Exercice de preuves de programmes

Fabrice Rossi

28 mars 2013

Rappels

Interprétation

Sauf mention contraire explicite, on suppose que l'interprétation des symboles de fonctions, des symboles de constantes et des symboles de prédicats est celle de l'arithmétique dans $\mathbb{Z}$. En particulier, le symbole / désigne la division euclidienne, c'est-à-dire que $5/2$ est le quotient de la division de 5 par 2 (soit 2). Le symbole % correspond au calcul du reste de la division (par exemple $5\%2 = 1$).

Notations

On rappelle que dans les triplets de Hoare, les accolades $\{\}$ sont utilisées pour la correction partielle (on ne considère que les cas où le programme s'arrête) alors que les crochets $\langle\rangle$ sont utilisés pour la correction totale (le programme doit toujours s'arrêter).

Si F est un terme (resp. une formule) du calcul des prédicats, $F[x \leftarrow T]$ est le terme obtenu (resp. la formule obtenue) en remplaçant toutes les occurrences libres de x par T. Si on autorise les variables booléennes, T peut être une formule, sinon T est un terme.

Logique de Hoare

La logique de Hoare repose sur des règles de déduction et des axiomes. Les axiomes sont ceux de l'affectation :

$$\frac{}{\langle F[x \leftarrow T]\rangle \ \texttt{x} \ \leftarrow \texttt{T} \ \langle F\rangle} \leftarrow \text{Hoare}$$

Dans l'axiome ci-dessus, il faut que x soit une variable libre dans F.

$$\frac{}{\langle F\rangle \ \texttt{x} \ \leftarrow \texttt{T} \ \langle(\exists y, (F[x \leftarrow y] \wedge (x = T[x \leftarrow y])))\rangle} \leftarrow \text{Floyd}$$

Le reste du système consiste en les règles de déduction suivantes :

$$\frac{\langle F\rangle \ \texttt{prog1} \ \langle G\rangle \qquad \langle G\rangle \ \texttt{prog2} \ \langle H\rangle}{\langle F\rangle \ \texttt{prog1; prog2} \ \langle H\rangle} \ ;$$

$$\frac{(F \Rightarrow G) \qquad \langle G\rangle \ \texttt{prog} \ \langle H\rangle \qquad (H \Rightarrow I)}{\langle F\rangle \ \texttt{prog} \ \langle I\rangle} \Rightarrow$$

$$\frac{\langle(F \wedge b)\rangle \ \texttt{prog1} \ \langle G\rangle \qquad \langle(F \wedge (\neg b))\rangle \ \texttt{prog2} \ \langle G\rangle}{\langle F\rangle \ \texttt{if (}b\texttt{) prog1 else prog2 end if} \ \langle G\rangle} \text{ if then}$$

$$\frac{\{(I \wedge b)\}\ \texttt{prog}\ \{I\}}{\{I\}\ \texttt{while(}b\texttt{) prog end while}\ \{(I \wedge (\neg b))\}}\ \text{while partiel}$$

Dans la règle précédente, I est appelé *invariant* de la boucle.

$$\frac{\langle (I \wedge b \wedge (V = n))\rangle\ \texttt{prog}\ \langle I \wedge (V < n) \wedge (V \geq 0))\rangle}{\langle I\rangle\ \texttt{while(}b\texttt{) prog end while}\ \langle (I \wedge (\neg b))\rangle}\ \text{while total}$$

Dans cette dernière règle, V est un terme et n une variable libre qui n'est utilisée nulle part ailleurs. Comme dans la règle précédente, I est un invariant, alors que V est un *variant* de la boucle.

1 Affectation

Exercice 1

Montrer que la correction du triplet suivant :

$$\langle x - y \geq 0\rangle\ \texttt{y} \leftarrow \texttt{y+x}\ \langle 2x \geq y\rangle$$

On donnera une preuve avec la règle d'affectation de Floyd et une autre avec celle de Hoare.

Exercice 2

Donner une postcondition non triviale Q pour laquelle le triplet suivant est totalement correct (on montrera ce point) :

$$\langle x - y \geq 0\rangle\ \texttt{x} \leftarrow \texttt{y-x ; y} \leftarrow \texttt{y+x}\ \langle Q\rangle$$

2 Sélection

Exercice 3

On considère le programme suivant :

prog

```
1 if (x>0)
2   y ← 1
3 else
4   y ← -1
5 end if
```

Question 1 Montrer que le triplet suivant est totalement correct :

$$\langle x \neq 0\rangle\ \texttt{prog}\ \langle yx > 0\rangle$$

Question 2 Donner une postcondition Q non triviale telle que le triplet suivant soit totalement correct (on donnera une preuve) :

$$\langle\rangle\ \texttt{prog}\ \langle Q\rangle$$

Exercice 4

On considère le programme suivant :

prog

```
1  if (x>0)
2    y ← 1
3    x ← x + 2
4  else
5    y ← -1
6    x ← x - 2
7  end if
```

Question 1 On considère la précondition $P \equiv ((x = a) \wedge (a > 0))$. Donner une postcondition telle que $\langle P \rangle$ `prog` $\langle Q \rangle$ soit vrai, en proposant une démonstration.

Question 2 Même question pour $P \equiv (x = a)$.

Question 3 Même question pour $P = \emptyset$.

3 Correction partielle de boucles

Exercice 5

On suppose que `tab.length` donne la longueur d'un tableau et que `tab[i]` permet d'accéder à sa case numéro `i` (la numérotation commence à 0). On considère le programme suivant :

prog

```
1  i ← 0
2  x ← tab[0]
3  j ← 1
4  while(j < tab.length)
5    if(tab[j] > x)
6      x ← tab[j]
7      i ← j
8    end if
9    j ← j+1
10 end while
```

On considère la précondition $P \equiv (tab.length > 0)$ et on cherche à montrer que x contient le plus grand élément de tab après l'exécution du programme.

Question 1 Montrer que I défini par

$$I = \left(x = \max_{0 \leq k \leq j-1} tab[k] \right) \wedge (j \leq tab.length)$$

est un invariant de boucle.

Question 2 En déduire la propriété recherchée (en explicitant la postcondition Q).

Question 3 Montrer que les accès au tableau sont toujours corrects (c'est-à-dire qu'on ne tente jamais d'accéder à une case qui n'existe pas).

Question 4 Montrer que i contient après l'exécution du programme le plus petit indice k tel que $tab[k]$ contienne la plus grande valeur du tableau.

Question 5 Proposer une modification du programme qui donne à i la position du plus grand indice k tel que $tab[k]$ contienne la plus grande valeur du tableau.

Question 6 Modifier le programme pour qu'il fonctionne même quand $tab.length = 0$. Par convention, on supposera que le maximum est alors $-\infty$ (valeur supposée représentable informatiquement) et que la position du maximum est -1. On montrera la correction partielle du programme proposé.

4 Correction totale de boucles

Exercice 6

Montrer que le triplet suivant est vrai

$$\langle x \geq 0 \rangle \texttt{ while(x>0) x} \leftarrow \texttt{x-1 end while } \langle x = 0 \rangle$$

Exercice 7

Soit le programme

prog

```
1 q ← 0
2 while (y<=r)
3   r ← r - y
4   q ← q + 1
5 end while
```

Question 1 Montrer que le triplet $\langle (y > 0) \wedge (r < y) \rangle$ `prog` $\langle (q = 0) \rangle$ est vrai.

Question 2 Montrer que le triplet $\langle (y > 0) \wedge (r > 0) \rangle$ `prog` $\langle (q = r/y) \rangle$ est vrai.