

Prof. Burkhart Wolff  
wolff@lri.fr

## Preuve de programmes

Date : 22 février 2023

### Exercice 1

Dériver les triplets de Hoare suivants en utilisant les règles d'inférence introduites dans le cours. Rappel : toutes les variables sont des entiers.

1.  $\vdash \{x \leq 0\} \ y := x+2 \ \{y \leq 2\}$
2.  $\vdash \{x \leq 0\} \ x := x-1 \ \{x < 0\}$
3.  $\vdash \{x \geq 0\} \ \text{WHILE } x \geq 0 \ \text{DO } x := x-1 \ \{x = -1\}$
4.  $\vdash \{a = x \wedge b = y\} \ a := a + b; \ b := a - 2*b; \ a := a * b \ \{a = x^2 - y^2\}$
5.  $\vdash \{i = 8\} \ \text{WHILE } i < 5 \ \text{DO } i := 2*i \ \{i \geq 5\}$

### Exercice 2

On considère le programme Prog suivant :

```
IF x > y
THEN max := x
ELSE max := y
```

Quelles sont les pré et post-conditions de ce programme ? Démontrer la validité du triplet de Hoare correspondant.

### Exercice 3

On considère le programme Prog suivant :

```
WHILE y != x DO
  x := x - 1;
  y := y - 2;
```

1. Quelles sont les pré et post-conditions de ce programme ?
2. Quel est l'invariant de la boucle ?
3. Démontrer la validité du triplet de Hoare correspondant à ce programme.
4. Donner un variant pour la boucle WHILE, c'est-à-dire une expression toujours positive et qui décroît strictement à chaque tour de boucle.

### Exercice 4

On veut prouver que le programme suivant calcule  $X^N$  pour  $N \geq 0$ .

```

S := 1;
P := N;
WHILE P >= 1 DO
  S := S * X;
  P := P - 1;

```

1. Écrire la spécification du programme sous forme de pré et post-conditions.
2. Quel est le triplet de Hoare à prouver ?
3. Trouver un invariant pour la boucle WHILE, puis donner la preuve de la deuxième partie du programme.
4. Donner la preuve de la première partie du programme S:=1; P:=N pour terminer la preuve du programme.
5. Donner un variant pour la boucle WHILE.
6. On considère maintenant l'implémentation suivante :

```

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

```

Comparer les spécifications, invariants et variants de ces deux implémentations. Quelle partie de la preuve du premier programme faut-il modifier pour obtenir une preuve de cette implémentation ?

### Calcul de Hoare

$$\begin{array}{c}
\frac{}{\vdash \{P\} \text{ SKIP } \{P\}} \text{ skip} \qquad \frac{}{\vdash \{P[x \mapsto \text{exp}]\} x := \text{exp} \{P\}} \text{ aff} \\
\\
\frac{\vdash \{P \wedge \text{cond}\} \text{ins}_1 \{Q\} \quad \vdash \{P \wedge \neg \text{cond}\} \text{ins}_2 \{Q\}}{\vdash \{P\} \text{ IF } \text{cond} \text{ THEN } \text{ins}_1 \text{ ELSE } \text{ins}_2 \{Q\}} \text{ if} \\
\\
\frac{\vdash \{P \wedge \text{cond}\} \text{ins} \{P\}}{\vdash \{P\} \text{ WHILE } \text{cond} \text{ DO } \text{ins} \{P \wedge \neg \text{cond}\}} \text{ while} \\
\\
\frac{P \Rightarrow P' \quad \vdash \{P'\} \text{ins} \{Q'\} \quad Q' \Rightarrow Q}{\vdash \{P\} \text{ins} \{Q\}} \text{ cons} \\
\\
\frac{}{\vdash \{false\} \text{ins} \{P\}} \text{ falseE} \qquad \frac{\vdash \{P\} \text{ins}_1 \{Q\} \quad \vdash \{Q\} \text{ins}_2 \{R\}}{\vdash \{P\} \text{ins}_1 ; \text{ins}_2 \{R\}} \text{ seq}
\end{array}$$