4

Thème Preuve de programme
Logique de Hoare

Exercices

Pour chacun des exercices suivants :

1. Déterminer l'invariant de boucle permettant de prouver la correction.
2. Déterminer le variant de boucle permettant de prouver la terminaison.
3. Annoter le programme en utilisant les règles de la logique de Hoare.

Exercice 1 Soit la fonction de $\mathbb{N}$ dans $\mathbb{N}^2$ définie par le programme itératif suivant :

$\{N \geq 0\}$
$K := 0;$
$F := 1;$
while $(K \neq N)$ do
  $K := K + 1;$
  $F := F \times K$
od
$\{F = N!\}$

Exercice 2 Soit la fonction de $\mathbb{N}$ dans $\mathbb{N}^2$ définie par le programme itératif suivant :

$\{N \geq 0\}$
$K := N;$
$F := 1;$
while $(K \neq 0)$ do
  $F := F \times K;$
  $K := K - 1$
od
$\{F = N!\}$

Exercice 3 Soit la fonction de $\mathbb{N}^2$ dans $\mathbb{N}^2$ définie par le programme itératif suivant :

$\{X \geq 0 \wedge Y > 0\}$
$Q := 0;$
$R := X;$
while $(Y \leq R)$ do
  $Q := Q + 1;$
  $R := R - Y$
od
$\{X = Q \times Y + R \ \wedge \ 0 \leq Q \ \wedge \ 0 \leq R < Y\}$

INV : $X = R + QY \wedge 0 \leq R < Y$.
V : R

Exercice 4 Soit la fonction de $\mathbb{N}^2$ dans $\mathbb{N}^2$ définie par le programme itératif suivant :

$\{A > 0, B > 0\}$ pgcd(A,B) = pgcd(A,B) ∧ A>0 ∧ B>0}.
$X := A;$ pgcd(x,B) = pgcd(A,B) ∧ X>0 ∧ B>0
$Y := B;$ pgcd(x,y) = pgcd(A,B) ∧ X>0 ∧ Y>0
while $(X \neq Y)$ do pgcd(x,y)
  if $(X > Y)$ then pgcd(x,y) = pgcd(A,B) ∧ X>Y ∧ X>0 ∧ Y>0
    $X := X - Y$. pgcd(x−y, y) = pgcd(A,B) ∧ X>0 ∧ Y>0 ∧ X>Y
  else pgcd(x,y) = pgcd(A,B) ∧ X≤Y ∧ X>0 ∧ Y>0
    $Y := Y - X$ pgcd(x, y−x) = pgcd(A,B) ∧ X≤Y ∧ X>0 ∧ Y>0
pgcd(x,y) = pgcd(A,B) fi
od {pgcd(x,y) = pgcd(A,B)} ∧ X=Y ∧ X>0 ∧ Y>0}.
$\{X = Y, X > 0, X = pgcd(A, B)\}$

Mathématiquement, celui-ci est défini par :

$$\forall A, B \in \mathbb{N}^\star, pgcd(A, B) = \max\{C \in \mathbb{N}^\star \mid A \cong_C 0, B \cong_C 0\}$$

La notation $A \cong_C$ correspond au calcul de A modulo C. Cette expression vaut 0 si C divise A. Le fonction *pgcd* vérifie les propriétés suivantes :

1) $\forall A \in \mathbb{N}^\star, pgcd(A, A) = A$
2) $\forall A, B \in \mathbb{N}^\star, pgcd(A, B) = pgcd(B, A)$
3) $\forall A, B \in \mathbb{N}^\star, A > B \Rightarrow pgcd(A, B) = pgcd(A - B, B)$

Rappels de cours distribués lors de l'examen écrit.

Logique de Floyd/Hoare

$$\frac{}{\{\psi\}\ skip\ \{\psi\}}\ \text{skip} \qquad \frac{}{\{[E/x]\,\psi\}\ x := E\ \{\psi\}}\ \text{assign}$$

$$\frac{\{\varphi\}\ P\ \{\chi\} \quad \{\chi\}\ Q\ \{\psi\}}{\{\varphi\}\ P\ ;\ Q\ \{\psi\}}\ \text{sequence}$$

$$\frac{\{\varphi \wedge C\}\ P\ \{\psi\} \quad \{\varphi \wedge \neg C\}\ Q\ \{\psi\}}{\{\varphi\}\ if\ C\ then\ P\ else\ Q\ fi\ \{\psi\}}\ \text{conditional}$$

$$\frac{\{\varphi \wedge C\}\ P\ \{\varphi\}}{\{\varphi\}\ while\ C\ invariant\ \varphi\ do\ P\ od\ \{\varphi \wedge \neg C\}}\ \text{partial loop}$$

$$\frac{\{\varphi \wedge C \wedge E \in \mathbb{N} \wedge V = E\}\ P\ \{\varphi \wedge E \in \mathbb{N} \wedge V < E\}}{\{\varphi \wedge P \in \mathbb{N}\}\ while\ C\ invariant\ \varphi\ variant\ P\ do\ E\ od\ \{\varphi \wedge \neg C\}}\ \text{total loop}$$

$$\frac{\varphi \to \chi \quad \{\chi\}\ P\ \{\psi\}}{\{\varphi\}\ P\ \{\psi\}}\ \text{weaken} \qquad \frac{\{\varphi\}\ P\ \{\chi\} \quad \chi \to \psi}{\{\varphi\}\ P\ \{\psi\}}\ \text{strenghen}$$

TD Mod

4.1 Preuve de programmes - Logique de Hoare

Pour le assign :

$[x+3/x](x>0)\{\underbrace{x+3}_{E}>0\}$

$x \leftarrow x+3$
$\{x>0\}$
ψ

$\{x+y-5+y>0\}$

$x \leftarrow \underbrace{x+y-5}_{E}$
$\psi\{x+y>0\}$.

Si je veux qu'une ppté $\psi_{(x)}$ soit vraie après avoir modifié x ($x \leftarrow E$), il faut qu'elle soit vraie pour E.

Partiel + terminaison = totale.

Invariant : vrai avant et ap la boucle

Exercice 1 :

Variant de boucle : $N-K$ (Variant doit être décroissant)

Invariant de boucle : $F=k! \wedge K<=N$ (Vrai avant et ap la boucle).

```
{N >= 0}
   ⇑
{1 = 0! ∧ 0 <= N}
K := 0
{1 = K! ∧ K <= N}
F := 1
{F = K! ∧ K <= N}
while K /= N LOOP
    {F = K! ∧ K <= N-1} => INV ∧ C
    {F * K+1 = (K+1)! ∧ K+1 <= N}      {V = N-(K+1)}
    K := K+1
    {F * K = K! ∧ K <= N}              {V = N-K}
    F := F * K
    {F = K! ∧ K <= N}.                 {V = N-K}
END LOOP
{F = K! ∧ K <= N ∧ ¬(K /= N)}.        {V = N-K}
   ⇓
{F = N!}
```

Exercice 2 :

```
{N >= 0}
   ⇑
{1 = N!/N! ∧ N >= 0}.
K := N
{1 = N!/K! ∧ K >= 0}.
F := 1
{F = N!/K! ∧ K >= 0}.
while (K /= 0) LOOP
    {F = N!/K ∧ K >= 1} = INV ∧ K /= 0)
    {F x K = N!/(K-1)! ∧ K >= 1}
    F : F x K.
    {F = N!/(K-1)! ∧ K-1 >= 0}.
    K := K-1
    {F = N!/K! ∧ K >= 0}
END LOOP.
{F = N!/K! ∧ K >= 0 ∧ K /= 0}.
{F = N!}
```

Variant de boucle : K

Invariant de boucle : $F = \frac{N!}{K!} \wedge K \geq 0$

$\{N \geq 0\}$

$\Uparrow$

$\{1 = \frac{N!}{N!} \wedge N >= 0\}$

$K := N$

$\{1 = \frac{N!}{K!} \wedge K >= 0\}$

$F := 1$

$\{F = \frac{N!}{K!} \wedge K >= 0\}$

while (K/=0) LOOP

$\{F = \frac{N!}{K!} \wedge K >= 1\} \Rightarrow INV \wedge (K /= 0)$

$\{F * K = \frac{N!}{(K-1)!} \wedge (K-1) >= 0\}$

$F : F * K$

$\{F = \frac{N!}{(K-1)!} \wedge (K-1) >= 0\}$ $\{V = K+1\}$

$K : K-1$

$\{F = \frac{N!}{K!} \wedge K >= 0\}$ $\{V = K\}$

END LOOP

$\{F = \frac{N!}{K!} \wedge K >= 0 \wedge \neg(K /= 0)\}$

$\Downarrow$

$\{F = N!\}$

Exercice 3 : INV : $\{X = Q * Y + R \wedge 0 \leq Q \wedge 0 \leq R < Y\}$

V : R

{

$R := R - 1$

{INV} ∧

END LOOP

$\{INV\} \wedge \neg (Y <= R)$

TD Mod

4.2. Exercice 4 : Variant de boucle : $X+Y$

Invariant de boucle : $pgcd(X,Y) = pgcd(A,B) \wedge X>0 \wedge Y>0$

$\{A>0, B>0\}$

$\Uparrow$

$\{pgcd(A,B) = pgcd(A,B) \wedge A>0 \wedge B>0\}$

$X := A$

$\{pgcd(x,B) = pgcd(A,B) \wedge x>0 \wedge B>0\}$

$Y := B$

$\{pgcd(x,y) = pgcd(A,B) \wedge x>0 \wedge y>0\}$

while $(X \mathrel{/=} Y)$ do

$\{pgcd(x,y) = pgcd(A,B) \wedge x>0 \wedge y>0 \wedge x \mathrel{/=} y\}$ car $Y>X$ ou $Y<X$

IF $X>Y$ then

$V = X+Y$ $\{pgcd(x,y) = pgcd(A,B) \wedge x>0 \wedge Y>0 \wedge X>Y\}$

$\Uparrow (3)$

$\{pgcd(x-y,y) = pgcd(A,B) \wedge x>Y \wedge Y>0\}$

$\Updownarrow$

$\{pgcd(x-y,y) = pgcd(A,B) \wedge X-Y>0 \wedge Y>0\}$

$X \leftarrow X-Y$ $X := X-Y$

$V = X-Y+Y$ $\{pgcd(x,y) = pgcd(A,B) \wedge X>0 \wedge Y>0\}$

else

$V = X+Y$ $\{pgcd(x,y) = pgcd(A,B) \wedge X>0 \wedge Y>0 \wedge \neg(X>Y)\}$

$\Uparrow (3)$

$\{pgcd(x, y-x) = pgcd(A,B) \wedge X<Y \wedge X>0\}$

$\{pgcd(x, y-x) = pgcd(A,B) \wedge Y-X>0 \wedge X>0\}$

$Y \leftarrow Y-X$ $Y := Y-X$

$V = X+Y-X$ $\{pgcd(x,y) = pgcd(A,B) \wedge X>0 \wedge Y>0\}$

End if

$\{pgcd(x,y) = pgcd(A,B) \wedge X>0 \wedge Y>0$

End

$\{pgcd(x,y) = pgcd(A,B) \wedge X>0 \wedge Y>0 \wedge \neg(X \mathrel{/=} Y)$

$\Downarrow (1)$

$\{X = Y \wedge X>0 \wedge X = pgcd(A,B)$