MPRI - TD Logique de Hoare Probabiliste (tiré de l'examen 21-22)

Exercice 1 : Correction du calcul de plus faible espérance (Issu de la thèse de Claire Jones, 1989) - 8 points

On considère le langage probabiliste suivant:

$$\begin{array}{rcl} E & ::= & \texttt{true} \mid \texttt{false} \mid n \mid x \mid E\, op\, E \mid \texttt{bernoulli p} \\ op & ::= & + \mid - \mid * \mid = \mid \leqslant \mid \textit{and} \mid \textit{not} \\ P & ::= & \texttt{skip} \mid x := E \mid P; P \mid \texttt{if } E \texttt{ then } P \texttt{ else } P \mid \texttt{while } E \texttt{ do } P \end{array}$$

Les **valeurs** sont $Val = \{\texttt{true}, \texttt{false}, n\}$.
Un **état** est une fonction des variables libres d'un programme dans les valeurs: $s : Var \to Val$.
On définit la mise à jour de la valeur de x par v dans l'état s par:
$s[x \mapsto v]$ est l'état dont la variable x est associée à v et les autres variables sont associées à la même valeur que dans s.
On note S l'ensemble des états et $\mathcal{V}(S) = (\mathbb{R}_+^\infty)^S$ l'ensemble des **facteurs**, c'est-à-dire des fonctions de S dans les réels positifs ou infinis.

Sémantique. On note $\mathbb{P}(E(s), v)$ la probabilité que l'expression E dans l'environnement s s'évalue vers la valeur v. Par exemple,

- Si $E = (n + m)$ et $s = [n \mapsto 2; m \mapsto 3]$, alors on a $\mathbb{P}(E(s), 5) = 1$ et $\mathbb{P}(E(s), 6) = 0$
- Si $E = (\texttt{bernoulli p or x})$ et $s = [x \mapsto \texttt{false}]$, alors on a $\mathbb{P}(E(s), \texttt{true}) = p$ et $\mathbb{P}(E(s), \texttt{false}) = 1 - p$

On note $\chi_s : S \to \mathbb{R}_+^\infty$ le facteur défini par: $\chi_s(s') = \begin{cases} 1 & \text{si } s = s' \\ 0 & \text{sinon} \end{cases}$

La sémantique $[\![P]\!] : S \to \mathcal{V}(S)$ d'un programme P est définie par induction sur la structure de P de la façon suivante: pour tous états s et s',

$$\begin{aligned} [\![\texttt{skip}]\!](s)(s') &= \chi_s(s') \\ [\![\texttt{x:=E}]\!](s)(s') &= \sum_{v \in Val} \chi_{s'}(s[x \mapsto v])\mathbb{P}(E(s), v) \\ [\![\texttt{P;Q}]\!](s)(s') &= \sum_{t \in S} [\![P]\!](s)(t)\ [\![Q]\!](t)(s') \\ [\![\texttt{if E then P else Q}]\!](s)(s') &= \mathbb{P}(E(s), \texttt{true})\, [\![P]\!](s)(s') + \mathbb{P}(E(s), \texttt{false})\, [\![Q]\!](s)(s') \\ [\![\texttt{while E do P}]\!](s)(s') &= \bigcup_n f_n(s)(s') \end{aligned}$$

$$\text{avec } f_0(s)(s') = 0 \quad \text{et} \quad f_{n+1}(s)(s') = \mathbb{P}(E(s), \texttt{true}) \sum_{t \in S} [\![P]\!](s)(t)\, f_n(t, s') + \mathbb{P}(E(s), \texttt{false})\chi_s(s')$$

Logique de Hoare probabiliste. Étant donnés des facteurs $f, g : S \to \mathbb{R}_+^\infty$ et programme P, on définit le système de preuve des triplets de Hoare probabilistes $f[P]g$ par les règles sur la figure page suivante.

Calcul de plus faible préfacteur Étant donnés un programme P et un facteur g, on définit le facteur $\texttt{wp}(P, g)$ par induction sur la structure de P:

$$\begin{aligned} &\texttt{wp}(\texttt{skip}, g) = g \\ &\texttt{wp}(\texttt{x:=E}, g) = \lambda s. \sum_{v \in Val} g(s[x \mapsto v]\mathbb{P}(E(s), v) \\ &\texttt{wp}(\texttt{P;Q}, g) = \texttt{wp}(\texttt{Q}, \texttt{wp}(\texttt{P}, g)) \\ &\texttt{wp}(\texttt{if E then P else Q}, g) = \mathbb{P}(E, \texttt{true})\texttt{wp}(P, g) + \mathbb{P}(E, \texttt{false})\texttt{wp}(P, g) \\ &\texttt{wp}(\texttt{while E do P}, g) = \bigvee f_n \text{ where } \begin{cases} f_0 = \lambda s.0 \\ f_{n+1} = \mathbb{P}(E, \texttt{true})\texttt{wp}(\texttt{P}, f_n) + \mathbb{P}(E, \texttt{false})g \end{cases} \end{aligned}$$

SKIP RULE

$$\frac{}{f\ \texttt{[skip]}\ f}$$

ASSIGN RULE

$$\frac{}{h\ \texttt{[x:=E]}\ g} \text{ where } h(s) = \sum_{v \in Val} g(s[x \mapsto v]\mathbb{P}(E(s), v)$$

SEQUENCE RULE

$$\frac{f\ \texttt{[P]}\ g \qquad g\ \texttt{[Q]}\ h}{f\ \texttt{[P;Q]}\ h}$$

IF RULE

$$\frac{f\ \texttt{[P]}\ g \qquad f'\ \texttt{[Q]}\ g}{\mathbb{P}(E, \texttt{true})f + \mathbb{P}(E, \texttt{false})f'\ \texttt{[if E then P else Q]}\ h}$$

WHILE RULE

$$\frac{f_{n+1}\ \texttt{[P]}\ \mathbb{P}(E, \texttt{true})f_n + \mathbb{P}(E, \texttt{false})k}{\mathbb{P}(E, \texttt{true})\bigvee_n f_n + \mathbb{P}(E, \texttt{false})k\ \texttt{[while E do P]}\ k} \text{ where } \begin{cases} f_0 = \lambda s.0 \\ \bigvee_n f_n = \lambda s. \sup_n f_n(s) \end{cases}$$

CONSEQUENCE RULE

$$\frac{f\ \texttt{[P]}\ g}{f'\ \texttt{[P]}\ g'} \qquad \text{where } \forall s,\ f'(s) \leqslant f(s) \text{ and } g(s) \leqslant g'(s)$$

Questions

1. Démontrer la **correction**:

   Si $f\,\texttt{[P]}\,g$ est dérivable dans la logique de Hoare, alors $\forall s \in S,\ \sum_{s' \in S} g(s')\, [\![P]\!]\,(s)(s') \geqslant f(s)$.

   Vous raisonnerez par induction sur la structure de la preuve de $f[P]g$. Vous indiquerez l'hypothèse d'induction et traiterez trois cas au choix.

2. Démontrer la **complétude**:

   Si $\forall s \in S,\ \sum_{s' \in S} g(s')\, [\![P]\!]\,(s)(s') \geqslant f(s)$, alors $f\,\texttt{[P]}\,g$ est dérivable dans la logique de Hoare.

   Vous raisonnerez par induction sur la structure du programme P. Vous indiquerez l'hypothèse d'induction et traiterez trois cas au choix.

3. Montrer que

   $$\texttt{wp}(P, g) = \sup\{h \mid h[P]g\}.$$

   Vous raisonnerez par induction sur la structure du programme P. Vous traiterez trois cas au choix.

4. En déduire le **théorème de dualité**:

   $$\texttt{wp}(\texttt{P}, g) = \lambda s. \sum_{s' \in S} g(s')\, [\![P]\!]\,(s)(s')$$

5. On note $\lambda s.1$ le facteur constant qui associe 1 à tout environnement s. Montrer en utilisant le théorème de dualité que $\texttt{wp}(P, \lambda s.1)(s)$ est la probabilité que le programme P termine en partant d'un état s.

6. On considère le programme `P`, défini par

   ```
   n:=1 ; while (bernoulli p) do n:=n+1
   ```

   Étant donné un facteur g, calculer $\texttt{wp}(\texttt{P}, g)$.

   Quelle est la probabilité que ce programme termine ?

7. Donner une implémentation de l'algorithme de l'exercice 2 et calculer la probabilité que ce programme termine.