Cours Modélisation et vérification des systèmes informatiques
Exercices
Annotation, Contrat, modélisation et vérification (rÃ©vision)
par Dominique Méry
24 novembre 2023

Exercice 1 *Evaluer la validité de chaque annotation dans les questions suivent.*

Question 1.1

$\ell_1 : x = 64 \ \wedge \ y = x{\cdot}z \ \wedge z = 2{\cdot}x$
$Y := X{\cdot}Z$
$\ell_2 : \ y{\cdot}z = 2{\cdot}x{\cdot}x{\cdot}z$

Question 1.2

$\ell_1 : x = 2 \ \wedge \ y = 4$
$Z := X{\cdot}Y{+}3{\cdot}Y{\cdot}Y{+}3{\cdot}X{\cdot}Y{\cdot}Y{+}X^6$
$\ell_2 : \ z = 6{\cdot}(x{+}y)^2$

Question 1.3

$\ell_1 : x = z \ \wedge \ y = x{\cdot}z$
$Z := X{\cdot}Y{+}3{\cdot}Y{\cdot}Y{+}3{\cdot}X{\cdot}Y{\cdot}Y{+}Y{\cdot}X{\cdot}Z{\cdot}Z{\cdot}X;$
$\ell_2 : \ z = (x{+}y)^3$

Exercice 2 *Soit l'annotation suivante :*

$\ell_1 : x = 1 \wedge y = 2$
$X := Y{+}2$
$\ell_2 : x{+}y \geq m$

où m est un entier ($m \in \mathbb{Z}$).

Question 2.1 *Ecrire la condition de vérification correspondant à cette annotation en upposant que X et Y sont deux variables entières.*

Question 2.2 *Etudier la validité de cette condition de vérification selon la valeur de m.*

Exercice 3

Question 3.1 *Montrer que chaque annotation est correcte ou incorrecte selon les conditions de vérifications énoncées comme suit* $\forall x, y, z, x', y', z'.P_{\ell_1}(x, y, z) \ \wedge \ cond_{\ell,\ell'}(x, y, z) \ \wedge (x', y', z') = f_{\ell,\ell'}(x, y) \Rightarrow P_{\ell'}(x', y', z')$

—

$\ell_1 : x = 1000 \ \wedge \ y = z{+}x \ \wedge z = 2{\cdot}x$
$y := z{+}x$
$\ell_2 : x = 2000/2 \ \wedge \ y = x{+}2{\cdot}1000$

Question 3.2 *Soit trois variables x,y,z qui ont des valeurs entières a priori. L'annotation est correcte si la propriété suivante est vraie :* $\forall x, y, z, x', y', z'.P_{\ell_1}(x, y, z) \ \wedge \ cond_{\ell,\ell'}(x, y, z) \ \wedge (x', y', z') = f_{\ell,\ell'}(x, y) \Rightarrow P_{\ell'}(x', y', z')$

$\ell_1 : x = 25 \ \wedge \ z = 2{\cdot}c \ \wedge y = (z{+}1)^2$
$y := x{+}z{+}1$
$\ell_2 : x = 25 \ \wedge \ z = 2{\cdot}c \wedge y = (c{+}1)^2$

En utilisant la condition de vérification, déterminer la valeur ou les valeurs de c pour que l'annotation soit correcte.

Exercice 4

Soit l'annotation suivante. On suppose que a et b sont des constantes entières et que x, y, z et t sont des variables entières.

$\ell_1 : x = a \wedge z = x^2 \wedge y = b{\cdot}b \wedge t = b$
$Y := X{\cdot}Z{+}3{\cdot}Z{\cdot}T{+}3{\cdot}X{\cdot}Y{+}Y{\cdot}T$
$\ell_2 : y = (t{+}x)^3$

Question 4.1 *Montrer que l'annotation est correcte ou incorrecte selon les conditions de vérifications énoncées comme suit*
$\forall v, v'.P_\ell(v) \ \wedge \ cond_{\ell,\ell'}(v) \ \wedge \ v' = f_{\ell,\ell'}(v) \Rightarrow P_{\ell'}(v')$. *Vous devez répondre en énonçant et en démontrant les conditions de vérification c'est-à-dire en indiquant les differents pas de transformation.*

Question 4.2 *Soit le module suivant qui est à compléter aux points indiqués :*

```
------------------------------ MODULE examen2021q1 ------------------
EXTENDS Naturals,Integers
CONSTANTS a,b,mini,maxi
VARIABLES  x,y,z,t,pc
---------------------------------------------------------------------
al0l1 == POINT1
---------------------------------------------------------------------- next == al0l1
init == POINT2
---------------------------------------------------------------------
i ==  POINT3
Safetypc ==  POINT4
Safetyrte == POINT5
=============================================
```

Donner les cinq points à compléter pour vérifier l'annotation avec TLC.

Question 4.3 *On propose de vérifier l'annotation en utilisant une traduction via le traducteur d'algorithmes annotés PlusCal en TLA. Ecrire un algorithme PlusCal qui permet de réaliser cette vérification.*

Exercice 5

VARIABLES N, V, S, I

$$pre(n_0, v_0, s_0, i_0) \stackrel{def}{=} \begin{cases} n_0 \in \mathbb{N} \wedge n_0 \neq 0 \\ v_0 \in 0..n_0{-}1 \longrightarrow \mathbb{Z} \\ s_0 \in \mathbb{Z} \wedge i_0 \in \mathbb{Z} \end{cases}$$

$$\textit{REQUIRES} \begin{pmatrix} n_0 \in \mathbb{N} \wedge n_0 \neq 0 \\ v_0 \in 0..n{-}1 \longrightarrow \mathbb{Z} \end{pmatrix}$$

$$\textit{ENSURES} \begin{pmatrix} s_f = \prod_{k=0}^{n_0-1} v_0(k) \\ n_f = n_0 \\ v_f = v_0 \end{pmatrix}$$

$$\ell_0 : \begin{pmatrix} pre(n_0, v_0, s_0, i_0) \\ (n, v, s, i) = (n_0, v_0, s_0, i_0) \end{pmatrix}$$

$S := V(0)$

$$\ell_1 : \begin{pmatrix} pre(n_0, v_0, s_0, i_0) \\ caches = \prod_{k=0}^{0} v(k) \\ (n, v, i) = (n_0, v_0, i_0) \end{pmatrix}$$

$I := 1$

$$\ell_2 : \begin{pmatrix} pre(n_0, v_0, s_0, i_0) \\ s = \prod_{k=0}^{i-1} v(k) \wedge i = 1 \\ (n, v) = (n_0, v_0) \end{pmatrix}$$

WHILE $I < N$ *DO*

$$\ell_3 : \begin{pmatrix} pre(n_0, v_0, s_0, i_0) \\ s = \prod_{k=0}^{i-1} v(k) \wedge i \in 1..n{-}1 \\ (n, v) = (n_0, v_0) \end{pmatrix}$$

$S := S{\cdot}V(I)$

$$\ell_4 : \begin{pmatrix} pre(n_0, v_0, s_0, i_0) \\ \\ (n, v) = (n_0, v_0) \end{pmatrix}$$

$I := I{+}1$

$$\ell_5 : \begin{pmatrix} pre(n_0, v_0, s_0, i_0) \\ \\ (n, v) = (n_0, v_0) \end{pmatrix}$$

OD;

$$\ell_6 : \begin{pmatrix} pre(n_0, v_0, s_0, i_0) \\ s = \prod_{k=0}^{n-1} v(k) \wedge i = n \\ (n, v) = (n_0, v_0) \end{pmatrix}$$

Question 5.1 *Compléter les annotations incomplètes ℓ_1, ℓ_4 et ℓ_5.*

Question 5.2 *Vérifier les conditions de vérification associées aux transitions suivantes :*

1. ℓ_0, ℓ_1
2. ℓ_2, ℓ_3
3. ℓ_3, ℓ_4
4. ℓ_5, ℓ_6

Question 5.3 *Donner et vérifier les points pour assurer la correction partielle de cet algorithme.*

Question 5.4 *Que faut-il faire pour vérifier que cet algorithme est bien annoté et qu'il est partiellement correct en utilisant TLA$^+$? Expliquer simplement les éléments à mettre en œuvre et les propriétés de sûreté à vérifier.*

Question 5.5 *Ecrire un module TLA$^+$ permettant de vérifier l'algorithme annoté à la fois pour la correction partielle et l'absence d'erreurs à l'exécution.*

On rappelle que la condition de vérification $\forall v. P_{\ell_1}(v) \wedge cond_{\ell_1,\ell_2}(v) \wedge (v') = f_{\ell_1,\ell_2}(v) \Rightarrow P_{\ell'}(v')$ et correspond à une instruction de la forme

$$\begin{array}{l} \ell_1 : P_{\ell_1}(v) \\ V := f_{\ell_1,\ell_2}(V) \\ \ell_2 : P_{\ell_2}(v) \end{array}$$

Exercice 6 *(6 points)*

Evaluer la validité de chaque annotation dans les questions suivent.

Question 6.1

$\ell_1 : x = 64 \ \wedge \ y = x{\cdot}z \ \wedge z = 2{\cdot}x$
$Y := X{\cdot}Z$
$\ell_2 : \ y{\cdot}z = 2{\cdot}x{\cdot}x{\cdot}z$

Question 6.2

$\ell_1 : x = 2 \ \wedge \ y = 4$
$Z := X{\cdot}Y{+}3{\cdot}Y{\cdot}Y{+}3{\cdot}X{\cdot}Y{\cdot}Y{+}X^6$
$\ell_2 : \ z = 6{\cdot}(x{+}y)^2$

Question 6.3

$\ell_1 : x = z \ \wedge \ y = x{\cdot}z$
$Z := X{\cdot}Y{+}3{\cdot}Y{\cdot}Y{+}3{\cdot}X{\cdot}Y{\cdot}Y{+}Y{\cdot}X{\cdot}Z{\cdot}Z{\cdot}X;$
$\ell_2 : \ z = (x{+}y)^3$

Exercice 7 *(2 points)*

Soit l'annotation suivante :

$\ell_1 : x = 1 \wedge y = 2$
$X := Y{+}2$
$\ell_2 : x{+}y \geq m$

où m est un entier ($m \in \mathbb{Z}$).

Question 7.1 *Ecrire la condition de vérification correspondant à cette annotation en upposant que X et Y sont deux variables entières.*

Question 7.2 *Etudier la validité de cette condition de vérification selon la valeur de m.*

Exercice 8 *Dans l'algorithm 8, on calcule le maximum d'une suite de valeurs entières. On vous demande :*

- *de définir la précondition et la postcondition.*
- *d'annoter cet algorithme*
- *de vérifier les conditions de vérification pour la correction partielle*
- *de vérifier les conditions pour l'absence d'erreurs à l'exécution*

Variables : F,N,M,I

Requires : $\left(\begin{array}{l} n_0 \in \mathbb{N} \wedge \\ n_0 \neq 0 \wedge \\ f_0 \in 0 \mathinner{..} n_0 - 1 \rightarrow \mathbb{N} \end{array} \right)$

Ensures : $\left(\begin{array}{l} m_f \in \mathbb{N} \wedge \\ m_f \in ran(f_0) \wedge \\ (\forall j \cdot j \in 0 \mathinner{..} n_0 - 1 \Rightarrow f_0(j) \leq m_f) \end{array} \right)$

$M := F(0)$;
$I := 1$;
while $I < N$ **do**
    if ***F(i)>M*** **then**
        $M := F(I)$;
    ;
    $I{+}{+}$;
;

Algorithme 1: Algorithme du maximum d'une liste non annotée