

Correction de la logique de HOARE

Antoine DEQUAY

21 septembre 2022

Notes

- Prof : Alan SCHMITT.
- Leçon : 927, 930.
- Référence :
 - NIELSON².

Théorème 1 La logique de HOARE est correcte (partiellement).

Preuve. On cherche à montrer que pour tout prédicats P, Q et toute instruction S du langage IMP, on a :

$$\vdash_H \{P\}S\{Q\} \implies \models_H \{P\}S\{Q\}.$$

On raisonne par induction sur l'arbre de preuve de $\vdash_H \{P\}S\{Q\}$.

- $[\text{aff}_H]$: On suppose qu'on a : $\langle x := a, s \rangle \rightarrow s'$ et $(P[x \mapsto \mathcal{A}[[a]]])s = \top$. On veut montrer que $P s' = \top$. Par $[\text{aff}_{ns}]$, on a $s' = s[x \mapsto \mathcal{A}[[a]]_s]$. $(P[x \mapsto \mathcal{A}[[a]]])s = Ps[x \mapsto \mathcal{A}[[a]]_s] = \top$, d'où le résultat !
- $[\text{skip}_H]$: Par la règle à grand pas, c'est évident.
- $[\text{comp}_H]$: On suppose que $\models_H \{P\}S_1\{Q\}$ et $\models_H \{Q\}S_2\{R\}$, montrons que $\models_H \{P\}S_1; S_2\{R\}$. Soit s, s'' tel que $\langle S_1; S_2, s \rangle \rightarrow s''$. Par la règle de composition de la sémantique à grand pas, il existe s' tel que $\langle S_1, s \rangle \rightarrow s'$ et $\langle S_2, s' \rangle \rightarrow s''$. Le reste s'en suit...
- $[\text{if}_H]$: On suppose que $\models_H \{\mathcal{B}[[b]] \wedge P\}S_1\{Q\}$ et $\models_H \{\neg \mathcal{B}[[b]] \wedge P\}S_2\{Q\}$, prouvons $\models_H \{P\}\text{if } b \text{ then } S_1 \text{ else } S_2\{Q\}$. Soient s, s' tels que $Ps = \top$ et $\langle \text{if } b \text{ then } S_1 \text{ else } S_2, s \rangle \rightarrow s'$.
 - Si $\mathcal{B}[[b]]_s = \top$, $(\mathcal{B}[[b]] \wedge P)s = \top$, et la règle de la sémantique à grand pas permet d'avoir $\langle S_1, s \rangle \rightarrow s'$, d'où $Qs' = \top$.
 - De même pour l'autre cas.
- $[\text{while}_H]$: On suppose $\models_H \{\mathcal{B}[[b]] \wedge P\}S\{P\}$. Soit s, s'' tels que $Ps = \top$ et $\langle \text{while } b \text{ do } S, s \rangle \rightarrow s''$. On veut montrer que $(\neg \mathcal{B}[[b]] \wedge P)s = \top$. On procède par récurrence sur l'arbre de la sémantique à grands pas.
 - Si $\mathcal{B}[[b]]_s = \perp$, alors $s = s''$, et on a bien le résultat voulu.
 - Sinon, $(\mathcal{B}[[b]] \wedge P)s = \top$, donc on peut considérer s' tel que $\langle S, s \rangle \rightarrow s'$ et $\langle \text{while } b \text{ do } S, s' \rangle \rightarrow s''$. Par hypothèse, on a $Ps' = \top$, et on peut appliquer la récurrence (finie par hypothèse, car on prouve la correction partielle). Le résultat s'en suit.
- $[\text{cons}_H]$: Ok, il suffit de l'écrire et de penser à : $\uparrow \rightarrow \downarrow$.

□