Faculté des Sciences Économiques et de Gestion de Sfax
Année universitaire: 2014-2015
Module: Méthodes Formelles
Enseignant: Mohamed TOUNSI
Auditoire: 1 année Master - SINT

Travaux Dirigés - 4

Un triplet de Hoare $\{P\}\ S\ \{R\}$ est valide si pour tout environnement v tel que $v^{\#}(P) = 1$ et $(S, v) \to^{+} (\emptyset, w)$ on a $w^{\#}(R) = 1$. C'est à dire que si la pré-condition P est safisfaite avant l'exécution du programme S et si S termine, alors la post-condition R est satisfaite après l'exécution de S. On parle de *correction partielle* car on ne demande pas de prouver que S termine. Néanmoins, nous ne considérons que des programmes sans boucles dans les exercices 1,2,3 et 4. Le calcul de Hoare permet de prouver des triplets valides:

$$\frac{}{\{R[e/x]\}x := e\{R\}}\ Aff \qquad \frac{\{P \wedge B\}S_1\{R\} \quad \{P \wedge \neg B\}S_2\{R\}}{\{P\}\texttt{if}\ B\ \texttt{then}\ S_1\ \texttt{else}\ S_2\ \texttt{end}\{R\}}\ Cond$$

$$\frac{\{P\}S_1\{Q\} \quad \{Q\}S_2\{R\}}{\{P\}S_1; S_2\{R\}}\ Seq \qquad \frac{P' \Rightarrow P \quad \{P\}S\{R\} \quad R \Rightarrow R'}{\{P'\}S\{R'\}}\ Cons$$

Exercice 1

Indiquez, en le justifiant, si les triplets de Hoare suivants sont valides. Vous utiliserez uniquement la règle d'affectation.

1. $\{3 = 3\}$ $\texttt{x := 3}$ $\{x = 3\}$
2. $\{y = z\}$ $\texttt{x := y}$ $\{x = z\}$
3. $\{x > 2\}$ $\texttt{x := y}$ $\{y > 2\}$
4. $\{1 \leq 7 \leq 3\}$ $\texttt{x := 7}$ $\{1 \leq x \leq 3\}$
5. $\{3(4x + y)/z = 2y - 7\}$ $\texttt{x := (4x + y)/z}$ $\{3x = 2y - 7\}$
6. $\{x = 4\}$ $\texttt{x := x + 1}$ $\{x = 3\}$
7. $\{y > 2\}$ $\texttt{x := y}$ $\{y > 2\}$

Exercice 2

Indiquez, en le justifiant, si les triplets de Hoare suivants sont valides. Vous utiliserez les règles d'affectation et de conséquence.

1. $\{true\}$ $\texttt{x} := \texttt{3}$ $\{x = 3\}$
2. $\{false\}$ $\texttt{x} := \texttt{3}$ $\{x = 3\}$
3. $\{x = 4\}$ $\texttt{x} := \texttt{x} + \texttt{1}$ $\{x = 3\}$
4. $\{x \geq 0\}$ $\texttt{x} := \texttt{x} + \texttt{1}$ $\{x > 0\}$
5. $\{x = 0\}$ $\texttt{x} := \texttt{x} + \texttt{1}$ $\{x = 2\}$
6. $\{x = 1\}$ $\texttt{x} := \texttt{x} + \texttt{2}$ $\{x > 0\}$
7. $\{true\}$ $\texttt{y} := \texttt{x} + \texttt{b} - \texttt{a}$ $\{y - x \geq 0\}$

Exercice 3

Indiquez, en le justifiant, si les triplets de Hoare suivants sont valides. Vous utiliserez les règles d'affectation, de conséquence et de séquence. Pour chaque triplet valide, calculez la preuve ainsi que l'annotation du programme.

1. $\{true\}$ $\texttt{y} := \texttt{3}; \texttt{x} := \texttt{y}$ $\{x = 3\}$
2. $\{p = m + a * b\}$ $\texttt{m} := \texttt{m} + \texttt{a}; \texttt{b} := \texttt{b} - \texttt{1}$ $\{p = m + a * b\}$
3. $\{true\}$ $\texttt{z} := \texttt{y} + \texttt{2}; \texttt{x} := \texttt{y} - \texttt{z}$ $\{x = 3\}$
4. $\{7 - z > 0\}$ $\texttt{x} := \texttt{7} - \texttt{z}; \texttt{x} := \texttt{y}$ $\{y > 0\}$
5. $\{(b\%2 = 1) \wedge (a * b = a' * b')\}$ $\texttt{a} := \texttt{2} * \texttt{a}; \texttt{b} := \texttt{b div 2}$ $\{a * b = a' * b'\}$

Exercice 4

Indiquez, en le justifiant, si les triplets de Hoare suivants sont valides. Vous utiliserez les règles d'affectation, de conséquence et la conditionnelle. Pour chaque triplet valide, calculez la preuve ainsi que l'annotation du programme.

1. {true}
if (x $\geq$ 0) ***then***
skip
else
x := -x
end
{x $\geq$ 0}

2. {true}
if (a $\geq$ b) ***then***
y := x + a - b
else
y := x + b - a
end
{ y - x = | a - b | }

Exercice 5

La règle suivante permet de prouver la *correction partielle* d'un programme avec boucle `while` dont on suppose la terminaison.

$$\frac{\{I \land B\}\ S\ \{I\}}{\{I\}\ \texttt{while}\ B\ \texttt{do}\ S\ \texttt{end}\ \{I \land \neg B\}}\ \textit{while}$$

Cette règle requiert de trouver un invariant de boucle I. La prémisse exprime la nécessité de prouver que I est invariant. Indiquez en le justifiant si les triplets de Hoare suivant sont valides.

1. $\{true\}$ $\texttt{while}$ $(\texttt{x} \leq \texttt{N})$ $\texttt{do}$ $\texttt{x} := \texttt{x} + \texttt{1}$ $\texttt{end}$ $\{x > N\}$
2. $\{true\}$ $\texttt{while}$ $(\texttt{true})$ $\texttt{do skip end}$ $\{false\}$
3. $\{true\}$ $\texttt{while}$ $(\texttt{false})$ $\texttt{do skip end}$ $\{false\}$