TD 9

Exercice 1. On considère le langage $\{*, \bullet\}^*$ équipé de la sémantique à petits pas suivante:

$$\begin{array}{ll} X * \bullet Y \to XY & \text{si } X = *^n \\ X \bullet * Y \to XY & \text{si } X = \bullet^n \end{array}$$

1. Montrez que cette sémantique est déterministe, *i.e.* si $A \to B$ et $A \to B'$ alors $B = B'$.
2. On considère le DCPO (non pointé) $\{0, 1\}$ équipé de l'ordre discret ("plat"), et on se donne la sémantique définie par:

$$\begin{array}{c} [\![\varepsilon]\!] = 0; \\ [\![aX]\!] = 1 - [\![X]\!] \quad a \in \{*, \bullet\} \end{array}$$

   Montrez que cette sémantique est correcte par rapport à la sémantique à petits pas.
3. Même question pour le DCPO (non pointé) des entiers relatifs équipés de l'ordre plat et la sémantique suivante:

$$\begin{array}{c} [\![\varepsilon]\!] = 0 \\ [\![*X]\!] = 1 + [\![X]\!] \\ [\![\bullet X]\!] = -1 + [\![X]\!] \end{array}$$

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

   $A \simeq B$ lorsque pour tout contexte $C[.]$, $C[A] \to^* \epsilon$ ssi $C[B] \to^* \epsilon$.

   Montrez qu'il s'agit d'une relation d'équivalence. Les deux sémantiques dénotationnelles ci-dessus sont-elles complètement abstraites pour cette équivalence observationnelle ?

Exercice 2. On considère le langage Imp et la logique $FO[0, 1, +, \times]$

$$\begin{array}{lcl} e & ::= & x \mid 0 \mid 1 \mid e + e \mid -e \mid e \times e \\ e' & ::= & e \mid i \\ b & ::= & e = e \mid \neg b \mid b \wedge b \\ c & ::= & \textbf{skip} \mid x := e \mid c; c \mid \textbf{if } b \textbf{ then } c \textbf{ else } c \textbf{ fi} \mid \textbf{while } b \textbf{ do } c \\ \varphi & ::= & e' = e' \mid \neg\varphi \mid \varphi \wedge \varphi \mid \exists i.\varphi \end{array}$$

où x est une variable de programme, et i est une variable à valeur entière.

On reprend la sémantique dénotationelle de Imp $[\![c]\!] : \mathbb{Z}^{\mathsf{Var}} \to \mathbb{Z}_\perp^{\mathsf{Var}}$ vue en en cours, et on définit pour une interprétation $\rho \in \mathbb{Z}^{\mathsf{Var}}$ la relation de satisfaction $\rho \models \varphi$ comme attendue:

$$\begin{array}{rl} \rho \models e_1 = e_2 & \text{iff } [\![e_1]\!]\rho = [\![e_2]\!]\rho \\ \rho \models \neg\varphi & \text{iff } \rho \not\models \varphi \\ \rho \models \phi \wedge \psi & \text{iff } \rho \models \varphi \text{ and } \rho \models \psi \\ \rho \models \exists i.\varphi & \text{iff } \rho \models \varphi[i \leftarrow n] \text{ for some } n \end{array}$$

On appelle triplet de Hoare un triplet $\{\varphi\}\ c\ \{\psi\}$. On dit qu'un triplet de Hoare $\{\varphi\}\ c\ \{\psi\}$ est valide, noté $\models \{\varphi\}\ p\ \{\psi\}$ ssi pour tout ρ,

$$(\rho \models \varphi \wedge [\![c]\!](\rho) \neq \perp) \Rightarrow [\![c]\!]\rho \models \psi$$

1. On introduit les règles de déduction suivantes:

$$\frac{}{\{\varphi\}\ \mathbf{skip}\ \{\varphi\}} \qquad \frac{}{\{\varphi[x := e]\}\ x := e\ \{\varphi\}} \qquad \frac{\{\varphi \wedge b\}\ c_1\ \{\psi\} \qquad \{\varphi \wedge \neg b\}\ c_2\ \{\psi\}}{\{\varphi\}\ \mathbf{if}\ b\ \mathbf{then}\ c_1\ \mathbf{else}\ c_2\ \mathbf{fi}\ \{\psi\}}$$

$$\frac{\models \varphi \Rightarrow \varphi' \qquad \{\varphi'\}\ c\ \{\psi'\} \qquad \models \psi' \Rightarrow \psi}{\{\varphi\}\ c\ \{\psi\}}$$

   Montrez que tout triplet de Hoare prouvable est valide.

2. Proposez une règle pour le while et la composition séquentielle, et étendez le résultat de la question précédente au nouveau système.

3. A l'aide de ce système de preuve, donnez une preuve du triplet de Hoare

$$\{x = 0 \wedge y = 0 \wedge z = 0 \wedge n \geq 0\}\ c\ \{x = n^3\}$$

   où c est le programme $\mathbf{while}\ z < 3n\ \mathbf{do}\ z := z + 3\ ;\ y := y + 2z - 3\ ;\ x := x + y - z + 1$.

4. Prouvez la correction de l'exponentiation rapide.

5. On appelle plus faible précondition libérale l'ensemble

$$\mathsf{wlp}(c, \varphi) := \{\rho \in \mathbb{Z}^{\mathsf{Var}} \mid [\![c]\!](\rho) = \bot \text{ ou } [\![c]\!](\rho) \models \varphi\}$$

   Montrez que pour tout programme c sans boucle while et toute formule φ, il existe une formule $\mathsf{WLP}(c, \varphi)$ qui caractérise $\mathsf{wlp}(c, \varphi)$, c'est à dire que pour tout ρ, $\rho \models \mathsf{WLP}(c, \varphi)$ ssi $\rho \in \mathsf{wlp}(c, \varphi)$.

6. On admet que l'on peut définir une formule $\mathsf{WLP}(c, \varphi)$ pour tout programme c. En déduire que la logique de Hoare est complète : si le triplet $\{\varphi\}\ c\ \{\psi\}$ est valide, alors il est prouvable.

   Indication: on pourra commencer par montrer que le triplet $\{\mathsf{WLP}(c, \varphi)\}\ c\ \{\varphi\}$ est prouvable.

7. On suppose fixé un système de preuve $\mathcal{S}$ de triplets de Hoare tel que

   - $\mathcal{S}$ est correct : tous les triplets de Hoare prouvables sont valides.
   - $\mathcal{S}$ est vérifiable : on peut décider, étant donné un arbre de preuve, si cet arbre de preuve est une preuve dans $\mathcal{S}$.

   Montrez que $\mathcal{S}$ est incomplet.

8. Pourquoi la logique de Hoare est-elle malgré tout complète?

9. On admet que la formule dont l'existence est admise en question 6 est de plus calculable. En déduire que le problème:

   - Entrée: une formule A
   - Question: est-ce que A est valide ?

   n'est pas récursivement énumérable.

Exercice 3. On étend le langage Imp avec deux nouvelles commandes **break** et **continue**. Un programme est dit bien formé si toute occurence de **break** et **continue** est à l'intérieur d'un while; dans la suite, on suppose toujours les programmes bien formés.

On généralise la notion de triplet de Hoare à des triplets de la forme $\Pi \vdash \{\varphi\}\ c\ \{\psi\}$ où Π est une pile de paires (φ, ψ), et on remplace la règle du while par la règle suivante.

$$\frac{(\varphi,\psi).\Pi \vdash \{\varphi \wedge b\}\ c; \textbf{continue}\ \{\bot\} \qquad \varphi \wedge \neg b \models \psi}{\Pi \vdash \{\varphi\}\ \textbf{while}\ b\ \textbf{do}\ c\ \{\psi\}}$$

1. Proposez deux règles pour **break** et **continue** de sorte que l'on puisse prouver le triplet de Hoare suivant.

$$\vdash \{y \geq 0\}\ \textbf{while}\ y > 0\ \textbf{do if}\ y = 1\ \textbf{then break else}\ y := y - 2\ \textbf{fi}\ \{y = 0 \vee y = 1\}$$

2. On appelle continuation une fonction $\kappa : \mathbb{Z}^{\mathsf{Var}} \to (\mathbb{Z}^{\mathsf{Var}})_\bot$ et on note K l'ensemble des continuations. Proposez une nouvelle sémantique dénotationelle $[\![c]\!]_{cps} : K \times (K \times K)^* \to K$ qui à une continuation k et à une pile de paires de continuations π associe la continuation $[\![c]\!]_{cps}(k, \pi)$.

3. On veut maintenant montrer que la logique de Hoare définie en première question est correcte. On introduit les définitions suivantes.

   - Une continuation k est φ-*sûre*, $\mathsf{safe}(k, \varphi)$, si pour tout environnement ρ, $\rho \models \varphi$ implique $k(\rho) = \bot$.
   - Une pile de paires de continuation $\pi = (k_{c,1}, k_{b,1}) \dots (k_{c,n}, k_{b,n})$ est sûre pour une pile de paire de formules $\Pi = (\varphi_1, \psi_1) \dots (\varphi_n, \psi_n)$, $\mathsf{safe}(\pi, \Pi)$, si pour tout $i = 1 \dots n$, $\mathsf{safe}(k_{c,i}, \varphi_i)$ et $\mathsf{safe}(k_{b,i}, \psi_i)$.
   - un triplet de Hoare $\Pi \vdash \{\varphi\}\ c\ \{\psi\}$ est valide si pour tout k, π, $\mathsf{safe}(k, \psi)$ et $\mathsf{safe}(\pi, \Pi)$ impliquent $\mathsf{safe}([\![c]\!]_{cps}(k, \pi), \varphi)$.

   Montrez que la logique de Hoare définie à la question 1 est correcte.