UFR IMA Master 1 juin 2005

Option OGL

Exercice corrigé de calcul du $\mathcal{WP}$ d'un programme.

Prenons le programme suivant, écrit décrit dans un pseudo langage proche du langage ADA :

```
01.  x, y, v, z, t : integer
02.  tab : array(5..10) of integer
03.  begin
04.      read(x) ;
05.      v := 2 * x ;
06.      if x > 0 then y := x + 1 else z := 2 * x end ;
07.      if v > 0 then t := y else t := z end ;
08.      if t = 5 then write("Ok") end ;
09.      tab(t) := 3 ;
10.  end
```

Question 1 : Caractériser toutes les entrées permettant d'afficher *ok*.

Les données sont lues en ligne 04, donc leur traitement commence en ligne 05, et nous voulons qu'avant exécution de la ligne 08 la variable t vaille 5. Pour cela on pose :

$$\begin{array}{l} S_1 \hat{=} v := 2 * x \\ S_2 \hat{=} \textbf{if } x > 0 \textbf{ then } y := x + 1 \textbf{ else } z := 2 * x \textbf{ end} \\ S_3 \hat{=} \textbf{if } v > 0 \textbf{ then } t := y \textbf{ else } t := z \textbf{ end} \end{array}$$

De telle sorte que S_1 ; S_2 ; S_3 représente le traitement des données entre leur capture et leur utilisation. On cherche donc à calculer P tel que :
$P \equiv [S_1][S_2][S_3](t = 5)$

Remplacement de S_3 par sa valeur

$$\equiv [S_1][S_2][\textbf{if } v > 0 \textbf{ then } t := y \textbf{ else } t := z \textbf{ end}](t = 5)$$

Développement du **if**

$$\equiv [S_1][S_2][v > 0 \Longrightarrow t := y \; [\!] \; v \leq 0 \Longrightarrow t := z](t = 5)$$

$\mathcal{WP}$ du Choix borné

$$\equiv [S_1][S_2]([v > 0 \Longrightarrow t := y]t = 5 \; \wedge \; [v \leq 0 \Longrightarrow t := z]t = 5)$$

$\mathcal{WP}$ de la substitution gardée

$$\equiv [S_1][S_2]((v > 0 \Rightarrow y = 5) \; \wedge \; (v \leq 0 \Rightarrow z = 5))$$

Remplacement de S_2 par sa valeur

$$\equiv [S_1][\textbf{if } x{>}0 \textbf{ then } y{:=}x{+}1 \textbf{ else } z{:=}2{*}x \textbf{ end}]((v{>}0{\Rightarrow}y{=}5) \wedge (v{\leq}0{\Rightarrow}z{=}5))$$

Développement du **if**

$$\equiv [S_1][x{>}0 \Longrightarrow y{:=}x{+}1 \; [\!] \; x{\leq}0 \Longrightarrow z{:=}2{*}x]((v{>}0{\Rightarrow}y{=}5) \; \wedge \; (v{\leq}0{\Rightarrow}z{=}5))$$

$\mathcal{WP}$ du Choix borné

$$\begin{aligned} &\equiv [S_1]([x{>}0 \Longrightarrow y{:=}x{+}1]((v{>}0{\Rightarrow}y{=}5) \; \wedge \; (v{\leq}0{\Rightarrow}z{=}5)) \\ &\qquad \wedge \; [x{\leq}0 \Longrightarrow z{:=}2{*}x]((v{>}0{\Rightarrow}y{=}5) \; \wedge \; (v{\leq}0{\Rightarrow}z{=}5))) \end{aligned}$$

$\mathcal{WP}$ de la substitution gardée

$$\begin{aligned} &\equiv [S_1]((x > 0 \Rightarrow ((v > 0 \Rightarrow x + 1 = 5) \; \wedge \; (v \leq 0 \Rightarrow z = 5))) \\ &\qquad \wedge \; (x \leq 0 \Rightarrow ((v > 0 \Rightarrow y = 5) \; \wedge \; (v \leq 0 \Rightarrow 2 * x = 5)))) \end{aligned}$$

Simplification logique de l'implication : $A \Rightarrow ((B \Rightarrow C) \; \wedge \; (D \Rightarrow E)) \equiv (A \; \wedge \; B \Rightarrow C) \; \wedge \; (A \; \wedge \; D \Rightarrow E)$

$$\begin{aligned} &\equiv [S_1]((x > 0 \; \wedge \; v > 0 \Rightarrow x + 1 = 5) \\ &\qquad \wedge \; (x > 0 \; \wedge \; v \leq 0 \Rightarrow z = 5) \\ &\qquad \wedge \; (x \leq 0 \; \wedge \; v > 0 \Rightarrow y = 5) \\ &\qquad \wedge \; (x \leq 0 \; \wedge \; v \leq 0 \Rightarrow 2 * x = 5)) \end{aligned}$$

Remplacement de S_1 par sa valeur

$$\begin{aligned} &\equiv [v := 2 * x]((x > 0 \; \wedge \; v > 0 \Rightarrow x + 1 = 5) \\ &\qquad \wedge \; (x > 0 \; \wedge \; v \leq 0 \Rightarrow z = 5) \\ &\qquad \wedge \; (x \leq 0 \; \wedge \; v > 0 \Rightarrow y = 5) \\ &\qquad \wedge \; (x \leq 0 \; \wedge \; v \leq 0 \Rightarrow 2 * x = 5)) \end{aligned}$$

$\mathcal{WP}$ de la substitution simple

$$\begin{aligned} &\equiv ((x > 0 \; \wedge \; 2 * x > 0 \Rightarrow x + 1 = 5) \\ &\qquad \wedge \; (x > 0 \; \wedge \; 2 * x \leq 0 \Rightarrow z = 5) \\ &\qquad \wedge \; (x \leq 0 \; \wedge \; 2 * x > 0 \Rightarrow y = 5) \\ &\qquad \wedge \; (x \leq 0 \; \wedge \; 2 * x \leq 0 \Rightarrow 2 * x = 5)) \end{aligned}$$

Simplifications logiques : $A \; \wedge \; \neg A \equiv \mathsf{false}$

$$\equiv ((x > 0 \Rightarrow x = 4) \wedge (\mathsf{false} \Rightarrow z = 5) \wedge (\mathsf{false} \Rightarrow y = 5) \wedge (x \leq 0 \Rightarrow 2{*}x = 5))$$

Simplifications logiques : $\mathsf{false} \Rightarrow A \equiv \mathsf{true}$

$$\equiv ((x > 0 \Rightarrow x = 4) \; \wedge \; (x > 0 \; \vee \; x = 5/2))$$

Simplification logique : Comme x est un $integer$ alors $x = 5/2$ est false

$$\equiv ((x > 0 \Rightarrow x = 4) \; \wedge \; (x > 0)$$

Simplification logique : $(A \Rightarrow B) \; \wedge \; A \equiv A \; \wedge \; B$

$$\equiv (x = 4 \; \wedge \; x > 0)$$

Simplification logique et arithmétique

$$\equiv x = 4$$

Question 2 : Caractériser toutes les entrées pour lesquelles il n'y aura pas d'erreur à l'exécution.

De la même manière qu'en question 1, les données sont lues en ligne 04, donc leur traitement commence en ligne 05, et nous voulons qu'avant exécution de la ligne 09 la variable t soit dans l'intervalle 5..10. Pour cela on pose :

$$
\boxed{\begin{array}{l}
S_1 \mathrel{\hat{=}} v := 2 * x \\
S_2 \mathrel{\hat{=}} \textbf{if } x > 0 \textbf{ then } y := x + 1 \textbf{ else } z := 2 * x \textbf{ end} \\
S_3 \mathrel{\hat{=}} \textbf{if } v > 0 \textbf{ then } t := y \textbf{ else } t := z \textbf{ end} \\
S_4 \mathrel{\hat{=}} \textbf{if } t = 5 \textbf{ then } write("Ok") \textbf{ end}
\end{array}}
$$

De telle sorte que $S_1\ ;\ S_2\ ;\ S_3\ ;\ S_4$ représente le traitement des données entre leur capture et leur utilisation. On cherche donc à calculer P tel que :
$P \equiv [S_1][S_2][S_3][S_4](t \in 5..10)$

Remplacement de S_4 par sa valeur

$\equiv [S_1][S_2][S_3][\textbf{if } t = 5 \textbf{ then } write("Ok") \textbf{ end}](t \in 5..10)$

S_4 ne modifie pas les variable. Cette substitution est assimilable à skip. On applique donc le $\mathcal{WP}$ de skip

$\equiv [S_1][S_2][S_3](t \in 5..10)$

$\mathcal{WP}$ de S_3

$\equiv [S_1][S_2]((v > 0 \Rightarrow y \in 5..10)\ \wedge\ (v \leq 0 \Rightarrow z \in 5..10))$

$\mathcal{WP}$ de S_2

$$
\begin{aligned}
&\equiv [S_1]((x > 0 \Rightarrow (v > 0 \Rightarrow x + 1 \in 5..10)\ \wedge\ (v \leq 0 \Rightarrow z \in 5..10)) \\
&\qquad \wedge (x \leq 0 \Rightarrow (v > 0 \Rightarrow y \in 5..10)\ \wedge\ (v \leq 0 \Rightarrow 2 * x \in 5..10)))
\end{aligned}
$$

$\mathcal{WP}$ de S_1

$$
\begin{aligned}
&\equiv (x > 0 \Rightarrow (2 * x > 0 \Rightarrow x + 1 \in 5..10)\ \wedge\ (2 * x \leq 0 \Rightarrow z \in 5..10)) \\
&\qquad \wedge (x \leq 0 \Rightarrow (2 * x > 0 \Rightarrow y \in 5..10)\ \wedge\ (2 * x \leq 0 \Rightarrow 2 * x \in 5..10))
\end{aligned}
$$

Simplification logique

$$
\begin{aligned}
&\equiv (x > 0\ \wedge\ 2 * x > 0 \Rightarrow x + 1 \in 5..10) \\
&\qquad \wedge (x > 0\ \wedge\ 2 * x \leq 0 \Rightarrow z \in 5..10) \\
&\qquad \wedge (x \leq 0\ \wedge\ 2 * x > 0 \Rightarrow y \in 5..10) \\
&\qquad \wedge (x \leq 0\ \wedge\ 2 * x \leq 0 \Rightarrow 2 * x \in 5..10)
\end{aligned}
$$

Simplification logique

$$
\begin{aligned}
&\equiv (x > 0 \Rightarrow x \in 4..9) \\
&\qquad \wedge (x \leq 0 \Rightarrow x \in 3..5)
\end{aligned}
$$

Simplification logique

$\equiv x \in 4..9$