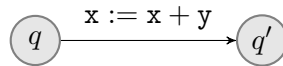


Abstraction par Prédicats — Exercices Corrigés

Grégoire Sutre

<http://www.labri.fr/~sutre/Teaching/INF555/>

Exercice 1 On considère le programme ci-dessous d'ensemble de variables $\mathbf{X} = \{x, y\}$, de localité initiale $q_{in} = q$ et de localité d'erreur $q_{bad} = q'$.



Donner l'abstraction par prédicats booléenne du programme pour les deux prédicats :

$$\varphi_1 : x \geq 0 \qquad \varphi_2 : y \geq 0$$

Corrigé. L'abstraction par prédicats booléenne du programme est la structure de Kripke étiquetée $\mathcal{M}^a = \langle S^a, In^a, Bad^a, \Sigma, \rightarrow^a \rangle$ définie par :

$$\begin{aligned} S^a &= \{q, q'\} \times (\{\varphi_1, \varphi_2\} \rightarrow \{0, 1\}) \\ In^a &= \{q_{in}\} \times (\{\varphi_1, \varphi_2\} \rightarrow \{0, 1\}) \\ \Sigma &= \{x := x + y\} \\ Bad^a &= \{q_{bad}\} \times (\{\varphi_1, \varphi_2\} \rightarrow \{0, 1\}) \end{aligned}$$

et de relation de transition étiquetée \rightarrow^a représentée graphiquement en figure 1. Sur cette figure, les étiquettes des transitions sont omises pour ne pas encombrer le dessin, et un couple (b_1, b_2) de booléens représente la fonction qui à φ_i associe b_i .

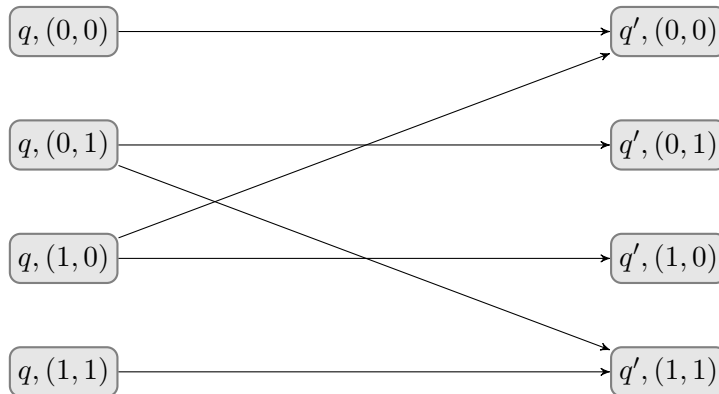


FIGURE 1 – Relation de transition abstraite \rightarrow^a de l'exercice 1

Pour illustrer comment la relation \rightarrow^a est obtenue, considérons quelques exemples :

- le triplet $((q, (1, 1)), \mathbf{x} := \mathbf{x} + \mathbf{y}, (q', (1, 1)))$ est dans \rightarrow^a si et seulement si la formule ψ ci-dessous est satisfaisable :

$$\begin{aligned}\psi &= (\varphi_1 \wedge \varphi_2) \bigwedge ((\varphi_1 \wedge \varphi_2)[(\mathbf{x} + \mathbf{y})/\mathbf{x}]) \\ &= (\mathbf{x} \geq 0 \wedge \mathbf{y} \geq 0) \bigwedge ((\mathbf{x} + \mathbf{y} \geq 0) \wedge \mathbf{y} \geq 0)\end{aligned}$$

Or cette formule est clairement satisfaisable (prendre $\mathbf{x} = 0, \mathbf{y} = 0$).

- le triplet $((q, (1, 1)), \mathbf{x} := \mathbf{x} + \mathbf{y}, (q', (1, 0)))$ est dans \rightarrow^a si et seulement si la formule ψ ci-dessous est satisfaisable :

$$\begin{aligned}\psi &= (\varphi_1 \wedge \varphi_2) \bigwedge ((\varphi_1 \wedge \neg\varphi_2)[(\mathbf{x} + \mathbf{y})/\mathbf{x}]) \\ &= (\mathbf{x} \geq 0 \wedge \mathbf{y} \geq 0) \bigwedge ((\mathbf{x} + \mathbf{y} \geq 0) \wedge \neg(\mathbf{y} \geq 0))\end{aligned}$$

Or cette formule est clairement insatisfaisable.

- le triplet $((q, (1, 1)), \mathbf{x} := \mathbf{x} + \mathbf{y}, (q', (0, 1)))$ est dans \rightarrow^a si et seulement si la formule ψ ci-dessous est satisfaisable :

$$\begin{aligned}\psi &= (\varphi_1 \wedge \varphi_2) \bigwedge ((\neg\varphi_1 \wedge \varphi_2)[(\mathbf{x} + \mathbf{y})/\mathbf{x}]) \\ &= (\mathbf{x} \geq 0 \wedge \mathbf{y} \geq 0) \bigwedge (\neg(\mathbf{x} + \mathbf{y} \geq 0) \wedge \mathbf{y} \geq 0)\end{aligned}$$

Or cette formule est clairement insatisfaisable.

- le triplet $((q, (1, 0)), \mathbf{x} := \mathbf{x} + \mathbf{y}, (q', (0, 1)))$ est dans \rightarrow^a si et seulement si la formule ψ ci-dessous est satisfaisable :

$$\begin{aligned}\psi &= (\varphi_1 \wedge \neg\varphi_2) \bigwedge ((\neg\varphi_1 \wedge \varphi_2)[(\mathbf{x} + \mathbf{y})/\mathbf{x}]) \\ &= (\mathbf{x} \geq 0 \wedge \neg(\mathbf{y} \geq 0)) \bigwedge (\neg(\mathbf{x} + \mathbf{y} \geq 0) \wedge \mathbf{y} \geq 0)\end{aligned}$$

Or cette formule est clairement insatisfaisable.

- le triplet $((q, (1, 0)), \mathbf{x} := \mathbf{x} + \mathbf{y}, (q', (1, 0)))$ est dans \rightarrow^a si et seulement si la formule ψ ci-dessous est satisfaisable :

$$\begin{aligned}\psi &= (\varphi_1 \wedge \neg\varphi_2) \bigwedge ((\varphi_1 \wedge \neg\varphi_2)[(\mathbf{x} + \mathbf{y})/\mathbf{x}]) \\ &= (\mathbf{x} \geq 0 \wedge \neg(\mathbf{y} \geq 0)) \bigwedge (\mathbf{x} + \mathbf{y} \geq 0 \wedge \neg(\mathbf{y} \geq 0))\end{aligned}$$

Or cette formule est clairement satisfaisable (prendre $\mathbf{x} = 2, \mathbf{y} = -1$).

- le triplet $((q, (1, 0)), \mathbf{x} := \mathbf{x} + \mathbf{y}, (q', (0, 0)))$ est dans \rightarrow^a si et seulement si la formule ψ ci-dessous est satisfaisable :

$$\begin{aligned}\psi &= (\varphi_1 \wedge \neg\varphi_2) \bigwedge ((\neg\varphi_1 \wedge \neg\varphi_2)[(\mathbf{x} + \mathbf{y})/\mathbf{x}]) \\ &= (\mathbf{x} \geq 0 \wedge \neg(\mathbf{y} \geq 0)) \bigwedge (\neg(\mathbf{x} + \mathbf{y} \geq 0) \wedge \neg(\mathbf{y} \geq 0))\end{aligned}$$

Or cette formule est clairement satisfaisable (prendre $\mathbf{x} = 1, \mathbf{y} = -2$). ■

Exercice 2 Donner l'abstraction par prédicats cartésienne du programme de l'exercice 1 et pour les mêmes prédicats.

Corrigé. L'abstraction par prédicats cartésienne du programme est la structure de Kripke étiquetée $\mathcal{M}^a = \langle S^a, In^a, Bad^a, \Sigma, \rightarrow^a \rangle$ définie par :

$$\begin{aligned} S^a &= \{q, q'\} \times (\{\varphi_1, \varphi_2\} \rightarrow \{0, 1, *\}) \\ In^a &= \{(q_{in}, \lambda \varphi . *)\} \\ \Sigma &= \{\mathbf{x} := \mathbf{x} + \mathbf{y}\} \\ Bad^a &= \{q_{bad}\} \times (\{\varphi_1, \varphi_2\} \rightarrow \{0, 1, *\}) \end{aligned}$$

et de relation de transition étiquetée \rightarrow^a représentée graphiquement en figure 2. Sur cette figure, les étiquettes des transitions sont omises pour ne pas encombrer le dessin, et un couple (b_1, b_2) d'éléments de $\{0, 1, *\}$ représente la fonction qui à φ_i associe b_i .

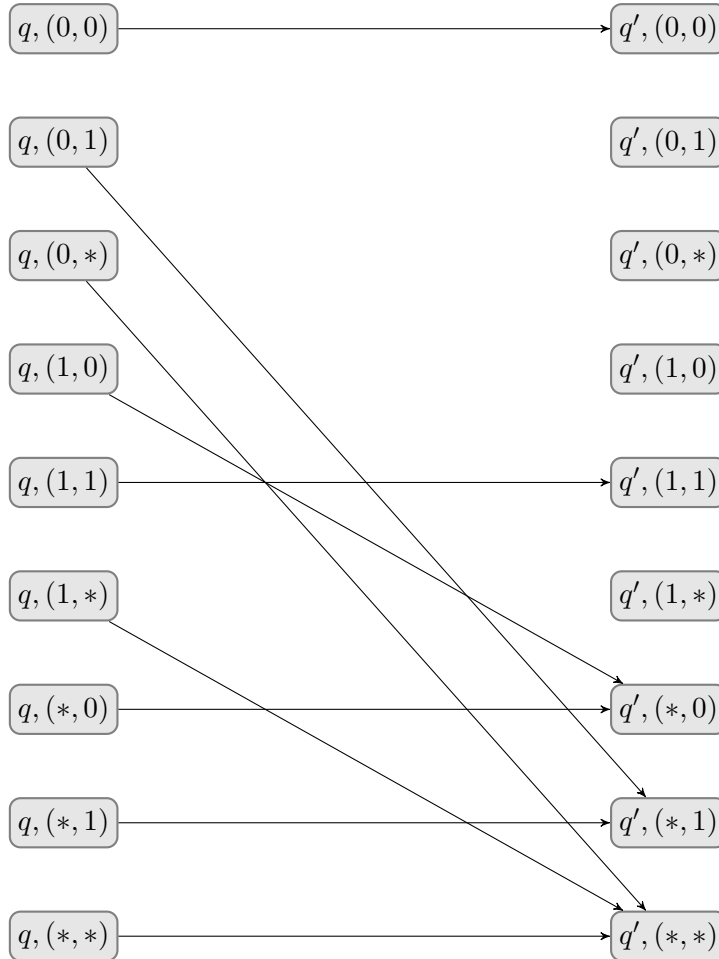


FIGURE 2 – Relation de transition abstraite \rightarrow^a de l'exercice 2

Pour illustrer comment la relation \rightarrow^a est obtenue, considérons quelques exemples :

- Pour calculer l'unique successeur potentiel de l'état abstrait $(q, (1, 1))$, on détermine la validité des formules suivantes :

	valide
$(\varphi_1 \wedge \varphi_2) \Rightarrow (\neg\varphi_1[(\mathbf{x} + \mathbf{y})/\mathbf{x}])$	non
$(\varphi_1 \wedge \varphi_2) \Rightarrow \varphi_1[(\mathbf{x} + \mathbf{y})/\mathbf{x}]$	oui
$(\varphi_1 \wedge \varphi_2) \Rightarrow (\neg\varphi_2[(\mathbf{x} + \mathbf{y})/\mathbf{x}])$	non
$(\varphi_1 \wedge \varphi_2) \Rightarrow \varphi_2[(\mathbf{x} + \mathbf{y})/\mathbf{x}]$	oui

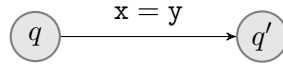
On en déduit que $(q', (1, 1))$ est l'unique successeur de $(q, (1, 1))$.

- Pour calculer l'unique successeur potentiel de l'état abstrait $(q, (1, 0))$, on détermine la validité des formules suivantes :

	valide
$(\varphi_1 \wedge \neg\varphi_2) \Rightarrow (\neg\varphi_1[(\mathbf{x} + \mathbf{y})/\mathbf{x}])$	non
$(\varphi_1 \wedge \neg\varphi_2) \Rightarrow \varphi_1[(\mathbf{x} + \mathbf{y})/\mathbf{x}]$	non
$(\varphi_1 \wedge \neg\varphi_2) \Rightarrow (\neg\varphi_2[(\mathbf{x} + \mathbf{y})/\mathbf{x}])$	oui
$(\varphi_1 \wedge \neg\varphi_2) \Rightarrow \varphi_2[(\mathbf{x} + \mathbf{y})/\mathbf{x}]$	non

On en déduit que $(q', (*, 0))$ est l'unique successeur de $(q, (1, 0))$. ■

Exercice 3 On considère le programme ci-dessous d'ensemble de variables $\mathbf{X} = \{\mathbf{x}, \mathbf{y}\}$, de localité initiale $q_{in} = q$ et de localité d'erreur $q_{bad} = q'$.



Donner l'abstraction par prédicats booléenne du programme pour les deux prédicats :

$$\varphi_1 : \mathbf{x} \geq 0 \qquad \varphi_2 : \mathbf{y} \geq 0$$

Corrigé. L'abstraction par prédicats booléenne du programme est la structure de Kripke étiquetée $\mathcal{M}^a = \langle S^a, In^a, Bad^a, \Sigma, \rightarrow^a \rangle$ définie par :

$$\begin{aligned} S^a &= \{q, q'\} \times (\{\varphi_1, \varphi_2\} \rightarrow \{0, 1\}) \\ In^a &= \{q_{in}\} \times (\{\varphi_1, \varphi_2\} \rightarrow \{0, 1\}) \\ \Sigma &= \{\mathbf{x} = \mathbf{y}\} \\ Bad^a &= \{q_{bad}\} \times (\{\varphi_1, \varphi_2\} \rightarrow \{0, 1\}) \end{aligned}$$

et de relation de transition étiquetée \rightarrow^a représentée graphiquement en figure 3. Sur cette figure, les étiquettes des transitions sont omises pour ne pas encombrer le dessin, et un couple (b_1, b_2) de booléens représente la fonction qui à φ_i associe b_i .

Rappelons que comme l'opération $\mathbf{x} = \mathbf{y}$ est une garde, tous les triplets $((q, (b_1, b_2)), \mathbf{x} := \mathbf{x} + \mathbf{y}, (q', (b'_1, b'_2)))$ dans la relation \rightarrow^a vérifient nécessairement $b_1 = b'_1$ et $b_2 = b'_2$. Pour illustrer comment la relation \rightarrow^a est obtenue, considérons quelques exemples :

FIGURE 3 – Relation de transition abstraite \rightarrow^a de l'exercice 3

- le triplet $((q, (1, 1)), \mathbf{x} = \mathbf{y}, (q', (1, 1)))$ est dans \rightarrow^a si et seulement si la formule ψ ci-dessous est satisfaisable :

$$\begin{aligned}\psi &= (\varphi_1 \wedge \varphi_2) \bigwedge (\mathbf{x} = \mathbf{y}) \\ &= (\mathbf{x} \geq 0 \wedge \mathbf{y} \geq 0) \bigwedge \mathbf{x} = \mathbf{y}\end{aligned}$$

Or cette formule est clairement satisfaisable (prendre $\mathbf{x} = 0, \mathbf{y} = 0$).

- le triplet $((q, (1, 0)), \mathbf{x} = \mathbf{y}, (q', (1, 0)))$ est dans \rightarrow^a si et seulement si la formule ψ ci-dessous est satisfaisable :

$$\begin{aligned}\psi &= (\varphi_1 \wedge \neg\varphi_2) \bigwedge (\mathbf{x} = \mathbf{y}) \\ &= (\mathbf{x} \geq 0 \wedge \neg(\mathbf{y} \geq 0)) \bigwedge \mathbf{x} = \mathbf{y}\end{aligned}$$

Or cette formule est clairement insatisfaisable. ■

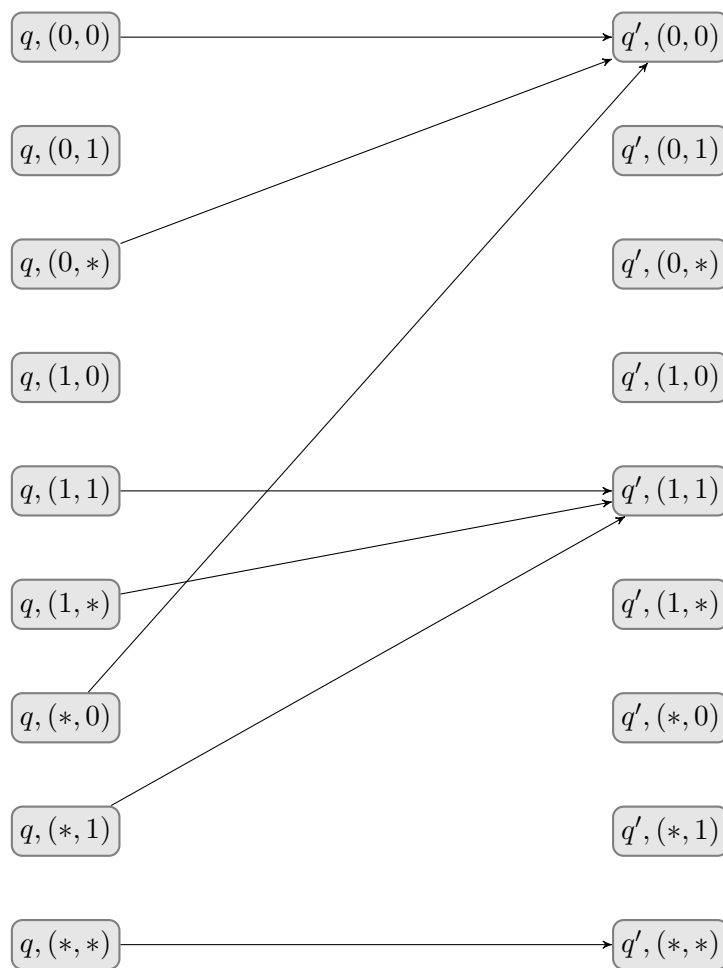
Exercice 4 Donner l'abstraction par prédicats cartésienne du programme de l'exercice 3 et pour les mêmes prédicats.

Corrigé. L'abstraction par prédicats cartésienne du programme est la structure de Kripke étiquetée $\mathcal{M}^a = \langle S^a, In^a, Bad^a, \Sigma, \rightarrow^a \rangle$ définie par :

$$\begin{aligned}S^a &= \{q, q'\} \times (\{\varphi_1, \varphi_2\} \rightarrow \{0, 1, *\}) \\ In^a &= \{(q_{in}, \lambda \varphi . *)\} \\ \Sigma &= \{\mathbf{x} = \mathbf{y}\} \\ Bad^a &= \{q_{bad}\} \times (\{\varphi_1, \varphi_2\} \rightarrow \{0, 1, *\})\end{aligned}$$

et de relation de transition étiquetée \rightarrow^a représentée graphiquement en figure 4. Sur cette figure, les étiquettes des transitions sont omises pour ne pas encombrer le dessin, et un couple (b_1, b_2) d'éléments de $\{0, 1, *\}$ représente la fonction qui à φ_i associe b_i .

Pour illustrer comment la relation \rightarrow^a est obtenue, considérons quelques exemples :

FIGURE 4 – Relation de transition abstraite \rightarrow^a de l'exercice 4

- Pour calculer l'unique successeur potentiel de l'état abstrait $(q, (1, 1))$, on détermine la validité des formules suivantes :

	valide
$(\varphi_1 \wedge \varphi_2 \wedge \mathbf{x} = \mathbf{y}) \Rightarrow (\neg\varphi_1)$	non
$(\varphi_1 \wedge \varphi_2 \wedge \mathbf{x} = \mathbf{y}) \Rightarrow \varphi_1$	oui
$(\varphi_1 \wedge \varphi_2 \wedge \mathbf{x} = \mathbf{y}) \Rightarrow (\neg\varphi_2)$	non
$(\varphi_1 \wedge \varphi_2 \wedge \mathbf{x} = \mathbf{y}) \Rightarrow \varphi_2$	oui

On en déduit que $(q', (1, 1))$ est l'unique successeur de $(q, (1, 1))$.

- Pour calculer l'unique successeur potentiel de l'état abstrait $(q, (1, *))$, on détermine la validité des formules suivantes :

	valide
$(\varphi_1 \wedge \mathbf{x} = \mathbf{y}) \Rightarrow (\neg\varphi_1)$	non
$(\varphi_1 \wedge \mathbf{x} = \mathbf{y}) \Rightarrow \varphi_1$	oui
$(\varphi_1 \wedge \mathbf{x} = \mathbf{y}) \Rightarrow (\neg\varphi_2)$	non
$(\varphi_1 \wedge \mathbf{x} = \mathbf{y}) \Rightarrow \varphi_2$	oui

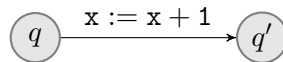
On en déduit que $(q', (1, 1))$ est l'unique successeur de $(q, (1, *))$.

- Pour calculer l'unique successeur potentiel de l'état abstrait $(q, (0, *))$, on détermine la validité des formules suivantes :

	valide
$(\neg\varphi_1 \wedge \mathbf{x} = \mathbf{y}) \Rightarrow (\neg\varphi_1)$	oui
$(\neg\varphi_1 \wedge \mathbf{x} = \mathbf{y}) \Rightarrow \varphi_1$	non
$(\neg\varphi_1 \wedge \mathbf{x} = \mathbf{y}) \Rightarrow (\neg\varphi_2)$	oui
$(\neg\varphi_1 \wedge \mathbf{x} = \mathbf{y}) \Rightarrow \varphi_2$	non

On en déduit que $(q', (0, 0))$ est l'unique successeur de $(q, (0, *))$. ■

Exercice 5 On considère le programme ci-dessous d'ensemble de variables $\mathbf{X} = \{\mathbf{x}, \mathbf{y}, \mathbf{z}\}$, de localité initiale $q_{in} = q$ et de localité d'erreur $q_{bad} = q'$.



Donner l'abstraction par prédicats booléenne du programme pour les trois prédicats :

$$\varphi_1 : \mathbf{x} = \mathbf{y} \qquad \varphi_2 : \mathbf{x} = \mathbf{z} \qquad \varphi_3 : \mathbf{y} = \mathbf{z} - 1$$

Corrigé. L'abstraction par prédicats booléenne du programme est la structure de Kripke étiquetée $\mathcal{M}^a = \langle S^a, In^a, Bad^a, \Sigma, \rightarrow^a \rangle$ définie par :

$$\begin{aligned} S^a &= \{q, q'\} \times (\{\varphi_1, \varphi_2, \varphi_3\} \rightarrow \{0, 1\}) \\ In^a &= \{q_{in}\} \times (\{\varphi_1, \varphi_2, \varphi_3\} \rightarrow \{0, 1\}) \\ \Sigma &= \{\mathbf{x} := \mathbf{x} + 1\} \\ Bad^a &= \{q_{bad}\} \times (\{\varphi_1, \varphi_2, \varphi_3\} \rightarrow \{0, 1\}) \end{aligned}$$

et de relation de transition étiquetée \rightarrow^a représentée graphiquement en figure 5. Sur cette figure, les étiquettes des transitions sont omises pour ne pas encombrer le dessin, et un triplet (b_1, b_2, b_3) de booléens représente la fonction qui à φ_i associe b_i .

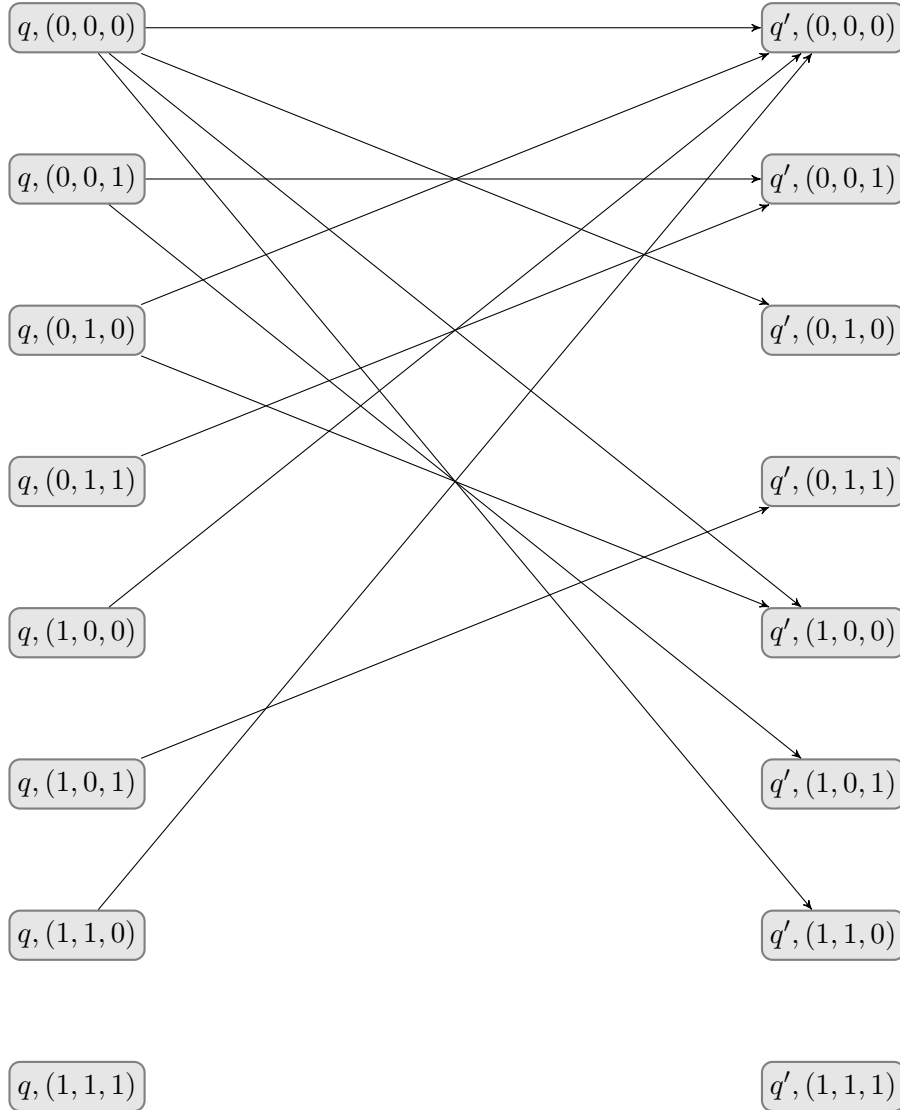


FIGURE 5 – Relation de transition abstraite \rightarrow^a de l'exercice 5

Pour illustrer comment la relation \rightarrow^a est obtenue, considérons quelques exemples :

- le triplet $((q, (1, 1, 0)), \mathbf{x} := \mathbf{x} + 1, (q', (0, 0, 0)))$ est dans \rightarrow^a si et seulement si la formule ψ ci-dessous est satisfaisable :

$$\begin{aligned} \psi &= (\varphi_1 \wedge \varphi_2 \wedge \neg\varphi_3) \bigwedge ((\neg\varphi_1 \wedge \neg\varphi_2 \wedge \neg\varphi_3)[(\mathbf{x} + 1)/\mathbf{x}]) \\ &= (\mathbf{x} = \mathbf{y} \wedge \mathbf{x} = \mathbf{z} \wedge \neg(\mathbf{y} = \mathbf{z} - 1)) \bigwedge (\neg(\mathbf{x} + 1 = \mathbf{y}) \wedge \neg(\mathbf{x} + 1 = \mathbf{z}) \wedge \neg(\mathbf{y} = \mathbf{z} - 1)) \end{aligned}$$

Or cette formule est clairement satisfaisable (prendre $\mathbf{x} = 0$, $\mathbf{y} = 0$ et $\mathbf{z} = 0$).

- le triplet $((q, (1, 1, 0)), \mathbf{x} := \mathbf{x} + 1, (q', (1, 1, 0)))$ est dans \rightarrow^a si et seulement si la formule ψ ci-dessous est satisfaisable :

$$\begin{aligned} \psi &= (\varphi_1 \wedge \varphi_2 \wedge \neg\varphi_3) \bigwedge ((\varphi_1 \wedge \varphi_2 \wedge \neg\varphi_3)[(\mathbf{x} + 1)/\mathbf{x}]) \\ &= (\mathbf{x} = \mathbf{y} \wedge \mathbf{x} = \mathbf{z} \wedge \neg(\mathbf{y} = \mathbf{z} - 1)) \bigwedge (\mathbf{x} + 1 = \mathbf{y} \wedge \mathbf{x} + 1 = \mathbf{z} \wedge \neg(\mathbf{y} = \mathbf{z} - 1)) \end{aligned}$$

Or cette formule est clairement insatisfaisable.

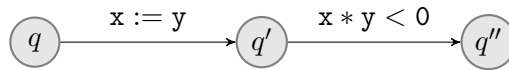
- En étendant (légèrement) l'optimisation vue en cours pour le calcul de \rightarrow^a (dans le cas des abstractions par prédicat booléennes), on peut réduire le nombre de triplets à explorer en remarquant par exemple que la formule $\mathbf{x} = \mathbf{y} \bigwedge (\mathbf{x} = \mathbf{y})[(\mathbf{x} + 1)/\mathbf{x}]$ s'écrit $\mathbf{x} = \mathbf{y} \wedge \mathbf{x} + 1 = \mathbf{y}$ et n'est donc pas satisfaisable. Par conséquent il ne peut y avoir dans \rightarrow^a de triplets de la forme $((q, (1, b_2, b_3)), \mathbf{x} := \mathbf{x} + 1, (q', (1, b_2, b_3)))$.
- le triplet $((q, (1, 0, 0)), \mathbf{x} := \mathbf{x} + 1, (q', (0, 1, 0)))$ est dans \rightarrow^a si et seulement si la formule ψ ci-dessous est satisfaisable :

$$\begin{aligned} \psi &= (\varphi_1 \wedge \neg\varphi_2 \wedge \neg\varphi_3) \bigwedge ((\neg\varphi_1 \wedge \varphi_2 \wedge \neg\varphi_3)[(\mathbf{x} + 1)/\mathbf{x}]) \\ &= (\mathbf{x} = \mathbf{y} \wedge \neg(\mathbf{x} = \mathbf{z}) \wedge \neg(\mathbf{y} = \mathbf{z} - 1)) \bigwedge (\neg(\mathbf{x} + 1 = \mathbf{y}) \wedge \mathbf{x} + 1 = \mathbf{z} \wedge \neg(\mathbf{y} = \mathbf{z} - 1)) \end{aligned}$$

La formule ψ est équivalente à la formule $\mathbf{x} = \mathbf{y} \wedge \mathbf{x} + 1 = \mathbf{z} \wedge \neg(\mathbf{y} = \mathbf{z} - 1)$ qui est clairement insatisfaisable.

On observe que les états abstraits $(q, (1, 1, 1))$ et $(q', (1, 1, 1))$ sont de concrétisation "sémantique" vide puisque la concrétisation "syntaxique" de la valuation abstraite $(1, 1, 1)$ est la formule $(x = y) \wedge (x = z) \wedge (y = z - 1)$ qui n'est pas satisfaisable. Ces états abstraits ne peuvent donc pas avoir de transition entrante ou sortante. ■

Exercice 6 On considère le programme ci-dessous d'ensemble de variables $\mathbf{X} = \{x, y\}$, de localité initiale $q_{in} = q$ et de localité d'erreur $q_{bad} = q''$.



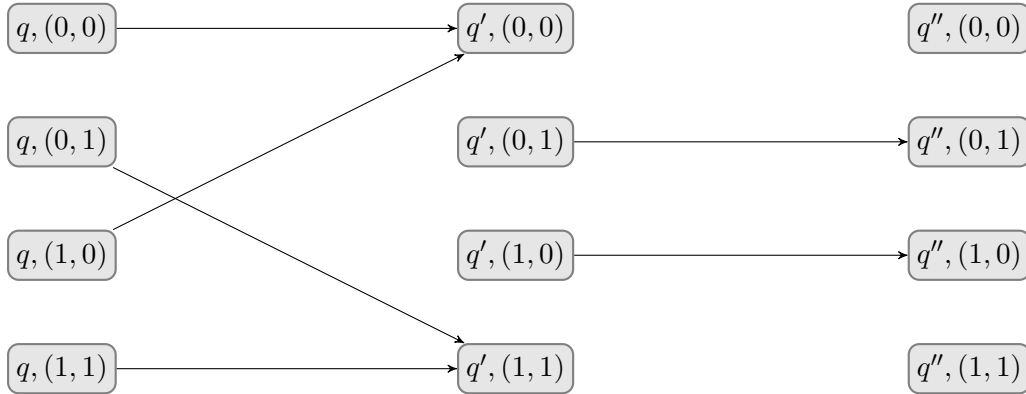
Donner l'abstraction par prédicats booléenne du programme pour les deux prédicats :

$$\varphi_1 : \mathbf{x} \geq 0 \qquad \varphi_2 : \mathbf{y} \geq 0$$

Cette abstraction est-elle sûre ?

Corrigé. L'abstraction par prédicats booléenne du programme est la structure de Kripke étiquetée $\mathcal{M}^a = \langle S^a, In^a, Bad^a, \Sigma, \rightarrow^a \rangle$ définie par :

$$\begin{aligned} S^a &= \{q, q', q''\} \times (\{\varphi_1, \varphi_2\} \rightarrow \{0, 1\}) \\ In^a &= \{q_{in}\} \times (\{\varphi_1, \varphi_2\} \rightarrow \{0, 1\}) \\ \Sigma &= \{\mathbf{x} := \mathbf{y}, \mathbf{x} * \mathbf{y} < 0\} \\ Bad^a &= \{q_{bad}\} \times (\{\varphi_1, \varphi_2\} \rightarrow \{0, 1\}) \end{aligned}$$

FIGURE 6 – Relation de transition abstraite \rightarrow^a de l'exercice 6

et de relation de transition étiquetée \rightarrow^a représentée graphiquement en figure 6. Sur cette figure, les étiquettes des transitions sont omises pour ne pas encombrer le dessin, et un couple (b_1, b_2) de booléens représente la fonction qui à φ_i associe b_i .

L'abstraction obtenue est sûre : il n'existe pas de chemin d'un état abstrait dans In^a vers un état abstrait dans Bad^a . ■

Exercice 7 Donner l'abstraction par prédicats cartésienne du programme de l'exercice 6 et pour les mêmes prédicats. Cette abstraction est-elle sûre ? Proposer le cas échéant un prédicat à ajouter de sorte que le raffinement obtenu soit sûr.

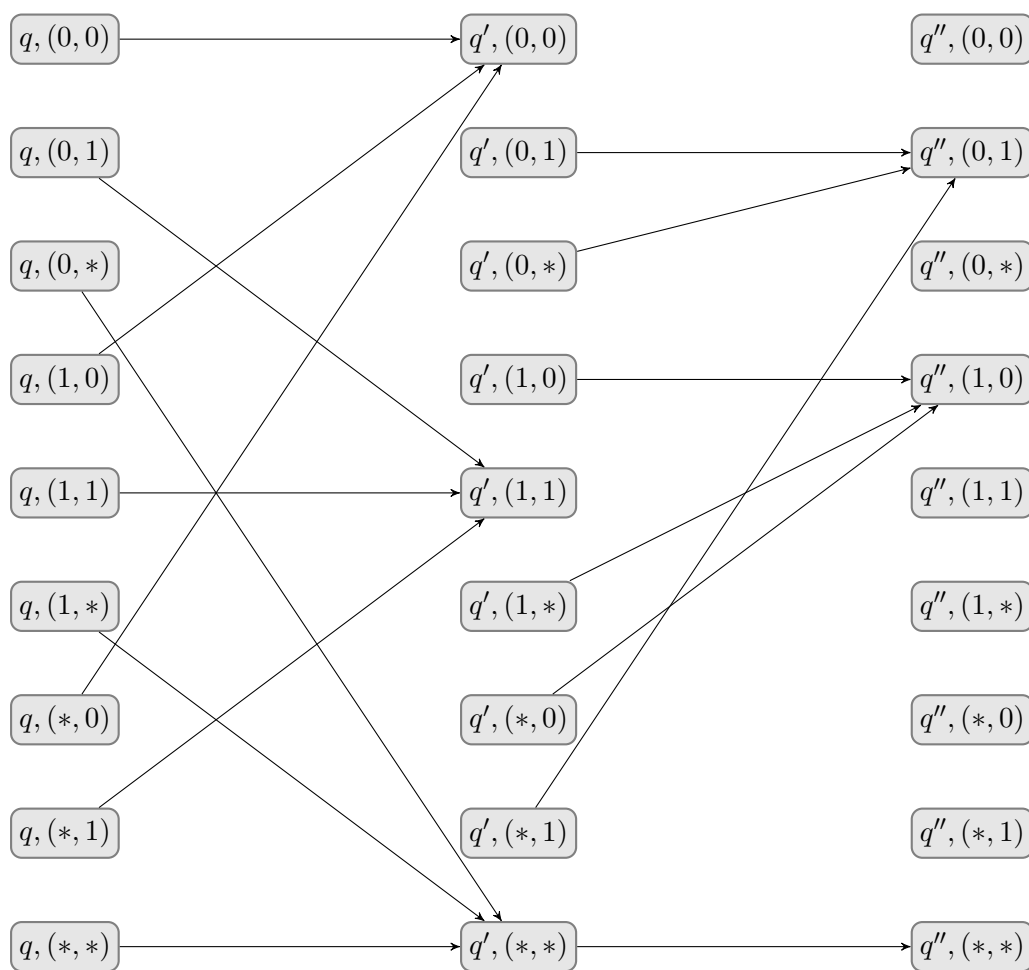
Corrigé. L'abstraction par prédicats cartésienne du programme est la structure de Kripke étiquetée $\mathcal{M}^a = \langle S^a, In^a, Bad^a, \Sigma, \rightarrow^a \rangle$ définie par :

$$\begin{aligned} S^a &= \{q, q', q''\} \times (\{\varphi_1, \varphi_2\} \rightarrow \{0, 1, *\}) \\ In^a &= \{(q_{in}, \lambda \varphi . *)\} \\ \Sigma &= \{\mathbf{x} := \mathbf{y}, \mathbf{x} * \mathbf{y} < 0\} \\ Bad^a &= \{q_{bad}\} \times (\{\varphi_1, \varphi_2\} \rightarrow \{0, 1, *\}) \end{aligned}$$

et de relation de transition étiquetée \rightarrow^a représentée graphiquement en figure 7. Sur cette figure, les étiquettes des transitions sont omises pour ne pas encombrer le dessin, et un couple (b_1, b_2) d'éléments de $\{0, 1, *\}$ représente la fonction qui à φ_i associe b_i .

L'abstraction obtenue n'est pas sûre : il existe un chemin d'un état abstrait de In^a vers un état abstrait de Bad^a .

En ajoutant le prédicat $\varphi_3 : \mathbf{x} = \mathbf{y}$, on obtient une nouvelle abstraction cartésienne qui est sûre. En effet, dans cette nouvelle abstraction, l'état abstrait initial $(q, (*, *, *))$ a un unique successeur $(q', (*, *, 1))$, et $(q', (*, *, 1))$ n'a pas de successeur. ■

FIGURE 7 – Relation de transition abstraite \rightarrow^a de l'exercice 7