Cours Modélisation et vérification des systèmes informatiques
Exercices
Modélisation TLA$^+$ (1)
par Dominique Méry
9 octobre 2024

Exercice 1 $\not\!\square$
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.*

Exercice 2 $\not\!\square$
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*

Exercice 3 $\not\!\square$
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. $\forall\ s \in \{\ s' \in S \mid (t,s') \in F\ \} : M(s) \leq K(s) - W(s,t)$.

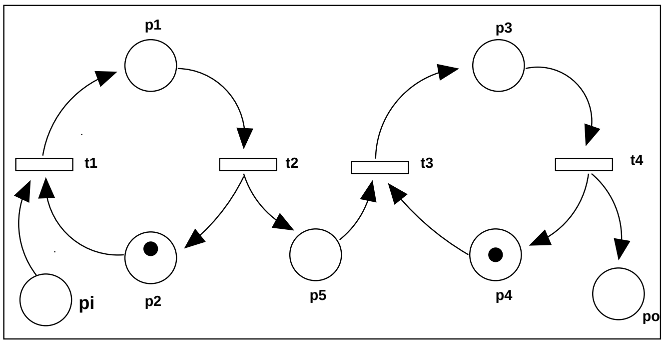
— *Pour chaque transition t de T, Pre(t) est l'ensemble des places conduisant à t et Post(t) est l'ensemble des places pointées par un lien depuis t :*
$Pre(t) = \{\ s' \in S : (s',t) \in F\ \}$ *et* $Post(t) = \{\ s' \in S : (t,s') \in F\ \}$
— *Soit une transition t de T activable à partir de M un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



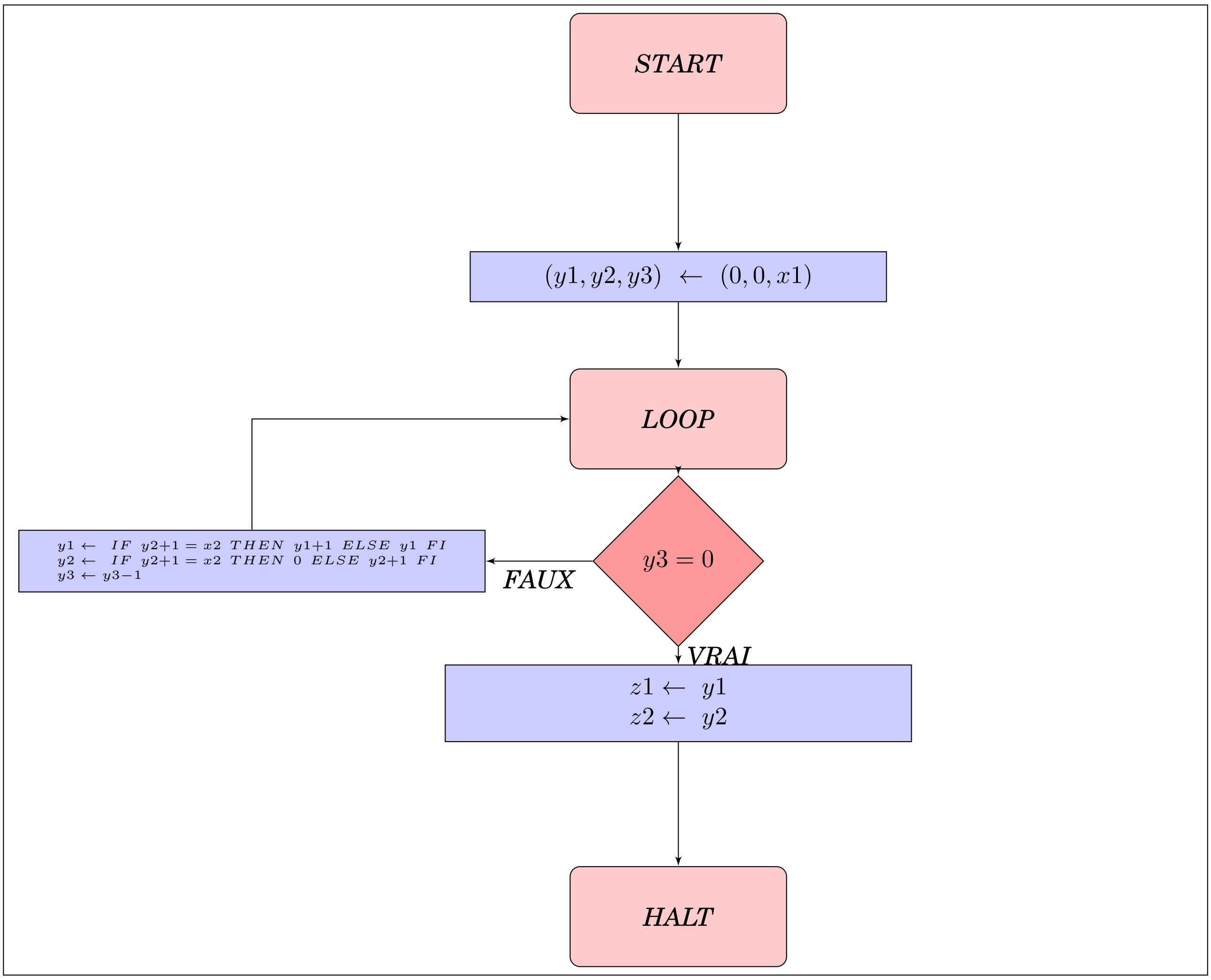
Question 3.1 *Traduire ce réseau en un module TLA*$^+$ *dont le squelette est donné dans le texte. Pour cela, on donnera la définition des quatre transitions* $t1$, $t2$, $t3$,$t4$. *On ne tiendra pas compte de la capacité des places : les places ont une capacité d'au plus un jeton, sauf la place pi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

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.*