Cours Modélisation et vérification des systèmes informatiques
Exercices (avec les corrections)
Modélisation TLA$^+$ (1)
par Dominique Méry
24 septembre 2020

Exercice 1 ☑
L'accès à une salle est contrôlé par un système permettant d'observer les personnes qui entrent ou qui sortent de cette salle. Ce système est un ensemble de capteurs permettant d'identifier le passage d'une personne de l'extérieur vers l'intérieur et de l'intérieur à l'extérieur. Le système doit garantir qu'au plus `max` *personnes soient dans la salle. Ecrire un module TLA$^+$ permettant de modéliser un tel système respectant la propriété attendue.*

◇— **Solution de l'exercice 1**

MODULE $ex1$

modules de base importables

EXTENDS *Naturals*, *TLC*

CONSTANTS *max*

VARIABLES *np*

---

tentative 1

$entrer \triangleq np' = np + 1$
$sortir \triangleq np' = np - 1$
$next \triangleq entrer \lor sortir$
$init \triangleq np = 0$

---

tentative 3

$entrer_2 \triangleq np < max \land np' = np + 1$
$next_2 \triangleq entrer_2 \lor sortir$

---

tentative 3

$sortir_2 \triangleq np > 0 \land np' = np - 1$
$next_3 \triangleq entrer_2 \lor sortir2$

$safety_1 \triangleq np \leq max$
$question_1 \triangleq np \neq 6$

Nous donnons trois solutions possibles selon notre analyse :

— la première solution propose deux actions *entrer* et *sortir* et on définit une relation de transition *next*. On définit un modèle en instanciant *max* et en testant les deux propriétés de sûreté *question1* et *safety1*. Les deux questions produisent un échec et donc la propriété de sûreté n'est pas vérifiée.

— la deuxième solution propose deux actions *entrer2* et *sortir* et on définit une relation de transition *next2*. On définit un modèle en instanciant *max* et en testant les deux propriétés de sûreté *question1* et *safety1*. Il n'y a pas de retour sur la question *safety1*.

— la troisième solution propose deux actions *entrer2* et *sortir2* et on définit une relation de transition *next3*. On définit un modèle en instanciant *max* et en testant les deux propriétés de sûreté *question1* et *safety1*. L'utilisation de l'outil conduit à la vérification de la propriété de *safety1*.

Fin 1

Exercice 2 ☑

Le PGCD de deux nombres vérifie les propriétés suivantes :

— $\forall a, b \in \mathbb{N}.pgcd(a, b) = pgcd(b, a)$
— $\forall a, b \in \mathbb{N}.pgcd(a, a+b) = pgcd(a, b)$
— *Ecrire une spécification TLA^+ calculant le PGCD de deux nombres donnés.*
— *Donner une explication ou une justification de la correction de cette solution*

◇— **Solution de l'exercice 2**

MODULE *pgcd*

EXTENDS *Naturals*, *TLC*
CONSTANTS a, b
VARIABLES x, y

Init $\triangleq x = a \land y = b$

$a1 \triangleq x > y \land x' = x - y \land y' = y$
$a2 \triangleq x < y \land y' = y - x \land x' = x$
over $\triangleq x = y \land x' = x \land y' = y$

Next $\triangleq a_1 \lor a_2 \lor$ *over*

---

test $\triangleq x \neq y$

Fin 2

Exercice 3 ☑

Un réseau de Petri est un uple R=(S,T,F,K,M,W) tel que

— *S est l'ensemble (fini) des places.*
— *T est l'ensemble (fini) des transitions.*
— $S \cap T = \varnothing$
— *F est la relation du flôt d'exécution :* $F \subseteq S \times T \cup T \times S$
— *K représente la capacité de chaque place :* $K \in S \rightarrow Nat$.
— *M représente le initial marquage chaque place :*
  $M \in S \rightarrow Nat$ *et vérifie la condition* $\forall s \in S : M(s) \leq K(s)$.
— *W représente le poids de chaque arc :* $W \in F \rightarrow Nat$
— *un marquage M pour R est une fonction de S dans Nat :*
  $M \in S \rightarrow Nat$ *et respectant la condition* $\forall s \in S : M(s) \leq K(s)$.
— *une transition t de T est activable à partir de M un marquage de R si*

  1. $\forall s \in \{ s' \in S \mid (s',t) \in F \} : M(s) \geq W(s,t)$.
  2. $\forall s \in \{ s' \in S \mid (t,s') \in F \} : M(s) \leq K(s) - W(s,t)$.

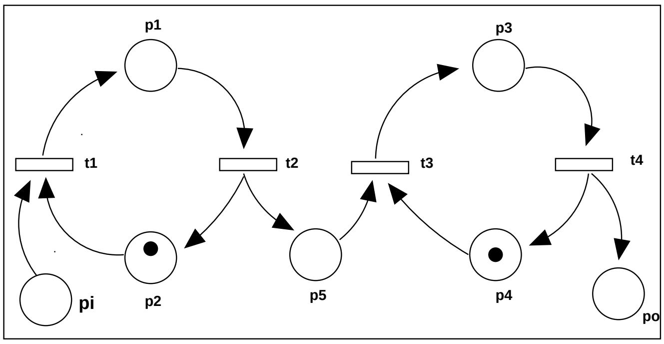
— *Pour chaque transition t de T, Pre(t) est l'ensemble des places conduisant à t et Post(t) est l'ensemble des places pointées par un lien depuis t :*
  $Pre(t) = \{ s' \in S : (s',t) \in F \}$ *et* $Post(t) = \{ s' \in S : (t,s') \in F \}$
— *Soit une transition t de T activable à partir de M un marquage de R :*

  1. $\forall s \in \{ s' \in S \mid (s',t) \in F \} : M(s) \geq W(s,t)$.
  2. $\forall s \in \{ s' \in S \mid (t,s') \in F \} : M(s) \leq K(s) - W(s,t)$.

— *un nouveau marquage M' est défini à partir de M par :* ' $\forall s \in S$,

$$M'(s) = \begin{cases} \text{M(s)} - \text{W(s,t), si s} \in \text{Pre(t) - Post(t)} \\ \text{M(s)} + \text{W(t,s), si s} \in \text{Post(t) - Pre(t)} \\ \text{M(s)} - \text{W(s,t)} + \text{W(t,s), si s} \in \text{Pre(t)} \cap \text{Post(t)} \\ \text{M(s), sinon} \end{cases}$$

On considère le réseau suivant :



Question 3.1 *Traduire ce réseau en un module TLA$^+$ dont le squelette est donné dans le texte. Pour cela, on donnera la définition des quatre transitions $t1$, $t2$, $t3$,$t4$. On ne tiendra pas compte de la capacité des places : les places ont une capacité d'au plus un jeton, sauf la place pi qui peut contenir N jetons, la place p5 peut contenir au plus B jetons et la place po peut contenir au plus Q.*

Question 3.2 *Donner une relation liant les places po,p1,p3,p5,pi et la valeur N. Justifiez votre réponse.*

Question 3.3 *Si on suppose que la place po peut contenir au plus Q jetons, donnez une condition sur Q pour que tous les jetons de pi soient consommés un jour. Justifiez votre réponse.*

Question 3.4 *Expliquez ce que modélise ce réseau de Petri.*

Solution de l'exercice 3

MODULE $petri10$

EXTENDS *Naturals*, *TLC*
CONSTANTS *Places*, N, Q, B
VARIABLES M

$t11 \triangleq$
$\quad \land M[\text{"p1"}] \geq 1 \land M[\text{"p5"}] \geq 1$
$\quad \land M' = [\,[[M \text{ EXCEPT}![\text{"p1"}] = @-1] \text{ EXCEPT}![\text{"p5"}] = @-1] \text{ EXCEPT}![\text{"p2"}] = @+1]$

$t1 \triangleq$
$\quad \land M[\text{"p2"}] = 1 \land M[\text{"pi"}] \geq 1$
$\quad \land M' = [[[M \text{ EXCEPT}![\text{"p1"}] = 1] \text{ EXCEPT}![\text{"pi"}] = M[\text{"pi"}]-1] \text{ EXCEPT}![\text{"p2"}] = 0]$

$t2 \triangleq$
$\quad \land M[\text{"p1"}] = 1 \land M[\text{"p5"}] < B$
$\quad \land M' = [[[M \text{ EXCEPT}![\text{"p1"}] = 0] \text{ EXCEPT}![\text{"p5"}] = M[\text{"p5"}]+1] \text{ EXCEPT}![\text{"p2"}] = 1]$

$t3 \triangleq$
$\quad \land M[\text{"p5"}] \geq 1 \land M[\text{"p4"}] = 1$
$\quad \land M' = [[[M \text{ EXCEPT}![\text{"p3"}] = 1] \text{ EXCEPT}![\text{"p5"}] = M[\text{"p5"}]-1] \text{ EXCEPT}![\text{"p4"}] = 0]$

$t4 \triangleq$
$\quad \land M[\text{"p3"}] = 1 \land M[\text{"po"}] < Q$
$\quad \land M' = [[[M \text{ EXCEPT}![\text{"p3"}] = M[\text{"p3"}]-1]$
$\qquad \text{EXCEPT}![\text{"po"}] = M[\text{"po"}]+1]$
$\qquad \text{EXCEPT}![\text{"p4"}] = M[\text{"p4"}]+1]$

$$Init_1 \triangleq M = [p \in \textit{Places} \mapsto \text{IF } p \in \{\text{"p4"}, \text{"p2"}\} \text{ THEN } 1 \text{ ELSE}$$
$$\text{IF } p = \text{"pi" THEN } N \text{ ELSE } 0\,]$$
$$Init \triangleq Init1$$
$$Next \triangleq t_1 \lor t_2 \lor t_3 \lor t_4 \lor M' = M$$

$$Petri \triangleq Init \land \Box[Next]_{\langle M \rangle}$$

$$TypeInvariant \triangleq \forall\, p \in Places : M[p] \geq 0$$

$$Inv_1 \triangleq M[\text{"pi"}]+M[\text{"p5"}]+M[\text{"po"}]+M[\text{"p1"}]+M[\text{"p3"}] = N$$

$$Inv_2 \triangleq M[\text{"po"}] \leq Q$$

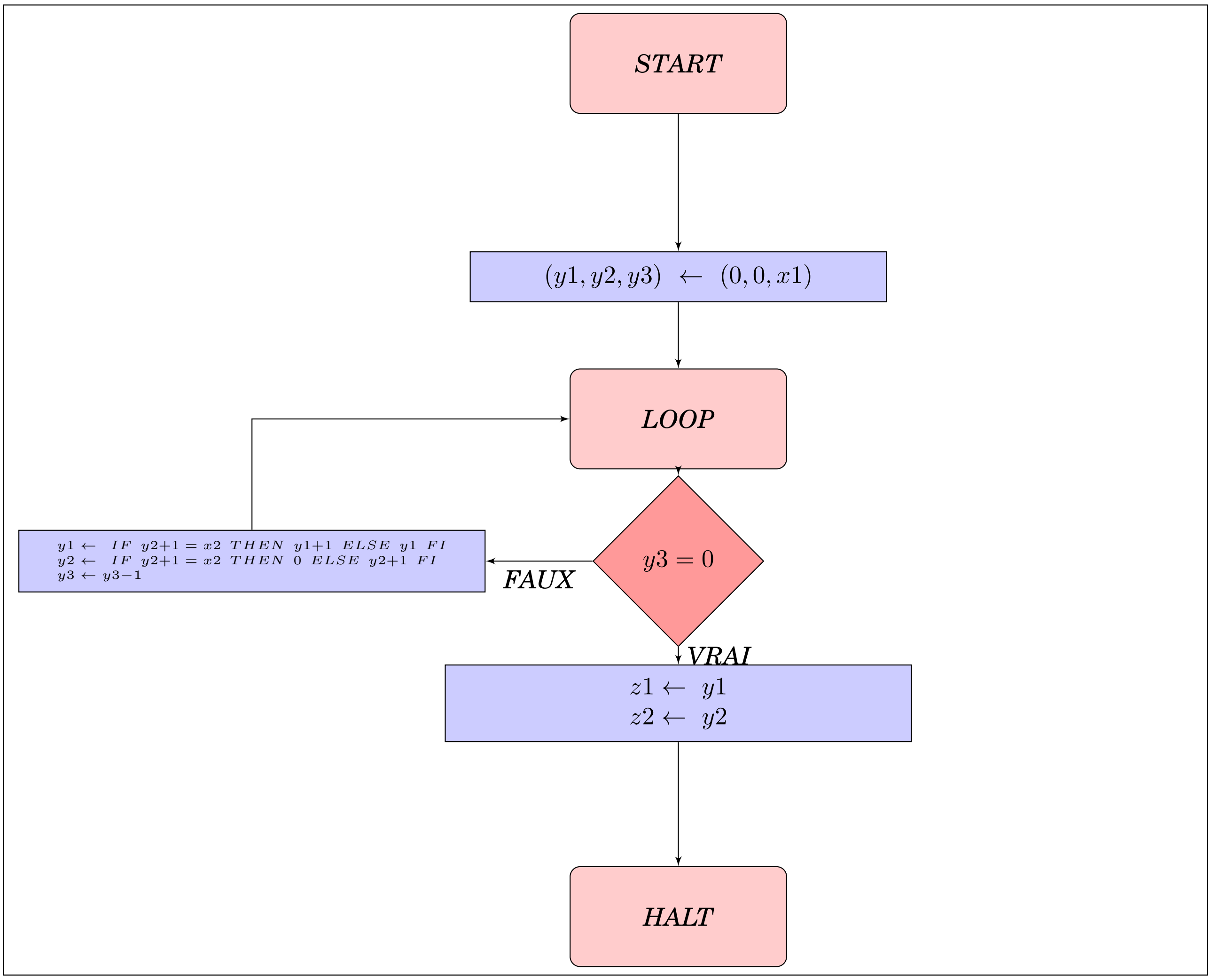
$$Inv_4 \triangleq M[\text{"pi"}]+M[\text{"p5"}]+M[\text{"po"}]+M[\text{"p2"}]+M[\text{"p4"}] = N+2$$
$$Inv_5 \triangleq M[\text{"p3"}]+M[\text{"p4"}]+M[\text{"p1"}]+M[\text{"p2"}] = 2$$

$$Inv_3 \triangleq M[\text{"p3"}] = 0$$
$$Inv \triangleq TypeInvariant$$

Fin 3

Exercice 4 ☑

On considère l'algorithme suivant décrit par un organigramme ou flowchart :



Question 4.1 *Traduire cet algorithme sous forme d'un module TLA$^+$.*

Question 4.2 *Tester les valeurs des variables à l'exécution.*

Question 4.3 *Montrer que cet algorithme est partiellement correct par rapport à sa précondition et à sa postcondition qu'il faudra énoncer.*

◇— **Solution de l'exercice 4**

MODULE *flowchart*

EXTENDS *Integers*, *TLC*, *Naturals*
CONSTANTS $x_1, x2, max, min$
VARIABLES $y_1, y2, y_3, z1, z_2, c$

$labels \triangleq \{\text{"START"}, \text{"QUOI"}, \text{"HALT"}\}$

$init \triangleq c = \text{"START"} \land y_1 = 0 \land y_2 = 0 \land y_3 = 0 \land z_1 = 0 \land z_2 = 0$

```
y1 \in min..max /\ y2 \in min..max /\ y3 \in min..max /\ z1 \in min..max /\ z2 \in min..max
```

$start\_quoi \triangleq$
$\quad \land c = \text{"START"}$
$\quad \land c' = \text{"QUOI"}$

$\land\ y_1' = 0\ \land\ y_2' = 0\ \land\ y_3' = x1$
$\land$ UNCHANGED $\langle z_1, z2 \rangle$

quoi_quoi $\triangleq$
$\land\ c\ =\ $ "QUOI" $\land\ y_3\ \neq\ 0$
$\land\ y_1'\ =\ \text{IF } y_2{+}1 = x_2 \text{ THEN } y_1{+}1 \text{ ELSE } y_1$
$\land\ y_2'\ =\ \text{IF } y_2{+}1 = x_2 \text{ THEN } 0 \text{ ELSE } y_2{+}1$
$\land\ y_3'\ =\ y_3 - 1$
$\land$ UNCHANGED $\langle c, z_1, z2 \rangle$

quoi_halt $\triangleq$
$\land\ c\ =\ $ "QUOI" $\land\ c' = $ "HALT" $\land\ y_3\ =\ 0$
$\land\ z_1'\ =\ y_1\ \land\ z_2' = y2$
$\land$ UNCHANGED $\langle y_1, y2, y_3 \rangle$

next $\triangleq$ *start_quoi* $\lor$ *quoi_quoi* $\lor$ *quoi_halt*

safety $\triangleq$ $c = $ "HALT" $\Rightarrow\ 0\ \leq\ z_2\ \land\ z_2\ <\ x_2\ \land\ x_1 = z1 \cdot x_2 + z2$

Fin 4