Homework 1

Indended to be solved until May 8.

Problem 1 In the below figures you find three suggestions for models that are intended to implement mutual exclusion between two processes. In all action systems, locations l_1 and m_1 are intended to represent the section of a process which is not interested in the critical section, locations l_2 and m_2 are intended to represent the section where the process is interested in entering the critical section, and locations l_3 and m_3 represent the critical sections themselves. The purpose of a mutual exclusion algorithm is to ensure that

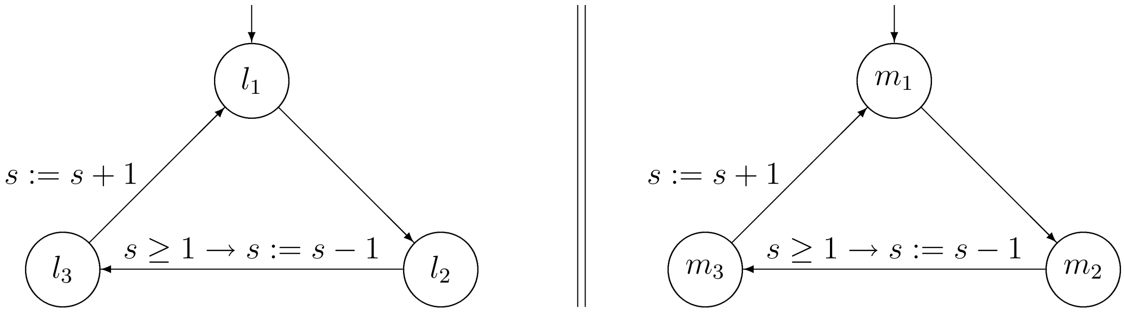
1. At most one process is in its critical section at any time
2. A process that intends to enter its critical section should be allowed to do so eventually, or after some reasonable waiting time

For each of the action systems you should determine how well it satisfies these two criteria. For the second criterion, you should check how it is affected under assumption of weak or strong fairness for each process.

Action System *mutex1*

declare s : integer

initially $s = 1$

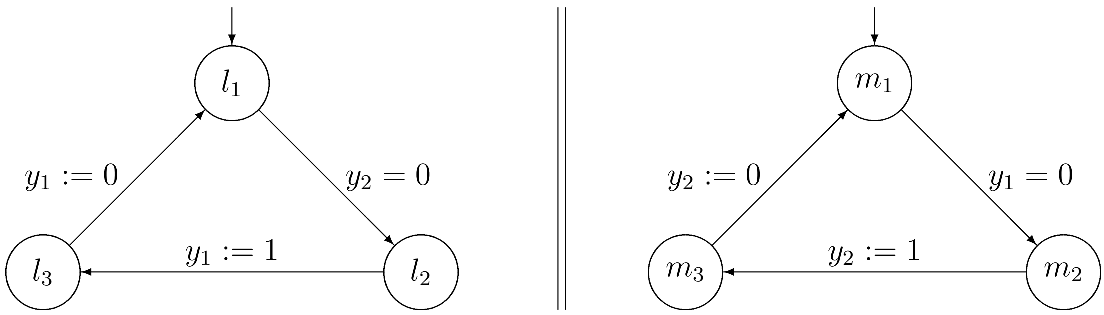


end

Action System *mutex2*

declare y_1, y_2 : integer

initially $y_1 = y_2 = 0$

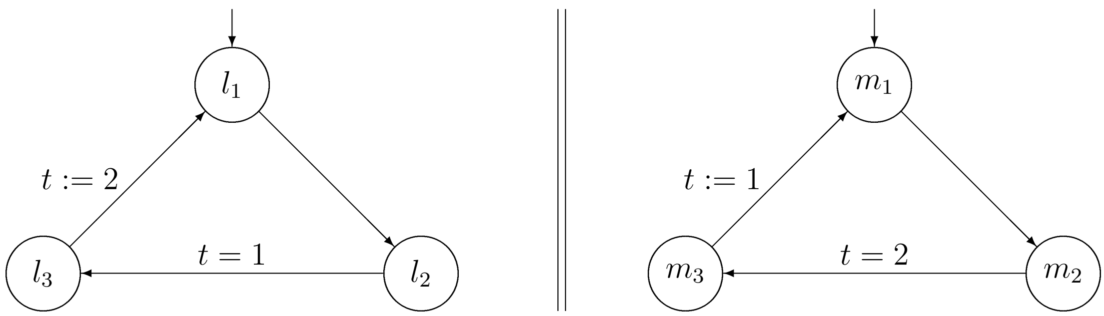


end

Action System *mutex3*

declare t : integer

initially $t = 1$



end

Problem 2. The following is an action system with two integer variables x and y. It does not perform too many useful things.

Action System *Foo1*
  variables
    x, y : integer
  initially
    $x = y = 0$
  actions
    $x \leq y \longrightarrow x := x + 1$
  $[\!]$
    $x \geq y \longrightarrow y := y + 1$
  $[\!]$
    $x > y + 1 \longrightarrow y := y + 10$
end

For each of the three actions, there is a (weak) fairness constraint, defined by letting each action be a (weak) fairness set. Which of the following properties are satisfied by the program? Motivate your answers:

a) $\Box\ (x \geq y)$

b) $x = 0\ \ leads-to\ \ x = 10$

c) $x > y\ \mathcal{U}\ x < y$

d) $x \geq y\ \mathcal{U}\ x < y$

e) $x \geq y\ \mathcal{W}\ x < y$

f) $(x > y + 1)\ \mathcal{W}\ (y = x + 20)$

Problem 3. Model the three algorithms of the first problem in Promela, and use SPIN to carry out the checking of how the properties are satisfied.

Problem 4. Solve the old Farmer, Wolf, Sheep, and Cabbage problem:

> A farmer must ship a wolf, a sheep, and a cabbage across a river. He has a boat which takes one of them. But he must not leave the wolf alone with the sheep, nor the sheep alone with the cabbage on either shore if he is not there himself to watch them.

Make a **beautiful** Promal model, by which SPIN can find a best solution to this problem. This means that your model should **not** give any hint about what is the solution. You model should have three clear parts:

- one part which just allows shipping, without checking that "bad pairs" are left alone,
- one part which aborts the search of SPIN if"bad pairs" are left alone,
- a condition, which SPIN interprets as an error, thereby generating an error trace, which is the final solution.