Sémantique et applications à la vérification
Examen (durée : 2h) — 3 juin 2016

June, 2nd, 2017

Exercice 1 : abstraction des congruences et points fixes

Cet exercice a pour but d'étudier le domaine abstrait des congruences entières et son application à l'approximation d'images de fonctions sur les ensembles d'entiers.

On définit une valeur abstraite du domaine des congruences comme étant

- soit $\bot$, qui décrit l'ensemble vide ;
- soit une paire (n, p) telle que $0 \leq p < n$ ou $n = 0$, qui décrit tout ensemble ne contenant que des entiers qui peuvent être écrits sous la forme $kn + p$ pour un certain entier k.

Dans la suite, nous étudions la relation entre le domaine concret $(\mathcal{P}(\mathbb{Z}), \subseteq)$ et le domaine abstrait correspondant à $\mathbb{A} = \{\bot\} \uplus \{(n, p) \mid n = 0 \vee 0 \leq p < n\}$.

Question 1 —Formalisation du domaine abstrait.

1. *Définir la fonction de concrétisation qui a été décrite informellement plus haut.*
2. *Définir la relation d'ordre induite sur les éléments abstraits.*
3. *Définir l'élément $\top$ décrivant l'ensemble de tous les entiers.*
4. *Donner la meilleure abstraction d'un singleton $\{i\}$.*
5. *Montrer que l'on peut compléter cette abstraction en une correspondance de Galois, et donner la fonction d'abstraction associée.*

Corrigé 1

1. *On traduit directement en formule :*

$$\begin{array}{rccl} \gamma : & \mathbb{A} & \longrightarrow & \mathcal{P}(\mathbb{Z}) \\ & \bot & \longmapsto & \emptyset \\ & (n,p) & \longmapsto & \{nk + p \mid k \in \mathbb{Z}\} \end{array}$$

2. *On note l'ordre abstrait induit (tel que $\gamma(x) \subseteq \gamma(y)$ si et seulement si $x \sqsubseteq y$), et on trouve $\bot \sqsubseteq x$ pour tout $x \in \mathbb{A}$ et*

$$(n_0, p_0) \sqsubseteq (n_1, p_1) \iff \left\{ \begin{array}{ll} & \exists k \in \mathbb{N},\ p_0 = kn_1 + p_1 \\ \wedge & \exists k \in \mathbb{N},\ n_0 = kn_1 \end{array} \right.$$

3. $\top = (1, 0)$
4. $\{i\}$ *est abstrait exactement par* $(0, i)$

5. *On obtient une correspondance de Galois avec la fonction α qui envoie $\emptyset$ sur $\bot$ et envoie tout ensemble non vide S sur la paire (n,p) où n est le pgcd de $\{i-i' \mid i,i' \in S\}$ et p est le reste dans la division euclidienne de n'importe quel élément de S par n.*

On étudie maintenant quelques opérations, et leur abstraction.

Question 2 —Approximation d'une fonction d'additition.

On note f_{+c} la fonction définie sur $\mathcal{P}(\mathbb{Z})$ par $f_{+c}(S) = \{i+c \mid i \in S\}$. Donner une fonction $f^\sharp_{+c}$ aussi précise que possible, telle que $f_{+c} \circ \gamma \subseteq \gamma \circ f^\sharp_{+c}$

Corrigé 2

Clairement, on peut prendre $f^\sharp_{+c}(\bot) = \bot$ puisque $f_{+c}(\emptyset) = \emptyset$. Considérons donc un élément de la forme (n,p). On a donc $f_{+c} \circ \gamma((n,p)) = \{nk+p+c \mid k \in \mathbb{Z}\}$. Cet élément correspond à la concrétisation de :

$$\begin{array}{ll} (n, p +_n c) & \text{si } n \neq 0 \quad (\text{et } +_n \text{ est l'addition modulo } n) \\ (0, p+c) & \text{si } n = 0 \end{array}$$

De plus on note qu'on a $f_{+c} \circ \gamma = \gamma \circ f^\sharp_{+c}$ donc on ne peut pas faire mieux.

Question 3 —Approximation d'une fonction de filtrage.

On note $f_{\leq c}$ la fonction définie sur $\mathcal{P}(\mathbb{Z})$ par $f_{\leq c}(S) = \{i \in S \mid i \leq c\}$. Donner une fonction $f^\sharp_{\leq c}$ aussi précise que possible, telle que $f_{\leq c} \circ \gamma \subseteq \gamma \circ f^\sharp_{\leq c}$.

Corrigé 3

De même, on peut prendre $f^\sharp_{\leq c}(\bot) = \bot$. Soit $(n,p) \in \mathbb{A}$. Si $n = 0$ et $p \leq c$, on peut prendre $f^\sharp_{\leq c}(n,p) = (n,p)$. Si $n = 0$ et $p > c$, on peut prendre $f^\sharp_{\leq c}(n,p) = \bot$. Si $n > 0$, alors le plus précis que l'on puisse choisir est $f^\sharp_{\leq c}(n,p) = (n,p)$, puisque $f_{\leq c}(\gamma(n,p))$ contient un nombre infini d'éléments congrus à p modulo n. De même que plus haut, on a $f_{\leq c} \circ \gamma = \gamma \circ f^\sharp_{\leq c}$.

Noter qu'on pourrait faire de même pour d'autres tests (par exemple pour le test $> c$).

Question 4 —Approximation d'une union ensembliste.

Définir un opérateur $\sqcup$ tel que, pour tous $a, a' \in \mathbb{A}$, on ait $\gamma(a) \cup \gamma(a') \subseteq \gamma(a \sqcup a')$. On souhaite bien sûr un opérateur aussi précis que possible.

Corrigé 4

Le cas où l'un des arguments est évident (on prend $a \sqcup \bot = \bot \sqcup a = a$).
Prenons $(n,p),(n',p') \in \mathbb{A}$.
Considérons d'abord le cas où $n = n' = 0$. Si $p = p'$, on obtient $(n,p) \sqcup (n',p') = (n,p)$. Sinon, on on montre que le plus précis résultat possible est (n'',p'') où n'' est la valeur absolue de $p-p'$ et p'' est le reste dans la division euclidienne de p par n''.
Si $n' = 0$ et $n \neq 0$, on montre que le plus précis que l'on puisse prendre est (n'',p'') où n'' est le PGCD de n et $p'-p$, et p'' le reste dans la division euclidienne de p par n''.
Enfin si $n \neq 0$ et $n' \neq 0$, le raisonnement est similaire, et on obtient (n'',p'') où n'' est le PGCD de n, n' et $p-p'$, et où p'' est le reste dans la division euclidienne de n par n''.

Nous allons maintenant effectuer une analyse très simple à l'aide de ce domaine abstrait. En fait, nous allons tout simplement rechercher une approximation des points-fixes d'une fonction donnée.

Question 5 —Point(s)-fixe(s) d'une fonction.
On considère la fonction suivante sur $\mathcal{P}(\mathbb{Z})$:

$$\begin{array}{rccl} F: & \mathcal{P}(\mathbb{Z}) & \longrightarrow & \mathcal{P}(\mathbb{Z}) \\ & X & \longmapsto & \{1\} \cup \{x+6 \mid x \in X \wedge x \leq 20\} \\ & & & \quad \cup \{x-12 \mid x \in X \wedge x \leq 20\} \\ & & & \quad \cup \{x+3 \mid x \in X \wedge x > 20\} \end{array}$$

Montrer que cette fonction admet un plus petit point fixe. Le calculer. A-t'elle d'autres points fixes ? Si oui, en donner au moins un autre.

Corrigé 5
La fonction F est continue, sur $(\mathcal{P}(\mathbb{Z}), \subseteq)$ qui est un treillis complet et donc également un CPO. En fait, on peut montrer pour toute famille $\mathcal{E} \subseteq \mathcal{P}(\mathbb{Z})$ telle que $\emptyset \notin \mathcal{E}$ que :

$$F(\bigcup \mathcal{E}) = \bigcup \{F(E) \mid E \in \mathcal{E}\}$$

On peut donc lui appliquer le théorême de Kleene qui prouve qu'elle a un plus petit point fixe qui se défini par :

$$\mathbf{lfp}\, F = \bigcup_{n \in \mathbb{N}} F^n(\emptyset)$$

Or :

$$\begin{array}{rcl} F^0(\emptyset) & = & \emptyset \\ F^1(\emptyset) & = & \{1\} \\ F^2(\emptyset) & = & \{-11, 1, 7\} \\ F^3(\emptyset) & = & \{-23, -11, -5, 1, 7, 13\} \\ F^4(\emptyset) & = & \{-35, -23, -17, -11, -5, 1, 7, 13, 19\} \\ F^5(\emptyset) & = & \{-47, -35, -29, -23, -17, -11, -5, 1, 7, 13, 19, 22\} \\ F^6(\emptyset) & = & \{-59, -47, -41, -35, -29, -23, -17, -11, -5, 1, 7, 13, 19, 22, 25\} \end{array}$$

On peut montrer que cette suite converge vers :

$$\{19 - 6k \mid k \in \mathbb{N}\} \cup \{22 + 3k \mid k \in \mathbb{N}\}$$

Cette fonction admet bien d'autres points fixes, comme par exemple :

$$\mathbb{Z}$$

ou

$$\{1 + 3k \mid k \in \mathbb{N}\}$$

ou

$$\{1 + 3k \mid k \in \mathbb{N}\} \cup \{2 + 3k \mid k \in \mathbb{N}\}$$

Question 6 —Approximation de plus petit point fixe d'une fonction.

Peut on espérer calculer ce plus petit point-fixe en utilisant le domaine des congruences ? Expliquer pourquoi.

Corrigé 6

Non, car il n'est pas exprimable dans le domaine des congruences. On peut seulement espérer en calculer une approximation.

Question 7 —Construction d'une approximation de plus petit point fixe d'une fonction.

- *Construire à partir de ce qui précède une fonction* $F^\sharp : \mathbb{A} \to \mathbb{A}$ *telle que* $F \circ \gamma \subseteq \gamma \circ F^\sharp$.
- *En déduire une technique pour calcule à l'aide de* $F^\sharp$ *une approximation dans le treillis des congruences du plus petit point fixe de* F.
- *Effectuer ce calcul.*
- *Comparer le résultat à celui obtenu dans la question précédente.*

Corrigé 7

- *Il suffit tout simplement d'utiliser les opérations que nous avons définies dans les précédentes questions :*

$$F^\sharp(a) = (1,0) \sqcup f^\sharp_{+6} \circ f^\sharp_{\leq 20}(a) \sqcup f^\sharp_{+(-12)} \circ f^\sharp_{\leq 20}(a) \sqcup f^\sharp_{+6} \circ f^\sharp_{>20}(a)$$

  (on montre facilement que l'opérateur $\sqcup$ *est associatif, et on ne parenthèse donc pas cette expression)*

  Par composition, on a bien $F^\sharp : \mathbb{A} \to \mathbb{A}$ *telle que* $F \circ \gamma \subseteq \gamma \circ F^\sharp$.
- *On peut montrer par récurrence sur* n *que :*

$$\bigcup_{k=0}^{n} F^k(\emptyset) \subseteq \gamma\left((F^\sharp)^0(\bot) \sqcup \ldots \sqcup (F^\sharp)^n(\bot)\right)$$

  La suite $(X_n)_{n\in\mathbb{N}}$ *définie par* $X_n = (F^\sharp)^0(\bot) \sqcup \ldots \sqcup (F^\sharp)^n(\bot)$ *est croissante, et le treillis des congruences est de hauteur finie. Par conséquent, on peut calculer la limite de cette suite, et celle-ci définit une approximation du plus petit point fixe de* F.
- *On obtient :*

$$\begin{array}{rcl} (F^\sharp)^0(\emptyset) & = & \bot \\ (F^\sharp)^1(\emptyset) & = & (0,1) \\ (F^\sharp)^2(\emptyset) & = & (6,1) \\ (F^\sharp)^3(\emptyset) & = & (3,1) \\ (F^\sharp)^4(\emptyset) & = & (3,1) \end{array}$$

  Cela nous donne donc l'approximation définie par $(3,1)$ *qui correspond à :*

$$\{1 + 3k \mid k \in \mathbb{N}\}$$

- *L'approximation du plus petit point fixe qui a été fournie par l'analyse est strictement moins précise que le plus petit point-fixe de* F. *Cela n'est pas surprenant, puisque le plus petit point fixe de* F *ne peut être représenté exactement dans le domaine des congruences.*

Exercice 2 : sémantiques définies en arrière et vérification

Dans cet exercice, nous nous intéressons à une définition de la sémantique des programmes qui procède *en arrière*, c'est-à-dire, en partant des états finaux et en remontant les transitions précédentes. Dans la suite, on ne considère pas les traces infinies.

Dans la suite, nous considérons un système de transition $\mathcal{S}$ défini par :

- l'ensemble d'états $\mathbb{S}$;
- l'ensemble d'états *finaux* $\mathbb{S}_\mathcal{F} \subseteq \mathbb{S}$, qui décrivent les configurations où l'exécution du système est terminée ;
- la relation de transition $\rightarrow \subseteq \mathcal{P}((\mathbb{S} \setminus \mathbb{S}_\mathcal{F}) \times \mathbb{S})$.

Nous considérerons parfois, à titre d'exemple le système de transition défini comme suit :

- $\mathbb{S} = \{s_0, s_1, s_2, s_3, s_4, s_5, s_6, s_7\}$;
- $\mathbb{S}_\mathcal{F} = \{s_5, s_7\}$;
- $s_0 \rightarrow s_1, s_1 \rightarrow s_2, s_2 \rightarrow s_3, s_3 \rightarrow s_1, s_2 \rightarrow s_5, s_6 \rightarrow s_7$.

On appelle *sémantique arrière des traces* (ou pour plus simplement *sémantique arrière*) l'ensemble de toutes les traces d'exécution dont le dernier état est un état final.

Question 8 —Définition extensive.

Donner la définition extensive de la sémantique arrière (c'est-à-dire sous la forme $\{\sigma \in X \mid P(\sigma)\}$ où l'ensemble X et la propriété P sont à définir).
La décrire dans le cas de l'exemple.

Corrigé 8

Comme dans le cours, on note $\mathbb{S}^*$ l'ensemble des traces finies définies par l'ensemble d'états $\mathbb{S}$. La sémantique arrière $[\![\mathcal{S}]\!]_\mathbf{b}$ est définie par :

$$[\![\mathcal{S}]\!]_\mathbf{b} = \{\langle s_0, \ldots, s_n\rangle \in \mathbb{S}^* \mid \forall i,\ s_i \rightarrow s_{i+1} \wedge s_n \in \mathbb{S}_\mathcal{F}\}$$

Dans le cas de l'exemple, nous avons :

$$\begin{aligned}[\![\mathcal{S}]\!]_\mathbf{b} \quad = \quad \{ \quad & \langle s_5\rangle, \langle s_7\rangle, \langle s_2, s_5\rangle, \langle s_6, s_7\rangle \\ & \langle s_1, s_2, s_5\rangle, \langle s_3, s_1, s_2, s_5\rangle, \langle s_2, s_3, s_1, s_2, s_5\rangle, \\ & \langle s_1, s_2, s_3, s_1, s_2, s_5\rangle, \langle s_3, s_1, s_2, s_3, s_1, s_2, s_5\rangle, \langle s_2, s_3, s_1, s_2, s_3, s_1, s_2, s_5\rangle, \\ & \ldots \\ & \langle s_0, s_1, \ldots, s_1, s_2, s_3, s_1, s_2, s_5\rangle \quad \}\end{aligned}$$

Nous avons vu dans le cadre du cours comment définir une sémantique sous forme constructive, si nécessaire à l'aide d'un point fixe.

Question 9 —Définition sous la forme d'un point fixe.

Faire de même pour la sémantique arrière. On attend une justification de l'existence de tout point fixe utilisé, ainsi que la preuve que cette nouvelle expression décrit bien la sémantique arrière définie plus haut.
Montrer cette construction dans le cas du système de transition donné plus haut en exemple.

Corrigé 9

On considère la function F_b définie comme suit :

$$\begin{array}{rccl} F_b: & \mathcal{P}(\mathbb{S}^*) & \longrightarrow & \mathcal{P}(\mathbb{S}^*) \\ & X & \longmapsto & \{\langle s\rangle \mid s \in \mathbb{S}_{\mathcal{F}}\} \cup \{\langle s_0, s_1, \ldots, s_n\rangle \mid s_0 \to s_1 \wedge \langle s_1, \ldots, s_n\rangle \in X\} \end{array}$$

Cette fonction est continue, et définie sur un CPO, donc elle admet un plus petit point fixe et :

$$\operatorname*{\mathbf{lfp}}_{\emptyset} F_b = \bigcup_{n\in\mathbb{N}} F_b^n(\emptyset)$$

On peut montrer par récurrence sur n la propriété suivante :

$$\begin{array}{c} \forall \sigma \in \mathbb{S}^*, \quad \textit{de longeur } n, \\ \sigma \in [\![\mathcal{S}]\!]_{\mathbf{b}} \iff \sigma \in F_b^n(\emptyset) \end{array}$$

En effet, il n'existe pas de telle trace au rang 0 ; au rang 1, on ne considère que les traces réduites à un état final, et pour tout rang supérieure, la preuve se fait comme en cours.
On en déduit :

$$[\![\mathcal{S}]\!]_{\mathbf{b}} = \operatorname*{\mathbf{lfp}}_{\emptyset} F_b = \bigcup_{n\in\mathbb{N}} F_b^n(\emptyset)$$

On observe cette construction en déroulant le calcul pour le système que nous avons donné comme exemple :

$$\begin{array}{rcl} F_b^0(\emptyset) & = & \emptyset \\ F_b^1(\emptyset) & = & \{\langle s_5\rangle, \langle s_7\rangle\} \\ F_b^2(\emptyset) & = & \{\langle s_5\rangle, \langle s_7\rangle, \langle s_2, s_5\rangle, \langle s_6, s_7\rangle\} \\ F_b^3(\emptyset) & = & \{\langle s_5\rangle, \langle s_7\rangle, \langle s_2, s_5\rangle, \langle s_1, s_2, s_5\rangle\} \\ & \vdots & \end{array}$$

Question 10 —Sémantique des traces maximales.

Supposons que l'on considère en plus pour cette question un ensemble d'états initiaux $\mathbb{S}_{\mathcal{I}} \subseteq \mathbb{S}$. Déduire de la question précédente une définition constructives des traces maximales (i.e., sous la forme de l'intersection de deux sémantiques sous forme de points fixes).
Construire cette sémantique dans le cas de l'exemple énoncé plus haut, en prenant $\mathbb{S}_{\mathcal{I}} = \{s_0\}$.

Corrigé 10

On peut définir directement la sémantique des traces maximales comme suit :

$$[\![\mathcal{S}]\!]_{\mathbf{m}} = \{\langle s_0, \ldots, s_n\rangle \mid s_0 \in \mathbb{S}_{\mathcal{I}} \wedge s_n \in \mathbb{S}_{\mathcal{F}} \wedge \forall i,\ s_i \to s_{i+1}\}$$

On peut aussi la voir comme l'intersection de la sémantique en arrière et de la sémantique en avant (que nous avons vue en cours) :

$$[\![\mathcal{S}]\!]_{\mathbf{m}} = [\![\mathcal{S}]\!]_{\mathbf{f}} \cap [\![\mathcal{S}]\!]_{\mathbf{b}}$$

où la sémantique en avant est définie par $[\![\mathcal{S}]\!]_{\mathbf{f}} = \mathbf{lfp}_{\emptyset} F_f = \bigcup_{n\in\mathbb{N}} F_f^n(\emptyset)$, avec

$$\begin{array}{rccl} F_f: & \mathcal{P}(\mathbb{S}^*) & \longrightarrow & \mathcal{P}(\mathbb{S}^*) \\ & X & \longmapsto & \{\langle s\rangle \mid s \in \mathbb{S}_{\mathcal{I}}\} \cup \{\langle s_0, s_1, \ldots, s_n, s_{n+1}\rangle \mid s_n \to s_{n+1} \wedge \langle s_0, \ldots, s_n\rangle \in X\} \end{array}$$

Donc :

$$[\![\mathcal{S}]\!]_{\mathbf{m}} = \left(\bigcup_{n\in\mathbb{N}} F_b^n(\emptyset)\right) \bigcap \left(\bigcup_{n\in\mathbb{N}} F_f^n(\emptyset)\right)$$

De manière similaire, nous pouvons définir une sémantique analogue à la sémantique dénotationnelle, et qui progresse en arrière. La sémantique d'un programme (décrit par un système de transitions) est alors une fonction qui prend un ensemble d'états X et renvoie tous les états à partir desquels on peut atteindre en zéro, une ou plusieurs étapes de calcul un état dans X.

Question 11 —Sémantique arrière à base de fonctions.

Définir cette sémantique, sous la forme d'une fonction des ensembles d'états vers les ensembles d'états. On donnera non seulement une définition extensive (sous le même format qu'à la question 8), mais aussi une définition constructive (sous le même format qu'à la question 9).
Montrer que cette fonction commute avec l'union.
En déduire une définition compacte de cette fonction dans le cadre du système utilisé comme exemple.

Corrigé 11

On note $[\![\mathcal{S}]\!]_{\mathbf{p}}$ cette nouvelle sémantique :

$$\begin{array}{rccl} [\![\mathcal{S}]\!]_{\mathbf{p}} : & \mathcal{P}(\mathbb{S}) & \longrightarrow & \mathcal{P}(\mathbb{S}) \\ & X & \longmapsto & \{s \in \mathbb{S} \mid \exists s' \in X,\ s \to^* s'\} \end{array}$$

De plus, on peut montrer que, pour tout $X \subseteq \mathbb{S}$,

$$[\![\mathcal{S}]\!]_{\mathbf{p}}(X) = \operatorname*{\mathbf{lfp}}_{\emptyset} F \qquad \textit{où} \qquad \left\{ \begin{array}{rccl} F : & \mathcal{P}(\mathbb{S}) & \longrightarrow & \mathcal{P}(\mathbb{S}) \\ & Y & \longmapsto & X \cup \{s \in \mathbb{S} \mid \exists s' \in Y,\ s \to^* s'\} \end{array} \right.$$

(les étapes de la preuve sont classiques : preuve de continuité, application du théorême de Kleene, et preuve par récurrence de l'égalité entre les deux définitions de la sémantique)
La commutation avec l'union se montre trivialement à l'aide de la première forme :

$$\begin{array}{rcl} [\![\mathcal{S}]\!]_{\mathbf{p}}(\cup\mathcal{X}) & = & \{s \in \mathbb{S} \mid \exists s' \in \cup\mathcal{X},\ s \to^* s'\} \\ & = & \{s \in \mathbb{S} \mid \exists X \in \mathcal{X},\ \exists s' \in X,\ s \to^* s'\} \\ & = & \bigcup_{X\in\mathcal{X}} \{s \in \mathbb{S} \mid \exists s' \in X,\ s \to^* s'\} \\ & = & \bigcup_{X\in\mathcal{X}} [\![\mathcal{S}]\!]_{\mathbf{p}}(X) \end{array}$$

Il suffit donc de définir $[\![\mathcal{S}]\!]_{\mathbf{p}}$ pour les singletons, donc dans le cas de notre exemple :

$$\begin{array}{rcl} [\![\mathcal{S}]\!]_{\mathbf{p}}(\{s_0\}) & = & \{s_0\} \\ [\![\mathcal{S}]\!]_{\mathbf{p}}(\{s_1\}) & = & \{s_0, s_1, s_2, s_3\} \\ [\![\mathcal{S}]\!]_{\mathbf{p}}(\{s_2\}) & = & \{s_0, s_1, s_2, s_3\} \\ [\![\mathcal{S}]\!]_{\mathbf{p}}(\{s_3\}) & = & \{s_0, s_1, s_2, s_3\} \\ [\![\mathcal{S}]\!]_{\mathbf{p}}(\{s_4\}) & = & \{s_4\} \\ [\![\mathcal{S}]\!]_{\mathbf{p}}(\{s_5\}) & = & \{s_0, s_1, s_2, s_3, s_5\} \\ [\![\mathcal{S}]\!]_{\mathbf{p}}(\{s_6\}) & = & \{s_6\} \\ [\![\mathcal{S}]\!]_{\mathbf{p}}(\{s_7\}) & = & \{s_6, s_7\} \end{array}$$

On souhaite maintenant s'intéresser à la preuve d'une propriété de sûreté. À titre d'exemple, on suppose donné un état $\delta \in \mathbb{S}$, et on souhaite construire une technique de vérification fondée sur la sémantique en arrière, et qui permet de s'assurer que δ n'est atteint par aucune exécution d'un programme partant d'un état initia (le programme pourra être formalisé à l'aide d'un système de transition défini par un ensemble d'états, un ensemble d'états initiaux, et une relation de transition).

Question 12 —Sémantique arrière et application à la vérification d'une propriété.

1. *Montrer comment on peut exprimer la propriété ci-dessus en utilisant une sémantique définie en arrière. On pourra s'intéresser à l'ensemble d'exécutions qui terminent en δ.*
2. *Que se passe-t'il dans le cas du système donné comme exemple, et si on prend $\delta = s_7$? Si on prend $\delta = s_7$? (les états et la relation de transition sont donnés au début de l'exercice, et on rappelle que le seul état initial est s_0).*
3. *Déduire de ce qui précède une méthode d'analyse fondée sur une interprétation abstraite et qui procède en arrière.*

Corrigé 12

On représente le programme à l'aide d'un système de transition $\mathcal{S} = (\mathbb{S}, \rightarrow, \mathbb{S}_\mathcal{I})$, où $\mathbb{S}$ est l'ensemble des états, $\rightarrow$ la relation de transition et $\mathbb{S}_\mathcal{I}$ l'ensemble des états initiaux.

1. *Pour montrer que δ n'est pas atteignable, il suffit de montrer que les états initiaux ne sont pas ancêtres de $\{\delta\}$ et donc de montrer que :*

$$[\![\mathcal{S}]\!]_\mathbf{p}(\{\delta\}) \cap \mathbb{S}_\mathcal{I} = \emptyset$$

2. *Supposons $\delta = s_5$. Alors :*

$$[\![\mathcal{S}]\!]_\mathbf{p}(\{\delta\}) \cap \mathbb{S}_\mathcal{I} = \{s_0, s_1, s_2, s_3, s_5\} \cap \{s_0\} = \{s_0\}$$

Donc δ_5 est atteignable depuis un état initial.
Supposons $\delta = s_7$. Alors :

$$[\![\mathcal{S}]\!]_\mathbf{p}(\{\delta\}) \cap \mathbb{S}_\mathcal{I} = \{s_6, s_7\} \cap \{s_0\} = \emptyset$$

Donc δ_7 n'est pas atteignable depuis un état initial.

3. *L'analyse vue en cours progresse en avant et calcule à partir des états initiaux une sur-approximation des états atteignables. De manière similaire, une analyse en arrière part d'une sur-approximation de $\{\delta\}$ et calcule pas à pas une sur-approximation de tous les états qui sont la source d'une trace atteignant finalement $\{\delta\}$ (autrement dit, on sur-approxime $[\![\mathcal{S}]\!]_\mathbf{p}(\{\delta\})$.*