Programmation 1

TD n°10

24 novembre 2020

1 Semantics and verification

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 1 : Warmup

1. Give denotational semantics for Boolean expressions.
2. Give semantics for logical formulae. We write $\rho \models^I \phi$ when the formula ϕ is valid in the environment ρ for the program variables and I for the logical variables.
3. Notice that the syntax of Boolean expressions of Imp is a subset of the syntax of the formulas. Do the two semantics then coincide ? Show that for all I, $\rho \models^I b \iff [\![b]\!]_\rho \neq 0$.
4. Show that we can assume that $x < y$ is a valid boolean expression.

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 2 : Hoare on a toy language

1. Show that for all ρ, I, for all terms u, v and variable x
$$\rho \models^I \phi[x \mapsto u] \iff \rho[x \mapsto [\![u]\!]_\rho] \models^I \phi$$
2. Show that every Hoare triple is valid. In other words, show that the system is correct.
3. Suggest a rule for the while condition. Show that it is correct.
4. With the help of the axiomatic system, prove the following triple
$$\{x \sim 0 \wedge y \sim 0 \wedge z \sim 0 \wedge n \geq 0\}\ c\ \{x \sim n^3\} \tag{1}$$
where
$$c \triangleq \textbf{while}\ z < 3n\ \textbf{do}\ z := z + 3; y := y + 2z - 3; x := x + y - z + 1$$

Plus faible précondition libérale

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

Exercise 3 : Weakest liberal precondition

1. Let I be an interpretation of logical variables. For all programs c without a while loop and formulas ψ, construct a formula $\phi_{c,\psi}$ such that $\rho \models^I \phi_{c,\psi}$ if and only if $\rho \in \mathsf{wlp}^I(c, \psi)$.
2. Let ϕ be a formula defining $\mathsf{wlp}^I(\textbf{while}\ b\ \textbf{do}\ c, \psi)$. Give an equation $\models^I \phi \iff \phi'$ where ϕ' is a formula involving ϕ.
3. Using infinite disjunction and conjunction, write two solutions to this equation.
4. Which one does ϕ correspond to ?

Exercise 4 : Completeness [1]

We admit that there exists a formula expressing the weakest liberal precondition for the while loop.

1. Show that the axiomatic definition is complete. In other words, prove that for all valid triples $\models \{\phi\}\ c\ \{\psi\}$ there exists a derivation of $\{\phi\}\ c\ \{\psi\}$. *Hint : We start by proving it for the WLPs* .
2. What about a system S of proof on the triplets of Hoare which is correct and verifiable ?
3. Why is Hoare's logic complete despite everything ?
4. We admit that the weakest liberal preconditions are calculable. Deduce that the following problem is not recursively enumerable.

   Input A closed formula $\phi \in \mathsf{FO}[0, 1, +, \times, \leq]$

   Output Is ϕ valid ?

1. Answers will be shared on 8 December