

---

*Delphine Longuet, Thibaut Balabonski, Robin Pelle, Hadi Zaatiti*  
*longuet@lri.fr, blsk@lri.fr, pelle@lri.fr, hadizaatiti@gmail.com*

## TD 6 - Preuve de programmes

Semaine du 28 novembre 2016

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

### 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 effectue la division euclidienne de  $A$  par  $B$  pour  $A \geq 0$  et  $B > 0$ .

```
Q := 0;
R := A;
WHILE R >= B DO
  R := R - B;
  Q := Q + 1
```

1. Écrire la spécification du programme sous forme de pré et post-conditions.
2. Quel est le triplet de Hoare à prouver ?
3. Énoncer une propriété vérifiée après le préambule du programme  $Q := 0; R := A$ , et donner la preuve du triplet de Hoare correspondant.
4. Trouver un invariant  $Inv$  pour la boucle WHILE.
5. Dériver le triplet de Hoare :

$$\{A = B \times Q + R \wedge R \geq B\} R := R - B; Q := Q + 1 \{A = B \times Q + R \wedge R \geq 0\}$$

*Indication* : trouvez une propriété  $S$  qui permette de démontrer le triplet

$$\{S\} Q := Q + 1 \{A = B \times Q + R \wedge R \geq 0\}$$

6. On note  $Loop$  la boucle WHILE du programme. Complétez la preuve précédente afin de dériver le triplet :

$$\{A = B \times Q + R \wedge R \geq 0\} Loop \{A = B \times Q + R \wedge R \geq 0 \wedge R < B\}$$

7. Terminez la preuve de la boucle WHILE en complétant votre preuve de manière à dériver le triplet :

$$\{A \geq 0 \wedge B > 0 \wedge Q = 0 \wedge R = A\} Loop \{A = B \times Q + R \wedge 0 \leq R < B\}$$

8. Donner un variant pour la boucle de ce programme.

### Calcul de Hoare

$$\frac{}{\{P\} \text{ SKIP } \{P\}} \text{ skip}$$

$$\frac{}{\{P[x \mapsto \text{exp}]\} x := \text{exp} \{P\}} \text{ affectation}$$

$$\frac{\{P \wedge \text{cond}\} \text{ins}_1 \{Q\} \quad \{P \wedge \neg \text{cond}\} \text{ins}_2 \{Q\}}{\{P\} \text{ IF } \text{cond} \text{ THEN } \text{ins}_1 \text{ ELSE } \text{ins}_2 \{Q\}} \text{ ifthenelse}$$

$$\frac{\{P \wedge \text{cond}\} \text{ins} \{P\}}{\{P\} \text{ WHILE } \text{cond} \text{ DO } \text{ins} \{P \wedge \neg \text{cond}\}} \text{ while}$$

$$\frac{P \Rightarrow P' \quad \{P'\} \text{ins} \{Q'\} \quad Q' \Rightarrow Q}{\{P\} \text{ins} \{Q\}} \text{ consequence}$$

$$\frac{}{\{false\} \text{ins} \{P\}} \text{ falseE}$$

$$\frac{\{P\} \text{ins}_1 \{Q\} \quad \{Q\} \text{ins}_2 \{R\}}{\{P\} \text{ins}_1 ; \text{ins}_2 \{R\}} \text{ sequence}$$

### Exercice 5

Donner la spécification sous-forme de pré et post-conditions, ainsi que les invariants de boucle pour les programmes suivants.

```
Minimum d'un tableau

int min(int t[],int n) {
    int i;
    int m = t[0];

    for(i = 1; i < n; i++) {
        if(t[i] < m) {
            m = t[i];
        }
    }
    return m;
}
```

```
Tri par sélection

void swap(int t[], int i, int j) {
    int tmp = t[i];
    t[i] = t[j];
    t[j] = tmp;
}

void tri_selection(int t[], int n) {
    int i = 0;
    int min;

    while(i < n) {
        int min = i;
        int j = i+1;
        while (j < n) {
            if (t[j] < t[min]) {
                min = j;
            }
            j = j+1;
        }
        swap(t,i,min);
        i = i + 1;
    }
}
```