Programmation 1

TD n°9

Aliaume Lopez

2 décembre 2019

♻ : reprise d'un exercice ❗ : exercice de compréhension
👍 : exercice fondamental de cours 🏆 : une solution complète par mail = un gâteau

Exercise 1 : Quelques aides

1. Sortir une feuille pour noter la correction.
2. Ne pas attendre la correction pour réfléchir sur une feuille.
3. Ne pas hésiter à demander à son voisin, ou mieux, au chargé de TD.
4. Rédiger et ne pas se contenter d'avoir une idée.

1 Retour vers le futur

♻ **Exercise 2 : Un petit langage**

On considère le langage $\{\star, \bullet\}$ équipé de la sémantique à petits pas suivante :

$$\begin{aligned} X \star \bullet Y &\to XY && \text{si } \exists n \geq 0, X = \star^n \\ X \bullet \star Y &\to XY && \text{si } \exists n \geq 0, X = \bullet^n \end{aligned}$$

1. Énoncer puis prouver un théorème de déterminisme.
2. On considère le DCPO $\{0, 1\}$ équipé de l'ordre plat et la sémantique suivante

$$\begin{aligned} [\![\varepsilon]\!]_2 &= 0 \\ [\![aX]\!]_2 &= 1 - [\![X]\!]_2 && \text{si } a \in \{\star, \bullet\} \end{aligned}$$

   Montrer que cette sémantique est correcte par rapport à la sémantique à petits pas.
3. Même question pour le DCPO des entiers relatifs équipé de l'ordre plat et la sémantique suivante

$$\begin{aligned} [\![\varepsilon]\!]_{\mathbb{Z}} &= 0 \\ [\![\star X]\!]_{\mathbb{Z}} &= 1 + [\![X]\!]_{\mathbb{Z}} \\ [\![\bullet X]\!]_{\mathbb{Z}} &= -1 \ + [\![X]\!]_{\mathbb{Z}} \end{aligned}$$

4. On se donne la notion d'équivalence observationnelle suivante :

$$A \equiv B \triangleq \forall C[\cdot], C[A] \to^* \varepsilon \iff C[B] \to^* \varepsilon$$

   (a) Montrer que c'est une relation d'équivalence
   (b) Les sémantiques dénotationnelles sont-elles complètement abstraites ?

! Exercise 3 : Back to Luc's answer

Posons $J \triangleq \{[a,b] \mid 0 \leq a \leq b \leq 1\}$ où a et b sont des nombres réels. Rappelons que $(J, \supseteq)$ est un DCPO et que cela donne lieu à une topologie τ sur J, la topologie de Scott.

1. Considérons M l'ensemble des éléments maximaux de J. Déterminer la topologie induite par τ sur M.
2. Montrer que toute propriété P continue sur M est constante.

2 Sémantique et vérification

Imp

On donne une version de Imp possédant non seulement des expressions arithmétiques, mais aussi des expressions booléennes.

$$e := x \mid 0 \mid 1 \mid e + e \mid -e \mid e \times e$$
$$b := (e \sim e) \mid e \leq e \mid \neg b \mid b \wedge b$$
$$c := \textbf{skip} \mid \textbf{while } b \textbf{ do } c \mid x := e \mid \textbf{if } b \textbf{ then } c \textbf{ else } c$$

Formules arithmétiques au premier ordre

Voici la construction des formules au premier ordre que nous autoriserons, leur ensemble est noté $\mathsf{FO}[0, 1, +, \times, \leq]$. Dans la suite i est une variable logique à valeur entière.

$$t := x \mid 0 \mid 1 \mid t + t \mid -t \mid t \times t \mid i$$
$$\phi := (t \sim t) \mid t \leq t \mid \neg\phi \mid \phi \wedge \phi \mid \exists i.\phi$$

Exercise 4 : Warmup

1. Donner une sémantique dénotationnelle aux expressions booléeenes.
2. Donner une sémantique aux formules logiques. On écrira $\rho \models^I \phi$ quand la formule ϕ est validée dans l'environnement ρ pour les variables de programme et I pour les variables logiques.
3. En remarquant que la syntaxe des expressions booléennes de Imp est un sous ensemble de la syntaxe des formules, on peut se demander si les deux sémantiques coïncident. Démontrer que pour tout I, $\rho \models^I b \iff [\![b]\!]_\rho \neq 0$.
4. Montrer que l'on peut supposer que $x < y$ est une expression booléeenne valide.
5. Pourquoi introduire des variables logiques ?

Triplets de Hoare

On appelle triplet de Hoare $\{\phi\}\ c\ \{\psi\}$. On dit que ce triplet est *valide* sous I, ce qui est noté $\models^I \{\phi\}\ c\ \{\psi\}$ quand

$$\forall \rho, \rho \models^I \phi \wedge [\![c]\!]_\rho \neq \bot \implies [\![c]\!]_\rho \models^I \psi$$

Une autre manière de présenter cela est d'étendre la sémantique des formules en posant $\bot \models^I \phi$ quelque soit la formule ϕ et l'environnement σ.
On notera $\models \{\phi\}\ c\ \{\psi\}$ quand pour tout I on a $\models^I \{\phi\}\ c\ \{\psi\}$.

Axiomatique de Hoare

On donne des règles de Hoare pour toutes les constructions excepté le while.

$$\frac{}{\{\phi\}\ \textbf{skip}\ \{\phi\}} \qquad \frac{\{\phi \wedge b\}\ c_1\ \{\psi\} \qquad \{\phi \wedge \neg b\}\ c_2\ \{\psi\}}{\{\phi\}\ \textbf{if}\ b\ \textbf{then}\ c_1\ \textbf{else}\ c_2\ \{\psi\}}$$

$$\frac{}{\{\phi[x := e]\}\ x := e\ \{\phi\}} \qquad \frac{\phi \implies \phi' \qquad \{\phi'\}\ c\ \{\psi'\} \qquad \psi' \implies \psi}{\{\phi\}\ c\ \{\psi\}}$$

Exercise 5 : Hoare sur un langage jouet

1. Montrer que pour tout ρ, I, pour tout u, v termes et x variable
$$\rho \models^I \phi[x \mapsto u] \iff \rho[x \mapsto [\![u]\!]_\rho] \models^I \phi$$
2. Montrer que tout triplet de Hoare est valide. C'est-à-dire que le système est correct.
3. Proposer une règle pour le while. Montrer que celle-ci est correcte.
4. À l'aide de ce système axiomatique, prouver le triplet suivant
$$\{x \sim 0 \wedge y \sim 0 \wedge z \sim 0 \wedge n \geq 0\}\ c\ \{x \sim n^3\} \tag{1}$$
Où
$$c \triangleq \textbf{while}\ z < 3n\ \textbf{do}\ z := z + 3; y := y + 2z - 3; x := x + y - z + 1$$

Plus faible précondition libérale

On note $\mathsf{wlp}^I\,(c, \phi) \triangleq \{\rho \mid [\![c]\!]_\rho \models^I \phi\}$.

Exercise 6 : Plus faible précondition libérale

1. Soit I une interprétation des variables logiques. Pour tout programme c sans boucle while et formule ψ, construire une formule $\phi_{c,\psi}$ telle que $\rho \models^I \phi_{c,\psi}$ si et seulement si $\rho \in \mathsf{wlp}^I\,(c, \psi)$.
2. Soit ϕ une formule définissant $\mathsf{wlp}^I\,(\textbf{while}\ b\ \textbf{do}\ c, \psi)$. Donnez une équation $\models^I \phi \iff \phi'$ où ϕ' est une formule faisant intervenir ϕ.
3. À l'aide de disjonctions et conjonctions infinies, écrire deux solutions à cette équation.
4. Laquelle correspond à ϕ ?

Exercise 7 : Complétude

On admet qu'il existe une formule exprimant la plus faible précondition libérale pour la boucle while.

1. Montrer que l'axiomatique définie est complète. C'est-à-dire, prouver que pour tout triplet valide $\models \{\phi\}\ c\ \{\psi\}$ il existe une dérivation de $\{\phi\}\ c\ \{\psi\}$. *Indication : On pourra commencer par le démontrer pour les plus faibles préconditions libérales.*
2. Que dire d'un système S de preuve sur les triplets de Hoare qui est correct et vérifiable ?
3. Pourquoi la logique de Hoare est-elle malgré tout complète ?
4. On admet que les plus faibles préconditions libérales sont calculables. En déduire que le problème suivant n'est pas récursivement énnumérable.
   Entrée Une formule close $\phi \in \mathsf{FO}[0, 1, +, \times, \leq]$
   Sortie Est-ce que ϕ est valide ?