Cours Modélisation et vérification des systèmes informatiques
Exercices
Utilisation d'un environnement de vérification Frama-c (III)
par Dominique Méry
18 novembre 2024

Exercice 1 *Utiliser frama-c pour vérifier ou non les annotations suivantes :*

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

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

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

— $\ell_1 : x = 3 \ \wedge\ y = z+x \ \wedge z = 2 \cdot x$
$y := z+x$
$\ell_2 : x = 3 \ \wedge\ y = x+6$

— $\ell_1 : x = 2^4 \ \wedge\ y = 2^{345} \ \wedge\ x \cdot y = 2^{350}$
$x := y+x+2^x$
$\ell_2 : x = 2^{56} \ \wedge\ y = 2^{345}$

— $\ell_1 : x = 1 \ \wedge\ y = 12$
$x := 2 \cdot y+x$
$\ell_2 : x = 1 \ \wedge\ y = 25$

Exercice 2 *Utiliser frama-c pour vérifier ke contrat suivant :*

Variables : X
Requires : $x_0 \in \mathbb{N}$
Ensures : $x_f = 0$

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

Algorithme 1: exemple annoté

Exercice 3 *Utiliser frama-c pour vérifier le contrat suivant :*

Exercice 4

Utiliser frama-c pour vérifier ke contrat suivant :
Soit l'algorithme annoté suivant se trouvant à la page suivante et les pré et postconditions définies pour cet algorithme comme suit : On suppose que $x1$ et $x2$ sont des constantes.

Variables : F,N,M,I

Requires : $\begin{pmatrix} n_0 \in \mathbb{N} \wedge \\ n_0 \neq 0 \wedge \\ f_0 \in 0\,..\,n_0{-}1 \rightarrow \mathbb{N} \end{pmatrix}$

Ensures : $\begin{pmatrix} m_f \in \mathbb{N} \wedge \\ m_f \in ran(f_0) \wedge \\ (\forall j \cdot j \in 0\,..\,n_0{-}1 \Rightarrow f_0(j) \leq m_f) \end{pmatrix}$

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

Algorithme 2: Algorithme du maximum d'une liste non annotée

Variables : X1,X2,Y1,Y2,Y3,Z
Requires : $x1_0 \in \mathbb{N} \wedge x2_0 \in \mathbb{N} \wedge x1_0 \neq 0$
Ensures : $z_f = x1_0^{x2_0}$

ℓ_0 : $\{x1_0 \in \mathbb{N} \wedge x2_0 \in \mathbb{N} \wedge x1_0 \neq 0 \wedge y1_0, y2_0, y3_0, z_0 \in \mathbb{Z} \wedge (x1, x2, y1, y2, y3, z) = (x1_0, x2_0, y1_0, y2_0, y3_0, z0)\}$
$(y_1, y_2, y_3) := (x_1, x_2, 1)$;
ℓ_1 : $\{x1_0 \in \mathbb{N} \wedge x2_0 \in \mathbb{N} \wedge x1_0 \neq 0 \wedge y1_0, y2_0, y3_0, z_0 \in \mathbb{Z} \wedge (x1, x2, z) = (x1_0, x2_0, z0) \wedge y_3 \cdot {y_1}^{y_2} = {x_1}^{x_2}\}$
while $y_2 \neq 0$ **do**
ℓ_2 : $\{x1_0 \in \mathbb{N} \wedge x2_0 \in \mathbb{N} \wedge x1_0 \neq 0 \wedge y1_0, y2_0, y3_0, z_0 \in \mathbb{Z} \wedge (x1, x2, z) = (x1_0, x2_0, z0) \wedge y_3 \cdot {y_1}^{y_2} = {x_1}^{x_2} \wedge 0 < y2 \leq x2\}$
if $impair(y_2)$ **then**
ℓ_3 : $\{x1_0 \in \mathbb{N} \wedge x2_0 \in \mathbb{N} \wedge x1_0 \neq 0 \wedge y1_0, y2_0, y3_0, z_0 \in \mathbb{Z} \wedge (x1, x2, z) = (x1_0, x2_0, z0) \wedge y_3 \cdot {y_1}^{y_2} = {x_1}^{x_2} \wedge 0 < y2 \leq x2 \wedge impair(y2)\}$
$y_2 := y_2 - 1$;
ℓ_4 : $\{x1_0 \in \mathbb{N} \wedge x2_0 \in \mathbb{N} \wedge x1_0 \neq 0 \wedge y1_0, y2_0, y3_0, z_0 \in \mathbb{Z} \wedge (x1, x2, z) = (x1_0, x2_0, z0) \wedge y_3 \cdot y1 \cdot {y_1}^{y_2} = {x_1}^{x_2} \wedge 0 \leq y2 \leq x2 \wedge pair(y2)\}$
$y_3 := y_3 \cdot y_1$;
ℓ_5 : $\{x1_0 \in \mathbb{N} \wedge x2_0 \in \mathbb{N} \wedge x1_0 \neq 0 \wedge y1_0, y2_0, y3_0, z_0 \in \mathbb{Z} \wedge (x1, x2, z) = (x1_0, x2_0, z0) \wedge y_3 \cdot {y_1}^{y_2} = {x_1}^{x_2} \wedge 0 \leq y2 \leq x2 \wedge pair(y2))\}$

;
ℓ_6 : $\{x1_0 \in \mathbb{N} \wedge x2_0 \in \mathbb{N} \wedge x1_0 \neq 0 \wedge y1_0, y2_0, y3_0, z_0 \in \mathbb{Z} \wedge (x1, x2, z) = (x1_0, x2_0, z0) \wedge y_3 \cdot {y_1}^{y_2} = {x_1}^{x_2} \wedge 0 \leq y2 \leq x2 \wedge pair(y2)\}$

$y_1 := y_1 \cdot y_1$;
ℓ_7 : $\{x1_0 \in \mathbb{N} \wedge x2_0 \in \mathbb{N} \wedge x1_0 \neq 0 \wedge y1_0, y2_0, y3_0, z_0 \in \mathbb{Z} \wedge (x1, x2, z) = (x1_0, x2_0, z0) \wedge y_3 \cdot {y_1}^{y_2 \; div \; 2} = {x_1}^{x_2} \wedge 0 \leq y2 \leq x2 \wedge pair(y2)\}$

$y_2 := y_2 \; div \; 2$;
ℓ_8 : $\{x1_0 \in \mathbb{N} \wedge x2_0 \in \mathbb{N} \wedge x1_0 \neq 0 \wedge y1_0, y2_0, y3_0, z_0 \in \mathbb{Z} \wedge (x1, x2, z) = (x1_0, x2_0, z0) \wedge y_3 \cdot {y_1}^{y_2} = {x_1}^{x_2} \wedge 0 \leq y2 \leq x2\}$

;
ℓ_9 : $\{x1_0 \in \mathbb{N} \wedge x2_0 \in \mathbb{N} \wedge x1_0 \neq 0 \wedge y1_0, y2_0, y3_0, z_0 \in \mathbb{Z} \wedge (x1, x2, z) = (x1_0, x2_0, z0) \wedge y_3 \cdot {y_1}^{y_2} = {x_1}^{x_2} \wedge y2 = 0\}$

$z := y_3$;
ℓ_{10} : $\{x1_0 \in \mathbb{N} \wedge x2_0 \in \mathbb{N} \wedge x1_0 \neq 0 \wedge y1_0, y2_0, y3_0, z_0 \in \mathbb{Z} \wedge (x1, x2) = (x1_0, x2_0) \wedge y_3 \cdot {y_1}^{y_2} = {x_1}^{x_2} \wedge y2 = 0 \wedge z = x1^{x2}\}$

Algorithme 3: Algorithme de l'exponentitaion indienne annoté