Review: What can happen with the Hoare-Calculus

- Hoare Triples can be :
  - not provovable (counter-example)
  - provable, but for trivial reasons
    - non termination of the program
    - precondition false (falseE) or equivalent
  - provable for interesting reasons

Exercice 1

- Task 1 : Variante :

$$\vdash \{x \le 0\}\ y := y+2\ \{y \le 2\}"$$

  - contre-example : y = 5

- Task 1 as such :

$$\dfrac{x \le 0 \longrightarrow y \le 2\,[y \mapsto x+2] \qquad \dfrac{}{\vdash \{y \le 2\,[y \mapsto x+2]\}\ y := x+2\ \{y \le 2\}}\,\text{affect} \qquad y \le 2 \longrightarrow y \le 2}{\vdash \{x \le 0\}\ y := x+2\ \{y \le 2\}}\,\text{conseq}$$

Side calculuation :

$x \le 0 \longrightarrow y \le 2\,[y \mapsto x+2]$

$\equiv x \le 0 \longrightarrow x+2 \le 2$

$\equiv \text{True}$

Exercice 1

- Task 2

$$\vdash \{x \le 0\}\ y := y+2\ \{y \le 2\}$$

$$\dfrac{x \le 0 \longrightarrow x<0\ [x\mapsto x-1] \qquad \dfrac{}{\vdash \{x<0\ [x\mapsto x-1]\}\ x := x-1\ \{x<0\}}\,\text{affect} \qquad x<0 \longrightarrow x<0}{\vdash \{x\le 0\}\, x := x-1 \{x<0\}}\,\text{conseq}$$

Side Calculations :

$x \le 0 \longrightarrow x<0\ [x\mapsto x-1]$

$\equiv x \le 0 \longrightarrow x-1 < 0$

$\equiv x \le 0 \longrightarrow x < 1$

$\equiv$ True

Exercice 1

- Task 3
  - Proposition : $I \equiv x \geq -1$
    Sise Calculations :

$$x \geq -1\ [x \mapsto x-1]$$
$$\equiv x-1 \geq -1 \equiv x \geq 0 \equiv x \geq -1 \wedge x \geq 0$$

$$\dfrac{x \geq 0 \longrightarrow I \qquad \dfrac{\dfrac{}{\vdash \{I \wedge x \geq 0\}\ x := x-1 \{I\}}\ \text{affect}}{\vdash \{I\} \text{WHILE } x \geq 0 \text{ DO } x := x-1 \{I \wedge x < 0\}}\ \text{while} \qquad I \wedge x<0 \longrightarrow x=-1}{\vdash \{x \geq 0\} \text{WHILE } x \geq 0 \text{ DO } x := x-1 \{x=-1\}}\ \text{conseq}$$

Exercice 1

Task 4

Prog ≡ a := a + b; b := a - 2*b; a := a * b

- Pre ≡ a = x ∧ b = y
- Post ≡ $a = x^2 - y^2$

4. *On applique deux fois la règle de séquence, et on va appliquer la règle de l'affectation de droite à gauche pour trouver les propriétés intermédiaires R et Q. Puis on devra montrer que* $\vdash \{Pre\}$ `a:=a+b` $\{Q\}$ *est valide avec la propriété Q qu'on aura trouvée.*

$$\dfrac{\dfrac{\dfrac{?}{\vdash \{Pre\}\ \texttt{a:=a+b}\ \{Q\}} \qquad \dfrac{}{\vdash \{Q\}\ \texttt{b:=a-2*b}\ \{R\}}\ \textsf{aff}}{\vdash \{a = x \wedge b = y\}\ \texttt{a:=a+b;\ b:=a-2*b}\ \{R\}}\ \textsf{seq} \qquad \dfrac{}{\vdash \{R\}\ \texttt{a:=a*b}\ \{Post\}}\ \textsf{aff}}{\vdash \{Pre\}\ \texttt{Prog}\ \{Post\}}\ \textsf{seq}$$

Exercice 1

- Task 4

Avec $Pre \Leftrightarrow (a = x \wedge b = y)$, $Post \Leftrightarrow (a = x^2 - y^2)$. *On a :*

$$R \Leftrightarrow Post[a \mapsto a * b] \Leftrightarrow (a * b = x^2 - y^2)$$
$$Q \Leftrightarrow R[b \mapsto a - 2 * b] \Leftrightarrow (a^2 - 2 * a * b = x^2 - y^2)$$

On calcule $Q[a \mapsto a + b]$ *:*

$$Q[a \mapsto a + b] \Leftrightarrow ((a + b)^2 - 2 * (a + b) * b = x^2 - y^2) \Leftrightarrow (a^2 - b^2 = x^2 - y^2)$$

Ce n'est pas directement équivalent à $a = x \wedge b = y$ *(si la différence des carrés est égale, on peut aussi avoir* $a = -x \wedge b = -y$*), mais l'implication* $(a = x \wedge b = y) \Rightarrow (a^2 - b^2 = x^2 - y^2)$ *est vraie. Donc on pose* $P' = a^2 - b^2 = x^2 - y^2$ *et on applique la règle de conséquence, pour pouvoir ensuite appliquer la règle de l'affectation.*

$$\dfrac{Pre \Rightarrow P' \qquad \dfrac{}{\vdash \{P'\}\ \texttt{a:=a+b}\ \{Q\}}\ \textsf{aff}}{\vdash \{Pre\}\ \texttt{a:=a+b}\ \{Q\}}\ \textsf{cons}$$

Exercice 1

- Task 4

Observation: it is very difficult to construct R, Q and finally P' from left to right ; however, it is perfectly possible to construct it from right to left and to « bridge » Pre to P' via a consequence rule...

$\vdash \{a = x \wedge b = y\}\ a := a + b;\ b := a - 2*b;\ a := a * b\ \{a = x^2 - y^2\}$

Exercice 1

- Task 5
  - Proposition Invariant : I ≡ i = 8 !!!
  - Proposition Invariant : I ≡True

$$\dfrac{i=8 \longrightarrow I \qquad \dfrac{\dfrac{}{\vdash \{I \wedge i < 5\} \ldots \{I\}}\ \text{falseE}}{\vdash \{I\}\text{WHILE } i < 5 \text{ DO} \ldots \{I \wedge i \geq 5\}} \qquad I \wedge i \geq 5 \longrightarrow i \geq 5}{\vdash \{i=8\}\text{WHILE } i < 5 \text{ DO } i := 2*i\{i \geq 5\}}\ \text{conseq}$$

Exercice 2

- $A \equiv (max=x \vee max = y) \wedge max \geq x \wedge max \geq y$
- Justification :

$$
\begin{aligned}
& x > y \longrightarrow A[max \mapsto x] \\
\equiv\ & x > y \longrightarrow (max=x \vee max = y) \wedge max \geq x \wedge max \geq y\ [max \mapsto x] \\
\equiv\ & x > y \longrightarrow (x=x \vee x = y) \wedge x \geq x \wedge x \geq y \\
\equiv\ & true
\end{aligned}
$$

$$
\dfrac{\dfrac{x > y \longrightarrow A[max \mapsto x] \qquad \dfrac{}{\vdash \{A[max \mapsto x]\}\ max := x\ \{A\}}\,\text{affect} \qquad A \longrightarrow A}{\vdash \{true\} IF\ x > y\ THEN\ max := x\ ELSE\ max := y\ \{A\}}\,\text{conseq} \qquad \ldots}{\vdash \{true \wedge x > y\} max := x\ \{(max=x \vee max = y) \wedge max \geq x \wedge max \geq y\}}\,\text{if}
$$

Rappel : La Logique Hoare

Calcul de Hoare

$$\frac{}{\vdash \{P\}\ \texttt{SKIP}\ \{P\}}\ \textsf{skip} \qquad \frac{}{\vdash \{P[x \mapsto exp]\}\ \texttt{x := exp}\ \{P\}}\ \textsf{aff}$$

$$\frac{\vdash \{P \land cond\}\ \texttt{ins}_1\ \{Q\} \qquad \vdash \{P \land \neg cond\}\ \texttt{ins}_2\ \{Q\}}{\vdash \{P\}\ \texttt{IF cond THEN ins}_1\ \texttt{ELSE ins}_2\ \{Q\}}\ \textsf{if}$$

$$\frac{\vdash \{P \land cond\}\ \texttt{ins}\ \{P\}}{\vdash \{P\}\ \texttt{WHILE cond DO ins}\ \{P \land \neg cond\}}\ \textsf{while}$$

$$\frac{P \Rightarrow P' \qquad \vdash \{P'\}\ \texttt{ins}\ \{Q'\} \qquad Q' \Rightarrow Q}{\vdash \{P\}\ \texttt{ins}\ \{Q\}}\ \textsf{cons}$$

$$\frac{}{\vdash \{false\}\ \texttt{ins}\ \{P\}}\ \textsf{falseE} \qquad \frac{\vdash \{P\}\ \texttt{ins}_1\ \{Q\} \qquad \vdash \{Q\}\ \texttt{ins}_2\ \{R\}}{\vdash \{P\}\ \texttt{ins}_1\ ;\ \texttt{ins}_2\ \{R\}}\ \textsf{seq}$$