Cours Modélisation et vérification des systèmes informatiques
Exercices
Modélisation d'algorithmes en TLA$^+$
Annotation, modélisation et vérification
par Dominique Méry
22 septembre 2021

annotation

Exercice 1 ☑

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

$\forall v, v'.P_\ell(v) \ \wedge \ cond_{\ell,\ell'}(v) \ \wedge \ v' = f_{\ell,\ell'}(v) \Rightarrow P_{\ell'}(v')$

Cette condition s'écrit initialement :

$\forall v, v', pc, pc'.pc = \ell \wedge P_\ell(v) \ \wedge \ pc = \ell \wedge \ cond_{\ell,\ell'}(v) \ \wedge \ v' = f_{\ell,\ell'}(v) \wedge \ pc' = \ell' \Rightarrow pc' = \ell' \wedge \ P_{\ell'}(v')$

mais on peut réduire en oubliant la variable pc.

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

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

— *On suppose que p est un nombre premier :*
$\ell_1 : x = 2^p \ \wedge \ y = 2^{p+1} \ \wedge \ x{\cdot}y = 2^{2{\cdot}p+1}$
$x := y{+}x{+}2^x$
$\ell_2 : x = 5{\cdot}2^p \ \wedge \ y = 2^{p+1}$

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

Exercice 2 ☑

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

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

— *(1)* $\ell_1 : x = 9 \ \wedge \ y = z{+}x$
$y := x{+}9$
$\ell_2 : x = 9 \ \wedge \ y = x{+}9$

— $\ell_1 : x = 3 \ \wedge \ y = 3$
$x := y{+}x$
$\ell_2 : x = 6 \ \wedge \ y = 3$

— *(2)* $\ell_1 : x = 1 \ \wedge \ y = 3 \ \wedge \ x{+}y = 12$
$x := y{+}x$
$\ell_2 : x = 567 \ \wedge \ y = 34$

— $\ell_1 : x = 1 \ \wedge \ y = 3$
$z := x; x := y; y := z;$
$\ell_2 : x = 3 \ \wedge \ y = 1$

Exercice 3 ☑

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

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

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

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

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

Exercice 4 ☑
Soit le petit algorithme annoté suivant :

$l0 : \{v = 3\}$
$v := v{+}2$
$l1 : \{v = 5\}$

Ecrire un module TLA$^+$ explicitant la relation de transition, les conditions initiales, l'invariant et la propriété de sûreté pour la correction partielle.

Exercice 5 ☑
Définir les conditions de vérification de la correction partielle pour les structures suivantes. Définir un modèle TLA$^+$ pour vérifier la bonne annotation.

Question 5.1

$\ell 1 : \{P_{\ell 1}(x, y)\}$
$x := x{+}y{+}7;$
$\ell 2 : \{P_{\ell 2}(x, y)\}$

Question 5.2

$\ell : \{P_{\ell}(x, y)\}$
$x, y := y, x;$
$\ell' : \{P_{\ell'}(x, y)\}$

Exercice 6 ☑
Déterminer les conditions de vérification pour la structure de boucle bornée.
On suppose que S ne modifie pas i.

$\ell_1 : \{P_{\ell_1}(x)\}$
FOR $i := 1$ ***TO*** n ***DO***
$\ell_2 : \{P_{\ell_2}(i, x)\}$
$S(x);$
$\ell_3 : \{P_{\ell_3}(i, x)\}$
ENDFOR
$\ell_4 : \{P_{\ell_4}(x)\}$

Exercice 7 ☑

Question 7.1 *Compléter l'algorithme 7 en l'annotant.*

precondition : $x = a \wedge y = b \wedge a, b \in \mathbb{N}$
postcondition : $z = max(a, b)$

$\ell_0 : \{\ldots\}$
if $x < y$ **then**
  $\ell_1 : \{\ldots\}$
  $z := y$;
  $\ell_2 : \{\ldots\}$
else
  $\ell_3 : \{\ldots\}$
  $z := x$;
  $\ell_4 : \{\ldots\}$
;
$\ell_5 : \{\ldots\}$

Algorithme 1: maximum de deux nombres non annotée

Question 7.2 *Vérifier la bonne annotation*

Question 7.3 *Enoncer et vérifier la correction partielle*

Exercice 8 ☑
Il s'agit d'étudier et d'annoter le programme proposé en vu d'obtenir sa correction partielle (c'est-à-dire sans la preuve de terminaison). On appelle état un ensemble de valeurs précises (spécifié par un prédicat) des variables du programme, nous allons considérer une étiquette (ℓ) entre chaque instruction du programme considéré. On appelle une annotation le prédicat décrivant les valeurs possibles des variables pour un état du programme. Cette annotation est notée : $P_\ell(v)$ et exprime la propriété satisfaite par la variable v en ℓ.
On vous demande :

1. *de dessiner le graphe de transition entre les étiquettes*
2. *d'annoter toutes les étiquettes du programme*
3. *de proposer un modèle TLA$^+$ pour vérifier les annotations et la correction partielle*

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

$\ell_0 : \{\ldots\}$
while $0 < x$ **do**
  $\ell_1 : \{\ldots\}$
  $x := x-1$;
  $\ell_2 : \{\ldots\}$
;
$\ell_3 : \{\ldots\}$

Algorithme 2: Exemple non annoté

Exercice 9 Question 9.1 *Soit un tableau t (dans $\mathbb{N}$), donner un prédicat $max(m, t, a, b) = \ldots$ exprimant qu'un nombre $m \in \mathbb{N}$ est le maximum de ce tableau t dans l'intervalle $a \,..\, b$.*

Question 9.2 *De même pour trié*(t, a, b)*, donnez un prédicat spécifiant que le tableau* t *est trié dans l'intervalle* $a \,..\, b$*.*

Exercice 10 *Dans l'algorithm 10, 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 : $\left(\begin{array}{l} n \in \mathbb{N} \wedge \\ n \neq 0 \wedge \\ f \in 0 \,..\, n{-}1 \to \mathbb{N} \end{array}\right)$

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

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: Algorithme du maximum d'une liste non annotée

Exercice 11 *On considère l'algorithme* $squareroot$ *11 calculant la racine carrée entière d'un nombre naturel* $x \in \mathbb{N}$*.*

Question 11.1 *Complétez cet algorithme en proposant trois assertions :*

- $P_{\ell_2}(z, y1, y2, y3)$
- $P_{\ell_4}(z, y1, y2, y3)$
- $P_{\ell_5}(z, y1, y2, y3)$

Question 11.2 *Pour chaque paire* (ℓ, ℓ') *d'étiquettes correspondant à un pas élémentaire ; on vérifie la propriété suivante :*
$\forall x, y, q, r, x', y', q', r'. P_\ell(y_1, y_2, y_3, z) \wedge cond_{\ell,\ell'}(y_1, y_2, y_3, z) \wedge (y'_1, y'_2, y'_3, z') = f_{\ell,\ell'}(y_1, y_2, y_3, z) \Rightarrow P_{\ell'}(y'_1, y'_2, y'_3, z')$
Enoncez et vérifiez cette propriété pour les paires d'étiquettes suivantes : (ℓ_1, ℓ_2)*;*(ℓ_1, ℓ_4)*;* (ℓ_2, ℓ_3)*;* (ℓ_3, ℓ_2)*;* (ℓ_3, ℓ_4)*;* (ℓ_4, ℓ_5)*;*

Question 11.3 *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 11.4 *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 : $y_1, y_2, y_3 \in \mathbb{N}$

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

Algorithme 4: *squareroot* partiellement annotée

Exercice 12

Montrer, pour chaque question, que chaque 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.*

Question 12.1

$\ell_1 : x = 12 \ \wedge \ y = 2 \ \wedge z = 3{\cdot}x$
$x := z{+}y$
$\ell_2 : x = 38 \ \wedge \ y = 2$

Question 12.2

$\ell_1 : x = 3 \ \wedge \ y = 9$
$x := 3{\cdot}y$
$\ell_2 : x = 27 \ \wedge \ y = 9$

Question 12.3 *Soit p un nombre différent d'une puissance de 3 c'est-à-dire différent de 3, 6, 9, 12, ...*

$\ell_1 : x = 3{+}z \ \wedge \ y = 1 \ \wedge \ z = 3 \ \wedge x = y$
$x := p{\cdot}y$
$\ell_2 : x = z \ \wedge \ y = z \ \wedge z = 4{\cdot}p$

Question 12.4 *Soit r un nombre cubique c'est-à-dire de la forme $p = q^3$.*

$\ell_1 : x = r \ \wedge \ u = x^r \ \wedge \ z = 6 \ \wedge x = u$
$y := r{\cdot}r{\cdot}r$
$\ell_2 : x = z \ \wedge \ y = z \ \wedge z = 4{\cdot}p$

Exercice 13

Soit l'algorithme annoté suivant se trouvant à la page suivante et les pré et postconditions définies pour cet algorithme comme suit :
— *Precondition :* $x_1 \in \mathbb{N} \wedge x_2 \wedge \mathbb{N} \wedge x_1 \neq 0$

— *Postcondition :* $z = {x_1}^{x_2}$

On suppose que x_1 *et* x_2 *sont des constantes.*

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 : $y_1, y_2, y_3 \in \mathbb{Z}$

$\ell_0 : \{y_1, y_2, y_3, z \in \mathbb{Z}\}$
$(y_1, y_2, y_3) := (x_1, x_2, 1)$;
$\ell_1 : \{y_3 \cdot {y_1}^{y_2} = {x_1}^{x_2} \wedge y_1, y_2, y_3 \in \mathbb{N} \wedge z \in \mathbb{Z}\}$
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**
    $\ell_3 : \{impair(y_2) \wedge y_2 \neq 0 \wedge \boxed{\bullet\bullet\bullet} \wedge y_1, y_2, y_3 \in \mathbb{N} \wedge z \in \mathbb{Z}\}$
    $y_2 := y_2 - 1$;
    $\ell_4 : \{y_2 \geq 0 \wedge pair(y_2) \wedge y_3 \cdot y_1 \cdot {y_1}^{y_2} = {x_1}^{x_2} \wedge y_1, y_2, y_3 \in \mathbb{N} \wedge z \in \mathbb{Z}\}$
    $y_3 := y_3 \cdot y_1$;
    $\ell_5 : \{y_2 \geq 0 \wedge pair(y_2) \wedge y_3 \cdot {y_1}^{y_2} = {x_1}^{x_2} \wedge y_1, y_2, y_3 \in \mathbb{N} \wedge z \in \mathbb{Z}\}$
  ;
  $\ell_6 : \{y_2 \geq 0 \wedge pair(y_2) \wedge \boxed{\bullet\bullet\bullet} \wedge y_1, y_2, y_3 \in \mathbb{N} \wedge z \in \mathbb{Z}\}$
  $y_1 := y_1 \cdot y_1$;
  $\ell_7 : \{y_2 \geq 0 \wedge pair(y_2) \wedge y_3 \cdot {y_1}^{y_2\ div 2} = {x_1}^{x_2} \wedge y_1, y_2, y_3 \in \mathbb{N} \wedge z \in \mathbb{Z}\}$
  $y_2 := y_2\ div\ 2$;
  $\ell_8 : \{y_2 \geq 0 \wedge \boxed{\bullet\bullet\bullet} \wedge y_1, y_2, y_3 \in \mathbb{N} \wedge z \in \mathbb{Z}\}$
;
$\ell_9 : \{y_2 = 0 \wedge \boxed{\bullet\bullet\bullet} \wedge y_1, y_2, y_3 \in \mathbb{N} \wedge z \in \mathbb{Z}\}$
$z := y_3$;
$\ell_{10} : \{y_2 = 0 \wedge y_3 \cdot {y_1}^{y_2} = {x_1}^{x_2} \wedge y_1, y_2, y_3 \in \mathbb{N} \wedge z \in \mathbb{Z} \wedge z = {x_1}^{x_2}\}$

Algorithme 5: Algorithme de l'exponentitaion indienne annoté

Question 13.1 *Compléter les annotations associées à chaque étiquette* $\ell \in \{\ell_3, \ell_6, \ell_8, \ell_9\}$. *Vous devez écrire les annotations complètes de chaque point de contrôle demandé.*

Question 13.2 *Pour chaque paire* (ℓ, ℓ') *d'étiquettes correspondant à un pas élémentaire ; on vérifie la propriété suivante :*
$\forall x, y, q, r, x', y', q', r'. P_\ell(y_1, y_2, y_3, z) \wedge cond_{\ell,\ell'}(y_1, y_2, y_3, z) \wedge (y'_1, y'_2, y'_3, z') = f_{\ell,\ell'}(y_1, y_2, y_3, z) \Rightarrow P_{\ell'}(y'_1, y'_2, y'_3, z')$
Enoncer et vérifier cette propriété pour les paires d'étiquettes suivantes : (ℓ_0, ℓ_1) *;* (ℓ_1, ℓ_2) *;* (ℓ_3, ℓ_4) *;* (ℓ_6, ℓ_7) *;* (ℓ_7, ℓ_8) *;* (ℓ_1, ℓ_9) *;* (ℓ_9, ℓ_{10}).
Il est clair que cette vérification confirmera les complétions réalisées dans la question précédente.

Question 13.3 *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 13.4 *Selon la définition mathématique de la puissance* $x_1^{x_2}$ *est définie pour une valeur* x_1 *non nulle et c'est pour cela que la précondition indique que* x_1 *est différent de* 0. *Cependant, si on utilise une valeur de* x_1 *nulle, l'algorithme fonctionne et renvoie une valeur. Un jour, un mathématicien a appliqué cet algorithme sans veiller à ce que la valeur de* x_1

soit nulle ou non nulle et il 'est emporté !... Il vous accuse de ne pas lui avoir fourni le bon algorithme répondant à son cahier des charges et il vous demande des dommages et intérêts. Expliquer de manière courte que le texte de l'algorithme et sa preuve de correction suffisent pour vous sauver, en expliquant clairement le rôle de la précondition et de la postcndition.