Modélisation et vérification des systèmes informatiques

Dominique Méry

12 octobre 2015

Table des matières

1 Modélisation et vérification de systèmes

2

1 Modélisation et vérification de systèmes

Exercice 1 On considère l'algorithme `squareroot` calculant la racine carrée entière d'un nombre naturel $x \in \mathbb{N}$.

Question 1.1 Complétez cet algorithme en proposant trois assertions :

- $P_{\ell_2}(z, y_1, y_2, y_3)$
- $P_{\ell_4}(z, y_1, y_2, y_3)$
- $P_{\ell_5}(z, y_1, y_2, y_3)$

Question 1.2 Pour chaque paire (ℓ, ℓ') d'étiquettes correspondant à un pas élémentaire ; on vérifie la propriété suivante :

$$\forall x, y, q, r, x', y', q', r'. P_{\ell}(y_1, y_2, y_3, z) \wedge \text{cond}_{\ell, \ell'}(y_1, y_2, y_3, z) \wedge (y'_1, y'_2, y'_3, z') = f_{\ell, \ell'}(y_1, y_2, y_3, z) \Rightarrow P_{\ell'}(y'_1, y'_2, y'_3, z')$$

Énoncez et vérifiez cette propriété pour les paires d'étiquettes suivantes : $(\ell_1, \ell_2); (\ell_1, \ell_4); (\ell_2, \ell_3); (\ell_3, \ell_2); (\ell_3, \ell_4); (\ell_4, \ell_5)$;

Question 1.3 On suppose que toutes les conditions de vérifications associées aux paires d'étiquettes successives de l'algorithme sont vérifiées. Quelles sont les deux conditions à montrer pour déduire que l'algorithme est partiellement correct par rapport aux pré et post conditions ? Vous donnerez explicitement les conditions et vous expliquerez pourquoi elles sont correctes.

Question 1.4 Expliquer que cet algorithme est sans erreurs à l'exécution, si les données initiales sont dans un domaine à définir inclus dans le domaine des entiers informatiques c'est-à-dire les entiers codables sur n bits. L'ensemble des entiers informatiques sur n bits est l'ensemble noté $\mathbb{Z}_n$ et défini par $\{i | i \in \mathbb{Z} \wedge -2^{n-1} \leq i \wedge i \leq 2^{n-1}-1\}$.

precondition : $x \in \mathbb{N}$

postcondition : $z^2 \leq x \wedge x < (z+1)^2$

local variables : $y_1, y_2, y_3 \in \mathbb{N}$

$\ell_0 : \{x \in \mathbb{N} \wedge z \in \mathbb{Z} \wedge y_1 \in \mathbb{Z} \wedge y_2 \in \mathbb{Z} \wedge y_3 \in \mathbb{Z}\}$

$(y_1, y_2, y_3) := (0, 1, 1)$;

$\ell_1 : \{y_2 = (y_1+1) \cdot (y_1+1) \wedge y_3 = 2 \cdot y_1 + 1 \wedge y_1 \cdot y_1 \leq x\}$

while $y_2 \leq x$ **do**

$\ell_2 : \{\dots\}$

$(y_1, y_2, y_3) := (y_1+1, y_2+y_3+2, y_3+2)$;

$\ell_3 : \{y_2 = (y_1+1) \cdot (y_1+1) \wedge y_3 = 2 \cdot y_1 + 1 \wedge y_1 \cdot y_1 \leq x\}$

;

$\ell_4 : \{\dots\}$

$z := y_1$;

$\ell_5 : \{\dots\}$

Algorithme 1: `squareroot` annotée

Exercice 2 Question 2.1 Soit un tableau t (dans $\mathbb{N}$), donner un prédicat $\text{max}(m, t, a, b) = \dots$ exprimant qu'un nombre $m \in \mathbb{N}$ est le maximum de ce tableau t dans l'intervalle $a .. b$.

Question 2.2 De même pour $\text{trié}(t, a, b)$, donnez un prédicat spécifiant que le tableau t est trié dans l'intervalle $a .. b$.

Exercice 3 Dans le programme qui suit, on calcule le maximum d'une suite de valeurs entières. On vous demande :

- Définir la précondition et la postcondition.
- Annoter cet algorithme
- Vérifier les conditions de vérification pour la correction partielle
- Vérifier les conditions pour l'absence d'erreurs à l'exécution

```

precondition :  $\left( \begin{array}{l} n \in \mathbb{N} \wedge \\ n \neq 0 \wedge \\ f \in 0..n-1 \rightarrow \mathbb{N} \end{array} \right)$ 

postcondition :  $\left( \begin{array}{l} m \in \mathbb{N} \wedge \\ m \in \text{ran}(f) \wedge \\ (\forall j. j \in 0..n-1 \Rightarrow f(j) \leq m) \end{array} \right)$ 

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

m := f(0);
i := 1;
while i < n do
  if f(i) > m then
    | m := f(i);
    | ;
    | i++;
  ;
;

```

Algorithme 2: MAXIMUM

Exercice 4 Dans le programme qui suit, on calcule le maximum d'une suite de valeurs entières. On vous demande :

- Définir la précondition et la postcondition.
- Annoter cet algorithme
- Vérifier les conditions de vérification pour la correction partielle
- Vérifier les conditions pour l'absence d'erreurs à l'exécution

```

precondition :  $\left( \begin{array}{l} n \in \mathbb{N} \wedge \\ n \neq 0 \wedge \\ f \in 0..n-1 \rightarrow \mathbb{N} \end{array} \right)$ 

postcondition :  $\left( \begin{array}{l} m \in \mathbb{N} \wedge \\ m \in \text{ran}(f) \wedge \\ (\forall j. j \in 0..n-1 \Rightarrow f(j) \leq m) \end{array} \right)$ 

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

m := f(0);
i := 1;
while i < n do
  if f(i) > m then
    | m := f(i);
    | ;
    | i++;
  ;
;

```

Algorithme 3: MAXIMUM

Exercice 5

Montrer que chaque annotation est correcte ou incorrecte selon les conditions de vérifications énoncées comme suit

$$\forall x, y, x', y'. P_\ell(x, y) \wedge \text{cond}_{\ell, \ell'}(x, y) \wedge (x', y') = f_{\ell, \ell'}(x, y) \Rightarrow P_{\ell'}(x', y')$$

- (1)	$\begin{aligned} \ell_1 : x = 9 \wedge y = z+x \\ y := x+9 \\ \ell_2 : x = 9 \wedge y = x+9 \end{aligned}$	-	$\begin{aligned} \ell_1 : x = 3 \wedge y = 3 \\ x := y+x \\ \ell_2 : x = 6 \wedge y = 3 \end{aligned}$
- (2)	$\begin{aligned} \ell_1 : x = 1 \wedge y = 3 \wedge x+y = 12 \\ x := y+x \\ \ell_2 : x = 567 \wedge y = 34 \end{aligned}$	-	$\begin{aligned} \ell_1 : x = 1 \wedge y = 3 \\ z := x; x := y; y := z; \\ \ell_2 : x = 3 \wedge y = 1 \end{aligned}$

Exercice 6

Montrer que chaque annotation est correcte ou incorrecte selon les conditions de vérifications énoncées comme suit

$$\forall x, y, x', y'. P_\ell(x, y) \wedge \text{cond}_{\ell, \ell'}(x, y) \wedge (x', y') = f_{\ell, \ell'}(x, y) \Rightarrow P_{\ell'}(x', y')$$

-	$\begin{aligned} \ell_1 : x = 3 \wedge y = z+x \wedge z = 2 \cdot x \\ y := z+x \\ \ell_2 : x = 3 \wedge y = x+6 \end{aligned}$	-	$\begin{aligned} \ell_1 : x = 1 \wedge y = 12 \\ x := 2 \cdot y+x \\ \ell_2 : x = 1 \wedge y = 25 \end{aligned}$
-	$\begin{aligned} \ell_1 : x = 2^4 \wedge y = 2^{345} \wedge x \cdot y = 2^{350} \\ x := y+x+2^x \\ \ell_2 : x = 2^{56} \wedge y = 2^{345} \end{aligned}$	-	$\begin{aligned} \ell_1 : x = 11 \wedge y = 13 \\ z := x; x := y; y := z; \\ \ell_2 : x = 26/2 \wedge y = 33/3 \end{aligned}$

Exercice 7

Soit l'algorithme annoté suivant se trouvant à la page suivante et les pré et postconditions définies pour cet algorithme comme suit :

- Precondition : $x_1 \in \mathbb{N} \wedge x_2 \in \mathbb{N}$

- Postcondition : $z = x_1^{x_2}$

On suppose que x_1 et x_2 sont des constantes.

Question 7.1 Donner les annotations complètes associées à chaque étiquette $\ell \in \{\ell_1, \dots, \ell_9\}$.

Question 7.2 Pour chaque paire (ℓ, ℓ') d'étiquettes correspondant à un pas élémentaire ; on vérifie la propriété suivante :

$$\forall x, y, q, r, x', y', q', r'. P_\ell(y_1, y_2, y_3, z) \wedge \text{cond}_{\ell, \ell'}(y_1, y_2, y_3, z) \wedge (y'_1, y'_2, y'_3, z') = f_{\ell, \ell'}(y_1, y_2, y_3, z) \Rightarrow P_{\ell'}(y'_1, y'_2, y'_3, z')$$

Énoncer et vérifier cette propriété pour les paires d'étiquettes suivantes : (ℓ_1, ℓ_2) ; (ℓ_2, ℓ_3) ; (ℓ_3, ℓ_4) ; (ℓ_4, ℓ_5) ; (ℓ_5, ℓ_6) ; (ℓ_6, ℓ_7) ; (ℓ_7, ℓ_8) ; (ℓ_8, ℓ_2) ; (ℓ_8, ℓ_9) .

Question 7.3 On suppose que toutes les conditions de vérifications associées aux paires d'étiquettes successives de l'algorithme sont vérifiées. Quelles sont les deux conditions à montrer pour déduire que l'algorithme est partiellement correct par rapport aux pré et post conditions ? Vous donnerez explicitement les conditions et vous expliquerez pourquoi elles sont correctes.

Question 7.4 Expliquer que cet algorithme est sans erreurs à l'exécution, si les données initiales sont dans un domaine à définir inclus dans le domaine des entiers informatiques c'est-à-dire les entiers codables sur n bits. L'ensemble des entiers informatiques sur n bits est l'ensemble noté $\mathbb{Z}_n$ et défini par $\{i | i \in \mathbb{Z} \wedge -2^{n-1} \leq i \wedge i \leq 2^{n-1}-1\}$.

precondition : $x_1 \in \mathbb{N} \wedge x_2 \in \mathbb{N} \wedge x_1 \neq 0$
postcondition : $z = x_1^{x_2}$
local variables : $y_1, y_2, y_3 \in \mathbb{Z}$

$\ell_0 : \{y_1, y_2, y_3, z \in \mathbb{Z}\}$
 $y_1 := x_1; y_2 := x_2; y_3 := 1;$
 $\ell_1 : \{y_1 = x_1 \wedge y_2 = x_2 \wedge y_3 = 1 \wedge y_1, y_2, y_3 \in \mathbb{N} \wedge z \in \mathbb{Z}\}$
 $\ell_{11} : \{y_3 \cdot y_1^{y_2} = x_1^{x_2} \wedge y_1, y_2, y_3 \in \mathbb{N} \wedge z \in \mathbb{Z}\}$

while $y_2 \neq 0$ **do**

$\ell_2 : \{y_2 \neq 0 \wedge y_3 \cdot y_1^{y_2} = x_1^{x_2} \wedge y_1, y_2, y_3 \in \mathbb{N} \wedge z \in \mathbb{Z}\}$
if *impair*(y_2) **then**

$\ell_3 : \{ \textit{impair}(y_2) \wedge y_2 \neq 0 \wedge y_3 \cdot y_1^{y_2} = x_1^{x_2} \wedge y_1, y_2, y_3 \in \mathbb{N} \wedge z \in \mathbb{Z}\}$
 $y_2 := y_2 - 1;$
 $\ell_4 : \{y_2 \geq 0 \wedge \textit{pair}(y_2) \wedge y_3 \cdot y_1 \cdot y_1^{y_2} = x_1^{x_2} \wedge y_1, y_2, y_3 \in \mathbb{N} \wedge z \in \mathbb{Z}\}$
 $y_3 := y_3 \cdot y_1;$
 $\ell_5 : \{y_2 \geq 0 \wedge \textit{pair}(y_2) \wedge y_3 \cdot y_1^{y_2} = x_1^{x_2} \wedge y_1, y_2, y_3 \in \mathbb{N} \wedge z \in \mathbb{Z}\}$

$\ell_6 : \{y_2 \geq 0 \wedge \textit{pair}(y_2) \wedge y_3 \cdot y_1^{y_2} = x_1^{x_2} \wedge y_1, y_2, y_3 \in \mathbb{N} \wedge z \in \mathbb{Z}\}$
 $y_1 := y_1 \cdot y_1;$
 $\ell_7 : \{y_2 \geq 0 \wedge \textit{pair}(y_2) \wedge y_3 \cdot y_1^{y_2 \textit{ div} 2} = x_1^{x_2} \wedge y_1, y_2, y_3 \in \mathbb{N} \wedge z \in \mathbb{Z}\}$
 $y_2 := y_2 \textit{ div} 2;$
 $\ell_8 : \{y_2 \geq 0 \wedge y_3 \cdot y_1^{y_2} = x_1^{x_2} \wedge y_1, y_2, y_3 \in \mathbb{N} \wedge z \in \mathbb{Z}\}$

Algorithme 4: *MACHIN* annoté