Preuve de la correction de la fonction FACTORIELLE à l'aide de la logique d'Hoare

Julie Parreaux

2018-2019

Référence du développement : Winskel [Win, p. =93, section 6.6]

Leçon où on présente le développement : 927 (Terminaison et correction).
Leçon où on peut l'évoquer : 930 (Sémantique).

1 Quelques rappels sur la logique de Hoare

Cette section permet d'introduire le développement et quelques remarques autours de la logique de Hoare. Elle n'est pas à vocation d'être évoquée dans le développement.

Le système de preuve de la logique de Hoare utilise les règles de déduction suivantes [Win, p. 89] :

Règle du SKIP

$$\{A\}\text{SKIP}\{A\}$$

Règle de l'affectation

$$\{B[a/X]\}X := a\{B\}$$

Règle de la séquence

$$\frac{\{A\}c_0\{C\}\ \{C\}c_1\{B\}}{\{A\}c_0;c_1\{C\}}$$

Règle de la conditionnelle

$$\frac{\{A\wedge b\}c_0\{B\}\ \{A\wedge\neg b\}c_1\{B\}}{\{A\}\text{IF } b \text{ THEN } c_0 \text{ ELSE } c_1\{B\}}$$

Règle de la boucle WHILE

$$\frac{\{A\wedge b\}c\{A\}}{\{A\}\text{WHILE } b \text{ DO } c\{A\wedge\neg b\}}$$

Règle de la conséquence

$$\frac{\models(A\Rightarrow A')\ \{A'\}c\{B'\}\ \models(B'\Rightarrow B)}{\{A\}c\{B\}}$$

Ce développement met en évidence deux méthodes généralement utilisée dans le cadre de preuves avec la logique de Hoare : on applique les règles de droite à gauche (on part de la conclusion et on évalue le programme dans le sens inverse) et on définit un invariant qui peut paraître un peut sur défini : il contient l'invariant (la variable X contient bien un résultat partiel) et la conjonction de l'entrée et de la sortie de la boucle WHILE (X est positif (rentre dans la boucle) ou nul (sortie de la boucle)).

2 Preuve de la correction de la fonction FACTORIELLE

On souhaite étudier la correction du programme FACTORIELLE (Algorithme 1) implémenté selon les principe de la programmation impérative.

Théorème. *La fonction* FACTORIELLE *est correct, i.e.*

$$\{n \geq 0\}\text{FACTORIELLE}(n)\{Y := n!\}$$

Démonstration. Il est clair, par les deux affectations en X et en Y, que $\{n \geq 0\}X := n; Y := 1\{n \geq 0 \wedge X = n; Y = 1\}$.

Il nous faut alors montrer que $\{n \geq 0 \wedge X = n \wedge Y = 1\}w\{n \geq 0\}$ où w est l'instruction WHILE.

Algorithm 1 La fonction FACTORIELLE dans un langage impératif simple.

```
function FACTORIELLE(n)
    X := n ;
    Y := 1 ;
    while X > 0 do
        Y := Y × X ;
        X := X − 1
    end while
end function
```

Commençons par montrer que $I = \{Y \times X! = n! \wedge X \geq 0\}$ est un invariant pour la boucle WHILE. Il nous faut donc montrer que $\{I \wedge X > 0\} Y := Y \times X; X := X - 1 \{I\}$. Pour cela, on applique un principe récurrent lorsqu'on souhaite prouver la correction d'un programme par la logique de Hoare : on part de la conclusion pour remonter jusqu'aux hypothèses. En effet, les règles de déductions sont plus naturelles dans cet ordre.

1. En appliquant la règle d'assignation à X, on obtient :
$$\{I[(X-1)/X]\} X := X - 1 \{I\}$$
où $I[(X-1)/X] = \{Y \times (X-1)! = n! \wedge (X-1) \geq 0\}$.
2. En appliquant la règle d'assignation à Y, on obtient :
$$\{Y \times X \times (X-1)! = n! \wedge (X-1) > 0\} Y := Y \times X \{I[(X-1)/X]\}$$
où $\{Y \times X \times (X-1)! = n! \wedge (X-1) \geq 0\} = \{Y \times X! = n! \wedge (X-1) \geq 0\}$
3. En appliquant la règle de séquence, on obtient :
$$\{Y \times X! = n! \wedge (X-1) \geq 0\} Y := Y \times X; X := X - 1 \{I\}$$
4. On souhaite appliquer la règle de la conséquence pour conclure que I est bien un invariant.
   (a) Montrons que $I \wedge X > 0 \Rightarrow \{Y \times X! = n! \wedge (X-1) \geq 0\}$.
   $$\begin{array}{rcll} I \wedge X > 0 & \Rightarrow & Y \times X! = n! \wedge X \geq 0 \wedge X > 0 & \text{(par réécriture de } I\text{)} \\ & \Rightarrow & Y \times X! = n! \wedge X \geq 1 & \text{(par } X > 0\text{)} \\ & \Rightarrow & Y \times X! = n! \wedge (X-1) \geq 0 & \text{(par } X \geq 1\text{)} \end{array}$$
   (b) Par la règle de la conséquence, on a
   $$\{I \wedge X > 0\} Y := Y \times X; X := X - 1 \{I\}$$

On en déduit que I est un invariant de boucle.

Maintenant nous pouvons montrer que $\{n \geq 0 \wedge X = n \wedge Y = 1\} w \{n \geq 0\}$.

1. Par la règle de la boucle WHILE, on obtient que
$$\{I\} w \{I \wedge X \not> 0\}$$
2. Pour conclure, nous devons vérifier que l'invariant de boucle I est bien vérifié quand on rentre dans la boucle. De plus, la sortie de boucle doit impliqué notre post-condition. Nous allons appliquer une dernière fois la règle de la conséquence.
   (a) Montrons maintenant que I est bien vérifié lorsque nous rentrons dans la boucle la première fois, i.e. $\{n \geq 0 \wedge X = n \wedge Y = 1\} \Rightarrow I$.
   En posant dans I, $X = n$ et $Y = 1$, on obtient le résultat souhaité, i.e. $\{n \geq 0 \wedge X = n \wedge Y = 1\}$.
   (b) Montrons que l'invariant de boucle et de la sortie de boucle implique la postcondition de FACTORIELLE, i.e. $I \wedge X \not> 0 \Rightarrow Y = n!$.
   $$\begin{array}{rcll} I \wedge X \not> 0 & \Rightarrow & Y \times X! = n! \wedge X \geq 0 \wedge X \not> 0 & \text{(par réécriture de } I\text{)} \\ & \Rightarrow & Y \times X! = n! \wedge X = 0 & \text{(par } X = 0 \text{ et } X \not> 0\text{)} \\ & \Rightarrow & Y \times 0! = n! & \text{(par } X = 0\text{)} \\ & \Rightarrow & Y = n! & \text{(par } 0! = 1\text{)} \end{array}$$

(c) Par la règle de la conséquence, on obtient :

$$\{n \geq 0 \wedge X = n \wedge Y = 1\} w \{Y := n!\}$$

Par la règle de la séquence, on en déduit que

$$\{n \geq 0\} \text{FACTORIELLE}(n) \{Y := n!\}$$

□

Références

[Win] G. Winskel. *The Formal Semantics of Programming Languages*.