris, une logique de séparation expressive

Une logique de séparation d'ordre supérieur indépendante du langage avec des fondements simples pour vérifier des programmes concurrents à grain fin en Coq.

Iris a été utilisée dans des domaines très variés :

- Méta-théories de systèmes de types
  - types à session, types avec notion de propriété, paramétricité, ..
- *Atomicité logique* pour exprimer la linéarisabilité
  - Vérification de structures de données concurrentes
- Vérification formelle de compilateurs
- ...

Partie 1 :

Utiliser l'état fantôme et les invariants

Le problème « 2+2=4 »

Un problème classique (déjà vu dans le cours du 1/4/2021) :

$$x := 0$$

$$\texttt{fetchandadd}(x, 2) \;\|\; \texttt{fetchandadd}(x, 2)$$

$$a := x$$

Où $\texttt{fetchandadd}(x, y)$ est la version atomique de $x := x + y$.

Le problème « 2+2=4 »

Un problème classique (déjà vu dans le cours du 1/4/2021) :

$$\{x \mapsto \_\}$$
$$x := 0$$

$$\texttt{fetchandadd}(x, 2) \parallel \texttt{fetchandadd}(x, 2)$$

$$a := x$$
$$\{a = 4\}$$

Où $\texttt{fetchandadd}(x, y)$ est la version atomique de $x := x + y$.

Le problème « 2+2=4 »

Un problème classique (déjà vu dans le cours du 1/4/2021) :

$$
\begin{array}{l}
\{x \mapsto \_\} \\
x := 0 \\
\{x \mapsto 0\} \\
\texttt{fetchandadd}(x, 2) \parallel \texttt{fetchandadd}(x, 2) \\
a := x \\
\{a = 4\}
\end{array}
$$

Où $\texttt{fetchandadd}(x, y)$ est la version atomique de $x := x + y$.

Le problème « 2+2=4 »

Un problème classique (déjà vu dans le cours du 1/4/2021) :

$$
\begin{array}{l}
\{x \mapsto \_\} \\
x := 0 \\
\{x \mapsto 0\} \\
\begin{array}{l|l}
\{??\} & \{??\} \\
\texttt{fetchandadd}(x, 2) & \texttt{fetchandadd}(x, 2) \\
\{??\} & \{??\}
\end{array} \\
a := x \\
\{a = 4\}
\end{array}
$$

Où $\texttt{fetchandadd}(x, y)$ est la version atomique de $x := x + y$.

Problème : on ne peut pas diviser la propriété de x !

Les invariants

L'assertion d'invariant $\boxed{R}$ affirme que R est un invariant de l'état du programme.

Les invariants

L'assertion d'invariant $\boxed{R}$ affirme que R est un invariant de l'état du programme.

Ouverture de l'invariant :

$$\frac{\{R * P\}\, e\, \{R * Q\} \qquad e \text{ atomique ou vide}}{\boxed{R} \quad \vdash \{P\}\, e\, \{Q\}}$$

Les invariants

L'assertion d'invariant $\boxed{R}$ affirme que R est un invariant de l'état du programme.

Ouverture de l'invariant :

$$\frac{\{R * P\}\, e\, \{R * Q\} \qquad e \text{ atomique ou vide}}{\boxed{R} \quad \vdash \{P\}\, e\, \{Q\}}$$

Création d'invariant :

$$\frac{\boxed{R} \quad \vdash \{P\}\, e\, \{Q\}}{\{R * P\}\, e\, \{Q\}}$$

Les invariants

L'assertion d'invariant $\boxed{R}^{\mathcal{N}}$ affirme que R est un invariant de l'état du programme.

Ouverture de l'invariant :

$$\frac{\{R * P\}\, e\, \{R * Q\}_{\mathcal{E}} \qquad e \text{ atomique ou vide}}{\boxed{R}^{\mathcal{N}} \vdash \{P\}\, e\, \{Q\}_{\mathcal{E} \uplus \mathcal{N}}}$$

Création d'invariant :

$$\frac{\boxed{R}^{\mathcal{N}} \vdash \{P\}\, e\, \{Q\}_{\mathcal{E}}}{\{R * P\}\, e\, \{Q\}_{\mathcal{E}}}$$

Détail technique : pour éviter qu'un invariant ne soit ouvert plusieurs fois sur la même variable, les invariants sont nommés.

Les invariants

L'assertion d'invariant $\boxed{R}^{\mathcal{N}}$ affirme que R est un invariant de l'état du programme.

Ouverture de l'invariant :

$$\frac{\{\triangleright R * P\}\, e\, \{\triangleright R * Q\}_{\mathcal{E}} \qquad e \text{ atomique ou vide}}{\boxed{R}^{\mathcal{N}} \vdash \{P\}\, e\, \{Q\}_{\mathcal{E} \uplus \mathcal{N}}}$$

Création d'invariant :

$$\frac{\boxed{R}^{\mathcal{N}} \vdash \{P\}\, e\, \{Q\}_{\mathcal{E}}}{\{\triangleright R * P\}\, e\, \{Q\}_{\mathcal{E}}}$$

Détail technique : pour éviter qu'un invariant ne soit ouvert plusieurs fois sur la même variable, les invariants sont nommés.

Autre détail technique : le comptage de pas (step-indexing) et la modalité plus tard $\triangleright$ sont nécessaire pour que les invariants soient impredicatifs, i.e., $\boxed{\ldots \boxed{R}^{\mathcal{N}_2} \ldots}^{\mathcal{N}_1}$

Variables fantôme exclusives

Notre invariant va ressembler à :

$$\boxed{\exists n.\, x \mapsto n * \ldots}$$

Comment peut-on relier la valeur quantifiée n à l'état d'exécution des fils d'exécution ?

Variables fantôme exclusives

Notre invariant va ressembler à :

$$\boxed{\exists n.\, x \mapsto n * \ldots}$$

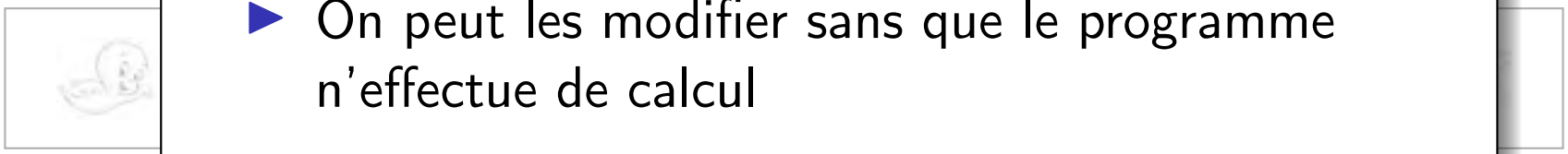
Comment peut-on relier la valeur quantifiée n à l'état d'exécution des fils d'exécution ?

Solution : variables fantôme exclusives

Variables fantôme exclusives

Notre invariant va ressembler à :

Comme
des fils



Les **variables fantôme exclusives** sont des variables purement logiques :

- Elles n'apparaissent pas dans le programme
- On peut les modifier sans que le programme n'effectue de calcul

Nouveau connecteur logique : $P \Rrightarrow\!\!\!\!\!\!\ast\ Q$ modélisant une action sur les variables logiques.

$$P \Rrightarrow\!\!\!\!\!\!\ast\ Q \quad \approx \quad \{P\}\,\texttt{nop}\,\{Q\}$$

« P se transforme en Q »

Variables fantôme exclusives

Notre invariant va ressembler à :

$$\boxed{\exists n.\, x \mapsto n * \ldots}$$

Comment peut-on relier la valeur quantifiée n à l'état d'exécution des fils d'exécution ?

Solution : variables fantôme exclusives

Les **variables fantôme exclusives** sont allouées en deux parties :

$$\text{True} \quad \Rrightarrow\!\!\!\!* \quad \exists\gamma.\ \underbrace{\gamma \hookrightarrow_\bullet n}_{\text{dans l'invariant}} \quad * \quad \underbrace{\gamma \hookrightarrow_\circ n}_{\text{dans le triplet de Hoare}}$$

Variables fantôme exclusives

Notre invariant va ressembler à :

$$\boxed{\exists n_1, n_2.\, x \mapsto (n_1 + n_2) * \gamma_1 \hookrightarrow_\bullet n_1 * \gamma_2 \hookrightarrow_\bullet n_2}$$

Comment peut-on relier la valeur quantifiée n à l'état d'exécution des fils d'exécution ?

Solution : variables fantôme exclusives

Les **variables fantôme exclusives** sont allouées en deux parties :

$$\text{True} \quad \Rrightarrow \quad \exists\gamma.\ \underbrace{\gamma \hookrightarrow_\bullet n}_{\text{dans l'invariant}} \quad * \quad \underbrace{\gamma \hookrightarrow_\circ n}_{\text{dans le triplet de Hoare}}$$

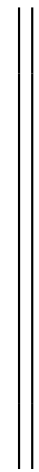
Quand on détient les deux parties d'une variable γ, on peut :

$$\gamma \hookrightarrow_\bullet n * \gamma \hookrightarrow_\circ m \quad \Rightarrow \quad n = m \qquad \text{déduire l'égalité}$$

$$\gamma \hookrightarrow_\bullet n * \gamma \hookrightarrow_\circ m \quad \Rrightarrow \quad \gamma \hookrightarrow_\bullet n' * \gamma \hookrightarrow_\circ n' \qquad \text{la modifier}$$

Les variables fantôme exclusives à l'œuvre

$\{x \mapsto \_\}$
$x := 0$



$\texttt{fetchandadd}(x, 2)$

$\texttt{fetchandadd}(x, 2)$

$a := x$

$\{a = 4\}$

Les variables fantôme exclusives à l'œuvre

$\{x \mapsto \_\}$
$x := 0$
$\{x \mapsto 0\}$

$\texttt{fetchandadd}(x, 2)$ $\quad\|\quad$ $\texttt{fetchandadd}(x, 2)$

$a := x$

$\{a = 4\}$

Les variables fantôme exclusives à l'œuvre

$\{x \mapsto \_\}$
$x := 0$
$\{x \mapsto 0\}$
$\{x \mapsto 0 * \gamma_1 \hookrightarrow_\bullet 0 * \gamma_1 \hookrightarrow_\circ 0 * \gamma_2 \hookrightarrow_\bullet 0 * \gamma_2 \hookrightarrow_\circ 0\}$

$\texttt{fetchandadd}(x, 2)$

$a := x$

$\{a = 4\}$

$\|$

$\texttt{fetchandadd}(x, 2)$

Les variables fantôme exclusives à l'œuvre

$\{x \mapsto \_\}$

$x := 0$

$\{x \mapsto 0\}$

$\{x \mapsto 0 * \gamma_1 \hookrightarrow_\bullet 0 * \gamma_1 \hookrightarrow_\circ 0 * \gamma_2 \hookrightarrow_\bullet 0 * \gamma_2 \hookrightarrow_\circ 0\}$

$\boxed{\exists n_1, n_2.\, x \mapsto n_1 + n_2 * \gamma_1 \hookrightarrow_\bullet n_1 * \gamma_2 \hookrightarrow_\bullet n_2}$ nouvel invariant

`fetchandadd`$(x, 2)$ || `fetchandadd`$(x, 2)$

$a := x$

$\{a = 4\}$

Les variables fantôme exclusives à l'œuvre

$\{x \mapsto \_\}$

$x := 0$

$\{x \mapsto 0\}$

$\{x \mapsto 0 * \gamma_1 \hookrightarrow_\bullet 0 * \gamma_1 \hookrightarrow_\circ 0 * \gamma_2 \hookrightarrow_\bullet 0 * \gamma_2 \hookrightarrow_\circ 0\}$

$\boxed{\exists n_1, n_2.\, x \mapsto n_1 + n_2 * \gamma_1 \hookrightarrow_\bullet n_1 * \gamma_2 \hookrightarrow_\bullet n_2}$ nouvel invariant

$\{\gamma_1 \hookrightarrow_\circ 0 * \gamma_2 \hookrightarrow_\circ 0\}$

`fetchandadd`$(x, 2)$	$\parallel$	`fetchandadd`$(x, 2)$
$a := x$		
$\{a = 4\}$		

Les variables fantôme exclusives à l'œuvre

$\{x \mapsto \_\}$

$x := 0$

$\{x \mapsto 0\}$

$\{x \mapsto 0 * \gamma_1 \hookrightarrow_\bullet 0 * \gamma_1 \hookrightarrow_\circ 0 * \gamma_2 \hookrightarrow_\bullet 0 * \gamma_2 \hookrightarrow_\circ 0\}$

$\boxed{\exists n_1, n_2.\, x \mapsto n_1 + n_2 * \gamma_1 \hookrightarrow_\bullet n_1 * \gamma_2 \hookrightarrow_\bullet n_2}$ nouvel invariant

$\{\gamma_1 \hookrightarrow_\circ 0 * \gamma_2 \hookrightarrow_\circ 0\}$

$\{\gamma_1 \hookrightarrow_\circ 0\}$

`fetchandadd`$(x, 2)$

$a := x$

$\{a = 4\}$

$\{\gamma_2 \hookrightarrow_\circ 0\}$

`fetchandadd`$(x, 2)$

Les variables fantôme exclusives à l'œuvre

$\{x \mapsto \_\}$
$x := 0$
$\{x \mapsto 0\}$
$\{x \mapsto 0 * \gamma_1 \hookrightarrow_\bullet 0 * \gamma_1 \hookrightarrow_\circ 0 * \gamma_2 \hookrightarrow_\bullet 0 * \gamma_2 \hookrightarrow_\circ 0\}$
$\boxed{\exists n_1, n_2.\, x \mapsto n_1 + n_2 * \gamma_1 \hookrightarrow_\bullet n_1 * \gamma_2 \hookrightarrow_\bullet n_2}$ nouvel invariant
$\{\gamma_1 \hookrightarrow_\circ 0 * \gamma_2 \hookrightarrow_\circ 0\}$

$\{\gamma_1 \hookrightarrow_\circ 0\}$	$\{\gamma_2 \hookrightarrow_\circ 0\}$
$\texttt{fetchandadd}(x, 2)$	$\texttt{fetchandadd}(x, 2)$
$\{\gamma_1 \hookrightarrow_\circ 2\}$	$\{\gamma_2 \hookrightarrow_\circ 2\}$

$\{\gamma_1 \hookrightarrow_\circ 2 * \gamma_2 \hookrightarrow_\circ 2\}$
$a := x$
$\{a = 4\}$

Les variables fantôme exclusives à l'œuvre

$\{x \mapsto \_\}$

$x := 0$

$\{x \mapsto 0\}$

$\{x \mapsto 0 * \gamma_1 \hookrightarrow_\bullet 0 * \gamma_1 \hookrightarrow_\circ 0 * \gamma_2 \hookrightarrow_\bullet 0 * \gamma_2 \hookrightarrow_\circ 0\}$

$\boxed{\exists n_1, n_2.\, x \mapsto n_1 + n_2 * \gamma_1 \hookrightarrow_\bullet n_1 * \gamma_2 \hookrightarrow_\bullet n_2}$ nouvel invariant

$\{\gamma_1 \hookrightarrow_\circ 0 * \gamma_2 \hookrightarrow_\circ 0\}$

$\{\gamma_1 \hookrightarrow_\circ 0\}$	$\{\gamma_2 \hookrightarrow_\circ 0\}$
$\{\gamma_1 \hookrightarrow_\circ 0 * x \mapsto (n_1+n_2) * \gamma_1 \hookrightarrow_\bullet n_1 * \gamma_2 \hookrightarrow_\bullet n_2\}$	
`fetchandadd`$(x, 2)$	`fetchandadd`$(x, 2)$
$\{\gamma_1 \hookrightarrow_\circ 2\}$	$\{\gamma_2 \hookrightarrow_\circ 2\}$

$\{\gamma_1 \hookrightarrow_\circ 2 * \gamma_2 \hookrightarrow_\circ 2\}$

$a := x$

$\{a = 4\}$

Les variables fantôme exclusives à l'œuvre

$\{x \mapsto \_\}$

$x := 0$

$\{x \mapsto 0\}$

$\{x \mapsto 0 * \gamma_1 \hookrightarrow_\bullet 0 * \gamma_1 \hookrightarrow_\circ 0 * \gamma_2 \hookrightarrow_\bullet 0 * \gamma_2 \hookrightarrow_\circ 0\}$

$\boxed{\exists n_1, n_2.\, x \mapsto n_1 + n_2 * \gamma_1 \hookrightarrow_\bullet n_1 * \gamma_2 \hookrightarrow_\bullet n_2}$ nouvel invariant

$\{\gamma_1 \hookrightarrow_\circ 0 * \gamma_2 \hookrightarrow_\circ 0\}$

$\{\gamma_1 \hookrightarrow_\circ 0\}$	$\{\gamma_2 \hookrightarrow_\circ 0\}$
$\{\gamma_1 \hookrightarrow_\circ 0 * x \mapsto (n_1+n_2) * \gamma_1 \hookrightarrow_\bullet n_1 * \gamma_2 \hookrightarrow_\bullet n_2\}$	
`fetchandadd`$(x, 2)$	`fetchandadd`$(x, 2)$
$\{\gamma_1 \hookrightarrow_\circ 2\}$	$\{\gamma_2 \hookrightarrow_\circ 2\}$

$\{\gamma_1 \hookrightarrow_\circ 2 * \gamma_2 \hookrightarrow_\circ 2\}$

$a := x$

$\{a = 4\}$

Les variables fantôme exclusives à l'œuvre

$\{x \mapsto \_\}$

$x := 0$

$\{x \mapsto 0\}$

$\{x \mapsto 0 * \gamma_1 \hookrightarrow_\bullet 0 * \gamma_1 \hookrightarrow_\circ 0 * \gamma_2 \hookrightarrow_\bullet 0 * \gamma_2 \hookrightarrow_\circ 0\}$

$\boxed{\exists n_1, n_2.\, x \mapsto n_1 + n_2 * \gamma_1 \hookrightarrow_\bullet n_1 * \gamma_2 \hookrightarrow_\bullet n_2}$ nouvel invariant

$\{\gamma_1 \hookrightarrow_\circ 0 * \gamma_2 \hookrightarrow_\circ 0\}$

$\{\gamma_1 \hookrightarrow_\circ 0\}$	$\{\gamma_2 \hookrightarrow_\circ 0\}$
$\{\gamma_1 \hookrightarrow_\circ 0 * x \mapsto (n_1+n_2) * \gamma_1 \hookrightarrow_\bullet n_1 * \gamma_2 \hookrightarrow_\bullet n_2\}$	
$\{\gamma_1 \hookrightarrow_\circ 0 * x \mapsto n_2 * \gamma_1 \hookrightarrow_\bullet 0 * \gamma_2 \hookrightarrow_\bullet n_2\}$	
`fetchandadd`$(x, 2)$	`fetchandadd`$(x, 2)$
$\{\gamma_1 \hookrightarrow_\circ 2\}$	$\{\gamma_2 \hookrightarrow_\circ 2\}$

$\{\gamma_1 \hookrightarrow_\circ 2 * \gamma_2 \hookrightarrow_\circ 2\}$

$a := x$

$\{a = 4\}$

Les variables fantôme exclusives à l'œuvre

$\{x \mapsto \_\}$

$x := 0$

$\{x \mapsto 0\}$

$\{x \mapsto 0 * \gamma_1 \hookrightarrow_\bullet 0 * \gamma_1 \hookrightarrow_\circ 0 * \gamma_2 \hookrightarrow_\bullet 0 * \gamma_2 \hookrightarrow_\circ 0\}$

$\boxed{\exists n_1, n_2.\, x \mapsto n_1 + n_2 * \gamma_1 \hookrightarrow_\bullet n_1 * \gamma_2 \hookrightarrow_\bullet n_2}$ nouvel invariant

$\{\gamma_1 \hookrightarrow_\circ 0 * \gamma_2 \hookrightarrow_\circ 0\}$

$\{\gamma_1 \hookrightarrow_\circ 0\}$	$\{\gamma_2 \hookrightarrow_\circ 0\}$
$\{\gamma_1 \hookrightarrow_\circ 0 * x \mapsto (n_1+n_2) * \gamma_1 \hookrightarrow_\bullet n_1 * \gamma_2 \hookrightarrow_\bullet n_2\}$	
$\{\gamma_1 \hookrightarrow_\circ 0 * x \mapsto n_2 * \gamma_1 \hookrightarrow_\bullet 0 * \gamma_2 \hookrightarrow_\bullet n_2\}$	
`fetchandadd`$(x, 2)$	`fetchandadd`$(x, 2)$
$\{\gamma_1 \hookrightarrow_\circ 2\}$	$\{\gamma_2 \hookrightarrow_\circ 2\}$

$\{\gamma_1 \hookrightarrow_\circ 2 * \gamma_2 \hookrightarrow_\circ 2\}$

$a := x$

$\{a = 4\}$

Les variables fantôme exclusives à l'œuvre

$\{x \mapsto \_\}$
$x := 0$
$\{x \mapsto 0\}$
$\{x \mapsto 0 * \gamma_1 \hookrightarrow_\bullet 0 * \gamma_1 \hookrightarrow_\circ 0 * \gamma_2 \hookrightarrow_\bullet 0 * \gamma_2 \hookrightarrow_\circ 0\}$
$\boxed{\exists n_1, n_2.\, x \mapsto n_1 + n_2 * \gamma_1 \hookrightarrow_\bullet n_1 * \gamma_2 \hookrightarrow_\bullet n_2}$ nouvel invariant
$\{\gamma_1 \hookrightarrow_\circ 0 * \gamma_2 \hookrightarrow_\circ 0\}$

$\{\gamma_1 \hookrightarrow_\circ 0\}$	$\{\gamma_2 \hookrightarrow_\circ 0\}$
$\{\gamma_1 \hookrightarrow_\circ 0 * x \mapsto (n_1+n_2) * \gamma_1 \hookrightarrow_\bullet n_1 * \gamma_2 \hookrightarrow_\bullet n_2\}$	
$\{\gamma_1 \hookrightarrow_\circ 0 * x \mapsto n_2 * \gamma_1 \hookrightarrow_\bullet 0 * \gamma_2 \hookrightarrow_\bullet n_2\}$	
`fetchandadd`$(x, 2)$	`fetchandadd`$(x, 2)$
$\{\gamma_1 \hookrightarrow_\circ 0 * x \mapsto (2+n_2) * \gamma_1 \hookrightarrow_\bullet 0 * \gamma_2 \hookrightarrow_\bullet n_2\}$	
$\{\gamma_1 \hookrightarrow_\circ 2\}$	$\{\gamma_2 \hookrightarrow_\circ 2\}$

$\{\gamma_1 \hookrightarrow_\circ 2 * \gamma_2 \hookrightarrow_\circ 2\}$

$a := x$

$\{a = 4\}$

Les variables fantôme exclusives à l'œuvre

$\{x \mapsto \_\}$
$x := 0$
$\{x \mapsto 0\}$
$\{x \mapsto 0 * \gamma_1 \hookrightarrow_\bullet 0 * \gamma_1 \hookrightarrow_\circ 0 * \gamma_2 \hookrightarrow_\bullet 0 * \gamma_2 \hookrightarrow_\circ 0\}$
$\boxed{\exists n_1, n_2.\, x \mapsto n_1 + n_2 * \gamma_1 \hookrightarrow_\bullet n_1 * \gamma_2 \hookrightarrow_\bullet n_2}$ nouvel invariant
$\{\gamma_1 \hookrightarrow_\circ 0 * \gamma_2 \hookrightarrow_\circ 0\}$

$\{\gamma_1 \hookrightarrow_\circ 0\}$	$\{\gamma_2 \hookrightarrow_\circ 0\}$
$\{\gamma_1 \hookrightarrow_\circ 0 * x \mapsto (n_1+n_2) * \gamma_1 \hookrightarrow_\bullet n_1 * \gamma_2 \hookrightarrow_\bullet n_2\}$	
$\{\gamma_1 \hookrightarrow_\circ 0 * x \mapsto n_2 * \gamma_1 \hookrightarrow_\bullet 0 * \gamma_2 \hookrightarrow_\bullet n_2\}$	
`fetchandadd`$(x, 2)$	`fetchandadd`$(x, 2)$
$\{\gamma_1 \hookrightarrow_\circ 0 * x \mapsto (2+n_2) * \gamma_1 \hookrightarrow_\bullet 0 * \gamma_2 \hookrightarrow_\bullet n_2\}$	
$\{\gamma_1 \hookrightarrow_\circ 2\}$	$\{\gamma_2 \hookrightarrow_\circ 2\}$
$\{\gamma_1 \hookrightarrow_\circ 2 * \gamma_2 \hookrightarrow_\circ 2\}$	

$a := x$

$\{a = 4\}$

Les variables fantôme exclusives à l'œuvre

$\{x \mapsto \_\}$

$x := 0$

$\{x \mapsto 0\}$

$\{x \mapsto 0 * \gamma_1 \hookrightarrow_\bullet 0 * \gamma_1 \hookrightarrow_\circ 0 * \gamma_2 \hookrightarrow_\bullet 0 * \gamma_2 \hookrightarrow_\circ 0\}$

$\boxed{\exists n_1, n_2.\, x \mapsto n_1 + n_2 * \gamma_1 \hookrightarrow_\bullet n_1 * \gamma_2 \hookrightarrow_\bullet n_2}$ nouvel invariant

$\{\gamma_1 \hookrightarrow_\circ 0 * \gamma_2 \hookrightarrow_\circ 0\}$

$\{\gamma_1 \hookrightarrow_\circ 0\}$	$\{\gamma_2 \hookrightarrow_\circ 0\}$
$\{\gamma_1 \hookrightarrow_\circ 0 * x \mapsto (n_1+n_2) * \gamma_1 \hookrightarrow_\bullet n_1 * \gamma_2 \hookrightarrow_\bullet n_2\}$	
$\{\gamma_1 \hookrightarrow_\circ 0 * x \mapsto n_2 * \gamma_1 \hookrightarrow_\bullet 0 * \gamma_2 \hookrightarrow_\bullet n_2\}$	
`fetchandadd`$(x, 2)$	`fetchandadd`$(x, 2)$
$\{\gamma_1 \hookrightarrow_\circ 0 * x \mapsto (2+n_2) * \gamma_1 \hookrightarrow_\bullet 0 * \gamma_2 \hookrightarrow_\bullet n_2\}$	
$\{\gamma_1 \hookrightarrow_\circ 2 * x \mapsto (2+n_2) * \gamma_1 \hookrightarrow_\bullet 2 * \gamma_2 \hookrightarrow_\bullet n_2\}$	
$\{\gamma_1 \hookrightarrow_\circ 2\}$	$\{\gamma_2 \hookrightarrow_\circ 2\}$

$\{\gamma_1 \hookrightarrow_\circ 2 * \gamma_2 \hookrightarrow_\circ 2\}$

$a := x$

$\{a = 4\}$

Les variables fantôme exclusives à l'œuvre

$\{x \mapsto \_\}$
$x := 0$
$\{x \mapsto 0\}$
$\{x \mapsto 0 * \gamma_1 \hookrightarrow_\bullet 0 * \gamma_1 \hookrightarrow_\circ 0 * \gamma_2 \hookrightarrow_\bullet 0 * \gamma_2 \hookrightarrow_\circ 0\}$
$\boxed{\exists n_1, n_2.\, x \mapsto n_1 + n_2 * \gamma_1 \hookrightarrow_\bullet n_1 * \gamma_2 \hookrightarrow_\bullet n_2}$ nouvel invariant
$\{\gamma_1 \hookrightarrow_\circ 0 * \gamma_2 \hookrightarrow_\circ 0\}$

$\{\gamma_1 \hookrightarrow_\circ 0\}$	$\{\gamma_2 \hookrightarrow_\circ 0\}$
$\{\gamma_1 \hookrightarrow_\circ 0 * x \mapsto (n_1+n_2) * \gamma_1 \hookrightarrow_\bullet n_1 * \gamma_2 \hookrightarrow_\bullet n_2\}$	
$\{\gamma_1 \hookrightarrow_\circ 0 * x \mapsto n_2 * \gamma_1 \hookrightarrow_\bullet 0 * \gamma_2 \hookrightarrow_\bullet n_2\}$	$\{\ldots\}$
`fetchandadd`$(x, 2)$	`fetchandadd`$(x, 2)$
$\{\gamma_1 \hookrightarrow_\circ 0 * x \mapsto (2+n_2) * \gamma_1 \hookrightarrow_\bullet 0 * \gamma_2 \hookrightarrow_\bullet n_2\}$	$\{\ldots\}$
$\{\gamma_1 \hookrightarrow_\circ 2 * x \mapsto (2+n_2) * \gamma_1 \hookrightarrow_\bullet 2 * \gamma_2 \hookrightarrow_\bullet n_2\}$	
$\{\gamma_1 \hookrightarrow_\circ 2\}$	$\{\gamma_2 \hookrightarrow_\circ 2\}$

$\{\gamma_1 \hookrightarrow_\circ 2 * \gamma_2 \hookrightarrow_\circ 2\}$

$a := x$

$\{a = 4\}$

Les variables fantôme exclusives à l'œuvre

$\{x \mapsto \_\}$
$x := 0$
$\{x \mapsto 0\}$
$\{x \mapsto 0 * \gamma_1 \hookrightarrow_\bullet 0 * \gamma_1 \hookrightarrow_\circ 0 * \gamma_2 \hookrightarrow_\bullet 0 * \gamma_2 \hookrightarrow_\circ 0\}$
$\boxed{\exists n_1, n_2.\, x \mapsto n_1 + n_2 * \gamma_1 \hookrightarrow_\bullet n_1 * \gamma_2 \hookrightarrow_\bullet n_2}$ nouvel invariant
$\{\gamma_1 \hookrightarrow_\circ 0 * \gamma_2 \hookrightarrow_\circ 0\}$

$\{\gamma_1 \hookrightarrow_\circ 0\}$	$\{\gamma_2 \hookrightarrow_\circ 0\}$
$\{\gamma_1 \hookrightarrow_\circ 0 * x \mapsto (n_1+n_2) * \gamma_1 \hookrightarrow_\bullet n_1 * \gamma_2 \hookrightarrow_\bullet n_2\}$	
$\{\gamma_1 \hookrightarrow_\circ 0 * x \mapsto n_2 * \gamma_1 \hookrightarrow_\bullet 0 * \gamma_2 \hookrightarrow_\bullet n_2\}$	$\{\ldots\}$
`fetchandadd`$(x, 2)$	`fetchandadd`$(x, 2)$
$\{\gamma_1 \hookrightarrow_\circ 0 * x \mapsto (2+n_2) * \gamma_1 \hookrightarrow_\bullet 0 * \gamma_2 \hookrightarrow_\bullet n_2\}$	$\{\ldots\}$
$\{\gamma_1 \hookrightarrow_\circ 2 * x \mapsto (2+n_2) * \gamma_1 \hookrightarrow_\bullet 2 * \gamma_2 \hookrightarrow_\bullet n_2\}$	
$\{\gamma_1 \hookrightarrow_\circ 2\}$	$\{\gamma_2 \hookrightarrow_\circ 2\}$

$\{\gamma_1 \hookrightarrow_\circ 2 * \gamma_2 \hookrightarrow_\circ 2\}$
$\{\gamma_1 \hookrightarrow_\circ 2 * \gamma_2 \hookrightarrow_\circ 2 * x \mapsto (n_1+n_2) * \gamma_1 \hookrightarrow_\bullet n_1 * \gamma_2 \hookrightarrow_\bullet n_2\}$
$a := x$
$\{a = 4\}$

Les variables fantôme exclusives à l'œuvre

$\{x \mapsto \_\}$
$x := 0$
$\{x \mapsto 0\}$
$\{x \mapsto 0 * \gamma_1 \hookrightarrow_\bullet 0 * \gamma_1 \hookrightarrow_\circ 0 * \gamma_2 \hookrightarrow_\bullet 0 * \gamma_2 \hookrightarrow_\circ 0\}$
$\boxed{\exists n_1, n_2.\, x \mapsto n_1 + n_2 * \gamma_1 \hookrightarrow_\bullet n_1 * \gamma_2 \hookrightarrow_\bullet n_2}$ nouvel invariant
$\{\gamma_1 \hookrightarrow_\circ 0 * \gamma_2 \hookrightarrow_\circ 0\}$

$\{\gamma_1 \hookrightarrow_\circ 0\}$	$\{\gamma_2 \hookrightarrow_\circ 0\}$
$\{\gamma_1 \hookrightarrow_\circ 0 * x \mapsto (n_1+n_2) * \gamma_1 \hookrightarrow_\bullet n_1 * \gamma_2 \hookrightarrow_\bullet n_2\}$	
$\{\gamma_1 \hookrightarrow_\circ 0 * x \mapsto n_2 * \gamma_1 \hookrightarrow_\bullet 0 * \gamma_2 \hookrightarrow_\bullet n_2\}$	$\{\ldots\}$
`fetchandadd`$(x, 2)$	`fetchandadd`$(x, 2)$
$\{\gamma_1 \hookrightarrow_\circ 0 * x \mapsto (2+n_2) * \gamma_1 \hookrightarrow_\bullet 0 * \gamma_2 \hookrightarrow_\bullet n_2\}$	$\{\ldots\}$
$\{\gamma_1 \hookrightarrow_\circ 2 * x \mapsto (2+n_2) * \gamma_1 \hookrightarrow_\bullet 2 * \gamma_2 \hookrightarrow_\bullet n_2\}$	
$\{\gamma_1 \hookrightarrow_\circ 2\}$	$\{\gamma_2 \hookrightarrow_\circ 2\}$

$\{\gamma_1 \hookrightarrow_\circ 2 * \gamma_2 \hookrightarrow_\circ 2\}$
$\{\gamma_1 \hookrightarrow_\circ 2 * \gamma_2 \hookrightarrow_\circ 2 * x \mapsto (n_1+n_2) * \gamma_1 \hookrightarrow_\bullet n_1 * \gamma_2 \hookrightarrow_\bullet n_2\}$
$a := x$
$\{a = 4\}$

Les variables fantôme exclusives à l'œuvre

$\{x \mapsto \_\}$
$x := 0$
$\{x \mapsto 0\}$
$\{x \mapsto 0 * \gamma_1 \hookrightarrow_\bullet 0 * \gamma_1 \hookrightarrow_\circ 0 * \gamma_2 \hookrightarrow_\bullet 0 * \gamma_2 \hookrightarrow_\circ 0\}$
$\boxed{\exists n_1, n_2.\, x \mapsto n_1 + n_2 * \gamma_1 \hookrightarrow_\bullet n_1 * \gamma_2 \hookrightarrow_\bullet n_2}$ nouvel invariant
$\{\gamma_1 \hookrightarrow_\circ 0 * \gamma_2 \hookrightarrow_\circ 0\}$

$\{\gamma_1 \hookrightarrow_\circ 0\}$	$\{\gamma_2 \hookrightarrow_\circ 0\}$
$\{\gamma_1 \hookrightarrow_\circ 0 * x \mapsto (n_1+n_2) * \gamma_1 \hookrightarrow_\bullet n_1 * \gamma_2 \hookrightarrow_\bullet n_2\}$	
$\{\gamma_1 \hookrightarrow_\circ 0 * x \mapsto n_2 * \gamma_1 \hookrightarrow_\bullet 0 * \gamma_2 \hookrightarrow_\bullet n_2\}$	$\{\ldots\}$
`fetchandadd`$(x, 2)$	`fetchandadd`$(x, 2)$
$\{\gamma_1 \hookrightarrow_\circ 0 * x \mapsto (2+n_2) * \gamma_1 \hookrightarrow_\bullet 0 * \gamma_2 \hookrightarrow_\bullet n_2\}$	$\{\ldots\}$
$\{\gamma_1 \hookrightarrow_\circ 2 * x \mapsto (2+n_2) * \gamma_1 \hookrightarrow_\bullet 2 * \gamma_2 \hookrightarrow_\bullet n_2\}$	
$\{\gamma_1 \hookrightarrow_\circ 2\}$	$\{\gamma_2 \hookrightarrow_\circ 2\}$

$\{\gamma_1 \hookrightarrow_\circ 2 * \gamma_2 \hookrightarrow_\circ 2\}$
$\{\gamma_1 \hookrightarrow_\circ 2 * \gamma_2 \hookrightarrow_\circ 2 * x \mapsto (n_1+n_2) * \gamma_1 \hookrightarrow_\bullet n_1 * \gamma_2 \hookrightarrow_\bullet n_2\}$
$\{\gamma_1 \hookrightarrow_\circ 2 * \gamma_2 \hookrightarrow_\circ 2 * x \mapsto 4 * \gamma_1 \hookrightarrow_\bullet 2 * \gamma_2 \hookrightarrow_\bullet 2\}$
$a := x$
$\{a = 4\}$

Les variables fantôme exclusives à l'œuvre

$\{x \mapsto \_\}$
$x := 0$
$\{x \mapsto 0\}$
$\{x \mapsto 0 * \gamma_1 \hookrightarrow_\bullet 0 * \gamma_1 \hookrightarrow_\circ 0 * \gamma_2 \hookrightarrow_\bullet 0 * \gamma_2 \hookrightarrow_\circ 0\}$
$\boxed{\exists n_1, n_2.\, x \mapsto n_1 + n_2 * \gamma_1 \hookrightarrow_\bullet n_1 * \gamma_2 \hookrightarrow_\bullet n_2}$ nouvel invariant
$\{\gamma_1 \hookrightarrow_\circ 0 * \gamma_2 \hookrightarrow_\circ 0\}$

$\{\gamma_1 \hookrightarrow_\circ 0\}$	$\{\gamma_2 \hookrightarrow_\circ 0\}$
$\{\gamma_1 \hookrightarrow_\circ 0 * x \mapsto (n_1+n_2) * \gamma_1 \hookrightarrow_\bullet n_1 * \gamma_2 \hookrightarrow_\bullet n_2\}$	
$\{\gamma_1 \hookrightarrow_\circ 0 * x \mapsto n_2 * \gamma_1 \hookrightarrow_\bullet 0 * \gamma_2 \hookrightarrow_\bullet n_2\}$	$\{\ldots\}$
`fetchandadd`$(x, 2)$	`fetchandadd`$(x, 2)$
$\{\gamma_1 \hookrightarrow_\circ 0 * x \mapsto (2+n_2) * \gamma_1 \hookrightarrow_\bullet 0 * \gamma_2 \hookrightarrow_\bullet n_2\}$	$\{\ldots\}$
$\{\gamma_1 \hookrightarrow_\circ 2 * x \mapsto (2+n_2) * \gamma_1 \hookrightarrow_\bullet 2 * \gamma_2 \hookrightarrow_\bullet n_2\}$	
$\{\gamma_1 \hookrightarrow_\circ 2\}$	$\{\gamma_2 \hookrightarrow_\circ 2\}$

$\{\gamma_1 \hookrightarrow_\circ 2 * \gamma_2 \hookrightarrow_\circ 2\}$
$\{\gamma_1 \hookrightarrow_\circ 2 * \gamma_2 \hookrightarrow_\circ 2 * x \mapsto (n_1+n_2) * \gamma_1 \hookrightarrow_\bullet n_1 * \gamma_2 \hookrightarrow_\bullet n_2\}$
$\{\gamma_1 \hookrightarrow_\circ 2 * \gamma_2 \hookrightarrow_\circ 2 * x \mapsto 4 * \gamma_1 \hookrightarrow_\bullet 2 * \gamma_2 \hookrightarrow_\bullet 2\}$
$a := x$
$\{a = 4\}$

Les variables fantôme exclusives à l'œuvre

$\{x \mapsto \_\}$
$x := 0$
$\{x \mapsto 0\}$
$\{x \mapsto 0 * \gamma_1 \hookrightarrow_\bullet 0 * \gamma_1 \hookrightarrow_\circ 0 * \gamma_2 \hookrightarrow_\bullet 0 * \gamma_2 \hookrightarrow_\circ 0\}$
$\boxed{\exists n_1, n_2.\, x \mapsto n_1 + n_2 * \gamma_1 \hookrightarrow_\bullet n_1 * \gamma_2 \hookrightarrow_\bullet n_2}$ nouvel invariant
$\{\gamma_1 \hookrightarrow_\circ 0 * \gamma_2 \hookrightarrow_\circ 0\}$

$\{\gamma_1 \hookrightarrow_\circ 0\}$	$\{\gamma_2 \hookrightarrow_\circ 0\}$
$\{\gamma_1 \hookrightarrow_\circ 0 * x \mapsto (n_1+n_2) * \gamma_1 \hookrightarrow_\bullet n_1 * \gamma_2 \hookrightarrow_\bullet n_2\}$	
$\{\gamma_1 \hookrightarrow_\circ 0 * x \mapsto n_2 * \gamma_1 \hookrightarrow_\bullet 0 * \gamma_2 \hookrightarrow_\bullet n_2\}$	$\{\ldots\}$
`fetchandadd`$(x, 2)$	`fetchandadd`$(x, 2)$
$\{\gamma_1 \hookrightarrow_\circ 0 * x \mapsto (2+n_2) * \gamma_1 \hookrightarrow_\bullet 0 * \gamma_2 \hookrightarrow_\bullet n_2\}$	$\{\ldots\}$
$\{\gamma_1 \hookrightarrow_\circ 2 * x \mapsto (2+n_2) * \gamma_1 \hookrightarrow_\bullet 2 * \gamma_2 \hookrightarrow_\bullet n_2\}$	
$\{\gamma_1 \hookrightarrow_\circ 2\}$	$\{\gamma_2 \hookrightarrow_\circ 2\}$

$\{\gamma_1 \hookrightarrow_\circ 2 * \gamma_2 \hookrightarrow_\circ 2\}$
$\{\gamma_1 \hookrightarrow_\circ 2 * \gamma_2 \hookrightarrow_\circ 2 * x \mapsto (n_1+n_2) * \gamma_1 \hookrightarrow_\bullet n_1 * \gamma_2 \hookrightarrow_\bullet n_2\}$
$\{\gamma_1 \hookrightarrow_\circ 2 * \gamma_2 \hookrightarrow_\circ 2 * x \mapsto 4 * \gamma_1 \hookrightarrow_\bullet 2 * \gamma_2 \hookrightarrow_\bullet 2\}$
$a := x$
$\{a = 4 \wedge \gamma_1 \hookrightarrow_\circ 2 * \gamma_2 \hookrightarrow_\circ 2 * x \mapsto 4 * \gamma_1 \hookrightarrow_\bullet 2 * \gamma_2 \hookrightarrow_\bullet 2\}$
$\{a = 4\}$

Les variables fantôme exclusives à l'œuvre

$\{x \mapsto \_\}$
$x := 0$
$\{x \mapsto 0\}$
$\{x \mapsto 0 * \gamma_1 \hookrightarrow_\bullet 0 * \gamma_1 \hookrightarrow_\circ 0 * \gamma_2 \hookrightarrow_\bullet 0 * \gamma_2 \hookrightarrow_\circ 0\}$
$\boxed{\exists n_1, n_2.\, x \mapsto n_1 + n_2 * \gamma_1 \hookrightarrow_\bullet n_1 * \gamma_2 \hookrightarrow_\bullet n_2}$ nouvel invariant
$\{\gamma_1 \hookrightarrow_\circ 0 * \gamma_2 \hookrightarrow_\circ 0\}$

$\{\gamma_1 \hookrightarrow_\circ 0\}$	$\{\gamma_2 \hookrightarrow_\circ 0\}$
$\{\gamma_1 \hookrightarrow_\circ 0 * x \mapsto (n_1+n_2) * \gamma_1 \hookrightarrow_\bullet n_1 * \gamma_2 \hookrightarrow_\bullet n_2\}$	
$\{\gamma_1 \hookrightarrow_\circ 0 * x \mapsto n_2 * \gamma_1 \hookrightarrow_\bullet 0 * \gamma_2 \hookrightarrow_\bullet n_2\}$	$\{\ldots\}$
`fetchandadd`$(x, 2)$	`fetchandadd`$(x, 2)$
$\{\gamma_1 \hookrightarrow_\circ 0 * x \mapsto (2+n_2) * \gamma_1 \hookrightarrow_\bullet 0 * \gamma_2 \hookrightarrow_\bullet n_2\}$	$\{\ldots\}$
$\{\gamma_1 \hookrightarrow_\circ 2 * x \mapsto (2+n_2) * \gamma_1 \hookrightarrow_\bullet 2 * \gamma_2 \hookrightarrow_\bullet n_2\}$	
$\{\gamma_1 \hookrightarrow_\circ 2\}$	$\{\gamma_2 \hookrightarrow_\circ 2\}$

$\{\gamma_1 \hookrightarrow_\circ 2 * \gamma_2 \hookrightarrow_\circ 2\}$
$\{\gamma_1 \hookrightarrow_\circ 2 * \gamma_2 \hookrightarrow_\circ 2 * x \mapsto (n_1+n_2) * \gamma_1 \hookrightarrow_\bullet n_1 * \gamma_2 \hookrightarrow_\bullet n_2\}$
$\{\gamma_1 \hookrightarrow_\circ 2 * \gamma_2 \hookrightarrow_\circ 2 * x \mapsto 4 * \gamma_1 \hookrightarrow_\bullet 2 * \gamma_2 \hookrightarrow_\bullet 2\}$
$a := x$
$\{a = 4 \wedge \gamma_1 \hookrightarrow_\circ 2 * \gamma_2 \hookrightarrow_\circ 2 * x \mapsto 4 * \gamma_1 \hookrightarrow_\bullet 2 * \gamma_2 \hookrightarrow_\bullet 2\}$
$\{a = 4\}$

Variables fantôme fractionnaires

Et si on avait n fils d'exécution parallèles ? Utiliser n variables fantôme exclusives différentes revient à avoir une preuve différente pour chaque fil d'exécution...

Une meilleure idée : variables fantôme avec *permissions fractionnaires* $(0, 1]_{\mathbb{Q}}$:

$$\gamma \overset{\pi_1+\pi_2}{\hookrightarrow}_\circ (n_1 + n_2) \quad \Leftrightarrow \quad \gamma \overset{\pi_1}{\hookrightarrow}_\circ n_1 * \gamma \overset{\pi_2}{\hookrightarrow}_\circ n_2$$

Variables fantôme fractionnaires

Et si on avait n fils d'exécution parallèles ? Utiliser n variables fantôme exclusives différentes revient à avoir une preuve différente pour chaque fil d'exécution...

Une meilleure idée : variables fantôme avec *permissions fractionnaires* $(0, 1]_{\mathbb{Q}}$:

$$\gamma \overset{\pi_1+\pi_2}{\hookrightarrow}_\circ (n_1 + n_2) \quad \Leftrightarrow \quad \gamma \overset{\pi_1}{\hookrightarrow}_\circ n_1 * \gamma \overset{\pi_2}{\hookrightarrow}_\circ n_2$$

On ne peut déduire l'égalité que si on la *propriété totale* $(\pi = 1)$:

$$\gamma \hookrightarrow_\bullet n * \gamma \overset{1}{\hookrightarrow}_\circ m \quad \Rightarrow \quad n = m$$

Variables fantôme fractionnaires

Et si on avait n fils d'exécution parallèles ? Utiliser n variables fantôme exclusives différentes revient à avoir une preuve différente pour chaque fil d'exécution...

Une meilleure idée : variables fantôme avec *permissions fractionnaires* $(0, 1]_{\mathbb{Q}}$:

$$\gamma \overset{\pi_1+\pi_2}{\hookrightarrow}_\circ (n_1 + n_2) \quad \Leftrightarrow \quad \gamma \overset{\pi_1}{\hookrightarrow}_\circ n_1 * \gamma \overset{\pi_2}{\hookrightarrow}_\circ n_2$$

On ne peut déduire l'égalité que si on la *propriété totale* $(\pi = 1)$:

$$\gamma \hookrightarrow_\bullet n * \gamma \overset{1}{\hookrightarrow}_\circ m \quad \Rightarrow \quad n = m$$

Modification possible avec la *propriété partielle* $(0 < \pi \leq 1)$:

$$\gamma \hookrightarrow_\bullet n * \gamma \overset{\pi}{\hookrightarrow}_\circ m \quad \Rrightarrow \quad \gamma \hookrightarrow_\bullet (n + i) * \gamma \overset{\pi}{\hookrightarrow}_\circ (m + i)$$

Variables fantôme fractionnaires

Et si on avait n fils d'exécution parallèles ? Utiliser n variables fantôme exclusives différentes revient à avoir une preuve différente pour chaque fil d'exécution...

Une meilleure idée : variables fantôme avec *permissions fractionnaires* $(0, 1]_{\mathbb{Q}}$:

$$\gamma \overset{\pi_1+\pi_2}{\hookrightarrow}_\circ (n_1 + n_2) \quad \Leftrightarrow \quad \gamma \overset{\pi_1}{\hookrightarrow}_\circ n_1 * \gamma \overset{\pi_2}{\hookrightarrow}_\circ n_2$$

On ne peut déduire l'égalité que si on la *propriété totale* $(\pi = 1)$:

$$\gamma \hookrightarrow_\bullet n * \gamma \overset{1}{\hookrightarrow}_\circ m \quad \Rightarrow \quad n = m$$

Modification possible avec la *propriété partielle* $(0 < \pi \leq 1)$:

$$\gamma \hookrightarrow_\bullet n * \gamma \overset{\pi}{\hookrightarrow}_\circ m \quad \Rrightarrow \quad \gamma \hookrightarrow_\bullet (n + i) * \gamma \overset{\pi}{\hookrightarrow}_\circ (m + i)$$

Propriété : tous les $\gamma \overset{\pi_i}{\hookrightarrow}_\circ n_i$ se combinent en $\gamma \hookrightarrow_\bullet \sum n_i$

Variables fantôme fractionnaires à l'œuvre

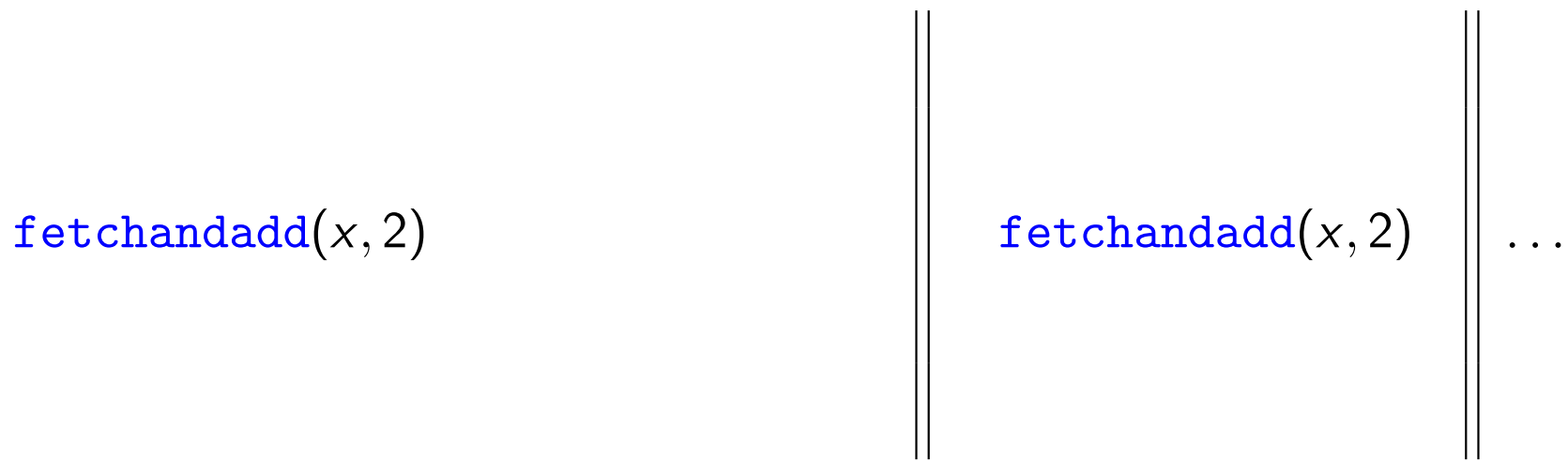
$\{x \mapsto \_\}$
$x := 0$

$a := x$

$\{a = 2k\}$

Variables fantôme fractionnaires à l'œuvre

$\{x \mapsto \_\}$
$x := 0$
$\{x \mapsto 0\}$



$a := x$

$\{a = 2k\}$

Variables fantôme fractionnaires à l'œuvre

$\{x \mapsto \_\}$
$x := 0$
$\{x \mapsto 0\}$
$\left\{x \mapsto 0 * \gamma \hookrightarrow_\bullet 0 * \gamma \overset{1}{\hookrightarrow}_\circ 0\right\}$

$\texttt{fetchandadd}(x, 2)$	$\Vert$	$\texttt{fetchandadd}(x, 2)$ $\Vert$ $\ldots$
$a := x$		
$\{a = 2k\}$		

Variables fantôme fractionnaires à l'œuvre

$\{x \mapsto \_\}$
$x := 0$
$\{x \mapsto 0\}$
$\left\{x \mapsto 0 * \gamma \hookrightarrow_\bullet 0 * \gamma \overset{1}{\hookrightarrow}_\circ 0\right\}$
$\boxed{\exists n.\, x \mapsto n * \gamma \hookrightarrow_\bullet n}$ Nouvel invariant

`fetchandadd`$(x, 2)$	$\parallel$	`fetchandadd`$(x, 2)$	$\parallel$ ...
$a := x$			
$\{a = 2k\}$			

Variables fantôme fractionnaires à l'œuvre

$\{x \mapsto \_\}$
$x := 0$
$\{x \mapsto 0\}$
$\left\{x \mapsto 0 * \gamma \hookrightarrow_\bullet 0 * \gamma \overset{1}{\hookrightarrow}_\circ 0\right\}$
$\boxed{\exists n.\, x \mapsto n * \gamma \hookrightarrow_\bullet n}$ Nouvel invariant

$\left\{\gamma \overset{1/k}{\hookrightarrow}_\circ 0\right\}$	$\left\{\gamma \overset{1/k}{\hookrightarrow}_\circ 0\right\}$	
$\texttt{fetchandadd}(x, 2)$	$\texttt{fetchandadd}(x, 2)$	$\ldots$
$\left\{\gamma \overset{1/k}{\hookrightarrow}_\circ 2\right\}$	$\left\{\gamma \overset{1/k}{\hookrightarrow}_\circ 2\right\}$	

$a := x$

$\{a = 2k\}$

Variables fantôme fractionnaires à l'œuvre

$\{x \mapsto \_\}$

$x := 0$

$\{x \mapsto 0\}$

$\left\{x \mapsto 0 * \gamma \hookrightarrow_\bullet 0 * \gamma \overset{1}{\hookrightarrow}_\circ 0\right\}$

$\boxed{\exists n.\, x \mapsto n * \gamma \hookrightarrow_\bullet n}$ Nouvel invariant

$\left\{\gamma \overset{1/k}{\hookrightarrow}_\circ 0\right\}$

$\left\{\gamma \overset{1/k}{\hookrightarrow}_\circ 0 * x \mapsto n * \gamma \hookrightarrow_\bullet n\right\}$

`fetchandadd`$(x, 2)$

$\left\{\gamma \overset{1/k}{\hookrightarrow}_\circ 2\right\}$

$\left\{\gamma \overset{1/k}{\hookrightarrow}_\circ 0\right\}$

`fetchandadd`$(x, 2)$

$\left\{\gamma \overset{1/k}{\hookrightarrow}_\circ 2\right\}$

$\ldots$

$a := x$

$\{a = 2k\}$

Variables fantôme fractionnaires à l'œuvre

$\{x \mapsto \_\}$

$x := 0$

$\{x \mapsto 0\}$

$\left\{x \mapsto 0 * \gamma \hookrightarrow_\bullet 0 * \gamma \overset{1}{\hookrightarrow}_\circ 0\right\}$

$\boxed{\exists n.\, x \mapsto n * \gamma \hookrightarrow_\bullet n}$ Nouvel invariant

$\left\{\gamma \overset{1/k}{\hookrightarrow}_\circ 0\right\}$

$\left\{\gamma \overset{1/k}{\hookrightarrow}_\circ 0 * x \mapsto n * \gamma \hookrightarrow_\bullet n\right\}$

$\texttt{fetchandadd}(x, 2)$

$\left\{\gamma \overset{1/k}{\hookrightarrow}_\circ 2 * x \mapsto (2+n) * \gamma \hookrightarrow_\bullet (2+n)\right\}$

$\left\{\gamma \overset{1/k}{\hookrightarrow}_\circ 2\right\}$

$\left\|\right.$

$\left\{\gamma \overset{1/k}{\hookrightarrow}_\circ 0\right\}$

$\texttt{fetchandadd}(x, 2)$

$\left\{\gamma \overset{1/k}{\hookrightarrow}_\circ 2\right\}$

$\left\|\right.$ ...

$a := x$

$\{a = 2k\}$

Variables fantôme fractionnaires à l'œuvre

$\{x \mapsto \_\}$
$x := 0$
$\{x \mapsto 0\}$
$\left\{x \mapsto 0 * \gamma \hookrightarrow_\bullet 0 * \gamma \overset{1}{\hookrightarrow}_\circ 0\right\}$
$\boxed{\exists n.\, x \mapsto n * \gamma \hookrightarrow_\bullet n}$ Nouvel invariant

$\left\{\gamma \overset{1/k}{\hookrightarrow}_\circ 0\right\}$
$\quad \left\{\gamma \overset{1/k}{\hookrightarrow}_\circ 0 * x \mapsto n * \gamma \hookrightarrow_\bullet n\right\}$
$\quad \texttt{fetchandadd}(x, 2)$
$\quad \left\{\gamma \overset{1/k}{\hookrightarrow}_\circ 2 * x \mapsto (2+n) * \gamma \hookrightarrow_\bullet (2+n)\right\}$
$\left\{\gamma \overset{1/k}{\hookrightarrow}_\circ 2\right\}$

$\left\{\gamma \overset{1/k}{\hookrightarrow}_\circ 0\right\}$
$\quad \{\ldots\}$
$\quad \texttt{fetchandadd}(x, 2)$
$\quad \{\ldots\}$
$\left\{\gamma \overset{1/k}{\hookrightarrow}_\circ 2\right\}$

$\ldots$

$a := x$

$\{a = 2k\}$

Variables fantôme fractionnaires à l'œuvre

$\{x \mapsto \_\}$
$x := 0$
$\{x \mapsto 0\}$
$\left\{x \mapsto 0 * \gamma \hookrightarrow_\bullet 0 * \gamma \overset{1}{\hookrightarrow}_\circ 0\right\}$
$\boxed{\exists n.\, x \mapsto n * \gamma \hookrightarrow_\bullet n}$ Nouvel invariant

$\left\{\gamma \overset{1/k}{\hookrightarrow}_\circ 0\right\}$
| $\left\{\gamma \overset{1/k}{\hookrightarrow}_\circ 0 * x \mapsto n * \gamma \hookrightarrow_\bullet n\right\}$
| $\texttt{fetchandadd}(x, 2)$
| $\left\{\gamma \overset{1/k}{\hookrightarrow}_\circ 2 * x \mapsto (2+n) * \gamma \hookrightarrow_\bullet (2+n)\right\}$
$\left\{\gamma \overset{1/k}{\hookrightarrow}_\circ 2\right\}$
| $\left\{\gamma \overset{1}{\hookrightarrow}_\circ 2k * x \mapsto n * \gamma \hookrightarrow_\bullet n\right\}$
| $a := x$
|
$\{a = 2k\}$

‖ $\left\{\gamma \overset{1/k}{\hookrightarrow}_\circ 0\right\}$
‖ | $\{\ldots\}$
‖ | $\texttt{fetchandadd}(x, 2)$
‖ | $\{\ldots\}$
‖ $\left\{\gamma \overset{1/k}{\hookrightarrow}_\circ 2\right\}$ ‖ ...

Variables fantôme fractionnaires à l'œuvre

$\{x \mapsto \_\}$
$x := 0$
$\{x \mapsto 0\}$
$\left\{x \mapsto 0 * \gamma \hookrightarrow_\bullet 0 * \gamma \overset{1}{\hookrightarrow}_\circ 0\right\}$
$\boxed{\exists n.\, x \mapsto n * \gamma \hookrightarrow_\bullet n}$ Nouvel invariant

$\left\{\gamma \overset{1/k}{\hookrightarrow}_\circ 0\right\}$
| $\left\{\gamma \overset{1/k}{\hookrightarrow}_\circ 0 * x \mapsto n * \gamma \hookrightarrow_\bullet n\right\}$
| $\texttt{fetchandadd}(x, 2)$
| $\left\{\gamma \overset{1/k}{\hookrightarrow}_\circ 2 * x \mapsto (2+n) * \gamma \hookrightarrow_\bullet (2+n)\right\}$
$\left\{\gamma \overset{1/k}{\hookrightarrow}_\circ 2\right\}$
| $\left\{\gamma \overset{1}{\hookrightarrow}_\circ 2k * x \mapsto n * \gamma \hookrightarrow_\bullet n\right\}$
| $a := x$
| $\left\{a = 2k \wedge \gamma \overset{1}{\hookrightarrow}_\circ 2k * x \mapsto 2k * \gamma \hookrightarrow_\bullet 2k\right\}$
$\{a = 2k\}$

‖ $\left\{\gamma \overset{1/k}{\hookrightarrow}_\circ 0\right\}$
| $\{\ldots\}$
| $\texttt{fetchandadd}(x, 2)$
| $\{\ldots\}$
$\left\{\gamma \overset{1/k}{\hookrightarrow}_\circ 2\right\}$ ‖ ...

Partie 2 :

Généraliser l'état fantôme avec des *algèbres de ressources*

Un peu de recul

Nous connaissons :

- Les invariants $\boxed{R}^{\mathcal{N}}$
- Les variables fantôme exclusives $\gamma \hookrightarrow_\bullet n$ et $\gamma \hookrightarrow_\circ n$
- Les variables fantôme fractionnaires $\gamma \hookrightarrow_\bullet n$ et $\gamma \overset{\pi}{\hookrightarrow}_\circ n$

Mais aussi :

- La propriété de variables physiques $\ell \mapsto v$
  - Avec fraction $\ell \overset{\pi}{\mapsto} v$
- Assertions sur les verrous : $\ell \bullet\!\!\overset{\pi}{\longrightarrow} \mathit{RI}$, $\blacksquare\,\ell$
- Crédits-temps $\$n$, reçus-temps $⧗n$, suspensions $\mathit{isThunk}\ t\ n\ \phi$
- ...

Serait-il possible d'unifier et de généraliser tous ces concepts ?

Un peu de recul

Nous connaissons :

- Les invariants $\boxed{R}^{\mathcal{N}}$
- Les variables fantôme exclusives $\gamma \hookrightarrow_\bullet n$ et $\gamma \hookrightarrow_\circ n$
- Les variables fantôme fractionnaires $\gamma \hookrightarrow_\bullet n$ et $\gamma \overset{\pi}{\hookrightarrow}_\circ n$

Mais aussi :

- La propriété de variables physiques $\ell \mapsto v$
  - Avec fraction $\ell \overset{\pi}{\mapsto} v$
- Assertions sur les verrous : $\ell \bullet\!\!\overset{\pi}{\longrightarrow} RI$, $\blacksquare \ell$
- Crédits-temps $\$n$, reçus-temps $⧗n$, suspensions $isThunk\ t\ n\ \phi$
- ...

Serait-il possible d'unifier et de généraliser tous ces concepts ?

$\Longrightarrow$ Iris introduit les ressources fantôme.

Généraliser les ressources

Toutes les formes de ressource ont des propriétés en commun :

- Les ressources de différents fils d'exécution peuvent être composées.
  Par exemple :

$$\gamma \xhookrightarrow{\pi_1+\pi_2}_\circ (n_1 + n_2) \quad \Leftrightarrow \quad \gamma \xhookrightarrow{\pi_1}_\circ n_1 * \gamma \xhookrightarrow{\pi_2}_\circ n_2$$

Généraliser les ressources

Toutes les formes de ressource ont des propriétés en commun :

- Les ressources de différents fils d'exécution peuvent être composées.
  Par exemple :

$$\gamma \xhookrightarrow{\pi_1+\pi_2}_\circ (n_1 + n_2) \quad \Leftrightarrow \quad \gamma \xhookrightarrow{\pi_1}_\circ n_1 * \gamma \xhookrightarrow{\pi_2}_\circ n_2$$

- La composition de ressources est associative et commutative
  Correspond à l'associativité et à la commutativité de la mise en parallèle et de la conjonction séparante $*$.

Généraliser les ressources

Toutes les formes de ressource ont des propriétés en commun :

- Les ressources de différents fils d'exécution peuvent être composées.
  Par exemple :

$$\gamma \xhookrightarrow{\pi_1+\pi_2}_{\circ} (n_1 + n_2) \quad \Leftrightarrow \quad \gamma \xhookrightarrow{\pi_1}_{\circ} n_1 * \gamma \xhookrightarrow{\pi_2}_{\circ} n_2$$

- La composition de ressources est associative et commutative
  Correspond à l'associativité et à la commutativité de la mise en parallèle et de la conjonction séparante $*$.
- Certaines combinaisons sont impossibles.
  Par exemple :

$$\gamma \hookrightarrow_{\bullet} 5 * \gamma \xhookrightarrow{1/2}_{\circ} 3 * \gamma \xhookrightarrow{1/2}_{\circ} 4 \quad \Rightarrow \quad \text{False}$$

(car $5 \neq 3 + 4$)

Les algèbres de ressource

Une *algèbre de ressource* (version simplifiée) est définie par :

- Son support M
- Sa loi de composition $(\cdot) : M \to M \to M$
- Son prédicat de validité $\mathcal{V} \subseteq M$

Avec :

$$a \cdot b = b \cdot a \qquad a \cdot (b \cdot c) = (a \cdot b) \cdot c \qquad (a \cdot b) \in \mathcal{V} \Rightarrow a \in \mathcal{V}$$

Les algèbres de ressource

Une *algèbre de ressource* (version simplifiée) est définie par :

- Son support M
- Sa loi de composition $(\cdot) : M \to M \to M$
- Son prédicat de validité $\mathcal{V} \subseteq M$

Avec :

$$a \cdot b = b \cdot a \qquad a \cdot (b \cdot c) = (a \cdot b) \cdot c \qquad (a \cdot b) \in \mathcal{V} \Rightarrow a \in \mathcal{V}$$

Iris a des *variables fantôme* $\boxed{a : M}^{\gamma}$ pour chaque algèbre de ressource M

$$a \in \mathcal{V} \Rrightarrow \exists \gamma.\, \boxed{a}^{\gamma} \qquad \boxed{a}^{\gamma} * \boxed{b}^{\gamma} \Leftrightarrow \boxed{a \cdot b}^{\gamma} \qquad \boxed{a}^{\gamma} \Rightarrow \mathcal{V}(a)$$

$$\frac{\forall a_{\mathrm{f}}.\, a \cdot a_{\mathrm{f}} \in \mathcal{V} \Rightarrow b \cdot a_{\mathrm{f}} \in \mathcal{V}}{\boxed{a}^{\gamma} \Rrightarrow \boxed{b}^{\gamma}}$$

Algèbre de ressource pour les variables fantôme exclusives

Une algèbre de ressource pour les variables fantôme exclusives :

$$M \triangleq \bullet\, n \mid \circ\, n \mid \bullet\!\!\circ\, n \mid \bot$$

$$\mathcal{V} \triangleq \{a \neq \bot \mid a \in M\}$$

$$\bullet\, n \cdot \circ\, n' = \circ\, n' \cdot \bullet\, n \triangleq \begin{cases} \bullet\!\!\circ\, n & \text{if } n = n' \\ \bot & \text{sinon} \end{cases}$$

$$\text{autres combinaisons} \triangleq \bot$$

On définit alors :

$$\gamma \hookrightarrow_\bullet n \triangleq \boxed{\bullet\, n}^{\gamma} \qquad \gamma \hookrightarrow_\circ n \triangleq \boxed{\circ\, n}^{\gamma}$$

Algèbre de ressource pour les variables fantôme exclusives

Une algèbre de ressource pour les variables fantôme exclusives :

$$M \triangleq \bullet\, n \mid \circ\, n \mid \bullet\!\!\circ\, n \mid \bot$$

$$\mathcal{V} \triangleq \{a \neq \bot \mid a \in M\}$$

$$\bullet\, n \cdot \circ\, n' = \circ\, n' \cdot \bullet\, n \triangleq \begin{cases} \bullet\!\!\circ\, n & \text{if } n = n' \\ \bot & \text{sinon} \end{cases}$$

$$\text{autres combinaisons} \triangleq \bot$$

On définit alors :

$$\gamma \hookrightarrow_\bullet n \triangleq \boxed{\bullet\, n}^{\gamma} \qquad \gamma \hookrightarrow_\circ n \triangleq \boxed{\circ\, n}^{\gamma}$$

Les règles de raisonnement sur les variables fantôme exclusives peuvent se déduire des règles générales :

$$\text{True} \Rrightarrow \exists \gamma.\, \gamma \hookrightarrow_\bullet n * \gamma \hookrightarrow_\circ n$$

Algèbre de ressource pour les variables fantôme exclusives

Une algèbre de ressource pour les variables fantôme exclusives :

$$M \triangleq \bullet\, n \mid \circ\, n \mid \bullet\!\!\circ\, n \mid \bot$$

$$\mathcal{V} \triangleq \{a \neq \bot \mid a \in M\}$$

$$\bullet\, n \cdot \circ\, n' = \circ\, n' \cdot \bullet\, n \triangleq \begin{cases} \bullet\!\!\circ\, n & \text{if } n = n' \\ \bot & \text{sinon} \end{cases}$$

$$\text{autres combinaisons} \triangleq \bot$$

On définit alors :

$$\gamma \hookrightarrow_\bullet n \triangleq \boxed{\bullet\, n}^{\gamma} \qquad \gamma \hookrightarrow_\circ n \triangleq \boxed{\circ\, n}^{\gamma}$$

Les règles de raisonnement sur les variables fantôme exclusives peuvent se déduire des règles générales :

$$\text{True} \Rrightarrow \exists\gamma.\, \boxed{\bullet\!\!\circ\, n}^{\gamma} \twoheadrightarrow \exists\gamma.\, \gamma \hookrightarrow_\bullet n * \gamma \hookrightarrow_\circ n$$

Algèbre de ressource pour les variables fantôme exclusives

Une algèbre de ressource pour les variables fantôme exclusives :

$$M \triangleq \bullet\, n \mid \circ\, n \mid \bullet\!\!\circ\, n \mid \bot$$

$$\mathcal{V} \triangleq \{a \neq \bot \mid a \in M\}$$

$$\bullet\, n \cdot \circ\, n' = \circ\, n' \cdot \bullet\, n \triangleq \begin{cases} \bullet\!\!\circ\, n & \text{if } n = n' \\ \bot & \text{sinon} \end{cases}$$

$$\text{autres combinaisons} \triangleq \bot$$

On définit alors :

$$\gamma \hookrightarrow_\bullet n \triangleq \boxed{\bullet\, n}^{\gamma} \qquad \gamma \hookrightarrow_\circ n \triangleq \boxed{\circ\, n}^{\gamma}$$

Les règles de raisonnement sur les variables fantôme exclusives peuvent se déduire des règles générales :

$$\text{True} \Rrightarrow \exists\gamma.\, \boxed{\bullet\!\!\circ\, n}^{\gamma} \twoheadrightarrow \exists\gamma.\, \gamma \hookrightarrow_\bullet n * \gamma \hookrightarrow_\circ n$$

$$\gamma \hookrightarrow_\bullet n * \gamma \hookrightarrow_\circ m \Rightarrow n = m$$

Algèbre de ressource pour les variables fantôme exclusives

Une algèbre de ressource pour les variables fantôme exclusives :

$$M \triangleq \bullet\, n \mid \circ\, n \mid \bullet\!\!\circ\, n \mid \bot$$

$$\mathcal{V} \triangleq \{a \neq \bot \mid a \in M\}$$

$$\bullet\, n \cdot \circ\, n' = \circ\, n' \cdot \bullet\, n \triangleq \begin{cases} \bullet\!\!\circ\, n & \text{if } n = n' \\ \bot & \text{sinon} \end{cases}$$

$$\text{autres combinaisons} \triangleq \bot$$

On définit alors :

$$\gamma \hookrightarrow_\bullet n \triangleq \boxed{\bullet\, n}^{\gamma} \qquad \gamma \hookrightarrow_\circ n \triangleq \boxed{\circ\, n}^{\gamma}$$

Les règles de raisonnement sur les variables fantôme exclusives peuvent se déduire des règles générales :

$$\text{True} \Rrightarrow \exists\gamma.\, \boxed{\bullet\!\!\circ\, n}^{\gamma} \twoheadrightarrow \exists\gamma.\, \gamma \hookrightarrow_\bullet n * \gamma \hookrightarrow_\circ n$$

$$\gamma \hookrightarrow_\bullet n * \gamma \hookrightarrow_\circ m \Rightarrow (\bullet\, n \cdot \circ\, m) \in \mathcal{V} \Rightarrow n = m$$

Modifier les variables fantôme

Les variables fantôme peuvent être *mises à jour* en utilisant des *transformation conservant le cadre :*

$$\frac{\forall a_{\mathrm{f}}.\, a \cdot a_{\mathrm{f}} \in \mathcal{V} \Rightarrow b \cdot a_{\mathrm{f}} \in \mathcal{V}}{\boxed{a}^{\gamma} \mathrel{-\!\!*} \boxed{b}^{\gamma}}$$

Idée-clef : une ressource peut être transformée si la transformation n'invalide pas les ressources des fils d'exécution concurrents.

Fil 1		Fil 2		...		Fil n	
a_1	$\cdot$	a_2	$\cdot$	$\ldots$	$\cdot$	a_n	$\in \mathcal{V}$
$\rightsquigarrow$							
b_1	$\cdot$	a_2	$\cdot$	$\ldots$	$\cdot$	a_n	$\in \mathcal{V}$

Modifier les variables fantôme

Les variables fantôme peuvent être *mises à jour* en utilisant des *transformation conservant le cadre :*

$$\frac{\forall a_{\mathrm{f}}.\, a \cdot a_{\mathrm{f}} \in \mathcal{V} \Rightarrow b \cdot a_{\mathrm{f}} \in \mathcal{V}}{\boxed{a}^{\gamma} \Rrightarrow \boxed{b}^{\gamma}}$$

Idée-clef : une ressource peut être transformée si la transformation n'invalide pas les ressources des fils d'exécution concurrents.

Fil 1		Fil 2		...		Fil n	
a_1	$\cdot$	a_2	$\cdot$	$\ldots$	$\cdot$	a_n	$\in \mathcal{V}$
$\rightsquigarrow$							
b_1	$\cdot$	a_2	$\cdot$	$\ldots$	$\cdot$	a_n	$\in \mathcal{V}$

On peut déduire la règle pour les variables fantôme exclusives directement :

$$\gamma \hookrightarrow_{\bullet} n * \gamma \hookrightarrow_{\circ} m \Rrightarrow \gamma \hookrightarrow_{\bullet} n' * \gamma \hookrightarrow_{\circ} n'$$

Ressources pour les variables fantôme fractionnaires

Rappel :

$$\gamma \xhookrightarrow{\pi_1+\pi_2}_{\circ} (n_1 + n_2) \quad \Leftrightarrow \quad \gamma \xhookrightarrow{\pi_1}_{\circ} n_1 * \gamma \xhookrightarrow{\pi_2}_{\circ} n_2$$

$$\gamma \hookrightarrow_{\bullet} n * \gamma \xhookrightarrow{1}_{\circ} m \quad \Rightarrow \quad n = m$$

$$\gamma \hookrightarrow_{\bullet} n * \gamma \xhookrightarrow{\pi}_{\circ} m \quad \equiv\!\!* \quad \gamma \hookrightarrow_{\bullet} (n + i) * \gamma \xhookrightarrow{\pi}_{\circ} (m + i)$$

Ressources pour les variables fantôme fractionnaires

Rappel :

$$\gamma \xhookrightarrow{\pi_1+\pi_2}_{\circ} (n_1 + n_2) \quad \Leftrightarrow \quad \gamma \xhookrightarrow{\pi_1}_{\circ} n_1 * \gamma \xhookrightarrow{\pi_2}_{\circ} n_2$$

$$\gamma \hookrightarrow_{\bullet} n * \gamma \xhookrightarrow{1}_{\circ} m \quad \Rightarrow \quad n = m$$

$$\gamma \hookrightarrow_{\bullet} n * \gamma \xhookrightarrow{\pi}_{\circ} m \quad \equiv\!\!* \quad \gamma \hookrightarrow_{\bullet} (n + i) * \gamma \xhookrightarrow{\pi}_{\circ} (m + i)$$

S'il n'y avait que des $\xhookrightarrow{\pi}_{\circ}$, on prendrait $M = (0, 1]_{\mathbb{Q}} \times \mathbb{N}$.

Ressources pour les variables fantôme fractionnaires

Rappel :

$$\gamma \overset{\pi_1+\pi_2}{\hookrightarrow}_\circ (n_1 + n_2) \quad \Leftrightarrow \quad \gamma \overset{\pi_1}{\hookrightarrow}_\circ n_1 * \gamma \overset{\pi_2}{\hookrightarrow}_\circ n_2$$

$$\gamma \hookrightarrow_\bullet n * \gamma \overset{1}{\hookrightarrow}_\circ m \quad \Rightarrow \quad n = m$$

$$\gamma \hookrightarrow_\bullet n * \gamma \overset{\pi}{\hookrightarrow}_\circ m \quad \text{⫲} \quad \gamma \hookrightarrow_\bullet (n + i) * \gamma \overset{\pi}{\hookrightarrow}_\circ (m + i)$$

S'il n'y avait que des $\overset{\pi}{\hookrightarrow}_\circ$, on prendrait $M = (0, 1]_{\mathbb{Q}} \times \mathbb{N}$.

Il faut rajouter à M des éléments $\gamma \hookrightarrow_\bullet n$, de façon à obtenir les propriétés ci-dessus.

Algèbre de ressource autoritaire $\textsc{Auth}(M)$

Soit M une algèbre de ressource *unitaire* (i.e., avec élément neutre).

Idée clef : une ressource $\bullet\, a$ (l'« autorité ») témoigne de la composition de toutes les autres ressources $\circ\, x$ (les « fragments »).

Algèbre de ressource autoritaire $\textsc{Auth}(M)$

Soit M une algèbre de ressource *unitaire* (i.e., avec élément neutre).

Idée clef : une ressource $\bullet a$ (l'« autorité ») témoigne de la composition de toutes les autres ressources $\circ x$ (les « fragments »).

Éléments :

- L'autorité $\bullet a$
  - $\mathcal{V}(\bullet a) \Leftrightarrow \mathcal{V}(a)$
  - Typiquement dans un invariant
  - Exclusif : $\bullet a \cdot \bullet b \triangleq \bot$
- Les fragments $\circ x$
  - $\mathcal{V}(\circ x) \Leftrightarrow \mathcal{V}(x)$
  - Typiquement détenus par les fils d'exécution
  - $\circ x \cdot \circ y \triangleq \circ (x \cdot y)$
- Leur composition $\bullet a \cdot \circ x$
  - $\mathcal{V}(\bullet a \cdot \circ x) \Leftrightarrow \mathcal{V}(a) \wedge \mathcal{V}(x) \wedge \exists x_{\mathtt{f}} . a = x \cdot x_{\mathtt{f}}$
  - Rarement utilisée directement dans la logique

Ressources pour les variables fantôme fractionnaires

- Soit l'algèbre de ressources $M \triangleq \textsc{Auth}(((0,1]_{\mathbb{Q}} \times \mathbb{N}) \uplus \{\epsilon\})$.
  - ϵ : élément neutre, ressource vide.
- On définit :

$$\gamma \hookrightarrow_{\bullet} n \triangleq \boxed{\bullet\,(1,n)}^{\gamma} \qquad \gamma \overset{\pi}{\hookrightarrow}_{\circ} n \triangleq \boxed{\circ\,(\pi,n)}^{\gamma}$$

Ressources pour les variables fantôme fractionnaires

- Soit l'algèbre de ressources $M \triangleq \textsc{Auth}(((0,1]_{\mathbb{Q}} \times \mathbb{N}) \uplus \{\epsilon\})$.
  - ϵ : élément neutre, ressource vide.
- On définit :
  $\gamma \hookrightarrow_\bullet n \triangleq \boxed{\bullet\,(1,n)}^{\gamma}$ $\qquad$ $\gamma \overset{\pi}{\hookrightarrow}_\circ n \triangleq \boxed{\circ\,(\pi,n)}^{\gamma}$
- On obtient :

$$\gamma \overset{\pi_1+\pi_2}{\hookrightarrow}_\circ (n_1+n_2) \quad \Leftrightarrow \quad \gamma \overset{\pi_1}{\hookrightarrow}_\circ n_1 * \gamma \overset{\pi_2}{\hookrightarrow}_\circ n_2$$

car $\circ\,(\pi_1,n_1) \cdot \circ\,(\pi_2,n_2) = \circ\,(\pi_1+\pi_2, n_1+n_2)$.

Ressources pour les variables fantôme fractionnaires

- Soit l'algèbre de ressources $M \triangleq \textsc{Auth}(((0,1]_{\mathbb{Q}} \times \mathbb{N}) \uplus \{\epsilon\})$.
  - ϵ : élément neutre, ressource vide.
- On définit :
  $\gamma \hookrightarrow_\bullet n \triangleq \boxed{\bullet\,(1,n)}^{\gamma} \qquad \gamma \overset{\pi}{\hookrightarrow}_\circ n \triangleq \boxed{\circ\,(\pi,n)}^{\gamma}$
- On obtient :
  $$\gamma \overset{\pi_1+\pi_2}{\hookrightarrow}_\circ (n_1+n_2) \quad \Leftrightarrow \quad \gamma \overset{\pi_1}{\hookrightarrow}_\circ n_1 * \gamma \overset{\pi_2}{\hookrightarrow}_\circ n_2$$
  car $\circ\,(\pi_1,n_1) \cdot \circ\,(\pi_2,n_2) = \circ\,(\pi_1+\pi_2, n_1+n_2)$.
- Et :
  $$\begin{aligned} \gamma \hookrightarrow_\bullet n * \gamma \overset{1}{\hookrightarrow}_\circ m \;&\Rightarrow\; \boxed{\bullet\,(1,n) \cdot \circ\,(1,m)}^{\gamma} \;\Rightarrow\; \mathcal{V}(\bullet\,(1,n) \cdot \circ\,(1,m)) \\ &\Rightarrow\; \exists x_{\mathtt{f}}.\;\; (1,m) \cdot x_{\mathtt{f}} = (1,n) \\ &\Rightarrow\; m = n \end{aligned}$$

Ressources pour les variables fantôme fractionnaires

- Soit l'algèbre de ressources $M \triangleq \textsc{Auth}(((0,1]_{\mathbb{Q}} \times \mathbb{N}) \uplus \{\epsilon\})$.
  - ϵ : élément neutre, ressource vide.
- On définit :
  $\gamma \hookrightarrow_\bullet n \triangleq \boxed{\bullet\,(1,n)}^{\gamma} \qquad \gamma \overset{\pi}{\hookrightarrow}_\circ n \triangleq \boxed{\circ\,(\pi,n)}^{\gamma}$
- On obtient :
  $$\gamma \overset{\pi_1+\pi_2}{\hookrightarrow}_\circ (n_1+n_2) \quad \Leftrightarrow \quad \gamma \overset{\pi_1}{\hookrightarrow}_\circ n_1 * \gamma \overset{\pi_2}{\hookrightarrow}_\circ n_2$$
  car $\circ\,(\pi_1,n_1) \cdot \circ\,(\pi_2,n_2) = \circ\,(\pi_1+\pi_2, n_1+n_2)$.
- Et :
  $$\begin{aligned} \gamma \hookrightarrow_\bullet n * \gamma \overset{1}{\hookrightarrow}_\circ m \;&\Rightarrow\; \boxed{\bullet\,(1,n) \cdot \circ\,(1,m)}^{\gamma} \;\Rightarrow\; \mathcal{V}(\bullet\,(1,n) \cdot \circ\,(1,m)) \\ &\Rightarrow\; \exists x_{\mathtt{f}}.\;\; (1,m) \cdot x_{\mathtt{f}} = (1,n) \\ &\Rightarrow\; m = n \end{aligned}$$
- Avec une transformation préservant le cadre, on peut prouver :
  $$\gamma \hookrightarrow_\bullet n * \gamma \overset{\pi}{\hookrightarrow}_\circ m \quad \Rrightarrow\!\!\!* \quad \gamma \hookrightarrow_\bullet (n+i) * \gamma \overset{\pi}{\hookrightarrow}_\circ (m+i)$$

Constructions d'algèbres de ressource

Nous avons vu :

- $\textsc{Auth}(M)$: algèbre de ressource autoritaire.
  - Un invariant peut mentionner la « composition du reste du contenu de la variable fantôme ».
- Fractions $(0, 1]_{\mathbb{Q}}$, et entiers $\mathbb{N}$, équipés de l'addition.
- Produits d'algèbres de ressource $M \times N$.
- Adjonction d'un élément neutre $M \uplus \{\epsilon\}$

Il existe aussi :

- $\textsc{Excl}(X)$: algèbre de ressource « exclusive »
  - Éléments valides : dans X, composition toujours invalide.
  - Variables fantôme exclusives : $\textsc{Auth}(\textsc{Excl}(\mathbb{N}) \uplus \{\epsilon\})$
- $M + N$, $\textsc{Map}(K, M)$
- ...

Partie 3 :
Exemples de protocoles construits avec invariant et état fantôme

Une bibliothèque de compteur partagé

```
def NouveauCompteur () =
  let c = Alloc(1) in
  c := 0
  Renvoyer c

def IncrCompteur(c) =
  let x = FetchAndAdd(c, 1) in
  Renvoyer x
```

Le compteur comme un générateur de symboles

La bibliothèque de compteur peut être utilisée pour générer des symboles uniques.

- Par exemple, pour créer des identifiants uniques dans un compilateur...

Le compteur comme un générateur de symboles

La bibliothèque de compteur peut être utilisée pour générer des symboles uniques.

- Par exemple, pour créer des identifiants uniques dans un compilateur...

En logique de séparation, on associe à chaque identifiant un *jeton exclusif* :

$$\textsc{Duplicable}(\mathsf{GenSym}_\gamma(c))$$

$$\mathsf{Jeton}_\gamma(x) * \mathsf{Jeton}_\gamma(y) \Rightarrow x \neq y$$

$$\{\mathsf{True}\}\, c := \texttt{NouveauCompteur}()\, \{\mathsf{GenSym}_\gamma(c)\}$$

$$\{\mathsf{GenSym}_\gamma(c)\}\, x := \texttt{IncrCompteur}(c)\, \{\mathsf{Jeton}_\gamma(x)\}$$

Prouver le générateur de symboles en Iris

Algèbre de ressource $\mathtt{Set}(\mathbb{N})$ pour modéliser les jetons :

- Éléments : sous-ensembles de $\mathbb{N}$, et $\bot$.
- Composition : $\uplus$

Prouver le générateur de symboles en Iris

Algèbre de ressource $\mathtt{Set}(\mathbb{N})$ pour modéliser les jetons :

- Éléments : sous-ensembles de $\mathbb{N}$, et $\bot$.
- Composition : $\uplus$

1. On utilise l'algèbre de ressource $\mathtt{Auth}(\mathtt{Set}(\mathbb{N}))$.
2. On définit :

$$\mathsf{Jeton}_\gamma(x) \triangleq \boxed{\circ\{x\}}^\gamma$$

$$\mathsf{GenSym}_\gamma(c) \triangleq \boxed{\exists n.\, c \mapsto n * \boxed{\bullet [0, n)_{\mathbb{N}}}^\gamma}$$

3. On vérifie les propriétés voulues. En particulier :
   - On peut créer un nouveau jeton lorsque n est incrémenté grâce à une transformation préservant le cadre.
   - Les jetons sont exclusifs car la loi de composition est $\uplus$.
   - $\mathsf{GenSym}_\gamma(c)$ est duplicable, puisque c'est un invariant.

Le compteur comme état monotone

On veut prouver que la valeur du compteur ne fait qu'augmenter :

$$\{\mathsf{CompteurMono}_{\gamma}(x)\}$$

$$x := \texttt{IncrCompteur}(c); \quad y := \texttt{IncrCompteur}(c)$$

$$\{x < y\}$$

Le compteur comme état monotone

On veut prouver que la valeur du compteur ne fait qu'augmenter :

$$\{\mathsf{CompteurMono}_\gamma(x)\}$$
$$x := \texttt{IncrCompteur}(c); \quad y := \texttt{IncrCompteur}(c)$$
$$\{x < y\}$$

Spécification : on utilise des *témoins* de la valeur du compteur.

$$\textsc{Duplicable}(\mathsf{CompteurMono}_\gamma(c)) \qquad \textsc{Duplicable}(\mathsf{Témoin}_\gamma(n))$$

$$n \leq m \vdash \mathsf{Témoin}_\gamma(m) \mathrel{-\!\!*} \mathsf{Témoin}_\gamma(n)$$

$$\{\mathsf{True}\}\, c := \texttt{NouveauCompteur}()\, \{\mathsf{CompteurMono}_\gamma(c)\}$$

$$\{\mathsf{CompteurMono}_\gamma(c) * (\mathsf{Témoin}_\gamma(n) \vee n = -1)\}$$
$$m := \texttt{IncrCompteur}(c)$$
$$\{n < m * \mathsf{Témoin}_\gamma(m)\}$$

Prouver la monotonie du compteur

On utilise l'algèbre de ressource $\mathtt{Auth}(\mathbb{N}_{\mathtt{max}})$. Elle donne :

$$\boxed{\bullet\, n}^{\gamma} * \boxed{\circ\, m}^{\gamma} \;\Rightarrow\; \mathcal{V}(\bullet\, n \cdot \circ\, m) \;\Rightarrow\; \exists m'.\, n = \mathsf{max}(m, m') \;\Rightarrow\; m \leq n$$

L'autorité $\bullet\, n$ est une borne inférieure pour les fragments $\circ\, m$!
Pour créer un fragment : $\boxed{\bullet\, n}^{\gamma} \Rrightarrow \boxed{\bullet\, n}^{\gamma} * \boxed{\circ\, n}^{\gamma}$

Prouver la monotonie du compteur

On utilise l'algèbre de ressource $\texttt{Auth}(\mathbb{N}_{\texttt{max}})$. Elle donne :

$$\boxed{\bullet\, n}^{\gamma} * \boxed{\circ\, m}^{\gamma} \;\Rightarrow\; \mathcal{V}(\bullet\, n \cdot \circ\, m) \;\Rightarrow\; \exists m'.\, n = \max(m, m') \;\Rightarrow\; m \leq n$$

L'autorité $\bullet\, n$ est une borne inférieure pour les fragments $\circ\, m$!
Pour créer un fragment : $\boxed{\bullet\, n}^{\gamma} \Rrightarrow \boxed{\bullet\, n}^{\gamma} * \boxed{\circ\, n}^{\gamma}$

On définit :

$\text{Témoin}_{\gamma}(n) \triangleq \boxed{\circ\,(n+1)}^{\gamma}$ $\quad \text{CompteurMono}_{\gamma}(c) \triangleq \boxed{\exists n.\, c \mapsto n * \boxed{\bullet\, n}^{\gamma}}$

Et on peut déduire les propriétés voulues !

Conclusion

- Pour que des fils d'exécutions puissent partager une ressource physique, ils doivent s'accorder sur un **protocole**.
- Ces protocoles font intervenir des permissions logiques, représentés en Iris par des **variables fantômes** contenant des éléments d'une **algèbre de ressource**, choisie par l'utilisateur.
- On relie les ressources physiques à l'état fantôme avec un **invariant**.

Conclusion

- Pour que des fils d'exécutions puissent partager une ressource physique, ils doivent s'accorder sur un **protocole**.
- Ces protocoles font intervenir des permissions logiques, représentés en Iris par des **variables fantômes** contenant des éléments d'une **algèbre de ressource**, choisie par l'utilisateur.
- On relie les ressources physiques à l'état fantôme avec un **invariant**.

Cette méthodologie est très générale et permet de définir une large variété de protocoles.

- Propriétés fractionnaires de cases mémoire $\ell \overset{\pi}{\mapsto} v$
- Verrous : $\ell \overset{\pi}{\bullet\!\!\rightarrow} RI$, $\blacksquare\, \ell$
- Division de la propriété dans le temps : « lifetime logic », utilisée pour prouver la cohérence du système de types de Rust