Review: What can happen with the Hoare-Calculus

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

Exercice 5

Task : $\vdash \{0 \leq x \wedge x \bmod 5 > 5\}\ x :== x * x\ \{x \operatorname{div} 2 = 1\}$

We compute : $0 \leq x \wedge x \bmod 5 > 5 \equiv False$

$$\frac{}{\vdash \{0 \leq x \wedge x \bmod 5 > 5\}\ x :== x * x\ \{x \operatorname{div} 2 = 1\}}\ \text{FalseE}$$

Exercice 6

- Task : $\vdash \{x \leq -2\}\text{WHILE } 0 < x*x \text{ DO } x:==x+1\{x=0\}$
- Justification :

$$\frac{}{\vdash \{x \leq 0[x \mapsto x+1]\}\ x:==x+1\ \{x \leq 0\}}\ \text{affect}$$

$$\frac{x \leq 0 \wedge 0 < x*x \longrightarrow (x \leq 0[x \mapsto x+1]) \quad \vdash \{x \leq 0[x \mapsto x+1]\}\ x:==x+1\ \{x \leq 0\} \quad x \leq 0 \longrightarrow x \leq 0}{\vdash \{x \leq 0 \wedge 0 < x*x\}\ x:==x+1\ \{x \leq 0\}}\ \text{Cons}$$

$$\frac{\vdash \{x \leq 0 \wedge 0 < x*x\}\ x:==x+1\ \{x \leq 0\}}{\vdash \{x \leq 0\}\text{WHILE } 0 < x*x \text{ DO } ...\ \{x*x \leq 0 \wedge x \leq 0\}}\ \text{while}$$

$$\frac{x \leq -2 \longrightarrow x \leq 0 \quad \vdash \{x \leq 0\}\text{WHILE } 0 < x*x \text{ DO } ...\ \{x*x \leq 0 \wedge x \leq 0\} \quad x*x \leq 0 \wedge x \leq 0 \longrightarrow x=0}{\vdash \{x \leq -2\}\text{WHILE } 0 < x*x \text{ DO } x:==x+1\{x=0\}}$$

Exercice 6

- Task : $\vdash \{x \leq -2\}\text{WHILE } 0 < x*x \text{ DO } x :== x+1 \{x=0\}$
- Justification : $x \leq 0 \wedge 0 < x*x \longrightarrow (x \leq 0[x \mapsto x+1])$

$\equiv (x<0 \vee x=0) \wedge 0<x*x \longrightarrow (x \leq 0[x \mapsto x+1])$

$\equiv (x=0) \wedge 0<x*x \longrightarrow (x \leq 0[x \mapsto x+1]) \vee$

$(x<0) \wedge 0<x*x \longrightarrow (x \leq 0[x \mapsto x+1])$

$\equiv \text{False} \vee (x<0 \wedge 0<x*x \longrightarrow x \leq -1) \equiv \text{True}$

$x \leq 0 \wedge 0<x*x \longrightarrow (x \leq 0[x \mapsto x+1])$ $\quad \vdash \{x \leq 0[x \mapsto x+1]\}\ x :== x+1\ \{x \leq 0\}$ (affect) $\quad x \leq 0 \longrightarrow x \leq 0$

Cons

$\vdash \{x \leq 0 \wedge 0 < x*x\}\ x :== x+1\ \{x \leq 0\}$

while

$x \leq -2 \longrightarrow x \leq 0$ $\quad \vdash \{x \leq 0\}\text{WHILE } 0 < x*x \text{ DO } \ldots \{x*x \leq 0 \wedge x \leq 0\}$ $\quad x*x \leq 0 \wedge x \leq 0 \longrightarrow x=0$

$\vdash \{x \leq -2\}\text{WHILE } 0 < x*x \text{ DO } x :== x+1 \{x=0\}$

Exercice 7

- Task :

```
S := 1; P := 0;
WHILE P < N DO
        S := S * X; P := P + 1;
```

Exercice 7

- Task :

  prelude $\equiv$ S := 1; P := 0;

  body $\equiv$ S := S * X; P := P + 1;

  A $\equiv$ $N \geq 0 \wedge S = 1 \wedge P = 0$

aff

$\vdash \{I[P \mapsto P+1][S \mapsto S*X]\}$ S := S * X $\{I[P \mapsto P+1]\}$

aff

$\vdash \{I[P \mapsto P+1]\}$ P := P + 1 $\{I\}$

cons

$I \wedge P < N \longrightarrow I[P \mapsto P-1][S \mapsto S*X]$

$\vdash \{I \wedge P < N\}$ body $\{I\}$

$I \longrightarrow I$

cons

$\vdash \{I \wedge P < N\}$ body $\{I\}$

while

...

$A \longrightarrow I$

$\vdash \{I\}$ WHILE P < N DO body $\{I \wedge P >= N\}$

$I \wedge P >= N \longrightarrow S = X\text{^}N$

cons

$\vdash \{N \geq 0\}$ prelude$\{A\}$

$\vdash \{A\}$ WHILE P < N DO body $\{S = X\text{^}N\}$

seq

$\vdash \{N \geq 0\}$ prelude ; WHILE P < N DO body $\{S = X\text{^}N\}$

Exercice 7

- Task :

prelude ≡ S := 1; P := 0;

body ≡ S := S * X; P := P + 1;

A ≡ $N \geq 0 \wedge S = 1 \wedge P = 0$

aff

$\vdash \{I[P \mapsto P+1][S \mapsto S*X]\} S := S * X \{I[P \mapsto P+1]\}$

aff

$\vdash \{I[P \mapsto P+1]\} P := P + 1 \{I\}$

cons

$I \wedge P < N \longrightarrow I[P \mapsto P-1][S \mapsto S*X]$

$\vdash \{I \wedge P < N\} \text{body} \{I\}$

$I \longrightarrow I$

cons

$\vdash \{I \wedge P < N\} \text{body} \{I\}$

while

...

$A \longrightarrow I$

$\vdash \{I\} \text{WHILE } P < N \text{ DO body } \{I \wedge P >= N\}$

$I \wedge P >= N \longrightarrow S = X\text{^}N$

cons

$\vdash \{N \geq 0\} \text{ prelude} \{A\}$

$\vdash \{A\} \text{WHILE } P < N \text{ DO body } \{ S = X\text{^}N\}$

seq

$\vdash \{N \geq 0\} \text{ prelude ; WHILE } P < N \text{ DO body } \{ S = X\text{^}N\}$

Exercice 7

- Task :
  prelude ≡ S := 1; P := 0;
  body ≡ S := S * X; P := P + 1;
  A ≡ $N \geq 0 \wedge S = 1 \wedge P = 0$
- Invariant Proposition : $0 <= P <= N \wedge S = X^P$
- $A \longrightarrow I \equiv N \geq 0 \wedge S = 1 \wedge P = 0 \longrightarrow 0 <= P <= N \wedge S = X^P \equiv$ True
- $I \wedge P < N \longrightarrow I[P \mapsto P+1][S \mapsto S*X]$
  $\equiv 0 <= P <= N \wedge S = X^P \wedge P < N$
  $\longrightarrow (0 <= P <= N \wedge S = X^P[P \mapsto P+1][S \mapsto S*X])$
  $\equiv 0 <= P <= N \wedge S = X^P \wedge P < N$
  $\longrightarrow (0 <= P+1 <= N \wedge S*X = X^{(P+1)})$

  $\equiv 0 <= P <= N \wedge S = X^P \wedge P < N$
  $\longrightarrow (0 <= P+1 <= N \wedge S*X = X * X^{(P)})$

  ≡ True
- $I \wedge P >= N \longrightarrow S = X^N \equiv 0 <= P <= N \wedge P >= N \wedge S = X^P \longrightarrow S = X^N \equiv$ True

Rappel : La Logique Hoare

- .

Calcul de Hoare

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

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

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

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

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