

TD7 : Logique de Hoare

Les boucles et les tableaux

1^{er} mars 2017

Exercice 1

Soit le programme $Prog_1$ suivant :

```
{ var a;  
  a=x  
  y=0  
  while(a!=0) {  
    y=y+1;  
    a=a-1;  
  }  
}
```

Question 1

Trouver un variant et un invariant de boucle.

Donner un argument concernant la terminaison du programme/

Ajouter le code de vérification de respect de l'invariant au programme.

Ajouter le code de vérification de décroissance stricte du variant.

Question 2

Prouver la spécification suivante (en logique de Hoare) :

$\{x \geq 0\}Prog_1\{x = y\}$

Exercice 2

La spécification suivante est-elle correcte (faire la démonstration) ?

$\{tab[i] = X \wedge tab[j] = Y\}$

```
{ var r;  
  r=tab[i];  
  tab[i]=tab[j];  
  tab[j]=r;  
}
```

$\{tab[i] = Y \wedge tab[j] = X\}$

Exercice 3

Question 1

Prouver la spécification suivante :

$\{n \geq 0\}$

```

{ var m; var y;
  m=n; p=1; y=x;
  if (x!=0)
    while (m!=0) {
      if(odd(m)) p=p*y;
      else p=p;
      m = m div 2;
      y = y * y;
    }
  else p=0
}

```

$$\{p = x^n\}$$

Question 2

Prouver la spécification suivante :

$$\{a \geq 0 \wedge b > 0\}$$

```

{ var x; var y;
  x=a;
  y=b;
  while (x*y!=0) {
    if (x>y) x=x-y
    else y=y-x
  }
  if(x==0)
    p = y;
  else
    p = x;
}

```

$$\{p = \text{pgcd}(a, b)\}$$

Annexe : Règles de la logique de Floyd/Hoare (Deuxième Partie)

$$\frac{\{P\}C\{Q\} \quad v_1, \dots, v_n \notin P \cup Q}{\{P\}\{\text{var } v_1; \dots; \text{var } v_n; C\}\{Q\}} (\text{let})$$

$$\frac{}{\{Q[A(\text{expr}_1 \leftarrow \text{expr}_2)/A]\}A[\text{expr}_1] = \text{expr}_2\{Q\}} (\text{tab})$$

avec :

$$\begin{cases} \text{expr}_1 = \text{expr}_3 \implies A(\text{expr}_1 \leftarrow \text{expr}_2)[\text{expr}_3] = \text{expr}_2 \\ \text{expr}_1 \neq \text{expr}_3 \implies A(\text{expr}_1 \leftarrow \text{expr}_2)[\text{expr}_3] = A[\text{expr}_3] \end{cases}$$

$$\frac{I \wedge S \implies I' \quad \{I'\}C\{I\} \quad I \wedge \neg S \implies Q}{\{I\}\text{while}(S)C\{Q\}} (\text{while})$$