TD Vérification statique et vérification dynamique — FEUILLE 3

Exercice 5. On s'intéresse à la définition du calcul de plus faible précondition pour une instruction for de la forme :

```
for i :=e1 to e2 do C invariant I end
```

avec C ne modifiant pas i.

▷ **Question 1** *Définition du wp : wp(`for i :=e1 to e2 do C invariant I end`, R) =*

$$
\begin{array}{l}
(e1 > e2 \Rightarrow\ R) \\
\wedge(e1 \leq e2 \Rightarrow\ \exists\ n.(n = e2 \wedge \\
\quad\quad ([i := e1]I \\
\quad\quad \wedge \forall\ x, i(I \wedge i \leq n \Rightarrow wp(C, I)) \\
\quad\quad \wedge \forall\ x, i(I \wedge i = n \Rightarrow R) \\
\quad\quad)
\end{array}
$$

Remarque : si les bornes ne sont pas modifiées par C on peut gader $e1$ et $e2$. x représente les variables du programme.

▷ **Question 2** *Traduction :*

```
if e1 > e2 then skip
else
   var temp, stop in
      i :=e1 ;
      temp :=e2 ;
      stop:=false ;
      while stop=false  do
          C ;
          if i=temp then stop:=true  else i:=i+1 end
      end
    end
end
```

▷ **Question 3** *Arrêt de la boucle :*

Variant : $temp + val(stop) - i$

avec $val(false) = 1$ et val(true)=0

Invariant J : $i \leq temp \wedge\ (stop = true \Rightarrow i = temp)$

Preuve :

$J \Rightarrow\ temp + val(stop) - i \geq 0$ *OK*

$J \wedge stop = false \Rightarrow$
$[n := temp + val(stop) - i]wp(C, wp(if\ i = temp\ then\ stop := true\ else\ i := i+1, temp + val(stop) - i < n))$

i.e. :

$J \wedge stop = false \Rightarrow$
$[n := temp + val(stop) - i]wp(C, (i = temp \Rightarrow\ temp + val(true) - i < n) \wedge (i \neq temp \Rightarrow temp + val(stop) - i - 1 < n)$

i.e. :

$J \wedge stop = false \Rightarrow$
$(i = temp \Rightarrow\ temp+val(true)-i < temp+val(stop)-i) \wedge (i \neq temp \Rightarrow\ temp+val(stop)-i-1 < temp + val(stop) - i)$

Preuve que J est un invariant :

avant la boucle : $e1 \leq e2 \Rightarrow e1 \leq e2 \wedge (false = true \Rightarrow i = temp\ OK$

$i \in e1..temp + 1 \wedge i \leq temp \Rightarrow\ i + 1 \in e1..temp + 1\ OK$

▷ **Question 4** *wp(*`for i :=e1 to e2 do C invariant I end`*, R) =*

$(e1 > e2 \Rightarrow\ R)$
$\wedge(e1 \leq e2 \Rightarrow [i := e1]I)$
$\wedge(I \wedge J \wedge i \leq temp \Rightarrow wp(C\ ;\ i := i + 1, I))$

▷ **Question 5** *On rappelle que la traduction précédente peut introduire un débordement arithmétique sur i. On propose la traduction suivante :*

▷ **Question 6** *Pour l'extension il faut prendre pour J :*

$stop = true \Rightarrow i = temp$