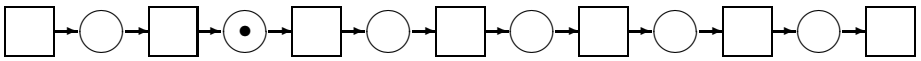
T-79.231 Parallel and Distributed Digital Systems
Homework 2, October 14, 2002 **Marko Mäkelä**

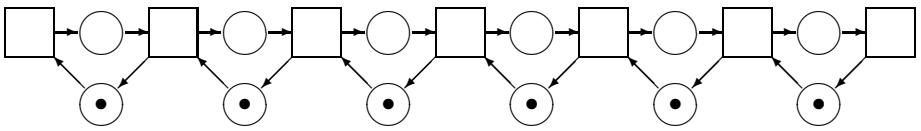
Design and Verification of a Safety-Critical System

A section of a railroad can be pictured as a place transition system. A token represents a train moving from left to right.

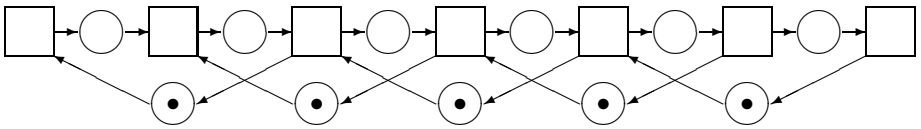


The system does not prevent collisions - i.e. a train moving faster will back-end the train in front of it.

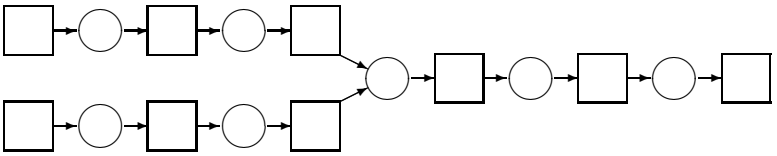
The model will be made safe by the addition of complement places which actually represent signalling in the railway system. I.e. a train may move forward only if there is a token in the complement place of the next railroad section.



Safety can be further increased by requiring that one empty section is always present between two trains moving in the same direction.



1. Design the signalling for the following railway junction, that has the property that there is always one section between two trains moving in the same direction.



2. In which markings of your model does there exist a race condition?

3. Let's suppose that the trains do not stop voluntarily, i.e. they will always move forward if the model allows it. Is it possible in your model that a train arriving at the junction will not be able to proceed for a long time or at all?

4. Model with High Level nets and Maria a straight railway track consisting of n sections, where there is always one section between trains. Repeat for the situation where we require two sections between trains.

5. Show with Maria that the safety requirements in the previous question are satisfied by your model. (Hint: Use `reject`-formula in Maria).

Return the answer to the mailbox located between rooms B 336 and B 337 in the Computer Science Building by 4 PM on November 11, 2002. You may also return the answer as postscript of pdf to the address Jukka.Honkola@hut.fi