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
$\{X = Q \times Y + R \ \wedge \ 0 \leq Q \ \wedge \ 0 \leq R < Y\}$

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

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

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 :

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

Rappels de cours distribués lors de l'examen écrit.

1 Logique de Floyd/Hoare

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

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

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

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

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

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