TD 15 : Sémantique axiomatique et logique de Hoare

{lionel.rieg,paolo.tranquilli}@ens-lyon.fr

Exercice 1. *Rappels de cours*

1. Rappeler la définition de $\vDash \{P\}\ C\ \{Q\}$.

2. Expliquer sous quelles conditions on a :

a) $\vDash \{P\}\ C\ \{\texttt{true}\}$;

b) $\vDash \{P\}\ C\ \{\texttt{false}\}$;

c) $\vDash \{\texttt{true}\}\ C\ \{P\}$;

d) $\vDash \{\texttt{false}\}\ C\ \{P\}$.

3. Donner les règles associées aux commandes usuelles de **IMP** pour la logique de Hoare.

4. Proposer un programme `swap` qui échange X et Y et en valider le comportement.

5. Proposer un programme qui calcule la factorielle et en valider le comportement.

6. Que faut-il rajouter aux formules pour prendre en compte l'allocation des variables (commandes **malloc** et **free**) afin d'assurer qu'une affectation ne se fait que sur une variable allouée ?

Exercice 2. *Valider des programmes*

Valider le comportement des programmes suivants, en montrant $\vdash \{n \geq 0\}\ C\ \{z = a^n\}$ pour les deux premiers et ce qu'il faut pour le dernier.

```
k := 0;
z := 1;
while k <> n do
  z := z * a;
  k := k + 1;
done
```

```
k := n;
z := 1;
x := a;
while k <> 0 do
  if pair(k) then
    skip
  else
    z := z * x
  fi;
  x := x * x;
  k := k / 2
  done
```

```
x := a;
y := b;
while x <> y do
  if y > x then
    y := y - x
  else
    x := x - y
  fi
  done
```

Exercice 3. *Terminaison*

La validité d'un triplet a été définie en cours comme suit :

$$\vDash \{P\}\ C\ \{Q\} \quad \equiv \quad \forall \sigma\, \sigma',\ \sigma \vDash P\ \Rightarrow\ \langle C, \sigma\rangle \to \sigma'\ \Rightarrow\ \sigma' \vDash Q.$$

Lorsque l'on s'intéresse à la terminaison des programmes, on peut définir $[P]\ C\ [Q]$ comme « partant d'un état qui satisfait P, le programme C termine et atteint un état satisfaisant Q ».

1. Définir formellement cette notion de validité.

2. Proposer de nouvelles règles pour la boucle.

3. Utilisez votre proposition pour prouver la terminaison des trois programmes de l'exercice précédent (lorsqu'ils terminent).

4. La validité d'un triplet $\{P\}\ C\ \{Q\}$ est-elle décidable ? Et celle d'un triplet $[P]\ C\ [Q]$?

Exercice 4. *Complétude*

La *plus faible pré-condition* d'un programme C et d'une formule Q, notée $\mathrm{wp}(C, Q)$, est l'ensemble des états σ tels que C mène à un état σ' satisfaisant Q :

$$\mathrm{wp}(C, Q) \stackrel{def}{=\!=} \{\ \sigma \mid \forall \sigma', \langle C, \sigma\rangle \to \sigma' \Rightarrow \sigma' \vDash Q\ \}.$$

Un langage logique est dit *suffisamment expressif* lorsque ces ensembles d'états peuvent être caractérisés par des formules, i.e., si pour tous C, Q il existe une formule P telle que

$$\sigma \in \mathrm{wp}(C, Q)\ \iff\ \sigma \vDash P.$$

Par abus de notation, on note également $\mathrm{wp}(C, Q)$ cette formule. Le langage de formules vu en cours est suffisamment expressif, mais $\mathrm{wp}(C, Q)$ est généralement illisible, à cause du cas de la boucle. Ainsi, on va prendre **IMP** sans boucles dans la suite.

1. Déterminer ce que valent les pré-conditions suivantes.
wp(skip, Q) wp(X:=a, Q) wp(C_1; C_2, Q) wp(**if** b then C_1 **else** C_2, Q)

2. Pour toute commande C et toute post-condition Q, montrer $\vdash \{\mathrm{wp}(C, Q)\}\ C\ \{Q\}$.

3. Montrer que $\vDash \{P\}\ C\ \{Q\}$ ssi $\vDash P \Rightarrow \mathrm{wp}(C, Q)$.

4. Énoncer et prouver le théorème de complétude. Que faire pour la boucle ?

Exercice 5. *Logique de séparation*

On veut étendre notre logique de Hoare pour parler de certaines propriétés de la mémoire. Celle-ci sera représentée par un tableau contigü de cellules mémoires. On rajoute donc au calcul des prédicats standard les symboles : **emp** (tas vide), $e \mapsto e'$ (l'adresse e contient la valeur e' où e et e' sont des expressions), $P \star Q$ (le tas peut être séparé en deux parties disjointes qui vérifient respectivement les formules P et Q), $P \mathrel{-\!\!\star} Q$ (si on étend le tas avec un tas satisfaisant P le tas étendu satisfait Q).

1. Inventer la règle de la logique de Hoare pour $\star$.

2. Pourquoi la règle $\dfrac{\{P\}\ C\ \{Q\}}{\{P \wedge R\}\ C\ \{Q \wedge R\}}$ n'est pas correcte ?

3. Les formules/règles suivantes sont elles correctes, si non, trouver des contre-exemples.

$$p \to (p \star p) \qquad (p \star q) \to p \qquad (p_1 \vee p_2) \star q \to (p_1 \star q) \vee (p_2 \star q) \qquad \frac{p_1 \star p_2 \to p_3}{p_1 \to (p_2 \mathrel{-\!\!\star} p_3)}$$

4. Pourquoi $\{\ x \mapsto [1, 2] \star ((x \mapsto [3, 4]) \mathrel{-\!\!\star} p)\ \}[x] := 3; [x + 1] := 4\{\ p\ \}$?