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 3

- $A \equiv$ WHILE y != x DO x := x - 1; y := y - 2;
- Pre $\equiv y \geq x$
  Post $\equiv x = y$
- $I \equiv y \geq x$
- Justification : $I \wedge x != y \equiv y > x \equiv y - 1 \geq x \equiv y - 2 \geq x - 1 \equiv y \geq x \, [y \mapsto y-2, x \mapsto x-1]$
  $y-2 \geq x \equiv y \geq x \, [y \mapsto y-2] \equiv I \, [y \mapsto y-2]$

$$\vdash \{y-2 \geq x-1\} \; x := x - 1 \; \{y-2 \geq x\} \quad (\text{aff}) \qquad \vdash \{y-2 \geq x\} \; y := y - 2 \; \{I\} \quad (\text{aff})$$

$$\vdash \{I \wedge x != y\} \; x := x - 1; y := y - 2 \; \{I\} \quad (\text{seq}) \quad \ldots$$

$$y \geq x \longrightarrow I \qquad \vdash \{I\} \; A \; \{I \wedge x = y\} \quad (\text{while}) \qquad I \wedge x = y \longrightarrow x = y$$

$$\vdash \{y \geq x\} \; A \; \{x = y\} \quad (\text{cons})$$

Exercice 4

- prelude ≡ S := 1; P := N;

  body ≡ S := S * X; P := P - 1;

  A ≡ N≥0 ∧ S =1 ∧ P=N

(aff) ⊢{I[P ↦P-1][S ↦S*X]}S := S * X {I[P ↦P-1]}   (aff) ⊢{I[P ↦P-1]}P := P - 1 {I}

(cons)

I∧P>=1 ⟶I[P ↦P-1][S ↦S*X]   ⊢{I ∧ P >= 1}body {I}   I ⟶ I

(cons)

⊢{I ∧ P >= 1}body {I}

(while)

...   A ⟶ I   ⊢{I}WHILE P >= 1 DO body {I∧P<1}   I∧P<1 ⟶ S=X^N

(cons)

⊢{N≥0} prelude{A}   ⊢{A}WHILE P >= 1 DO body { S = X^N}

(seq)

⊢{N≥0} prelude ; WHILE P >= 1 DO body { S = X^N}

Exercice 4

- prelude ≡ S := 1; P := N;

  body ≡ S := S * X; P := P - 1;

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

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

cons

$I \wedge P >= 1 \longrightarrow I[P \mapsto P-1][S \mapsto S*X]$ $\vdash \{I \wedge P >= 1\} body \{I\}$ $I \longrightarrow I$

cons

$\vdash \{I \wedge P >= 1\} body \{I\}$

while

... $A \longrightarrow I$ $\vdash \{I\} WHILE\ P >= 1\ DO\ body \{I \wedge P < 1\}$ $I \wedge P < 1 \longrightarrow S = X\hat{}N$

cons

$\vdash \{N \geq 0\}\ prelude \{A\}$ $\vdash \{A\} WHILE\ P >= 1\ DO\ body \{ S = X\hat{}N \}$

seq

$\vdash \{N \geq 0\}\ prelude\ ;\ WHILE\ P >= 1\ DO\ body \{ S = X\hat{}N \}$

Exercice 4

On cherche alors un I de sorte que :

- $N \geq 0 \wedge S = 1 \wedge P = N \longrightarrow I$
- $I \wedge P < 1 \longrightarrow S = X^N$
- $I \wedge P >= 1 \longrightarrow I[P \mapsto P-1][S \mapsto S*X]$

- Proposition 1 $I \equiv S = X^(N-P)$ (Probleme : N'établit pas la post-condition)
  Proposition 2 $I \equiv S = X^(N-P) \wedge P \geq 0$

$N \geq 0 \wedge S = 1 \wedge P = N \longrightarrow S = X^(N-P) \wedge P \geq 0$
$\equiv N \geq 0 \wedge S = 1 \wedge P = N \longrightarrow S = X^(0) \wedge P \geq 0 \equiv N \geq 0 \wedge S = 1 \wedge P = N \longrightarrow 1 = 1 \wedge N \geq 0 \equiv$ True

$S = X^(N-P) \wedge P \geq 0 \wedge P < 1 \longrightarrow S = X^N$
$\equiv S = X^(N-P) \wedge P = 0 \longrightarrow S = X^N \equiv$ True

$I \wedge P >= 1 \longrightarrow I[P \mapsto P-1][S \mapsto S*X]$
$\equiv S = X^(N-P) \wedge P \geq 0 \wedge P >= 1 \longrightarrow S = X^(N-P) \wedge P \geq 0 [P \mapsto P-1][S \mapsto S*X]$
$\equiv S = X^(N-P) \wedge P \geq 0 \wedge P >= 1 \longrightarrow S*X = X^(N-(P-1)) \wedge P-1 \geq 0$

$\equiv S = X^(N-P) \wedge P \geq 0 \wedge P >= 1 \longrightarrow S*X = X^(N-P)*X)) \wedge P-1 \geq 0$
$\equiv X^(N-P) * X = X^(N-P)*X \equiv$ True

Exercice 4

- prelude ≡ S := 1; P := N;

  body ≡ S := S * X; P := P - 1;

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

  $A[P \mapsto N] \equiv N \geq 0 \land S = 1$

  $A[P \mapsto N][S \mapsto 1] \equiv N \geq 0$

$$\dfrac{\dfrac{}{\vdash \{N \geq 0\}\ S := 1\ \{A[P \mapsto N]\}}\ \text{aff} \qquad \dfrac{}{\vdash \{A[P \mapsto N]\}\ P := N\ \{A\}}\ \text{aff}}{\vdash \{N \geq 0\}\ \text{prelude}\ \{A\}}\ \text{seq}$$

Rappel : La Logique Hoare

- ·

Calcul de Hoare

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

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

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

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

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