

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 :

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

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

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

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

$$\begin{split} &\{X \geq 0 \land Y > 0\} \\ &Q := 0; \\ &R := X; \\ &\text{while } (Y \leq R) \text{ do} \\ &Q := Q + 1; \\ &R := R - Y \\ &\text{od} \\ &\{X = Q \times Y + R \ \land \ 0 \leq Q \ \land \ 0 \leq R < Y\} \end{split}$$



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

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

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 :

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

Rappels de cours distribués lors de l'examen écrit.

1 Logique de Floyd/Hoare

$$\frac{\{\psi\}\operatorname{skip}\{\psi\}}{\{\psi\}\operatorname{skip}\{\psi\}} \text{ skip } \frac{\{[E/x]\psi\}x := E\{\psi\}}{\{[E/x]\psi\}x := E\{\psi\}} \text{ assign } \frac{\{\varphi\}P\{\chi\} - \{\chi\}Q\{\psi\}}{\{\varphi\}P : Q\{\psi\}} \text{ sequence } \frac{\{\varphi\wedge C\}P\{\psi\} - \{\varphi\wedge\neg C\}Q\{\psi\}}{\{\varphi\}\operatorname{if} C \text{ then } P \text{ else } Q \text{ fi } \{\psi\}} \text{ conditional } \frac{\{\varphi\wedge C\}P\{\varphi\}}{\{\varphi\}\operatorname{while } C \text{ invariant } \varphi \text{ do } P \text{ od } \{\varphi\wedge\neg C\}} \text{ partial loop } \frac{\{\varphi\wedge C\wedge E\in\mathbb{N}\wedge V = E\}P\{\varphi\wedge E\in\mathbb{N}\wedge V > E\}}{\{\varphi\wedge E\in\mathbb{N}\}\operatorname{while } C \text{ invariant } \varphi \text{ variant } E \text{ do } P \text{ od } \{\varphi\wedge\neg C\}} \text{ total loop } \frac{\varphi\to\chi-\{\chi\}P\{\psi\}}{\{\varphi\}P\{\psi\}} \text{ weaken } \frac{\{\varphi\}P\{\chi\}-\chi\to\psi}{\{\varphi\}P\{\psi\}} \text{ strengthen } \frac{\{\varphi\}P\{\psi\}}{\{\varphi\}P\{\psi\}} \text{ strengthen } \frac{\{\varphi\}P\{\psi\}}{\{\psi\}} \text{ strengthen } \frac{\{\psi\}P\{\psi\}P\{\psi\}}{\{\psi\}} \text{ strengthen } \frac{\{\psi\}P\{\psi\}P\{\psi\}}{\{\psi\}}$$