

TD n°8 - Correction

Calcul de Hoare

Exercice 1 On rappelle la règle de la conditionnelle :

$$\frac{\{p \wedge f\} S_1 \{q\} \quad \{p \wedge \neg f\} S_2 \{q\}}{\{p\} \text{ if } f \text{ then } S_1 \text{ else } S_2 \text{ fi } \{q\}} \quad \text{où } p, q, f \in BExpr, S_1, S_2 \in Imp$$

Montrer sa correction.

Correction : Supposons $\models \{p \wedge f\} S_1 \{q\}$ et $\models \{p \wedge \neg f\} S_2 \{q\}$, et montrons :

$$\models \{p\} \text{ if } f \text{ then } S_1 \text{ else } S_2 \text{ fi } \{q\}$$

Soit donc une affectation σ telle que $\sigma \models p$ et $\sigma' := \llbracket \text{if } f \text{ then } S_1 \text{ else } S_2 \text{ fi} \rrbracket \sigma \neq \perp$. Il s'agit de montrer $\sigma' \models q$. D'après la règle de transition associée à la conditionnelle, on a :

$$\sigma' = \begin{cases} \llbracket S_1 \rrbracket \sigma & \text{si } \sigma \models f \\ \llbracket S_2 \rrbracket \sigma & \text{sinon} \end{cases}$$

premier cas : $\sigma \models f$. Puisque $\sigma \models p$ par hypothèse, on a $\sigma \models p \wedge f$. Or $\{p \wedge f\} S_1 \{q\}$ est valide, et $\sigma' = \llbracket S_1 \rrbracket \sigma \models q \neq \perp$, donc $\sigma' \models q$.

deuxième cas : même chose en remplaçant S_1 par S_2 et f par $\neg f$.

Exercice 2 Étant donnée une condition p et un programme S , écrire une formule de Hoare qui est valide si et seulement si l'exécution de S boucle à partir de toute affectation vérifiant p , c'est-à-dire $\llbracket S \rrbracket \sigma = \perp$ pour tout $\sigma \models p$.

Montrer par le calcul de Hoare que le programme suivant boucle dans tout contexte où la valeur de x est strictement positive :

```
while (x>0) do
  x:=x+1
od
```

Correction : Une formule possible est $\{p\} S \{\text{False}\}$. Ici, il s'agit de montrer $\{x > 0\} S \{\text{False}\}$. On utilise la règle de la boucle :

$$\frac{\{p \wedge (x > 0)\} x := x + 1 \{p\}}{\{p\} \text{ while } (x > 0) \text{ do } x := x + 1 \text{ od } \{p \wedge \neg(x > 0)\}}$$

avec $p = (x > 0)$. Il faut montrer la prémisse : les formules $\{x + 1 > 0\} x := x + 1 \{x > 0\}$ et $p \wedge (x > 0) \rightarrow x + 1 > 0$ sont valides donc la prémisse est valide (règle de conséquence).

On conclut en remarquant que $p \wedge \neg(x > 0) \rightarrow \text{False}$ est valide (puis règle de conséquence).

Exercice 3 On considère l'instruction :

```
repeat S until f \quad \text{où } f \in BExpr, S \in Imp
```

Écrire un programme IMP équivalent à cette instruction, en déduire la règle d'inférence et sa correction.

Correction : L'instruction est équivalente au programme :

$S; \mathbf{while} \neg f \mathbf{do} S \mathbf{od}$

De l'arbre de preuve :

$$\frac{\frac{\frac{\{p\} S \{q\}}{q \rightarrow q} \quad \frac{\{q\} \mathbf{while} \neg f \mathbf{do} S \mathbf{od} \{q \wedge \neg f\}}{\{q\} \mathbf{while} \neg f \mathbf{do} S \mathbf{od} \{q \wedge \neg f\}} \quad \frac{\{q \wedge \neg f\} S \{q\}}{q \wedge \neg f \rightarrow q \wedge f}}{\{q\} \mathbf{while} \neg f \mathbf{do} S \mathbf{od} \{q \wedge f\}}}{\{p\} S; \mathbf{while} \neg f \mathbf{do} S \mathbf{od} \{q \wedge f\}}$$

on déduit la règle :

$$\frac{\{p\} S \{q\} \quad \{q \wedge \neg f\} S \{q\}}{\{p\} \mathbf{repeat} S \mathbf{until} f \{q \wedge f\}} \quad \text{où } p, q, f \in BExpr, S \in Imp$$

La correction des règles utilisées dans l'arbre de preuve implique la correction de cette règle.

Exercice 4 Considérons le programme suivant :

```

y1 := 0;
y2 := 1;
y3 := 1;
while (y3 ≤ x) do
  y1 := y1 + 1;
  y2 := y2 + 2;
  y3 := y3 + y2
od

```

Nous allons montrer avec le calcul de Hoare qu'il calcule la racine carrée. Plus précisément, qu'il est partiellement correct par rapport à la pré-condition ($x \geq 0$) et à la post-condition $(y_1 * y_1 \leq x) \wedge ((y_1 + 1) * (y_1 + 1) > x)$.

Appelons S_0 le sous-programme constitué des 3 premières instructions, et S le sous-programme qui forme le corps de la boucle **while**.

1. Calculer les valeurs que prennent les variables y_1 , y_2 et y_3 au début des premières exécutions du corps du **while**. Conjecturer la valeur de y_2 et y_3 en fonction de y_1 . On note p la conjonction de ces 2 égalités et de $(y_1 * y_1 \leq x)$.
2. p va être l'invariant de la boucle. C'est-à-dire que l'on va montrer :

$$\{p\} \mathbf{while} (y_3 \leq x) \mathbf{do} S \mathbf{od} \{p \wedge \neg(y_3 \leq x)\}$$

en utilisant la règle d'inférence du **while**. Ecrire la prémisse que l'on doit utiliser, et la montrer par le calcul de Hoare (indication : partir de la post-condition pour trouver les conditions intermédiaires).

3. Montrer par le calcul de Hoare que p est vérifié après les 3 premières instructions du programme, sous la condition $(x \geq 0)$. C'est-à-dire, montrer que $\{x \geq 0\} S_0 \{p\}$ est valide.
4. Conclure.

Correction :

1. $y_2 = 2 * y_1 + 1$ et $y_3 = (y_1 + 1)^2$. Donc p est :

$$\underbrace{(y_2 = 2 * y_1 + 1)}_{f_1} \wedge \underbrace{(y_3 = (y_1 + 1) * (y_1 + 1))}_{f_2} \wedge \underbrace{(y_1 * y_1 \leq x)}_{f_3}$$

2. La règle s'écrit ici :

$$\frac{\{p \wedge (y_3 \leq x)\} S \{p\}}{\{p\} \text{ while } (y_3 \leq x) \text{ do } S \text{ od } \{p \wedge \neg(y_3 \leq x)\}}$$

On part de la fin de S . Par simples applications de la règle de l'affectation, on a :

$$\begin{array}{lll} \{p'\} & y_3 := y_3 + y_2 & \{p\} \\ \{p''\} & y_2 := y_2 + 2 & \{p'\} \\ \{p'''\} & y_1 := y_1 + 1 & \{p''\} \end{array}$$

avec

$$\begin{array}{llll} p' = & f_1 & \wedge & (y_3 + y_2 = (y_1 + 1)^2) & \wedge & f_3 \\ p'' = & (y_2 + 2 = 2 * y_1 + 1) & \wedge & (y_3 + y_2 + 2 = (y_1 + 1)^2) & \wedge & f_3 \\ p''' = & (y_2 + 2 = 2 * (y_1 + 1) + 1) & \wedge & (y_3 + y_2 + 2 = (y_1 + 2)^2) & \wedge & ((y_1 + 1)^2 \leq x) \end{array}$$

ce qui, par règle de composition, donne $\{p'''\} S \{p\}$.

Or $p''' \models (y_2 = 2 * y_1 + 1) \wedge (y_3 = (y_1 + 1)^2) \wedge (y_3 \leq x)$ c'est-à-dire $f_1 \wedge f_2 \wedge (y_3 \leq x)$. Mais cette formule est une conséquence de $p \wedge (y_3 \leq x)$. Donc par règle de conséquence on obtient la prémisse $\{p \wedge (y_3 \leq x)\} S \{p\}$.

3. En remontant, on obtient facilement :

$$\begin{array}{llll} \{(1 = 1) \wedge (1 = 1) \wedge (0 \leq x)\} & y_1 := 0 & \{(1 = 2 * y_1 + 1) \wedge (1 = (y_1 + 1)^2) \wedge f_3\} \\ \{(1 = 2 * y_1 + 1) \wedge (1 = (y_1 + 1)^2) \wedge f_3\} & y_2 := 1 & \{f_1 \wedge (1 = (y_1 + 1)^2) \wedge f_3\} \\ \{f_1 \wedge (1 = (y_1 + 1)^2) \wedge f_2\} & y_3 := 1 & \{p\} \end{array}$$

La première condition étant équivalente à $(x \geq 0)$, on conclut par règles de conséquence et de composition, que $\{x \geq 0\} S_0 \{p\}$ est valide.

4. En composant les 2 morceaux, on obtient la validité de :

$$\{x \geq 0\} P \{p \wedge y_3 > x\}$$

On conclut en utilisant la validité de la formule $p \wedge \neg(y_3 \leq x) \rightarrow (y_1 * y_1 \leq x) \wedge ((y_1 + 1) * (y_1 + 1) > x)$ et la règle de conséquence. Ouf.