

## Modélisation et vérification avec TLA<sup>+</sup>

### Exercice 1 (*disapp\_td1\_ex1.tla*)

**Question 1.1** *Modéliser sous forme d'un module TLA<sup>+</sup> le réseau de Petri de la figure 1. Donner une instanciation possible des constantes. Préciser les conditions initiales correspondant à un système avec cinq (5) processeurs et deux (2) bus.*

**Question 1.2** *On désire analyser le comportement de ce réseau et, pour cela, on souhaite savoir si la place  $p_5$  contiendra au moins un jeton. Expliquer comment on doit procéder pour obtenir une réponse en un temps fini. Préciser le message donné par le système TLAPS.*

**Question 1.3** *Est-ce que le réseau peut atteindre un point de deadlock ?*

**Question 1.4** *Enoncez trois propriétés de sûreté de ce réseau établissant une relation entre au moins deux places.*

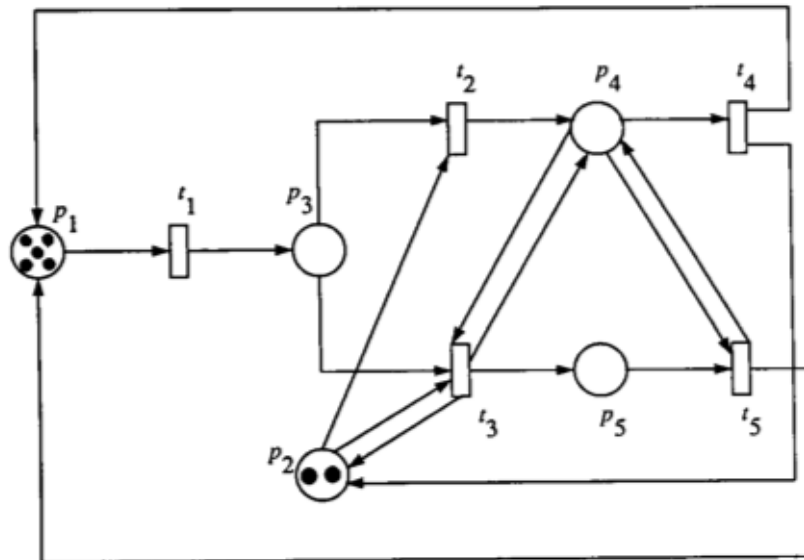
```

----- MODULE disapp_td1_ex1 -----
(* Petri-net for the multiprocessor system *)
EXTENDS Naturals, TLC
CONSTANTS Places, IPlaces, FPlaces, P, B
VARIABLES M

-----
(* Auxiliary Definitions *)
K == [p \in FPlaces |-> IF p \in {"p3"} THEN 1 ELSE 0 ]
TOKENS == 1..20
-----
TypeOK == M \in [Places |-> SUBSET TOKENS]
-----
t1 ==
  /\ M["p1"] \geq 1 /\ M["p3"]+1 \leq K["p3"]
  /\ M' = [[M EXCEPT!["p3"]=M["p3"]+1] EXCEPT!["p1"]=M["p1"]-1]

t2 ==
  /\ M["p2"] \geq 1 /\ M["p3"] \geq 1
  /\ M' = [[M EXCEPT!["p3"]=M["p3"]-1]

```



**Fig. 14.** A Petri-net model of a multiprocessor system, where tokens in  $p_1$  represent active processors,  $p_2$  available buses,  $p_3$ ,  $p_4$ , and  $p_5$  processors waiting for, having access to, queued for common memories, respectively.

FIGURE 1 – Réseau de Petri

```

EXCEPT![" p2"]=M[" p2"]-1]
EXCEPT![" p4"]=M[" p4"]+1]

```

```

t3 ==
  /\ M[" p2"] \geq 1 /\ M[" p3"] \geq 1 /\ M[" p4"] \geq 1
  /\ M'=[M  EXCEPT![" p3"]=M[" p3"]-1]
           EXCEPT![" p5"]=M[" p5"]+1]

```

```

t4 ==
  /\ M[" p4"] \geq 1
  /\ M'=[M  EXCEPT![" p4"]=M[" p4"]-1]
           EXCEPT![" p2"]=M[" p2"]+1]
           EXCEPT![" p1"]=M[" p1"]+1]

```

```

t5 ==
  /\ M[" p4"] \geq 1 /\ M[" p5"] \geq 1
  /\ M'=[M  EXCEPT![" p5"]=M[" p5"]-1]
           EXCEPT![" p1"]=M[" p1"]+1]

```

---

```

Init == M = [p \in Places |->
  IF p \in {"p1"} THEN P
  ELSE IF p \in {"p2"}
  THEN B ELSE 0 ]

```

```

Next == t1 \/ t2 \/ t3 \/ t4 \/ t5

```

```

Petri == Init /\ [][Next]_<<M>>

```

```

I0 == \A p \in Places : M[p] \geq 0

```

```

I1 == 0 \leq M["p3"] /\ M["p3"] \leq 1
I2 == M["p1"] \leq 5 /\ M["p2"] \leq 2
I3 == \A p \in {"p5"} : 0 \leq M[p] /\ M[p] \leq 5
I4 == \A p \in {"p4"} : 0 \leq M[p] /\ M[p] \leq 2

```

AP4 == M["p4"] = 0  
 AP5 == M["p5"] = 0  
 Test == I0 /\ I1 /\ I2 /\ I3 /\ I4

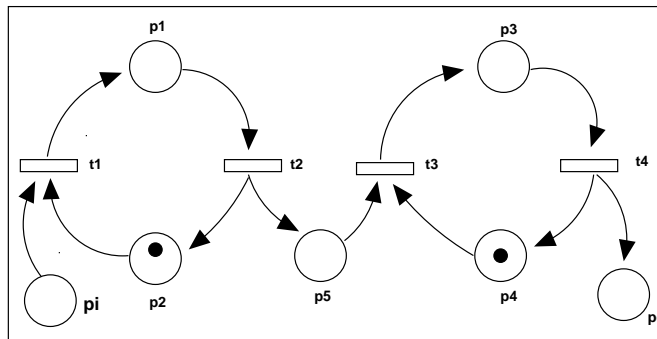
---

**Exercice 2** (*disapp\_td1\_ex2.tla*)

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.
- $S \cap T = \emptyset$
- $F$  est la relation du flot d'exécution :  $F \subseteq S \times T \cup T \times S$
- $K$  représente la capacité de chaque place :  $K \in S \rightarrow \text{Nat}$ .
- $M$  représente le initial marquage chaque place :  
 $M \in S \rightarrow \text{Nat}$  et vérifie la condition  $\forall s \in S : M(s) \leq K(s)$ .
- $W$  représente le poids de chaque arc :  $W \in F \rightarrow \text{Nat}$
- un marquage  $M$  pour  $R$  est une fonction de  $S$  dans  $\text{Nat}$  :  
 $M \in S \rightarrow \text{Nat}$  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  $T$ ,  $\text{Pre}(t)$  est l'ensemble des places conduisant à  $t$  et  $\text{Post}(t)$  est l'ensemble des places pointées par un lien depuis  $t$  :  
 $\text{Pre}(t) = \{s' \in S : (s',t) \in F\}$  et  $\text{Post}(t) = \{s' \in S : (t,s') \in F\}$
- 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 :  $\forall s \in S$ ,
 
$$M'(s) = \begin{cases} M(s) - W(s,t), & \text{SI } s \in \text{PRE}(t) - \text{POST}(t) \\ M(s) + W(t,s), & \text{SI } s \in \text{POST}(t) - \text{PRE}(t) \\ M(s) - W(s,t) + W(t,s), & \text{SI } s \in \text{PRE}(t) \cap \text{POST}(t) \\ M(s), & \text{SINON} \end{cases}$$

On considère le réseau suivant :



---

MODULE *petri10*

---

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

$t1 \triangleq$   
 $t2 \triangleq$   
 $t3 \triangleq$   
 $t4 \triangleq$

$Init1 \triangleq M = [p \in Places \mapsto \text{IF } p \in \{ "p4", "p2" \} \text{ THEN } 1 \text{ ELSE } \\ \text{IF } p = "pi" \text{ THEN } N \text{ ELSE } 0]$

$Next \triangleq t1 \vee t2 \vee t3 \vee t4$

---

**Question 2.1** 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 2.2** Donner une relation liant les places  $po, p1, p3, p5, pi$  et la valeur  $N$ . Justifiez votre réponse.

**Question 2.3** 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 2.4** Expliquez ce que modélise ce réseau de Petri.

◇— **Solution de l'exercice 2** \_\_\_\_\_

```

----- MODULE disapp_td1_ex2 -----
EXTENDS Naturals, TLC
CONSTANTS Places, N, Q, B
VARIABLES M

t11 ==
  /\ M["p1"] \geq 1 /\ M["p5"] \geq 1
  /\ M' = [ [M EXCEPT!["p1"]=@-1] EXCEPT!["p5"]=@-1] EXCEPT!["p2"]=@+1]

t1 ==
  /\ M["p2"] = 1 /\ M["pi"] \geq 1
  /\ M' = [ [M EXCEPT!["p1"]=1] EXCEPT!["pi"]=M["pi"]-1] EXCEPT!["p2"]=0]

t2 ==

```

```

/\ M["p1"] = 1 /\ M["p5"] < B
/\ M=  [[ [M EXCEPT!["p1"]=0] EXCEPT!["p5"]=M["p5"]+1] EXCEPT!["p2"]=1]

t3 ==
/\ M["p5"] \geq 1 /\ M["p4"]=1
/\ M=  [[ [M EXCEPT!["p3"]=1] EXCEPT!["p5"]=M["p5"]-1] EXCEPT!["p4"]=0]

t4 ==
/\ M["p3"] = 1 /\ M["po"] < Q
/\ M=  [[ [M EXCEPT!["p3"]= M["p3"]-1] EXCEPT!["po"]=M["po"]+1] EXCEPT!["p4"]

-----

Init1 == M = [p \in Places |-> IF p \in {"p4","p2"} THEN 1 ELSE
              IF p = "pi" THEN N ELSE 0 ]

Init == Init1

Next == t1 \/ t2 \/ t3 \/ t4 \/ M=M

Petri == Init /\ [][Next]_<<M>>

TypeInvariant == \A p \in Places : M[p] \geq 0

Inv1 == M["pi"]+M["p5"]+M["po"]+M["p1"]+M["p3"] = N

Inv2 == M["po"] \leq Q

Inv4 == M["pi"]+M["p5"]+M["po"]+M["p2"]+M["p4"] = N+2
Inv5 == M["p3"]+M["p4"]+M["p1"]+M["p2"] = 2

Inv3 == M["po"] # Q
Inv == TypeInvariant /\ Inv1 /\ Inv2 /\ Inv5
Test == Inv3
=====

```

---

**Fin 2**