Théorie de la Programmation, L3IF – TD

mercredi 17 octobre 2018

1 Induction

Definitions

Considerez les definitions inductives suivantes :

Inductive expr :

$\texttt{Const}$: nat → expr

$\texttt{Plus}$: expr → expr → expr

$\texttt{IfZero}$: expr → expr → expr → expr

$$\frac{}{eval\ (\texttt{Const}\ n)\ n} \qquad \frac{eval\ a_1\ n_1 \qquad eval\ a_2\ n_2}{eval\ (\texttt{Plus}\ a_1\ a_2)\ (n_1 + n_2)}$$

$$\frac{eval\ a_1\ 0 \qquad eval\ a_2\ n}{eval\ (\texttt{IfZero}\ a_1\ a_2\ a_3)\ n} \qquad \frac{eval\ a_1\ (S\ k) \qquad eval\ a_3\ n}{eval\ (\texttt{IfZero}\ a_1\ a_2\ a_3)\ n}$$

$$\frac{}{(\texttt{Plus}\ (\texttt{Const}\ n_1)\ (\texttt{Const}\ n_2)) \to (\texttt{Const}\ (n_1 + n_2))} \qquad \frac{a_1 \to a_1'}{(\texttt{Plus}\ a_1\ a_2) \to (\texttt{Plus}\ a_1'\ a_2)}$$

$$\frac{a_2 \to a_2'}{(\texttt{Plus}\ (\texttt{Const}\ n_1)\ a_2) \to (\texttt{Plus}\ (\texttt{Const}\ n_1)\ a_2')} \qquad \frac{a_1 \to a_1'}{(\texttt{IfZero}\ a_1\ a_2\ a_3) \to (\texttt{IfZero}\ a_1'\ a_2\ a_3)}$$

$$\frac{}{(\texttt{IfZero}\ (\texttt{Const}\ 0)\ a_2\ a_3) \to a_2} \qquad \frac{}{(\texttt{IfZero}\ (\texttt{Const}\ (S\ k))\ a_2\ a_3) \to a_3}$$

$$\frac{}{a \to^* a} \qquad \frac{a_1 \to a_2 \qquad a_2 \to^* a_3}{a_1 \to^* a_3}$$

1.1 Exercice 1

Montrez $\forall a\ b, (a \to b \Rightarrow (\forall n, eval\ a\ n \Leftrightarrow eval\ b\ n))$ par induction sur $\to$ en utilisant l'hypothese d'induction $P\ a_1\ a_2 \equiv (\forall n, eval\ a_1\ n \Leftrightarrow eval\ a_2\ n)$.

1.2 Exercice 2

Maintenant, prouvez que la relation $\to^*$ est transitive.

1.3 Exercice 3 (A la maison)

Prouvez que $\forall a, k, (a \to^* \texttt{Const}\ k) \Leftrightarrow eval\ a\ k$

2 Dériver des triplets de Hoare

2.1 Dérivations dans la logique de Hoare

Dériver les triplets suivants:

1. $\{x \geq 0\} x := x + 1;\ x := x + 1 \{x \geq 2\}$
2. $\{\} i := 0;$ `while` $i < 100$ `do` $(i := i + 1) \{i = 100\}$
3. $\{x = a, y = b\} t := x;\ x := y;\ y := t \{x = b, y = a\}$

2.2 Spécification de programmes

Spécifier le comportement attendu des programmes suivants (pré et post-conditions), puis dériver cette spécification dans la logique de Hoare.

Min-Max

```
if y < x do
  t := x;
  x := y;
  y := t
else
  skip
```

Carré

```
i := 0;
s := 0;
while i < n do
  s := s + 2i + 1;
  i := i + 1
```

Mult

```
r := 0;
k := 0;
while k ≤ n do
  r := r + k;
  k := k + 1
```

3 Correction totale

La *correction totale* d'un triplet de Hoare est notée $[A]c[A']$. Un triplet $[A]c[A']$ est *valide*, noté $\models [A]c[A']$, si pour tout σ, si $\sigma \models A$, alors il existe σ' tel que $c, \sigma \Downarrow \sigma'$, et $\sigma' \models A'$.

Noter que l'on *garantit* la terminaison du programme. Pour ce faire, on associe à chaque boucle `while` un invariant et un *variant*, quantité qui décroît strictement à chaque passage dans le corps de la boucle.

1. Inventer une règle de logique de Hoare pour la correction totale dans le cas des boucles `while`.
2. Établir la correction totale pour **Carré**.

4 À propos de la correction de la logique de Hoare

1. Montrez que pour tous c et A, le triplet de Hoare $\{\texttt{false}\}\, c\, \{A\}$ est dérivable, ce que l'on note $\vdash \{\texttt{false}\}\, c\, \{A\}$ (pas le droit pour ce faire de s'appuyer sur le résultat de complétude pour la logique de Hoare).
2. On rappelle la règle de la logique de Hoare pour la conditionnelle:
$$\frac{\vdash \{A \wedge b\}\, c_1\, \{A'\} \qquad \vdash \{A \wedge \neg b\}\, c_2\, \{A'\}}{\vdash \{A\}\, \texttt{if}\ b\ \texttt{then}\ c_1\ \texttt{else}\ c_2\, \{A'\}}$$
Que peut-on dire sur les usages de la règle ci-dessus, pour une commande de la forme $\texttt{if false then}\ c_1\ \texttt{else}\ c_2$?
3. On rappelle l'énoncé du théorème de correction pour la logique de Hoare:
$$\forall c, A, A',\ \text{si}\ \vdash \{A\}\, c\, \{A'\},\ \text{alors} \quad \forall \sigma, \sigma',\ \sigma, c \Downarrow \sigma'\ \text{implique}\ (\sigma \models A\ \Rightarrow\ \sigma' \models A')\ .$$
Il a été dit en cours qu'il était préférable de faire la preuve par induction sur la dérivation de $\vdash \{A\}\, c\, \{A'\}$, et c'est ce qui a été fait.
Imaginons que l'on fasse fi de ce conseil avisé, et que l'on fait la preuve par induction sur c. Il y a donc 5 cas.
Écrivez *rigoureusement* le cas de cette preuve où c est de la forme $\texttt{if}\ b\ \texttt{then}\ c_1\ \texttt{else}\ c_2$.

4. Supposons maintenant que l'on remplace la règle de la logique de Hoare pour la conditionnelle par la règle suivante:

$$\frac{\vdash \{A\}\, c_1\, \{A'\} \qquad \vdash \{A\}\, c_2\, \{A'\}}{\vdash \{A\}\, \texttt{if}\ b\ \texttt{then}\ c_1\ \texttt{else}\ c_2\, \{A'\}}$$

   (a) Étudiez le cas de `if then else` dans la preuve de correction de la logique de Hoare, et expliquez pourquoi cette propriété tient toujours.

   On travaillera donc avec cette version modifiée des règles de la logique de Hoare, en repartant de la preuve vue en cours, par induction sur la dérivation de $\vdash \{A\}\, c\, \{A'\}$.

   (b) Qu'en est-il de la complétude ?

   Vous pouvez considérer le triplet de Hoare suivant pour répondre à cette question:

$$\{\top\}\, \texttt{if}\ X \geq 3\ \texttt{then}\ (\texttt{if}\ X \geq 2\ \texttt{then}\ X := 0\ \texttt{else}\ X := 12)\ \texttt{else}\ X := 0\, \{X = 0\}$$