Cours MCFSI
...
ModÃ©lisation, v'erification et validation de modèles
Dominique Méry
2 octobre 2024

Exercice 1 *(alg-maxtwonumbers)*
Soit le contrat suivant annoté qui calcule le maximum de deux entiers naturels x_0 et y_0

Variables : X,Y,Z
Requires : $x_0, y_0 \in \mathbb{N} \wedge z_0 \in \mathbb{Z}$
Ensures : $z_f = max(x_0, y_0)$

$\ell_0 : \{x = x_0 \wedge y = y_0 \wedge z = z_0 \wedge x_0, y_0 \in \mathbb{N} \wedge z_0 \in \mathbb{Z}\}$
if $X < Y$ **then**
  $\ell_1 : \{x < y \wedge x = x_0 \wedge y = y_0 \wedge z = z_0 \wedge x_0, y_0 \in \mathbb{N} \wedge z_0 \in \mathbb{Z}\}$
  $Z := Y;$
  $\ell_2 : \{x < y \wedge x = x_0 \wedge y = y_0 \wedge x_0, y_0 \in \mathbb{N} \wedge z_0 \in \mathbb{Z} \wedge z = y_0\}$
else
  $\ell_3 : \{x \geq y \wedge x = x_0 \wedge y = y_0 \wedge z = z_0 \wedge x_0, y_0 \in \mathbb{N} \wedge z_0 \in \mathbb{Z}\}$
  $Z := X;$
  $\ell_4 : \{x \geq y \wedge x = x_0 \wedge y = y_0 \wedge x_0, y_0 \in \mathbb{N} \wedge z_0 \in \mathbb{Z} \wedge z = x_0\}$
;
$\ell_5 : \{z = max(x_0, y_0) \wedge x = x_0 \wedge y = y_0 \wedge x_0, y_0 \in \mathbb{N} \wedge z_0 \in \mathbb{Z}\}$

Algorithme 1: maximum de deux nombres non annotée

Question 1.1 *Traduire l'automate de cet algorithme sous la forme d'une machine modifiant les variables x, y, z, pc.*

Question 1.2 *Valider la traduction en simulant quelques*

Question 1.3 *Ajouter les annotations et les pré et post conditions.*

Question 1.4 *Vérifier la correction partielle et l'absence d'erreurs à l'exécution.*

Exercice 2 *Show that each annotation is sound or unsound with respect to the proof obligations :*
$\forall x, y, , x', y'.P_\ell(x, y) \wedge cond_{\ell,\ell'}(x, y) \wedge (x', y') = f_{\ell,\ell'}(x, y) \Rightarrow P_{\ell'}(x', y')$
You will use a context and a machine for expressing these conditions.

— $\ell_1 : x = 10 \wedge y = z{+}x \wedge z = 2{\cdot}x$
  $y := z{+}x$
  $\ell_2 : x = 10 \wedge y = x{+}2{\cdot}10$

— $\ell_1 : x = 1 \wedge y = 12$
  $x := 2{\cdot}y$
  $\ell_2 : x = 1 \wedge y = 24$

— *We assume that p is a prime number.*
  $\ell_1 : x = 2^p \wedge y = 2^{p+1} \wedge x{\cdot}y = 2^{2\cdot p+1}$
  $x := y{+}x{+}2^x$
  $\ell_2 : x = 5{\cdot}2^p \wedge y = 2^{p+1}$

— $\ell_1 : x = 11 \wedge y = 13$
  $z := x; x := y; y := z;$
  $\ell_2 : x = 26/2 \wedge y = 33/3$

precondition : $x = x_0 \wedge x_0 \in \mathbb{N}$
postcondition : $x = 0$

$\ell_0 : \{\ x = x_0 \wedge x_0 \in \mathbb{N}\}$
while $0 < x$ **do**
  $\ell_1 : \{O < x \leq x_0 \wedge x_0 \in \mathbb{N}\}$
  $x := x{-}1;$
  $\ell_2 : \{0 \leq x \leq x_0 \wedge x_0 \in \mathbb{N}\}$
;
$\ell_3 : \{x = 0\}$

Algorithme 2: Exercice 3

Exercice 3 *(alg-simple)*
Let the following partially annotated algorithm :

Question 3.1 *Translate each transition ℓ, ℓ' into an event modifying the variables according to the statements.*

Question 3.2 *Define an invariant attaching to each label an assertion satisfied at the control point.*

Question 3.3 *Verify proof obligations and deduce that the algorithm is partially correct.*

Question 3.4 *Prove that the algorithm has no runtime error.*

Exercice 4 *(alg-squareroot)*
Let the following annotated invariant.

precondition : $x \in \mathbb{N}$
postcondition : $z^2 \leq x \wedge x < (z{+}1)^2$
local variables : $y_1, y_2, y_3 \in \mathbb{N}$

$pre : \{x \in \mathbb{N}\}$
$post : \{z{\cdot}z \leq x {\wedge} x < (z{+}1){\cdot}(z{+}1)\}$
$\ell_0 : \{x \in \mathbb{N} \wedge z \in \mathbb{Z} {\wedge} y1 \in \mathbb{Z} {\wedge} y2 \in \mathbb{Z} {\wedge} y3 \in \mathbb{Z}\}$
$(y_1, y_2, y_3) := (0, 1, 1);$
$\ell_1 : \{y2 = (y1{+}1){\cdot}(y1{+}1) {\wedge} y3 = 2{\cdot}y1{+}1 {\wedge} y1{\cdot}y1 \leq x\}$
while $y_2 \leq x$ **do**
  $\ell_2 : \{y2 = (y1{+}1){\cdot}(y1{+}1) {\wedge} y3 = 2{\cdot}y1{+}1 {\wedge} y2 \leq x\}$
  $(y_1, y_2, y_3) := (y_1{+}1, y_2{+}y_3{+}2, y_3{+}2);$
  $\ell_3 : \{y2 = (y1{+}1){\cdot}(y1{+}1) {\wedge} y3 = 2{\cdot}y1{+}1 {\wedge} y1{\cdot}y1 \leq x\}$
;
$\ell_4 : \{y2 = (y1{+}1){\cdot}(y1{+}1) {\wedge} y3 = 2{\cdot}y1{+}1 {\wedge} y1{\cdot}y1 \leq x {\wedge} x < y2\}$
$z := y_1;$
$\ell_5 : \{y2 = (y1{+}1){\cdot}(y1{+}1) {\wedge} y3 = 2{\cdot}y1{+}1 {\wedge} y1{\cdot}y1 \leq x {\wedge} x < y2 {\wedge} z = y1 {\wedge} z{\cdot}z \leq x {\wedge} x < (z{+}1){\cdot}(z{+}1)\}$

Algorithme 3: *squareroot* annotée Exercice 4

Question 4.1 *Translate each transition ℓ, ℓ' into an event modifying the variables according to the statements.*

Question 4.2 *Define an invariant attaching to each label an assertion satisfied at the control point.*

Question 4.3 *Verify proof obligations and deduce that the algorithm is partially correct.*

Question 4.4 *Prove that the algorithm has no runtime error.*

Exercice 5 *(alg-maximum)*
Soit l'algorithme suivant annoté partiellement :

Question 5.1 *Translate each transition ℓ, ℓ' into an event modifying the variables according to the statements.*

Question 5.2 *Define an invariant attaching to each label an assertion satisfied at the control point.*

Question 5.3 *Verify proof obligations and deduce that the algorithm is partially correct.*

Question 5.4 *Prove that the algorithm has no runtime error.*

Exercice 6 *()*
Cet exercice comprend plusieurs questions indépendantes. Il s'agit d'écrire un événement Event-B qui modélise une transformation décrite en langue naturelle.

Question 6.1 *On suppose que les variables sont x, y, z et que $x, y, z \in \mathbb{Z}$. Ecrire un événement E1 qui modélise la transformation décrite comme suit :*

/* algorithme de calcul du maximum avec une boucle while de l'exercice **??** */

precondition : $\begin{pmatrix} n \in \mathbb{N} \wedge \\ n \neq 0 \wedge \\ f \in 0 \,..\, n-1 \rightarrow \mathbb{N} \end{pmatrix}$

postcondition : $\begin{pmatrix} m \in \mathbb{N} \wedge \\ m \in ran(f) \wedge \\ (\forall j \cdot j \in 0 \,..\, n-1 \Rightarrow f(j) \leq m) \end{pmatrix}$

local variables : $i \in \mathbb{Z}$

$\ell_0 : \{ \begin{pmatrix} n \in \mathbb{N} \wedge \\ n \neq 0 \wedge \\ f \in 0 \,..\, n-1 \rightarrow \mathbb{N} \end{pmatrix} \wedge i \in \mathbb{Z} \wedge m \in \mathbb{Z} \}$

$m := f(0);$

$\ell_1 : \{ \begin{pmatrix} n \in \mathbb{N} \wedge \\ n \neq 0 \wedge \\ f \in 0 \,..\, n-1 \rightarrow \mathbb{N} \end{pmatrix} \wedge i \in \mathbb{Z} \wedge m = f(0) \}$

$i := 1;$

$\ell_2 : \{ \begin{pmatrix} n \in \mathbb{N} \wedge \\ n \neq 0 \wedge \\ f \in 0 \,..\, n-1 \rightarrow \mathbb{N} \end{pmatrix} \wedge i = 1 \wedge \begin{pmatrix} m \in \mathbb{N} \wedge \\ m \in ran(f[0..i-1]) \wedge \\ (\forall j \cdot j \in 0 \,..\, i-1 \Rightarrow f(j) \leq m) \end{pmatrix} \}$

while $i < n$ **do**

$\ell_3 : \{ \begin{pmatrix} n \in \mathbb{N} \wedge \\ n \neq 0 \wedge \\ f \in 0 \,..\, n-1 \rightarrow \mathbb{N} \end{pmatrix} \wedge i \in 1..n-1 \wedge \begin{pmatrix} m \in \mathbb{N} \wedge \\ m \in ran(f[0..i-1]) \wedge \\ (\forall j \cdot j \in 0 \,..\, i-1 \Rightarrow f(j) \leq m) \end{pmatrix} \}$

if *f(i)>m* **then**

$\ell_4 : \{ \begin{pmatrix} n \in \mathbb{N} \wedge \\ n \neq 0 \wedge \\ f \in 0 \,..\, n-1 \rightarrow \mathbb{N} \end{pmatrix} \wedge i \in 1..n-1 \wedge \begin{pmatrix} m \in \mathbb{N} \wedge \\ m \in ran(f[0..i-1]) \wedge \\ (\forall j \cdot j \in 0 \,..\, i-1 \Rightarrow f(j) \leq m) \end{pmatrix} \wedge$
$f(i) > m \}$

$m := f(i);$

$\ell_5 : \{ \begin{pmatrix} n \in \mathbb{N} \wedge \\ n \neq 0 \wedge \\ f \in 0 \,..\, n-1 \rightarrow \mathbb{N} \end{pmatrix} \wedge i \in 1..n-1 \wedge \begin{pmatrix} m \in \mathbb{N} \wedge \\ m \in ran(f[0..i]) \wedge \\ (\forall j \cdot j \in 0 \,..\, i \Rightarrow f(j) \leq m) \end{pmatrix} \}$

;

$\ell_6 : \{ \begin{pmatrix} n \in \mathbb{N} \wedge \\ n \neq 0 \wedge \\ f \in 0 \,..\, n-1 \rightarrow \mathbb{N} \end{pmatrix} \wedge i \in \mathbb{Z} \wedge \wedge i \in 1..n-1 \wedge \begin{pmatrix} m \in \mathbb{N} \wedge \\ m \in ran(f[0..i]) \wedge \\ (\forall j \cdot j \in 0 \,..\, i \Rightarrow f(j) \leq m) \end{pmatrix} \}$

$i{+}{+};$

$\ell_7 : \{ \begin{pmatrix} n \in \mathbb{N} \wedge \\ n \neq 0 \wedge \\ f \in 0 \,..\, n-1 \rightarrow \mathbb{N} \end{pmatrix} \wedge i \in 2..n \wedge \begin{pmatrix} m \in \mathbb{N} \wedge \\ m \in ran(f[0..i-1]) \wedge \\ (\forall j \cdot j \in 0 \,..\, i-1 \Rightarrow f(j) \leq m) \end{pmatrix} \}$

;

$\ell_8 : \{ \begin{pmatrix} n \in \mathbb{N} \wedge \\ n \neq 0 \wedge \\ f \in 0 \,..\, n-1 \rightarrow \mathbb{N} \end{pmatrix} \wedge i = n \wedge \begin{pmatrix} m \in \mathbb{N} \wedge \\ m \in ran(f) \wedge \\ (\forall j \cdot j \in 0 \,..\, n-1 \Rightarrow f(j) \leq m) \end{pmatrix} \}$

Algorithme 4: Algorithme du manimum d'une liste annoté Exercice **??**