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.*

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 $f_{+c} \circ \gamma \subseteq \gamma \circ f^\sharp_{+c}$

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 $f_{\leq c} \circ \gamma \subseteq \gamma \circ f^\sharp_{\leq c}$.

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.

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.

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.

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.*

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 $\to \subseteq \mathcal{P}((\mathbb{S} \setminus \mathbb{S}_\mathcal{F}) \times \mathbb{S})$.

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

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

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.

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.

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 $\mathbb{S}_{\mathcal{I}} = \{s_0\}$.

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.

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.*