CAP - Exercise: Hoare Logic (chapter 10)

Laure Gonnord

Dec. 2016

Exercise ▶ A first Hoare Proof

Let S be the following program :

$$\texttt{if} \quad (i{*}b{=}a)\ \texttt{then}\ r := \texttt{true}\ \texttt{else}\ r := \texttt{false}$$

Show that : $\{\texttt{true}\}\ S\ \{r = \texttt{true} \iff i * b = a\}$

Solution. En français, désolée On essaie de construire un arbre de preuve correct pour le triplet $\{true\}S\{post\}$ où $post = \big(r = true \iff i * b = a\big)$:

$$\dfrac{\overset{\text{Branche 1}}{\{true \land i * b = a\}r := true\{r = true \iff i * b = a\}} \qquad \overset{\text{Branche 2}}{\{true \land \neg(i * b = a)\}r := false\{r = true \iff i * b = a\}}}{\{true\}\ \text{if}\ (i * b = a)\text{then ... else ...}\{r = true \iff i * b = a\}}\ [\text{if}]$$

Ensuite :

- La branche 1 est close ssi $(true \land i * b = a) \Rightarrow post[true/r]$ (axiome de l'affectation et règle de la conséquence). Or $post[true/r] = (true = true \iff i*b = a) \equiv (i*b = a)$ et $(true \land i * b = a) \equiv i * b = a$, donc finalement on n'avait pas besoin de la conséquence et la branche 1 est close.
- La branche 2 est close car $\neg(i * b) = a \equiv post[false/r]$ (car $(false \iff P) \equiv \neg P$ en logique classique).

□

Exercise ▶ A second one

Let S be the program :

```
r :=a;
q :=0;
while (r≥ b) do
      r :=r-b;
      q :=q+1
done
```

Show $\{a = A\ \land\ b = B\ \land\ A \geq 0\ \land B\ \geq 0\}\ S\ \{A = q * B + r\ \land\ q \geq 0\ \land\ r < B\}$.

Solution. En français, désolée.

Essayons de construire un arbre de preuve pour $\{pre\}S\{post\}$, où :

— $pre = \big(a = A \wedge b = B \wedge A \geq 0 \wedge B \geq 0\big)$

— $post = \big(A = q * B + r \wedge q \geq 0 \wedge r < B\big)$

— $cond = r \geq b$

$$\dfrac{\overset{\text{Feuille 2}}{\{pre\}S_{init}\{I\}} \qquad \dfrac{\dfrac{\overset{\text{Feuille 1}}{\{I \wedge cond\}S'\{I\}}}{\{I\}\ \texttt{while}\ cond\ \texttt{do}\ S'\{\neg cond \wedge I\}}}{\{I\}\ \texttt{while}\ cond\ \texttt{do}\ S'\{post\}}\,[\text{csq}]\ \ 3\text{:}\ I \wedge \neg con}{\{pre\}S\{post\}}\,[\text{seq}]$$

Soit $I = \big(A = Bq + r \wedge q \geq 0 \wedge B = b\big)$, et il nous reste à prouver :

— $\{pre\}r := a; q := 0\{I\}$. Soit donc $I_1 = I[0/q] = (A = r \wedge b = B)$, ce qui fournit une branche axiome, et $I_2 = I_1[a/r] = (A = a \wedge B = b)$ (idem). Il reste à appliquer la règle de la conséquence avec $pre \Rightarrow I_2$.

— $\{I \wedge (r \geq b)\}S'\{I\}$ avec S' le corps de la boucle. Soit donc $I'_1 = I[q+1/q] = (A = (q+1)B + r \wedge q + 1 \geq 0 \wedge B = b)$ qui fournit une branche axiome, puis $I'_2 = I'_1[r-b/r] = (A = qB + r \wedge q + 1 \geq 0 \wedge B = b)$ (idem). A ce stade on a par construction $\{I'_2\}S'\{I\}$. Il reste à appliquer la règle de la conséquence avec $I \wedge cond \Rightarrow I'_2$ (vrai car $q \geq 0 \Rightarrow q + 1 \geq 0$)

— $(I \wedge \neg cond) \Rightarrow post$: on calcule $I \wedge \neg(r \geq b) \equiv \big(A = Bq + r \wedge q \geq 0 \wedge B = b \wedge r < b\big) \equiv \big(A = Bq + r \wedge q \geq 0 \wedge B = b \wedge r < B\big)$ (Remarquer ici que $B = b$ est indispensable dans I.)

□