Ensimag 2A ISI Mai 2011

Sémantique et Analyse de programmes

Durée : 3h.
Documents : tous documents autorisés.

Exercice 1 (4 points) Calcul d'intervalles
Soit le programme suivant :

```
y = x + 3;
z = x - y;
```

▷ **Question 1** (1 points) Donnez les bornes $[l_z, u_z]$ du plus petit intervalle contenant z, en fonction des bornes $[l_x, u_x]$ sur x.

▷ **Question 2** (4 points)

(a) En ne vous intéressant qu'à la première ligne du programme, donnez les bornes $[l_y, u_y]$ du plus petit intervalle contenant y, en fonction des bornes $[l_x, u_x]$ sur x.

(b) En ne vous intéressant qu'à la deuxième ligne du programme (donc, en ignorant ce que fait la première), donnez les bornes $[l_z, u_z]$ du plus petit intervalle contenant z, en fonction des bornes $[l_y, u_y]$ sur y.

(c) En ne vous basant que les bornes obtenues aux points a et b, donnez les bornes d'un intervalle contenant z, en fonction des bornes $[l_x, u_x]$ sur x.

(d) Commentez les éventuelles différences avec les bornes obtenues à la question 1.

▷ **Question 3** (2 points)

Soit la boucle suivante, où n est une constante entière ($\mathbb{Z}$) :

```
x = 0;
while(x >= n) { x = x-1; }
```

Donnez, en fonction de n, le plus petit intervalle invariant (inductif) de boucle $[l_x, u_x]$. Nous vous rappelons qu'un tel invariant doit contenir les valeurs initiales des variables à l'entrée dans la boucle, et être stable par passage à l'itération suivante.

Exercice 2 (5 points)Sémantique concrète par relation entrée-sortie

Soit un programme P dont l'ensemble des états des variables est X ; par exemple, si P calcule sur 3 variables entières, X sera $\mathbb{Z}^3$. Soit $[\![P]\!]$ la relation entre les entrées et les sorties du programme : il s'agit donc d'un sous-ensemble de $X \times X$. Autrement dit, $(x, x') \in [\![P]\!]$ si et seulement si le programme peut arriver dans l'état final x' en étant lancé dans l'état initial x.

Nous supposerons dans cette partie que les opérations des programmes sont des opérations entières idéales, c'est-à-dire que $+$, $-$ etc. ont leur sens mathématique habituel sur $\mathbb{Z}$.

▷ **Question 1** Soit $x \in X$ tel qu'il n'y a aucun $x' \in X$ tel que $(x, x') \in [\![P]\!]$. Interprétez ce comportement : qu'est-ce que cela veut dire sur l'exécution du programme sur cette entrée, en termes simples et intuitifs ?

▷ **Question 2** Soit $x \in X$ tel qu'il y a $x'_1, x'_2 \in X$ tels que $x_1 \neq x_2$, $(x, x'_1) \in [\![P]\!]$ et $(x, x'_2) \in [\![P]\!]$. Interprétez ce comportement : que dire du déterminisme du programme ?

▷ **Question 3** Pour cette question uniquement, prenons le programme suivant, avec trois variables $(x, y, z) \in \mathbb{Z}^3$:

Listing 1 – Programme P_1

```
y = x;
z = x - y;
```

1. Calculez l'ensemble défini par :

$$\{x \in \mathbb{Z} \mid (x, x, 1) \in [\![P_1]\!]\} \tag{1}$$

2. Calculez l'ensemble défini par :

$$\{x \in \mathbb{Z} \mid (x, x, 0) \in [\![P_1]\!]\} \tag{2}$$

▷ **Question 4** Soit $X_0 \subseteq X$ un ensemble d'états initiaux. Nous définissons :

$$\phi(X_1) = X_0 \cup \{x' \mid \exists x \in X_1 \ (x, x') \in [\![P]\!]\} \tag{3}$$

Montrez que, quelle que soit $[\![P]\!]$, la fonction ϕ définie ci-dessus est toujours monotone (c'est-à-dire que si $X \subseteq Y$, $\phi(X) \subseteq \phi(Y)$).

▷ **Question 5** Soient P_1 et P_2 deux programmes. Soit $P_1; P_2$ le programme exécutant d'abord P_1, puis P_2. Définissez $[\![P_1; P_2]\!]$ à l'aide de $[\![P_1]\!]$ et $[\![P_2]\!]$.

Considérons une boucle :

```
while (condition) {
  P
}
```

Nous supposons que condition ne peut produire d'effets de bord. Nous noterons alors $[\![\text{condition}]\!]$ l'ensemble des éléments de X tels que la condition est réalisée. Pour $Y \subseteq X$, nous noterons $X \setminus Y$ le complémentaire de Y dans X.

▷ **Question 6** Exprimez l'ensemble des états accessibles à la sortie de la boucle à l'aide de l'ensemble X_0 des états initiaux, de $[\![\text{condition}]\!]$, de $[\![P]\!]$.

(Nous rappelons que toute fonction monotone f a un plus petit point fixe, noté lfp f.)

Exercice 3 (7 points) Preuve de programmes

On s'intéresse au tri par sélection d'un tableau t défini sur l'intervalle $1..n$ avec $n > 0$. Soit le programme suivant :

```
i:= 1;
while i<n do
   j:=i+1 ;
   while j < n+1 do
      if t(j]< t[i] then
         tmp := t[i] ;
         t[i] := t[j] ;
         t[j] := tmp ;
      end ;
      j:=j+1 ;
   variant ...                --1
   invariant ...              --2
   end
 -- assertion 1
   i:=i+1
variant ...                   --3
invariant ...                 --4
end
```

▷ **Question 1** (2 points) Donner une expression entière (dans $\mathbb{N}$) qui permet d'établir la terminaison de la boucle la plus imbriquée (variant 1). Compléter les invariants (2 et 4) permettant de prouver cette terminaison. On posera clairement toutes les formules à établir et on justifiera leur validité.

▷ **Question 2** (2 points) On note $P(u)$ le prédicat suivant :

$$\forall k \;.\; (k \in i..u \Rightarrow t[i] \leq t[k])$$

Montrer que la formule $P(j-1)$ est un invariant de la boucle la plus imbriquée (invariant 2). En déduire que l'on peut établir après cette boucle (assertion 1) la formule : $P(n)$.

On supposera ici qu'on peut établir que les cases $t[i]$ et $t[j]$ sont disjointes. On pourra donc considérer dans les formules et les affectations que $t[i]$ et $t[j]$ sont représentées par des variables.

▷ **Question 3** (2 points) On note $P(u_1, u_2)$ le prédicat suivant :

$$\forall k, l \;.\; (k \in 1..u_1 \wedge \; j \in 1..u_2 \wedge \; l < k \Rightarrow t[l] \leq t[k])$$

Montrer que la formule $P(i, j)$ est un invariant de la boucle la plus imbriquée (invariant 2).

▷ **Question 4** (2 points)

Et on veut établir la postcondition $P(n, n)$. Compléter l'invariant 4 permettant d'établir cette postcondition. Justifier en quoi la formule proposée est bien un invariant.

Comment faudrait-il compléter la postcondition pour garantir que le programme proposé effectue bien un tri du tableau ? On pourra utiliser la notation $t0$ pour désigner la valeur initiale du tableau.

Exercice 4 (4 points) Vérification et test ?