Correction des règles de Hoare

On ommet dans les assertions les notations pour les interprétations, ce qui n'a aucune conséquence dans le déroulement de la preuve. Pour le reste, la preuve est celle de [1].

Lemme 1. Soient $a, a_0 \in \text{Aexpv}$, et $X \in \text{Var}$. Alors pour tout état σ,

$$\mathcal{A}\text{v}[\![a_0[a/X]]\!]\sigma = \mathcal{A}\text{v}[\![a_0]\!]\sigma[\mathcal{A}\text{v}[\![a]\!]\sigma/X]$$

Démonstration. Induction structurelle sur a_0. □

Lemme 2. Soit $B \in \text{Assn}$, $X \in \text{Var}$ et $a \in \text{Aexp}$. Alors pour tout état σ :

$$\sigma \models B[a/X] \text{ ssi } \sigma[\mathcal{A}[\![a]\!]\sigma/X] \models B.$$

Démonstration. Induction structurelle sur B. □

Théorème 3. Soit un triplet de Hoare $\{A\}c\{B\}$. Alors $\vdash \{A\}c\{B\}$ implique $\models \{A\}c\{B\}$.

On remarque que pour montrer le théorème, il suffit de prouver que chaque règle de Hoare est correcte, car on peut alors déduire le théorème par induction sur le nombre de règles dans une preuve.

Skip : $\models \{A\}\textbf{skip}\{A\}$ est clair.

Affectation : Notons $c \equiv (\texttt{X := a})$. On a $\sigma \models B[a/X]$ ssi $\sigma[\mathcal{A}[\![a]\!]\sigma/X] \models B$ d'après le lemme 2, donc $\sigma \models B[a/X] \implies C[\![\texttt{X := a}]\!]\sigma \models B$, d'où $\models \{B[a/X]\}X := a\{B\}$.

Séquence : Supposons $\models \{A\}c\{C\}$ et $\models \{C\}c_1\{B\}$. Supposons $\sigma \models A$. Alors $C[\![c_0]\!]\sigma \models C$ car $\models \{A\}c_0\{C\}$. On a aussi $C[\![c_1]\!](C[\![c_0]\!]\sigma) \models B$ car $\models \{C\}c_1\{B\}$. D'où $\models \{A\}c_0\ c_1\{B\}$.

Conditionnelle : Supposons $\models \{A \wedge b\}c_0\{B\}$ et $\models \{A \wedge \neg b\}c_1\{B\}$. Supposons $\sigma \models A$. Ou bien $\sigma \models b$ ou bien $\sigma \models \neg b$. Dans le premier cas $\sigma \models A \wedge b$ donc $C[\![c_0]\!]\sigma \models B$. Dans le deuxième analoguement $C[\![c_1]\!]\sigma \models B$ aussi, donc $\models \{A\}$ **if** b **then** c_0 **else** $c_1\{B\}$.

Boucles While : Supposons $\models \{A \wedge b\}c\{A\}$, i.e A invariant de $w \equiv$ **while** b **do** c. On sait que $C[\![w]\!] = \lim_n \theta_n$ avec des θ_n de domaine croissant, et définis de sorte que :

$$\theta_{n+1} : \sigma \mapsto \begin{cases} \sigma & \text{si } \mathcal{B}[\![b]\!]\sigma = \textbf{false} \\ (\theta_n \circ C[\![c]\!])\sigma & \text{si } \mathcal{B}[\![b]\!]\sigma = \textbf{true}. \end{cases}$$

Montrons par induction sur n, $P(n) : \forall \sigma, \sigma' \in \Sigma$,

$$(\theta_n(\sigma) = \sigma' \text{ et } \sigma \models A) \implies (\sigma' \models A \wedge \neg b)$$

On aura alors $\sigma \models A \implies C[\![w]\!]\sigma \models A \wedge \neg b$ pour tout $\sigma \in \Sigma$, d'où $\models \{A\}w\{A \wedge \neg b\}$ comme voulu.

Cas $n = 0$. Il est très vrai. *Induction.* On suppose $P(n)$ pour un $n \geqslant 0$. Supposons $\theta_{n+1}\sigma = \sigma'$, et $\sigma \models A$. Deux cas sont possibles :

1. $\mathcal{B}[\![b]\!]\sigma = \textbf{true}$ et $\sigma' = (\theta_n \circ C[\![c]\!])\sigma$;
2. $\mathcal{B}[\![b]\!]\sigma = \textbf{false}$ et $\sigma = \sigma'$.

Montrons que dans les deux cas $\sigma' \models A \wedge \neg b$.

1. On a $\sigma \models b$ donc $\sigma \models A \wedge b$. D'où il existe $\sigma'' \in \Sigma$ tel que $\sigma'' = C[\![c]\!]\sigma$ et $\sigma' = \theta_n\sigma''$. D'où $\sigma'' \models A$ car $\models \{A \wedge b\}c\{A\}$ (hypothèse du while). Par hypothèse d'induction $\sigma' \models A \wedge \neg b$.
2. Ici $\sigma \models A \wedge \neg b$. Mais $\sigma = \sigma'$ donc c'est fini.

Conséquence : Supposons $\models (A \implies A')$ et $\models \{A'\}c\{B'\}$ et $\models (B' \implies B)$. Supposons $\sigma \models A$. Alors $\sigma \models A'$, d'où $C[\![c]\!]\sigma \models B'$ et donc $C[\![c]\!]\sigma \models B$. D'où $\models \{A\}c\{B\}$.

Références

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