MVSI – Modelling and Verification of Computer Systems

TLA$^+$ modelling (1)

Tutorial

Dominique Méry – 20th November 2026

✎ Exercise 1

`appex1_1.tla, appex1_1.cfg`

Access to a room is controlled by a system which observes the people entering or leaving the room. This system is a set of sensors identifying the passage of a person from the outside to the inside and from the inside to the outside. The system must guarantee that at most `max` people are in the room.
Write a TLA$^+$ module modelling such a system and satisfying the expected property.

✎ Exercise 2

The GCD of two numbers satisfies the following properties:

- $\forall a,b \in \mathbb{N}.gcd(a,b) = gcd(b,a)$
- $\forall a,b \in \mathbb{N}.gcd(a,a+b) = gcd(a,b)$
- Write a TLA$^+$ specification computing the GCD of two given numbers.
- Give an explanation or a justification of the correctness of this solution.

✎ Exercise 3

`appex1_3.tla,appex1_3.cfg, petri10`

A Petri net is a tuple $R = (S,T,F,K,M,W)$ where

- S is the (finite) set of places.
- T is the (finite) set of transitions.
- S ∩ T = ∅
- F is the flow relation: F ⊆ S × T ∪ T × S
- K is the capacity of each place: K ∈ S ⇸ Nat.

The function K assigns to every place s of S the maximum number of tokens that it may contain. If this function is not defined, then the capacity is infinite.

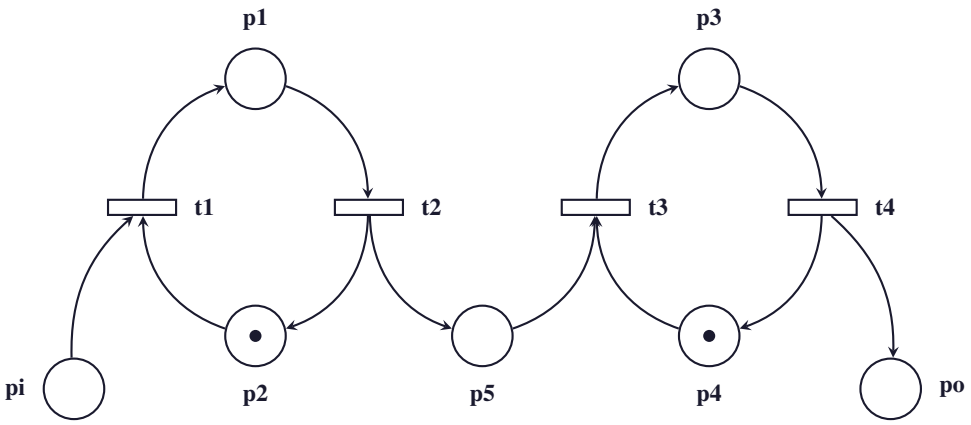
- M is the initial marking of each place:
  M ∈ S → Nat and satisfies the condition ∀ s ∈ S : M(s) ≤ K(s).
- W is the weight of each arc: W ∈ F → Nat
- a marking M for R is a function from S to Nat:
  M ∈ S → Nat, satisfying the condition ∀ s ∈ dom(K) : M(s) ≤ K(s).
- a transition t of T is enabled from a marking M of R if
  1. ∀ s ∈ { s' ∈ S ∣ (s',t) ∈ F } : M(s) ≥ W(s,t).
  2. ∀ s ∈ { s' ∈ S ∣ (t,s') ∈ F } : M(s) ≤ K(s) - W(s,t).
- For each transition t of T, Pre(t) is the set of places leading to t, and Post(t) is the set of places pointed to by an arc from t:
  Pre(t) = { s' ∈ S : (s',t) ∈ F } and Post(t) = { s' ∈ S: (t,s') ∈ F }
- Let t be a transition of T enabled from a marking M of R:

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

- a new marking M' is defined from M by: $\forall$ s $\in$ S,

$$M'(s) = \begin{cases} M(S) - W(S,T), \text{ IF } S \in PRE(T) - POST(T) \\ M(S) + W(T,S), \text{ IF } S \in POST(T) - PRE(T) \\ M(S) - W(S,T) + W(T,S), \text{ IF } S \in PRE(T) \cap POST(T) \\ M(S), \text{ OTHERWISE} \end{cases}$$

We consider the following net:



Skeleton of the module:

```
---------------------- MODULE petri10 ----------------------
EXTENDS Naturals, TLC
CONSTANTS Places, N, Q, B
VARIABLES M
Init == M = [p \in Places |-> IF p \in {"p4","p2"} THEN 1 ELSE
                              IF p = "pi" THEN N ELSE 0]
t1 == ...
t2 == ...
t3 == ...
t4 == ...
Next == t1 \/ t2 \/ t3 \/ t4
=============================================================
```

Question 3.1 Translate this net into a TLA$^+$ module whose skeleton is given in the text. To do so, give the definition of the four transitions $t1$, $t2$, $t3$, $t4$. The capacity of the places is not taken into account: the places have a capacity of at most one token, except the place pi which may contain N tokens; the place p5 may contain at most B tokens and the place po may contain at most Q tokens.

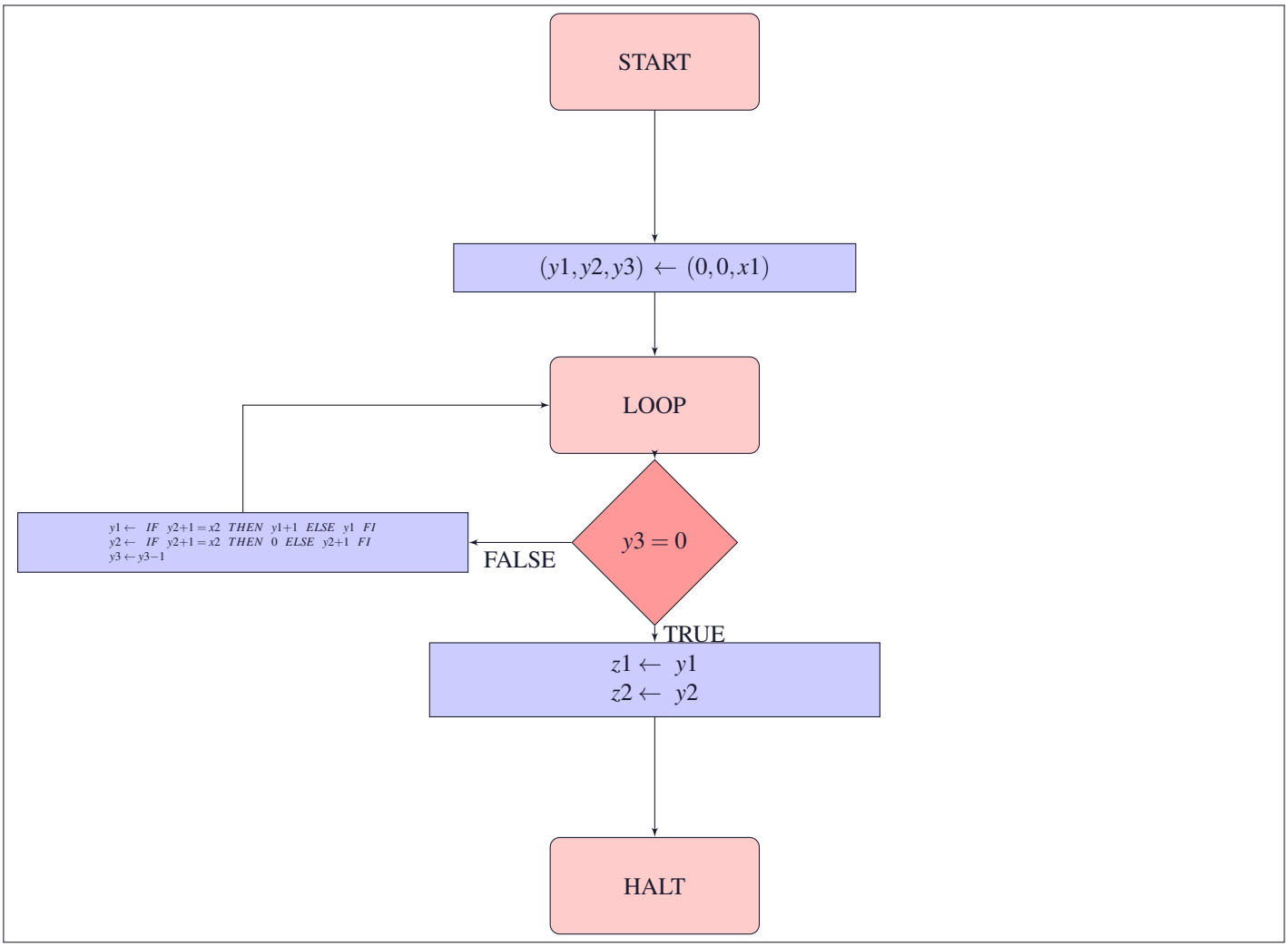
Question 3.2
Give a relation linking the places po, p1, p3, p5, pi and the value N. Justify your answer.

Question 3.3
Assuming that the place po may contain at most Q tokens, give a condition on Q such that all the tokens of pi are eventually consumed. Justify your answer.

Question 3.4 Explain what this Petri net models.

✎ Exercise 4 `appex1_4`

We consider the following algorithm, described by a flowchart:



Question 4.1 Translate this algorithm into a TLA$^+$ module.

Question 4.2 Write a contract for this algorithm.

Question 4.3 Test the values of the variables at run time.

Question 4.4 Show that this algorithm is partially correct with respect to its precondition and its postcondition.