

1 Exercice (6 pts)

Montrer les triplets suivants (on demande dans cet exercice de préciser à chaque étape quelle règle du calcul de Hoare est appliquée).

1.1

```
{x ∈ ℕ ∧ x ≥ 3} x := x * 2 ; y := x + 1 {y > 6}
```

1.2

```
{x, y, z ∈ ℕ ∧ x < z < y} x := x + 1 ; y := y - 1 {x ≤ y}
```

1.3

```
{ x, y ∈ ℕ }  
if x < y then x := y + 1 else x := x + 1 endif  
{ y < x }
```

2 Exercice (4 pts)

2.1

Montrer que le triplet suivant est correct :

```
{ x, y ∈ ℕ ∧ x ≤ y }  
while x < y  
do x := x + 2 done  
{ x = y ∨ x = y + 1 }
```

Suggestion : On pourra choisir comme invariant de boucle la proposition ci-dessous :

$$x, y \in \mathbb{N} \wedge x \leq y + 1$$

3 Problème (10 pts)

Un programmeur dispose d'un clavier d'ordinateur sur lequel la touche “-” ne fonctionne pas. Afin de pouvoir quand même réaliser des soustractions de nombres entiers naturels, il écrit le programme suivant :

```
int d := 0;  
int x := a;  
while x < b  
do  
  d := d + 1;  
  x := x + 1  
done
```

On veut démontrer que si a et b sont deux entiers naturels tels que $a \leq b$, alors la variable d contient la différence $b - a$ à la fin de l'exécution du programme. Pour ce faire, vous devez répondre aux questions suivantes :

3.1 Question (2 points)

Donner un exemple simple d'exécution de ce programme. Comment se comporte le programme lorsque la pré-condition $a \leq b$ n'est pas satisfaite ?

3.2 Question (2 points)

Exprimer, à l'aide de triplets, la correction partielle et la correction totale de ce programme, pour la spécification considérée.

3.3 Question (4 points)

Donner un invariant de boucle pour ce programme. Vous devrez démontrer que votre proposition est bien un invariant permettant de prouver la correction du programme.

3.4 Question (2 points)

Démontrer que ce programme termine toujours, dans les conditions précisées plus haut ($a \leq b$).

4 Annexe : Règles du Calcul de Hoare

4.1 Règles de base

4.1.1 Instruction vide

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

4.1.2 Affectation $x := e$

$$\frac{}{\{P[e/x]\} x := e \{P\}}$$

4.1.3 Composition $S;T$

$$\frac{\{P\} S \{R\} \quad \{R\} T \{Q\}}{\{P\} S ; T \{Q\}}$$

4.1.4 Règle de la conséquence

$$\frac{P \Rightarrow P_1 \quad \{P_1\} S \{Q_1\} \quad Q_1 \Rightarrow Q}{\{P\} S \{Q\}}$$

4.1.5 Règle de la conditionnelle

$$\frac{\{P \wedge b\} S \{Q\} \quad \{P \wedge \neg b\} T \{Q\}}{\{P\} \text{ if } b \text{ then } S \text{ else } T \text{ endif } \{Q\}}$$

4.1.6 Règle pour la boucle **while**

$$\frac{\{P \wedge b\} S \{P\}}{\{P\} \text{ while } b \text{ do } S \text{ done } \{P \wedge \neg b\}}$$

4.2 Règles utiles

4.2.1 Conjonction des post-conditions

$$\frac{\{P\} S \{Q\} \quad \{P\} S \{R\}}{\{P\} S \{Q \wedge R\}}$$

4.2.2 Disjonction des pré-conditions

$$\frac{\{P\} S \{R\} \quad \{Q\} S \{R\}}{\{P \vee Q\} S \{R\}}$$

4.2.3 Invariant de boucle

$$\frac{P \Rightarrow \text{Inv} \quad \text{Inv} \wedge \neg b \Rightarrow Q \quad \{\text{Inv} \wedge b\} S \{\text{Inv}\}}{\{P\} \text{ while } b \text{ do } S \text{ done } \{Q\}}$$